Advanced Sciences and Technologies for Security Applications

Hamid Jahankhani
Ayman El Hajjar *Editors*

Wireless Networks

Cyber Security Threats and Countermeasures

Springer

Advanced Sciences and Technologies for Security Applications

Indexed by SCOPUS

The series Advanced Sciences and Technologies for Security Applications comprises interdisciplinary research covering the theory, foundations and domain-specific topics pertaining to security. Publications within the series are peer-reviewed monographs and edited works in the areas of:

- biological and chemical threat recognition and detection (e.g., biosensors, aerosols, forensics)
- crisis and disaster management
- terrorism
- cyber security and secure information systems (e.g., encryption, optical and photonic systems)
- traditional and non-traditional security
- energy, food and resource security
- economic security and securitization (including associated infrastructures)
- transnational crime
- human security and health security
- social, political and psychological aspects of security
- recognition and identification (e.g., optical imaging, biometrics, authentication and verification)
- smart surveillance systems
- applications of theoretical frameworks and methodologies (e.g., grounded theory, complexity, network sciences, modelling and simulation)

Together, the high-quality contributions to this series provide a cross-disciplinary overview of forefront research endeavours aiming to make the world a safer place.

The editors encourage prospective authors to correspond with them in advance of submitting a manuscript. Submission of manuscripts should be made to the Editor-in-Chief or one of the Editors.

Hamid Jahankhani · Ayman El Hajjar
Editors

Wireless Networks

Cyber Security Threats and Countermeasures

Springer

Editors
Hamid Jahankhani
Department of Information Security
and Cyber Criminology
Northumbria University London
London, UK

Ayman El Hajjar
Department of Computer Science
and Engineering
University of Westminster
London, UK

ISSN 1613-5113 ISSN 2363-9466 (electronic)
Advanced Sciences and Technologies for Security Applications
ISBN 978-3-031-33630-0 ISBN 978-3-031-33631-7 (eBook)
https://doi.org/10.1007/978-3-031-33631-7

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Contents

Key-Pre Distribution for the Internet of Things Challenges, Threats and Recommendations 1
Ayman El Hajjar

Approaches and Methods for Regulation of Security Risks in 5G and 6G 43
Hamid Jahankhani, Stefan Kendzierskyj, and Osama Hussien

Investigating Gesture Control of Robotic Arm via Lora Technology for Smart Cities 71
Amaechi Stanley Okoro, Sufian Yousef, and Akram Qashou

Safety and Security Issues in Employing Drones 103
Durga Prasad Srirangam, K. Hemalatha, Ashok Vajravelu, and N. Ashok Kumar

Security Threats of Unmanned Aerial Vehicles 133
Ashok Vajravelu, N. Ashok Kumar, Swagata Sarkar, and Sheshang Degadwala

A Machine Learning Based Approach to Detect Cyber-Attacks on Connected and Autonomous Vehicles (CAVs) 165
Safwan Abdul Nazaruddin and Umair B. Chaudhry

Security and Privacy Concerns in Next-Generation Networks Using Artificial Intelligence-Based Solutions: A Potential Use Case 205
Murat Kuzlu, Ferhat Ozgur Catak, Yanxiao Zhao, Salih Sarp, and Evren Catak

A Blockchain-Enabled Approach for Secure Data Sharing in 6G-based Internet of Things Networks 227
Hussein El Ghor and Bilal Nakhal

Combining NFC Authenticated Tags with NFTs to Spot Counterfeit Luxury Products Using Solana Blockchain 247
Matteo Zocca and Hamid Jahankhani

An Investigation into the State of Cybersecurity Preparedness with Respect to Operational Technology 301
Farouk Akrama and Hamid Jahankhani

Key-Pre Distribution for the Internet of Things Challenges, Threats and Recommendations

Ayman El Hajjar

Abstract The Internet of Things is the next evolution of the Internet which will substantially affect human life. IoT is important because it is the first of its kind that is propelling an evolution of the Internet and smart environment; It is clear that secure communication between IoT devices is essential and the threats and risks for having an insecure IoT are a lot bigger than for conventional Internet connected devices. The motivation behind this chapter is to set variables needed to investigate the performance of both the probabilistic scheme or the deterministic scheme approaches and to find a reliable and efficient mechanism for nodes within the IoT and to establish trust by securing end-to-end communication by having a certain pre distributed key scheme that will enable such communication by the use of a Key Pre-distribution scheme KPS.

Keywords IoT · Distributed Sensor Networks · Key Pre-distribution scheme · Threat Model for IoT · SCADA attack · Man in the middle MiTM

1 Introduction

In this chapter we will introduce the challenges that comes with implementing a key distribution algorithm in the context of the Internet of Things. We look at the threats on key distribution in IoT environment and how key distribution can be performed between devices using the routing protocol for 6LoWPAN, RPL routing protocol.

The motivation behind this chapter is to find a reliable and efficient mechanism for nodes within the IoT and to establish trust by securing end-to-end communication by having a certain pre distributed key scheme that will enable such communication by the use of a Key Pre-distribution scheme KPS. Many KPS were proposed for Distributed Sensor Networks (DSN). DSN shares a lot of the IoT characteristics and can be used as a starting point for this research.

A. El Hajjar (✉)
University of Westminster, London, UK
e-mail: A.ElHajjar@westminster.ac.uk

H. Jahankhani and A. El Hajjar (eds.), *Wireless Networks*, Advanced Sciences and Technologies for Security Applications,
https://doi.org/10.1007/978-3-031-33631-7_1

2 Chapter Question

The question this chapter is looking to investigate is whether the probabilistic key distribution scheme (KPS) proposed in [1] and the deterministic Key Pre-distribution proposed in [2] can be used in an Internet of Things (IoT) environment similarly to how they are in used in the context Wireless Sensor Networks (WSN).

While looking at the research question, we can deduce several sub questions that need to be answered in order to identify the effectiveness of KPS for the IoT. We first need to establish the differences between DSN and IoT in order to assess whether different KPS schemes used in DSN are suitable for the IoT. This will be done by investigating whether the identified schemes can provide the same security measure without any modification of the parameters used. We will then evaluate the impact of those KPS schemes use on the IoT devices and networks without any modification. Based on the answer of the previous question, we will be able to identify the required modifications that are needed to achieve the necessary security measures in the context of the IoT with acceptable security performance and an affordable resource usage on its devices. After identifying the required modifications needed, if any, we should look at what can be optimized in the IoT in order to determine the most effective security measure with the least cost in term of resources.

The main objective in this research is to establish a reliable and efficient mechanism for nodes within the IoT to establish trust by a mean of establishing a secure end-to-end communication by having certain pre distributed key scheme that will enable such a communication. A Pre-distribution Key (KPS) is therefore needed. Not a lot of research was done in this field. Many PKS were proposed for WSN and ZigBee. Both network technologies share a lot of the IoT characteristics and can be used as a starting point for this research. Some of the research was done on securing the communication of between the nodes in the IoT network but not in securing the routing topology formation. To my knowledge, using a Key Pre-Distribution Scheme in the context of the IoT is something that was not looked at before to secure the routing formation. Future research needs to find the answers for the following questions in order to develop/identify the most suitable (KPS) for the IoT are: To achieve our main objective the research needs to find the answer for the following questions:

1. Determine the advantage and disadvantages of using the probabilistic or deterministic key pre distribution schemes for distributed sensor networks in the context of the Internet of Things.
2. Evaluate the performance of the simulated key management schemes for distributed sensor networks on the Internet of Things using the same variables used in the distributed sensor networks to achieve full connectivity and assess if they are enough to achieve full connectivity in the Internet of Things network.
3. Evaluate the overhead of experiments to determine the quality of service obtained from implementing the key management scheme for distributed sensor networks on the Internet of Things.

2.1 Differences Between DSN and IoT

Many KPS were proposed for Distributed Sensor Networks (DSN). DSN shares a lot of the IoT characteristics and can be used as a starting point for this research.

Although both DSN and IoT are considered infrastructure-less networks and operate on an Ad-Hoc basis, many essential characteristics (by definition) between them are not shared. Those characteristics change the whole environment of IoT in comparison with DSN. Distributed Sensor Networks are not able to use classical IP based protocols simply because it is very difficult to allocate a universal identifier scheme for a large DSN network and proprietary protocols are usually used to identify unique devices. A distributed sensor network can operate by itself sending data to a centralized entity in order to monitor the physical conditions of an environment. An IoT network requires one or more devices to act as a sink and to connect the network to other types of networks such as the Internet in order to send data collected. The devices in an IoT network do not need to be the same and all can communicate to complete a specific task.

For that reason, DSN nodes cannot inter-operate and communication between various nodes only exist for routing purposes and to allow data to reach the centralized location. Since IoT nodes are able to inter-operate with the existing Internet infrastructure, each of them needs its own unique identifiable Internet protocol (IP) address rather than a proprietary protocol.

The challenge of the addressing and identifying nodes in DSN present us with a complete set of challenges that differs in the scenario of an IoT network. The flow of data in a DSN network is most of the time in one direction towards the sink connected directly to the centralized location. The flow of data in an IoT network is bi-directional as a mote can either send data to the Internet or receive instructions from another entity. This difference means that the routing protocols used for a DSN network cannot be used in an IoT network. In most applications of DSN networks, route discovery base routing protocols are used; Ad Hoc On Demand Distance Vector (AODV), Dynamic Source Routing (DSR) and Optimized Link State Routing (OLSR). Each of those protocols have their own characteristics however they all share two important features. All are proprietary protocols and are not IP based protocols but proprietary classless protocols and they only allow route discovery and route establishment messages to be exchanged between nodes in both directions in comparison with the IoT where data can only travel through one direction at a time.

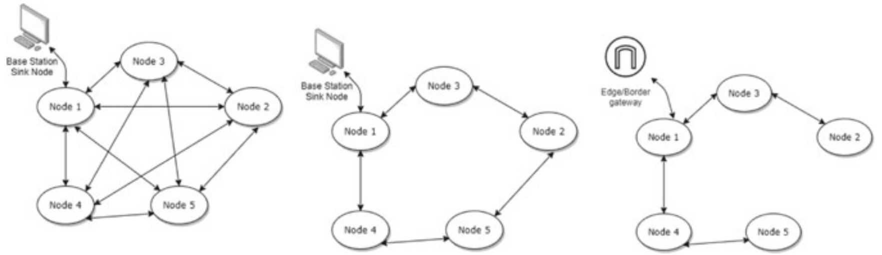
There are some challenges that need to be taken into consideration when implementing the KPS in the context of the Internet of Thing. The use of a suitable symmetric encryption protocol is also essential. Different encryption protocols require different time to decrypt as each will present different limitations in terms of computation and processing speed.

DSN network nodes were assumed to have proprietary unique identifiers simply because they were never intended to be used as part of a large network such as the Internet. This is not a practical solution for the IoT as data is needed to travel between two directions and sometimes directly to the internet. For that reason, it requires an IP based routing protocol. Most of the conventional devices on the Internet uses the Transmission Control Protocol/Internet Protocol TCP/IP communication suite to identify how data should travel between devices, in which format and using which route. This suite however was not intended to be used with the IoT and it is not suitable for the IoT as the devices that participate in this type of network are considered lightweight resource constraints devices. Some attempts were made to develop a unique addressing scheme for the IoT until most researchers and IoT device manufacturers agreed that devices should use the same addressing scheme as the Internet to make it easier for devices to communicate with the Internet. Using IP protocols in sensor networks simplify the connectivity model as the hierarchy of the devices in the network can be flattened. This also removes the complexity of having devices to translate between proprietary protocols and standard Internet protocols as explained in [3].

However, the TCP/IP suite was still considered heavy and IPv6 over Low Power Wireless Personal Area Networks (6LoWPAN) which is a new communication suite designed specifically for the IoT was created. 6LoWPAN defines how to layer, transmit and deal with data using IPv6 over low data rate, low power, and small footprint radio networks as identified by IEEE 802.15.4 in [4] radio. Routing is a fundamental piece of the overall IPV6 architecture for the Internet of Things. The networks in these environments can be described as Low Power and Lossy Networks (LLN), meaning they often operate with significant constraints on processing power, memory and energy translating into high data loss rates and low data transfer rates and instability. Routing protocol for Low Power and Lossy Networks (RPL) was developed to translate the potential of Internet of Things into reality. The objective of RPL is to target networks which comprise of thousands of RPL DODAG where the majority of the nodes have very constrained resources. RPL solves the unique challenges that IoT brings to the exchange of messages between nodes in a conventional DSN network.

The physical nature of the IoT devices makes it difficult to implement security schemes to secure communication between nodes. In an IoT device, limited resources are available such as the limitation of storage capacity and processing power. A KPS used to secure communication between DSN devices assumes the presence of several routes to a mote and if a shared key between two nodes does not exist an alternative secured route can be found. This is not the case in the IoT and therefore a large number of keys is needed to ensure that all links between nodes is secure. This will require a large storage space for a large scale IoT network. This solution will present a problem for IoT devices.

The architecture of the IoT, similarly to the DSN is of Ad-Hoc mode (also known as peer to peer). It means that there is no centralized entity that organizes the distribution of the keys between nodes. It also means that all links between any two nodes needs to contain a shared key. This will naturally result in an increase of the number of keys that each node should have to make sure that all links between two nodes are secured by the use of the shared link. This presents us with another challenge as the implementation of any suggested solution will be limited by the storage capacity of devices used regardless of which KPS scheme is used. The difference in how



Decentralized WSN representation

DSN representation

IoT representation

Fig. 1 Five nodes physical topology comparison for WSN, DSN and IoT networks. Each node in Wireless and Distributed Sensor networks can have one or more links. Distributed sensor networks establish enough links to have a route to the sink node. IoT nodes establish nodes with preferred parent to reach root node

devices communicate in an IoT in comparison with DSN as explained in Sect. 2.1 means that devices that do not share a secure key cannot communicate indirectly if a secure route between them cannot be identified when the routing table is formed using RPL. This will lead to several devices in the network not being included in the routing table and thus will not be allowed to join the network.

Secure communication between end to end IoT devices is essential. IoT devices are meant to exchange data from critical infrastructure such as devices in smart cities, smart houses, SCADA systems and other important infrastructure. Those devices will not only be exchanging important data but also participating in automated decision making and this makes the security of the communication between those devices more important. An attacker listening to the communication between those devices, if the devices are communicating in plain text, can simply intercept the message and understand it. For example, a camera device sending a message to a heating source in a smart home, informing the heater that there is no one at home in order for the heating to automatically go off, will give clues to any attacker who is listening to this communication and thus be able to deduct that the house is empty and a theft can take place.

The differences between WSN, DSN and IoT can be summarized by two main differences, first how the nodes connect with each other and report to the sink node or gateway and the number of connections between the different nodes in the network. An example of how five nodes form a network in the different networks is shown in Fig. 1. Wireless and Distributed Sensor networks can take the form of different physical topologies outlined in [5] and can be summarized by three topologies decentralized self organizing, centralized architecture and grid networking techniques.

In order to transform WSN into a viable technology to make the IoT vision cost-effective and deployable, authors in [6] claim the need for middleware-layer solutions fully compliant with accepted standards (or largely adopted specifications). This in fact is essential to allow sensor nodes in IoT to communicate with the Internet to process its data.

2.2 Threat Model for IoT and the Research Problem

In this section we will look at the threats on Internet of Things and identify where the research problem that this research is attempting to solve fits. Authors in [7–9] categorized the attacks in different categories as shown in Fig. 2. As we can see from Fig. 2, several attacks can be mitigated if nodes in an IoT network communicate in a secure way. The motivation to mitigate those threats all at once is because by ensuring that only nodes that share one or more secret key can communicate we ensure that all nodes that have joined that network are genuine and trusted.

In Sect. 6.6 we present the attack surfaces that exploits threats identified in this section as relevant to this research problem such as attack surfaces on key distribution, key storage or the process of routing formation and maintenance.

The threats that this research is attempting to solve and shown in Fig. 2 highlighted in blue or gray can be summarized below.

Generalized category threats on IoT identifies threats that do not only exist in IoT environments or multi-layer threats. Security and user privacy are essential to maintain in any network and protecting the confidentiality and integrity of data from violation will prevent devices from leaking private user data and confidential data. Researcher in [10, 11] have identified that IoT devices have higher chances of leaking private and confidential data due to the lack of reliable authentication, the lack of data encryption and the lack of network access control measures.

Cryptanalytic attacks explained in [12, 13] exploits the weaknesses in the cryptographic algorithm and can result if successful in the attacker discovering the original message. There are several cryptanalytic attacks that all networks can be vulnerable to depending on the cryptographic algorithm used. Cryptanalytic attacks will result in the violation of confidentiality, integrity and availability of data transmitted in such networks. The type of encryption used to encrypt data will be essential to ensure that the IoT secure DODAG is not vulnerable to cryptanalytic attacks. Ensuring that no malicious node can compromise the network will also prevent this type of attacks as devices will not be able to participate in the network in order to carry such attacks. The solution proposed in this research will have a direct impact on mitigating this attack.

Denial of Service (DoS) attacks on IoT devices explained in [14] result in resources exhaustion due to the physical features of the internet of Things devices such as low processing power and low battery consumption. Resources exhaustion attacks include jamming of communication channels, extensive unauthorized access and malicious utilization of critical IoT resources and those attacks result in operational functionality of IoT devices or non availability which result in disruption of services. 96% of the devices involved in Distributed Denial of Service DDoS attacks were IoT devices and participated in Botnets as discussed in [14, 15]. Although this attack is out of context of the research and having encrypted data between nodes do not prevent it directly, however some DoS attacks are carried out by malicious nodes that exhausts the resources of other nodes until they crash. Securing the routing formation will prevent malicious nodes from joining the network and hence protecting networks against DoS attacks. DDoS on the other hand cannot be prevented if it is the result of nodes participating in a botnet.

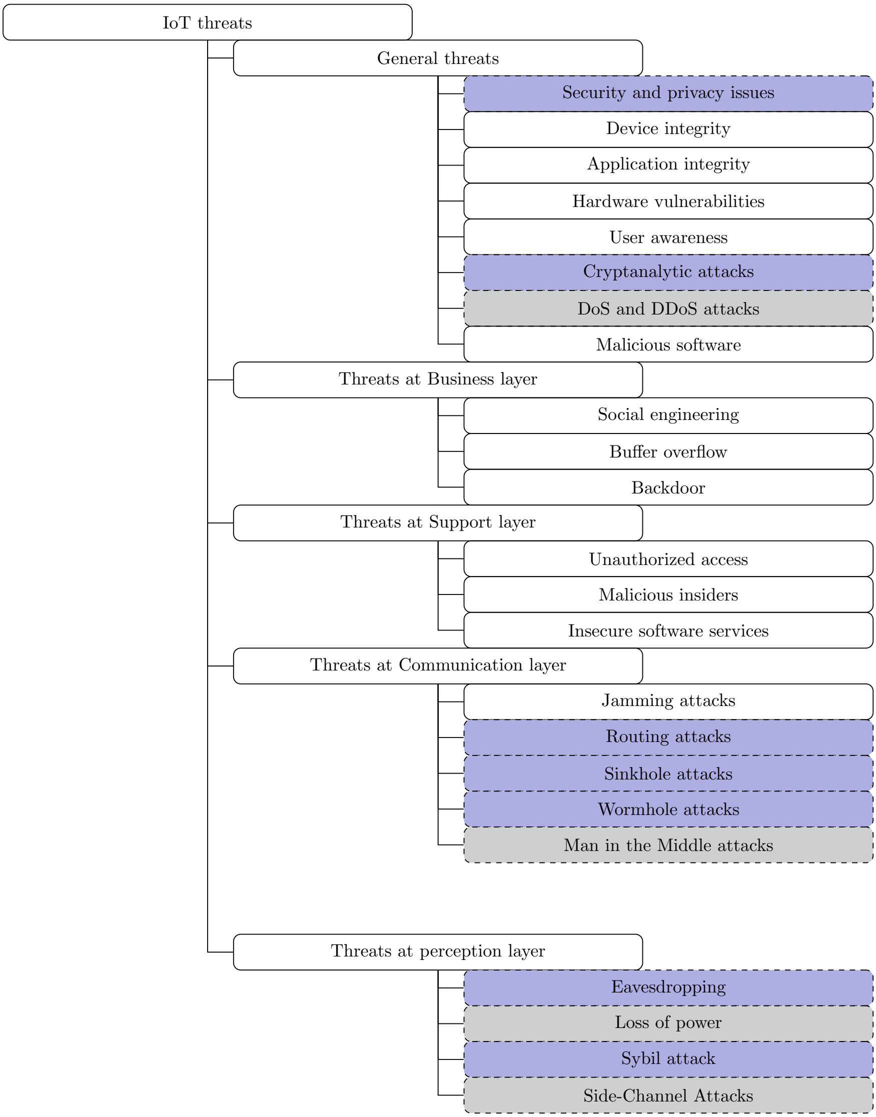


Fig. 2 IoT threats categorized based on the IoT layers that is affected. For each category, the threats are either considered not related to the chapter topic (in white background), directly related (blue background), indirectly related (gray background)

Various attacks threaten the Internet of Things routing formation and routing process as investigated in [16–19]. IoT RPL DODAG is vulnerable to a selective forwarding attack. In this attack malicious nodes do not participate in transmitting the packets received by it and destroys the routing path of the network by doing so as explained in [16, 20]. The Blackhole attack explained in [21] is an example of a selective forwarding attack in which a malicious node do not forward any packet and breaks the DAG in the routing table. HELLO flood attacks threaten the RPL DODAG formation process. In this attack when a genuine node utilizes HELLO messages to join a network a malicious node can capture this packet and use it to declare itself a neighbour. In this case, the DODAG Information Object DIO messages can be utilized with strong routing metrics in order to start such an attack as in [20] and leads to the malicious node joining the RPL DODAG. Rank attacks in RPL are other type of attacks in which malicious nodes advertise falsely their rank as discussed in [22, 23]. Increased rank attack and decreased rank attack are two examples of rank attacks examples in which a malicious node falsely advertise its rank either lower or higher and repeatedly does this in a way that it disrupts the routing topology as nodes will have to regularly update their preferred parent based on the new rank that the malicious node is advertising.

Routing attacks are at the core of the motivation of this research since preventing routing attacks will mitigate several other threats such as preventing malicious nodes from joining the network. Other type of routing attacks discussed in [20, 24, 25] are the sinkhole attack and the wormhole attack. In the sink node attack, malicious nodes redirect the traffic of a network to a specific node that acts as a sink node. Several malicious nodes participate in this attack by advertising a particular route that leads to the malicious node that is acting as a sink node. In the wormhole attack investigated in [20, 26, 27], the malicious nodes create direct links with each other and force the network traffic data through those links rather than links with intermediate nodes. Sinkhole attack and wormhole attack can be prevented by securing the routing formation process and encrypting the traffic between nodes as it will prevent malicious nodes from joining the network.

Other Man in the middle MiTM attacks discussed in [11, 28, 29] are defined as a form of eavesdropping in which malicious actors can intercept the traffic exchanged between two nodes and tamper with the exchanged node or use the captured packets to carry on further attacks. Different examples of MiTM can threaten the confidentiality and authenticity of the Internet of Things network such as Neighbor Discovery Protocol NDP poisoning explained in [30, 31], Address Resolution Protocol (ARP) poisoning identified in [32], replay attacks in [33, 34] and session hijacking in [35, 36]. Man in the Middle attacks can be prevented indirectly since encrypted traffic will prevent malicious node from carrying on such attacks and they are unable to decrypt the traffic to get the parameters and values needed to tamper the data in session in hijacking or to replay the traffic.

Threats at perception/physical layer consists of sensors, actuators, computational hardware, identification and addressing of the things. Securing data sensing and data collection in this layer is essential as they are done at this layer as explained in [8]. Threats in this layer are related to the physical aspects of the device such as resources exhaustion that causes battery drainage and loss of power by preventing a node from sleeping or going into saving mode. Malicious actors investigated in [11, 37] can physically install unauthorized devices in order to sniff the traffic and extract valuable information. Eavesdropping and traffic analysis can go together as the sniffed traffic can be captured and analysed by a network packets analyser to gather information about the nodes and their environment in the network. The solution protect against the threat of eavesdropping since malicious nodes cannot decrypt or understand the context of the captured or sniffed traffic. Loss of power if it is caused by the threat of DoS attacks can be indirectly protected by the proposed solution as it prevents malicious nodes from joining the network in order to generate large amount of traffic and exhausts nodes until the battery is drained. If the loss of power is the result of physical tampering of the devices then this solution will not prevent it.

Sybil Attack investigated in [9, 38, 39] is a form of attack that the IoT networks can be subject to. In this attack a malicious node impersonate one or more genuine nodes in the network and generate fake data and thus violating the trust and confidentiality between the nodes in the network. This attack can be prevented by this solution as the malicious nodes will be prevented from joining the network.

Side channel attacks as defined by [40] is based on side-channel information about the encryption device that are found on the physical device when data is being processed in the perception and physical layers of the device such as information about data processing time or power consumption of the device when encrypting/decrypting various messages and during the computation of different security protocols. This threat can be mitigated indirectly if a strong encryption algorithm is used to prevent malicious actors from data information leaked generated when the encryption and decryption process of the keys takes place.

3 Internet of Things

Internet of Things (IoT) is the next evolution of the Internet which will substantially affect human life. IoT is important because it is the first of its kind that is propelling an evolution of the Internet and smart environment—an evolution that will lead to innovative applications that have the ability to revolutionize our lives and our surroundings.

The vision of having a variety of physical elements “Objects” and “things” connected to the Internet is what forms the IoT. In the conventional Internet, most of the devices connected to the Internet were used directly by humans and needed a direct interaction from a human being to be able to generate data. The IoT vision enabled objects and things to interact with an external entity and send data without the interference of a human. No human participation is needed and objects are able to take decisions based on data received, sent or generated.

Thus the term of the Internet of Things explained in [41] is now considered as a global network which allows the communication between human-to-human, human-to-things and things-to-things that is anything in the world by providing a unique digital identity to each and every object.

The idea is that all objects connected to the IoT will contain embedded technology, allowing them to interact with internal states or an external environment. Those objects will be able to sense and communicate thus changing how and where decisions are made and who makes them [42].

The IoT is an emerging technology closely related to other research areas like Peer to Peer Networking, Mobile computing, Pervasive or Ubiquitous computing, Wireless Sensor Networks, Cyber Physical Systems, Real Time Analytics, etc. Technologies like ZigBee and Wi-Fi Direct can be widely deployed to achieve the notion of smart cities, eventually achieving a globally integrated smart world. However, there are ongoing issues like architecture design, hardware design, cost accountability, identity, privacy, and security issues for building new ices and solutions in IoT [43].

The applications and usage of the Internet are multifaceted and expanding on a daily basis. The Internet of Things (loT), Internet of Everything (loE) and Internet of Nano Things are new approaches for incorporating the Internet into the generality of personal, professional and societal life [44].

Applications of IoT encompasses medical implants, alarm clocks, wearable systems, automotives, washing machines, traffic lights, and the energy grid. It is expected that 50 billion devices will be interconnected by 2030. Having this huge Global Network will result in the generation of a huge unprecedented amount of data.

Internet protocols have always been considered too heavy for sensor networks and thus the 6LoWPAN protocol stacks were created [45]. 6LoWPAN concept originated from the idea that "the Internet Protocol could and should be applied even to the smallest devices" and that low-power devices with limited processing capabilities should be able to participate in the Internet of Things [4].

4 6LoWPAN

To achieve the vision of the Internet of Things, a review of the currently used Internet protocols and standards was needed. The Internet Protocol (IP) was always considered a protocol for Local Area Networks, Wide Area Networks, PCs and servers. The IP protocol was not intended to be used with Wireless sensor networks, Personal Area Networks and the sensor itself. The main reason why it was not intended to be used is that the IP is too heavy for those applications. Sensor networks are meant to be lightweight resource constraints devices.

However, recently there has been a rethinking of the many misconceptions about the IP. The main discussion was to answer this question "why invent a new protocol when we already have IP" thus the development and standardization of 6LoWPAN (IPv6 over Low Power Wireless Personal Area Networks) was carried out. A simple 6LoWPAN architecture is shown in Fig. 3 and outlines the basic concept of connecting low power devices in a 6LoWPAN network with a conventional IPv4/v6 network by using an edge router.

6LoWPAN technology realizes the IPv6 packet transmission in the IEEE 802.15.4 based WSN. And 6LoWPAN is regarded as one of the ideal technologies to realize the interconnection between WSN and Internet which is the key to build the IoT [46].

6LoWPAN defines how to layer, transmit and deal with data using IPv6 over low data rate, low power, and small footprint radio networks 6LoWPAN as identified by IEEE 802.15.4 radio. 6LoWPAN protocols resides between the data link layer

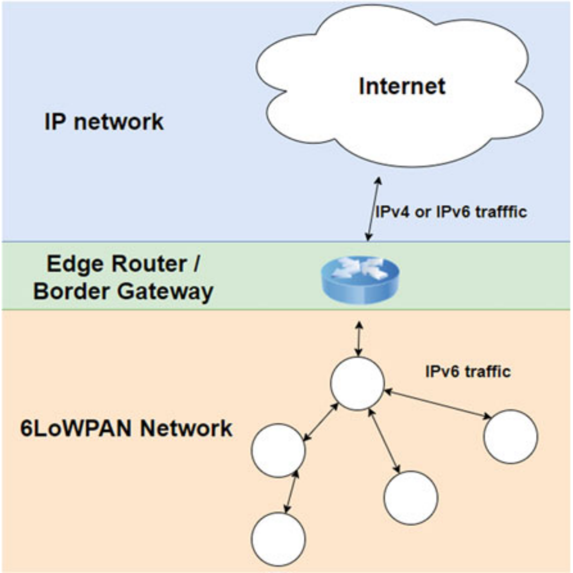
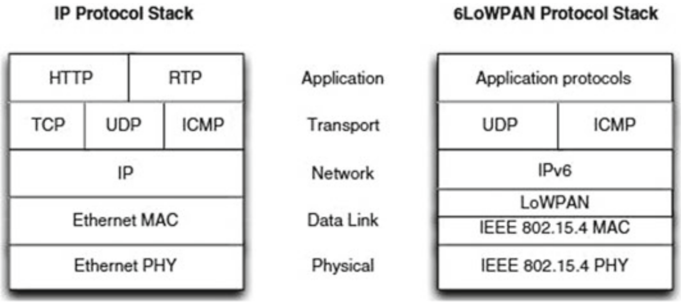


Fig. 3 The 6LoWPAN simple architecture comprises the IoT network layer, the edger router and the connection to the Internet where the data collected from lower layers are analysed and processed [45]



IP Protocol Stack				6LoWPAN Protocol Stack	
HTTP	RTP		Application	Application protocols	
TCP	UDP	ICMP	Transport	UDP	ICMP
IP			Network	IPv6	
Ethernet MAC			Data Link	LoWPAN IEEE 802.15.4 MAC	
Ethernet PHY			Physical	IEEE 802.15.4 PHY	

Fig. 4 IP and 6LoWPAN protocol stacks as presented in 6LoWPAN the wireless embedded Internet by Shelby and Bormann [45]. The representation of each layer in the 6LoWPAN shows how the logical communication between the layers at the same level can be interpreted, i.e. communication between the IP network layer and IPv6

and the network layer. The adaptation of the full IP format and the 6LoWPAN in performed by the edge router that translates conventional IP traffic to 6LoWPAN traffic as is shown in Fig. 4 in relation to an IPv6 stack.

Using IP protocols in Sensor networks simplify the connectivity model, as the hierarchy of the devices in the network can be flattened. This also removes the complexity of having devices to translate between proprietary protocols and standard Internet protocols [3].

IoT applications are implemented using a wide range of proprietary technologies which are difficult to integrate with larger networks and Internet-based services. Where as the 6LoWPAN approach is an IP based one, these devices can be connected easily to other IP networks which doesn't require any translation gateways or proxies, and which can use the existing network infrastructures [47].

It is normal to assume that using IP is too heavy in terms of code size, protocol complexity, required configuration infrastructure or head and protocol overhead. Implementation of 6LoWPAN can easily fit into 32 kb flash memory parts which is suitable for the Internet of Things devices and wireless Networks. 6LoWPAN uses the IPv6 thus the need for configuration servers such as DHCP and NAT is not available as the IPv6 has the Zero Configure and Neighbour Discovery capabilities. The use of IPv6 also allowed the protocol to define a unique stateless header compression mechanism for the transmission of IPv6 packets in as few as 4 bytes.

A key attribute to 6LoWPAN is the IPv6 (Internet Protocol version 6) stack, which has been a very important introduction in recent years to enable the IoT. IPv6 provides a basic transport mechanism to produce complex control systems and to communicate with devices in a cost-effective manner via a low-power wireless network.

The challenges to develop Internet of Things applications using 6LoWPAN stack similarly but with more complexity and can be identified specifically to routing and security of all nodes on the network.

5 Routing

Routing is a fundamental piece of the overall IPv6 architecture for the Internet of Things. It became clear as intelligent devices were proliferating into all aspects of life, that a new routing protocol would be required for devices on the smart grid as well as other smart devices operating in harsh environments such as smart grids, manufacturing plants, commercial buildings, and on transportation networks. The networks in these environments can be described as Low Power and Lossy Networks LLN, meaning they often operate with significant constraints on processing power, memory and energy translating into high data loss rates, low data transfer rates and instability. Routing Protocol for Low-Power and Lossy Networks RPL is a routing protocol on IPv6 that will translate the potential of Internet of Things into reality.

As of 2011, RPL has been deemed ready by the IETF as a proposed standard RFC. The objective of RPL is to target networks which comprise of thousands of nodes where the majority of the nodes have very constrained resources. RPL protocol consists of routing techniques that organize networks in units called Directed Acyclic Graphs DAG. DAG is structure where all nodes are connected but there is no available round trip path from one node to another [48].

Each DAG structure is called Destination Oriented Directed Acyclic Graph (DODAG). The DODAG starts at the root node or sink. The root node is initially the only node that is a part of the DODAG, until it spreads gradually to cover the whole IoT as DODAG Information Object DIOs are received down in the network. In a converged IoT network, each RPL router has identified a stable set of parents, each of which is a potential next hop on a path towards the root of the DODAG as well as the calculated rank for each preferred parent for each node.

When a router needs to decide on the preferred route to use and on the preferred parent, it will emit DODAG Information Object (DIO) messages using link local multicast thus indicating its respective rank in the DODAG (usually the distance to the root is considered the metric "hop count"). All routers will do the same and each router will receive several DIO messages. Once it receives all DIO messages, it will calculate its own rank and select its preferred parent and then itself start emitting DIO messages.

Since RPL is a Distance Vector routing protocol, it restricts the ability for a router to change rank. A router can freely assume a lower rank but it can assume a higher rank, it is restricted to avoid count to infinity problem. For a router to assume a greater rank, it has to ask the root to trigger global recalculation of the DODAG by increasing a sequence number DODAG version in DIO messages. The protocol tries to avoid routing loops by computing a node's position relative to other nodes with respect to the DODAG root. RPL is mostly communication between multipoint to point routes from the sensors inside the LLN and towards the root. RPL by way of the DIO generation provides this as upward routers.

Downward routes are only used by parents to issue Destination Advertisement Object (DAO) messages, propagating as unicast via parents towards the DODAG root. In RPL routers two modes exist one that is non storing mode, where an RPL router originates DAO messages, advertising one or more of its parents and unicast it to the DODAG root. The root once it receives all DAOs from all routers, it can use source routing for reaching advertised destinations inside the LLN. The second mode, the storing mode, where each RPL router on the path and the root records a route to the prefixes advertised in the DAO and the next hop.

A routing metric is a quantitative value used to find the cost of a path and helps in making the routing decision in case there are different routes available. In Low power Lossy Networks a metric is a scalar used to find the best path according to the objective function.

Another important fact about the protocol's design is the maintenance of the topology. Since most of the devices in LLN and 6LoWPAN networks are typically battery powered, it is crucial to limit the amount of sent control messages over the network. To do that, a trickle timer algorithm is used since the time for each router to send a DIO message is relevant to how the network topology is changing. If the network topology keeps on changing, which means if routers keep on finding in DIO message out dated messages, it means the trickle timer for DIO messages needs to be smaller. If routers keep on finding messages and information stored up to date (similar) it means no need for DIO messages at this rate, the timer is made bigger.

5.1 RPL Messages

To understand the messages of RPL and how they propagate over a RPL DODAG, we need to first look at how the messages of RPL are sent. RPL messages typically exist in an IEEE 802.15.4 network. The data frame of the IEEE 802.15.4 encapsulates a compressed header of the IPv6 as shown in Table 1 and the payload shown in Fig. 5. The compressed header of IPv6 is used since a full IPv6 packet does not fit in an IEEE 802.15.4 frame [49]. The IEEE 802.15.4 standard specifies a maximum transmission size (MTU) of 127 bytes, yielding about 122 bytes of actual Media Access Control (MAC) payload [50]. The payload also contains the ICMPv6 control message contained with the IP datagram, also shown in Fig. 5. The type of messages in ICMPv6 is set to 155 when RPL control messages are being sent [51]. Thus an IPv6 header compression is used, encapsulated in the IEEE 802.15.4 header as per IEEE 802.15.4 specifications in [52]. The IPv6 compressed header of IEEE 802.15.4 header is of 5 bytes in size and shown in Table 1.

RPL messages are considered part of the data frame message and they are sent in the payload of an 802.15.4 packet. Control of RPL and the order for a root to form a DODAG and for a node to join a DODAG are shown below:

1. DODAG Information Solicitation message (DIS) (Sect. 5.1.1)
2. DODAG Information Object (DIO) (Sect. 5.1.2)

Table 1 Size of the different fields of the IEEE 802.15.4 frames

Name of field	Size in bytes
LOWPAN_IPHC base encoding	2
Context identifier extension	1
Next header	1
Group ID to identify all-RPL-nodes multicast address	1

This is encapsulated in the IPv6 compressed header

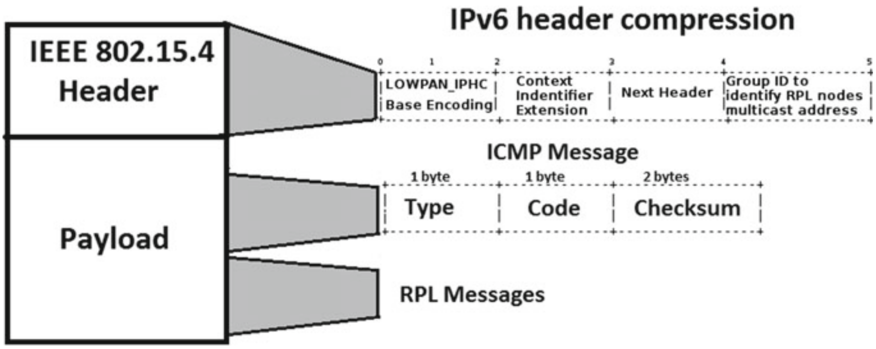


Fig. 5 IEEE 802.15.4 frame with the header and the payload sizes as defined by the 802.15.4 specifications

3. Destination Advertisement Object (DAO) (Sect. 5.1.3)
4. Destination Advertisement Object Acknowledgement (DAO-ACK) (Sect. 5.1.4)—Optional.

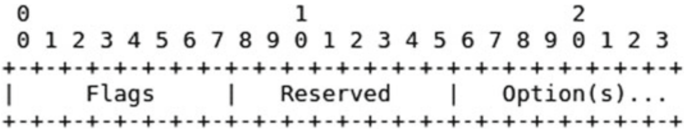
5.1.1 DODAG Information Solicitation (DIS)

The DODAG Information Solicitation (DIS) message shown in Fig. 6 as per the definition of RPL messages in [53] may be used to solicit a DODAG Information Object from a RPL node. Its use is analogous to that of a Router Solicitation as specified in IPv6 Neighbour Discovery. A node may use DIS to probe its neighbourhood for nearby DODAGs.

5.1.2 DODAG Information Object (DIO)

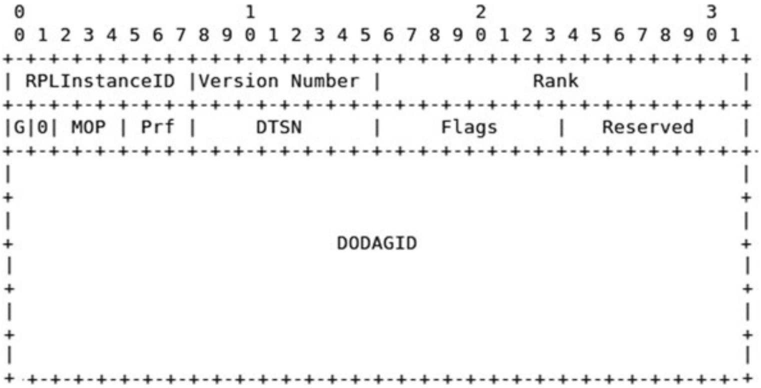
A DIO base object structure shown in Fig. 7, as per the definition of RPL messages in [53] consists of 24 bytes. This is followed by the route information bytes and metric container bytes.

The RPLInstanceID is an 8 bits field set by the DODAG root that indicates which RPL instance the DODAG is part of. The version number is set by the DODAG root



```
 0                   1                   2
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Flags     |   Reserved    |   Option(s)...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Fig. 6 DIS base object frame with the 8 bits unused field reserved for flags. This field is ignored by the receiver and set to zero by the sender. The reserved and the option fields are ignored by the receiver

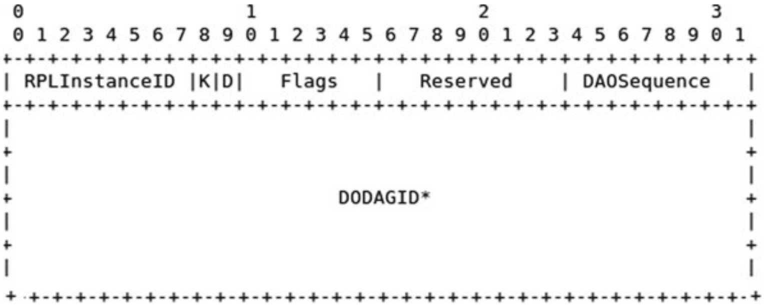


```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| RPLInstanceID |Version Number |             Rank              |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|G|0| MOP | Prf |     DTSN      |     Flags     |   Reserved    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
+                                                               +
|                                                               |
+                            DODAGID                            +
|                                                               |
+                                                               +
|                                                               |
+                                                               +
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Fig. 7 DIO message embedded in a 6LoWPAN frame

Table 2 DIO message fields

Name of field	Size in bytes
DIO base object (Fig. 7)	24
DODAG configuration option	16
Route information option	24
Metric container	16



```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| RPLInstanceID |K|D|    Flags    |   Reserved    | DAOSequence   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
+                                                               +
|                                                               |
+                           DODAGID*                            +
|                                                               |
+                                                               +
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Fig. 8 Destination Advertisement Object (DAO) base object

and the rank is a 16 bit unsigned integer indicating the DODAG Rank of the node sending the DIO message. This defines how the nod receiving the DAO will decide how it will respond to the DIS message. The DODAGID is a 128 bit IPv6 address set by the DODAG root that uniquely identifies a DODAG. The DODAGID must be a rootable IPv6 address belonging to the DODAG root as defined in [53].

The DIO message shown in Fig. 7 is embedded in the payload of the IEEE 802.15.4 data frame and takes 80 bytes as defined by Routing Over Low power and Lossy networks (ROLL) in ROLL and shown in Table 2.

The metric container shown in Table 2 takes 16 bytes from the IEEE 802.15.4 message. This consists of 2 bytes for "type and option length", 6 bytes for "ETX metric object" and 6 bytes "ETX constraint object".

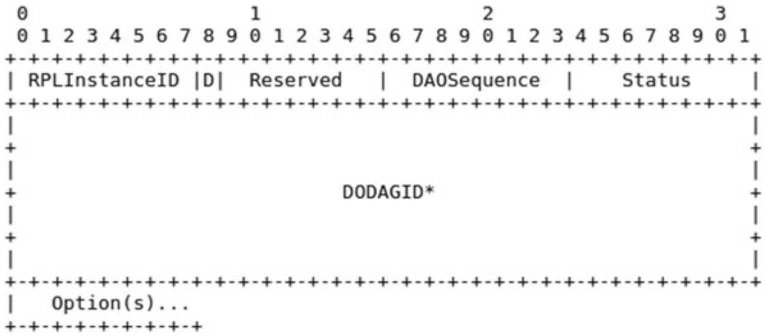
5.1.3 Destination Advertisement Object (DAO)

A DAO base object format shown in Fig. 8 as per the definition of RPL messages in [53] consists of 24 bytes. This is followed by the route information bytes, metric containers bytes and other IPv6 bytes.

The structure of a DAO message shown in Table 3 is 60 bytes.

Table 3 DAO message fields

Name of field	Size in bytes
DAO base object (Fig. 8)	20
DODAG configuration option	16
Route information option	24



```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| RPLInstanceID |D|  Reserved    |  DAOSequence  |    Status     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
+                                                               +
|                                                               |
+                            DODAGID*                           +
|                                                               |
+                                                               +
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   Option(s)...
+-+-+-+-+-+-+-+-+
```

Fig. 9 Destination Advertisement Object Acknowledgement (DAO) base object

Table 4 DAO-ACK message fields

Name of field	Size in bytes
DAO-ACK base object	20
DODAG configuration option	16
Route information option	24

5.1.4 Destination Advertisement Object Acknowledgement (DAO-ACK)

The DAO-ACK message shown in Fig. 9 as per the definition of RPL messages in [53] is sent as a unicast packet by a DAO recipient (a DAO parent or DODAG root) in response to a unicast DAO message. It consists of 20 bytes. This is followed by route information bytes, metric containers bytes and other IPv6 bytes.

The 69 bytes of the DAO-ACK message are shown in Table 4.

5.2 RPL Routing Metrics and Constraints

For a DODAG to be constructed, the root will need to first broadcast a DODAG Information Object (DIO) message, discussed in details in Sect. 5.1.2 to all its neighbours. This DIO message will propagate through the network. Each node that receives a

DIO message will consider the sender node a preferred parent to reach the root node until it receives another DIO message with better metrics to reach the root from another node [53]. The DIO message contains the DAG Metric Container option that is used to report metrics along the DODAG. The DAG metric Container may contain one specific metric or various numbers of metrics and constraints as chosen by the implementer [53]. Should multiple metrics and/or constraints be present in the DAG Metric Container, their use to determine the “best” path can be defined by an Objective Function (OF). Directed Acyclic Graph (DAG) that attempts to minimise path costs to the DAG root according to a set of metrics and Objective Functions. There are circumstances where loops may occur and RPL is designed to use a data-path loop detection method. This is one of the known requirements of RPL, and other data-path usage might be defined in the future. The graph is constructed by the use of an Objective Function (OF) which defines how the routing metric is computed. In other words, the OF specifies how routing constraints and other functions are taken into account during topology construction.

The Routing Metrics and Constraints for RPL are defined in [53]. Those metrics and constraints are used in addition to other variables together and identified as OCP 0 for Objective Function Zero (OF0). When the DAG Metric container contains a single metric, called an aggregated metric, that adjusts its value as the DIO message travels along the DAG. A node decides on its preferred parent and thus its rank based on this single rank only [54]. For example if the node Energy metric is aggregated along paths with an explicit Min function. The best path is selected through an implied Max function because the metric is Energy and thus the node with the highest Energy is selected as preferred parent. However, when a DAG Metric Container contains several metrics, then they need to be used in the order of criteria to be achieved. Each Metric criterion will be first met before moving to the next metric when deciding on a rank of a node (preferred parent). Several Metrics/Constraint Objects exist. In this section, the Metrics and Constraint Objects are discussed.

Each of the objects below is a metric that can be considered a criterion in selecting a preferred parent. When chosen, it will be defined in the DAG Metric Container. Only one object of each metric can exist in the DAG Metric Container. Those metrics objects fall into two categories:

1. Node Metric/Constraint Objects (Sect. 5.2.1)
2. Link Metric/Constraint Objects (Sect. 5.2.2).

5.2.1 Node Metric/Constraint Objects

Node Metric/Constraint Objects are metrics or constraints related to nodes such as node processing power, node memory, congestion situation, node energy (e.g. in power mode, estimated remaining lifetime and hop count to reach the node). Several metrics exist to calculate those criterias

1. Node State and Attribute Object (NSA): The NSA object is used to provide information on node characteristics. Those characteristics of node state and attribute are defined by an 8 bit flag. This flag can have the value 'A' flag or '0' flag. 'A' flag means that applications in this node may use aggregation node attribute in their routing decision to minimize the amount of traffic on the network. '0' flag means that node workload may be hard to determine and express in some scalar form. Node workload will then be set based upon CPU overload, lack of memory or any other node-related conditions.
2. Node Energy Object: The Node Energy Object is used as a metric when it is desirable to avoid selecting a node with low energy. Power and energy are clearly critical resources in most LLNs. Node Energy Object is calculated by determining the node Energy Consumption needed for each node [55].

   $$EE = \frac{Power_{now}}{Power_{max}} \times 100$$

   where EE is the energy estimation for each node.
3. Hop Count Object (HP): The Hop Count Object (HP) is used to report the number of traversed nodes along the path. The HP object may be used as a constraint or a metric. When used as a constraint, the DAG root indicates the maximum number of hops that a path may traverse. When that number is reached, no other node can join that path. When used as a metric, each visited node simply increments the Hop Count field.

5.2.2 Link Metric/Constraint Objects

Link Metric/Constraint Objects are metrics related to links connecting nodes together such as link quality, link latency, throughput and reliability. Similarly to the Node Metric Objects, only one of each of the objects discussed below can be used at a time in the DAG Metric Container. Several link objects exist to calculate those criteria.

1. Throughput: The throughput is the amount of data moved successfully from one point in the network to another in a given time period. The throughput object is calculated by calculating the estimated actual throughput. This is done when each node reports the range of throughput that their link can handle in addition to the currently available throughput.
2. Latency: The latency is the amount of time a packet takes to travel from one point in the network to another. The latency object is calculated by calculating the estimated actual latency. This is done when each node report the range of latency that they allow in addition to the latency they are suffering based on the power consumption.
3. The Link Quality Level Reliability Metric (LQL) [53]: The Link Quality Level (LQL) object is used to quantify the link reliability using a discrete value, from 0 to 7, where 0 indicates that the link quality level is unknown and 1 reports the

highest link quality level. The LQL can be used either as a metric or a constraint. When used as a metric, the LQL metric can only be recorded. For example, the DAG Metric object may request all traversed nodes to record the LQL of their incoming link into the LQL object. Each node can then use the LQL record to select its parent based on some user defined rules.

4. The ETX Reliability Object: The ETX metric is the number of transmissions a node expects to make to a destination in order to successfully deliver a packet. In contrast with the LQL routing metric, the ETX provides a discrete value (which may not be an integer) computed according to the formula below:

$$ETX = \frac{1}{PRR_{down} \times PRR_{up}}$$

and where PRR is (Packet Reception Rate)

$$PRR = \frac{\text{Number of Received Packets}}{\text{Number of Sent Packets}}$$

and ETX is expected transmission count.

5.3 RPL Objective Functions

An Objective Function defines how a RPL node selects the optimised path within a RPL instance based on the routing metrics and constraints. It provides specific optimisation criteria like minimise hop count, path ETX, Latency etc. RPL forms Directed Acyclic Graph (DAGs) based on the objective function. The OF guides RPL in selection of the preferred parents and candidate parents. It is also used by RPL to compute the ranks of a node. All upward traffic is forwarded via the preferred parent. The ETX metric of a wireless link is the expected number of transmissions required to successfully transmit a packet on the link. Objective Function ETX uses ETX metric while computing the shortest path.

The Objective Function (OF) is identified by an Objective Code Point (OCP) within the DIO Configuration option. An OF defines how nodes translate one or more metrics and constraints, which are themselves defined in [55], into a value called Rank, which approximates the node's distance from a DODAG root in term of the number of hops it needs to reach it. An OF also defines how nodes select parents. When a new DIO is received, the OF that corresponds to the Objective Code Point (OCP) in the DIO is triggered with the content of the DIO. OCP is an identifier assigned by the Internet assigned Numbers Authority (IANA). Two OCP values are assigned, one for OF0 given identifier OCP 0 and the other for the Minimum Rank with Hysteresis Objective Function (MRHOF) given the identifier OCP 1. It is worth noting that OF0 and MRHOF are the only two Objective Functions that are fully defined by IETF. ETX is still a draft however it is widely used. Two other draft

Objective Functions that are not used as much and are proven not to be effective are Load Balancing Objective Function (LBOF) and Traffic Aware Objective Function (TAOF).

In this section, the objective functions overview is shown with how each of them format the Destination Advertisement Object (DAO) message with values relevant to the OF and the decision of the preferred parent.

5.3.1 Objective Function Zero

The metrics and constraints objects discussed above in Sect. 5.2 are used, if selected in the DAG Metric Container to select the preferred parent. Each of those individually can be used to determine the path for a node to the root. However when multiple DAG Metric Containers are used, those metrics are grouped together in a Objective Function.

An OF0 implementation first computes a new variable called step of rank (SR). This variable is associated with a given parent from relevant link properties and metrics as explained below.

The SR is used to compute the amount by which to increase the rank along a particular link. It first starts by making sure the node is a candidate preferred parent (received DIO message) by making sure the link is valid in terms of connectivity and suitability. After this, the node makes sure that the candidate node has acceptable node attribute (power, energy, CPU, memory, battery) to be able to act as a preferred parent. If all those criteria are fulfilled, the node selects the candidate as a preferred parent and changes the value of its rank in the RPL DAO message by increasing the rank it received in the DIO of the candidate by 1.

The variable rank increase RI is represented in units expressed by the variable M, which defaults to the fixed constant that is defined in [53] as the default minimum hop rank increase $DRI = 256$.

The SR is then computed for that link by multiplying by the rank factor Rf and then possibly stretched by a term Sr that is less than or equal to the configured stretch of rank. The resulting RI is added to the Rank of preferred parent $R(P)$ to obtain that of this node as below:

$$R(N) = R(P) + RI$$

where

$$RI = (Rf \times SR + Sr) \times M$$

5.3.2 The Minimum Rank with Hysteresis Objective Function (MRHOF)

The Routing Protocol for Low-Power and Lossy Networks (RPL) is a distance vector IPv6 routing protocol designed for LLN networks. RPL is designed for networks which comprise thousands of nodes where the majority of the nodes have very constrained energy and/or channel capacity. To conserve precious resources, a routing protocol must generate control traffic sparingly [56]. However, this is at odds with the need to quickly propagate any new routing information to resolve routing inconsistencies quickly.

RPL organises its topology in a Directed Acyclic Graph (DAG). An RPL DAG must have at least one RPL root and a Destination Oriented DAG (DODAG) is constructed for each root. The root acts as a sink for the topology by storing all routes to all nodes in the DODAG in the routing table. The root may also act as a border router for the DODAG to allow nodes that belong to different DODAGs to communicate [53].

For a DODAG to be constructed, the root will need first to broadcast a DODAG Information Object (DIO) message, discussed in detail in Sect. 5.1.2, to all its neighbours. This DIO message will propagate through the network. Each node that receives a DIO message will consider the sender node a preferred parent to reach the root node until it receives another DIO message with better metrics to reach the root from another node [53].

The DIO message contains the DAG Metric Container option that is used to report metrics along the DODAG. The DAG metric Container may contain one specific metric or various numbers of metrics and constraints as chosen by the implementer [53]. Should multiple metrics and/or constraints be present in the DAG Metric Container, their use to determine the “best” path can be defined by an Objective Function (OF).

The Objective Function (OF) is identified by an Objective Code Point (OCP) within the DIO Configuration option. An OF defines how nodes translate one or more metrics and constraints, which are themselves defined in [55], into a value called Rank, which approximates the node’s distance from a DODAG root in term of the number of hops it needs to reach it. An OF also defines how nodes select parents. When a new DIO is received, the OF that corresponds to the Objective Code Point (OCP) in the DIO is triggered with the content of the DIO. For example, OF0 explained in Sect. 5.3.1, is identified by OCP 0 by the Internet assigned Numbers Authority (IANA). The Minimum Rank with Hysteresis Objective Function (MRHOF) explained in Sect. 5.3.2, is the other Objective Function defined by IANA and given the identifier OCP 1.

Several Objective Functions were designed in order to fulfil specific tasks. A Destination Advertisement Object (DAO) message, for each node receiving the DIO message, will be sent to the candidate node (DIO message origin) with values relevant to the OF and the decision of the preferred parent.

This Objective Function describes the Minimum Rank with Hysteresis Objective Function (MRHOF) [57], an Objective Function that selects routes that minimise a metric, while using hysteresis to reduce lagging in response to small metric changes. First, it finds the minimum cost path, i.e., path with the minimum Rank. Second, it switches to that minimum Rank path only if it is shorter (in terms of path cost) than the current path by at least a given threshold. This second mechanism is called "hysteresis". MRHOF works with additive metrics along a route, and the metrics it uses are determined by the metrics that the RPL Destination Information Object (DIO) messages advertise.

MRHOF uses current minimum path cost for the cost of the path from a node through its preferred parent to the root computed at the last parent selection. It also uses the following parameters

- MAX LINK METRIC: Maximum allowed value for the selected link metric for each link on the path.
- MAX PATH COST: Maximum allowed value for the path metric of a selected path.
- PARENT SWITCH THRESHOLD: The difference between the cost of the path through the preferred parent and the minimum cost path in order to trigger the selection of a new preferred parent.
- PARENT SET SIZE: The number of candidate parents including the preferred parent, in the parent set.
- ALLOW FLOATING ROOT: If set to 1, allows a node to become a floating root. A node MAY declare itself as a Floating root, and hence have no preferred parent, depending on system configuration.

The calculation of the ETX metric is given constant selected metrics based on [58]. The metrics are:

- MAX LINK METRIC: Disallow links with greater than 4 expected transmission counts on the selected path (Set to 512).
- MAX PATH COST: Disallow paths with greater than 256 expected transmission counts (Set to 32,768).
- PARENT SWITCH THRESHOLD: Switch to a new path only if it is expected to require at least 1.5 fewer transmissions than the current path (Set to 192).
- PARENT SET SIZE: If the preferred parent is not available, two candidate parents are still available without triggering a new round of route discovery (Set to 3).
- ALLOW FLOATING ROOT: Do not allow a node to become a floating root (Set to 0). If FR is 0 and no neighbours are discovered, the node does not have a preferred parent and must set the minimum path cost to PS.

5.3.3 ETX

The expected transmission count ETX metric discuss is based on the number of expected transmissions required to successfully transmit and acknowledge a packet on a wireless link. The ETX metric is commonly used in wireless routing to distinguish between paths that require a large number of packet transmissions from those that require a smaller number of packet transmissions for successful packet delivery and acknowledgement however RPL uses this metric to establish preferred parent based on the value of the ETX metric of the link as defined in [55, 59] and make it available for route selection. This is called ETX Objective Function (ETX).

In ETX, ETX metric allows RPL to find a minimum-ETX path from the nodes to a root in the DAG instance. This is the minimum ETX path between a node and the DAG root is the path (among other paths between the source and the destination) that requires the least number of packet transmissions per packet delivery to the DAG root. Thus, minimum-ETX paths are generally also the most energy-efficient paths in the network.

The ETX uses the ETX metric to find the path to be used to deliver packets in a DAG instance with the minimum number of transmission required by using the ETX link metric to compute an ETX path metric based on the ETX link metric of each hop and choosing paths with smallest path ETX.

At first, the root node set the parameters to identify the smallest ETX path for each node:

- min_path_etx: A variable that determines the ETX path metric of the path from a node through its preferred parent to the root computed at the last parent selection.
- $MIN\_ETX\_PATH\_CONST$: A constant that defines the maximum ETX value that can be considered for a node to be considered for parent selection.

Each other node in the DAG (non root) computes the ETX path metric for a path to the root through each candidate neighbour by using the two parameters explained below:

- $ETX\_Neighbor\_Metric$: A variable that identifies the ETX metric for the link to a candidate neighbour.
- MIN_PATH_ETX: A variable that assigns a value for each neighbour and the minimum ETX path advertised by that neighbour.

A node computes the ETX path metric for the path by comparing all the MIN_PATH_ETX received for each candidate neighbour. If a neighbour ETX metric cannot be computed, it is set to infinity to avoid selecting it and potentially having high ETX paths.

A node SHOULD compute the ETX Path metric for the path through each candidate neighbour reachable through all interfaces. If a node cannot compute the ETX path metric for the path through a candidate neighbour, the node MUST NOT make that candidate neighbor its preferred parent.

If the ETX metric of the link to a neighbour is not available, the ETX Path metric for the path through that neighbour SHOULD be set to INFINITY. This metric value will prevent this path from being considered for path selection, hence avoiding potentially high ETX paths.

The ETX Path metric corresponding to a neighbour MUST be re-computed each time the ETX metric of the link to the candidate neighbour is updated or if the a node receives a new min_path_ETX advertisement from the candidate neighbour.

After computing the ETX path metric for all candidate neighbours reachable for the current DAG instance, a node selects the preferred parent. The selection process is based on the condition that the ETX path metric corresponding to that neighbour is smaller than the ETX path metric of all the other neighbours.

Once the preferred parent is selected, the node sets its min_path_ETX variable to ETX path metric of the preferred parent. The vale of this variable is then carried in the metric container whenever DIO messages are sent.

5.3.4 Load Balancing Objective Function

Load Balancing Objective Function LBOF adds Child Node Count (CNC) as a metric, and uses it to select paths in a way that maintains a balanced number of children per preferred parent in the DODAG [60]. This will balance the traffic between the nodes, resulting in lower power consumption (hence longer network lifetime), a lower possibility of bottlenecks, and better delivery rate. An evaluation for this OF was carried in [61] with a comparison to OF0 and MRHOF, and it shows that LBOF provides longer network lifetime (by 16–40%) and better delivery rate (by 10–15%). However, with larger networks the LBOF seems to consume more energy due to parents churn. For this reason LBOF is considered out of context of this research.

5.3.5 Traffic Aware Objective Function

Traffic Aware Objective Function (TAOF) uses a combination of EXT and Packet Transmission Rate (PTR) as routing metrics, and uses it to select paths with less traffic towards the root and is defined in [62]. Authors in [63] defines TAOF which balances the traffic load that each node processes in order to ensure node lifetime maximization. They alter the DIO message format, introduced a new RPL metric, named Traffic Rate and used a new parent selection algorithm. The results in [63] show that TAOF achieves enhanced performance in terms of Packet Delivery Ratio (PDR) and that it builds more stable networks with fewer parent changes. However, it doesn't cope well with a dynamic network as it will increase the packet delivery ratio if the number of hops to reach the border gateway increases. For this reason TAOF is considered out of context of this research.

6 Security

Security is a major issue in the roadmap as explained in [64] to implementing the Internet of things mainly because it is not possible to directly apply existing Internet-centric security mechanisms due to the intrinsic features of WSN (e.g. the capabilities of the nodes, the bandwidth of the wireless channel).

The purpose of those readings was to understand the standards and protocols that are becoming the driving force for securing a large network of sensors and small devices that will form the Internet of Things. This security involves securing the key establishment process and the routing discovery and establishment process.

Like any other network, the primary goals of securing the Wireless Sensor Network are the standard security goals such as confidentiality, integrity, authentication and availability.

- Confidentiality: the ability for a message to remain confidential but concealing it from a passive attacker. For WSN, a sensor node should not reveal its data to its neighbours.
- Authentication: the ability to ensure that the message reliable by confirming and identifying the source of this message (origin). Data authentication can be achieved by verifying the identity of source through symmetric or asymmetric mechanisms.
- Integrity: the ability of nodes to ensure that the message was not tampered and modified during transmission.
- Availability: the ability to use the resources and retain them for the whole duration of the communication of messages.

Other security goals such as data freshness, self-organization and secure localization are also of importance. Data freshness is the ability to ensure that the message received is the most recent one and that no newer messages were relayed. Self-organization in a network is when a node is able to self-organize and self-heal itself when it was compromised. Secure localization is the ability to locate accurately a node in a network.

Security challenges for the IoT and its integration within the IoT is studied as the challenges are tightly applicable to other relevant technologies of the IoT such as embedded systems, mobile phones and RFID. Security Threats for IoT based on the goals mentioned above are:

- Confidentiality: threats for confidentiality in IoT involves an attacker eavesdropping and overhearing critical information such as sensing data and routing information. Based on this the adversary may cause severe damage since they can use the sensing data for many illegal purposes [7].
- Authentication: threats for authentication in IoT involves attacks on the network that can alter the packets. It can also inject false packets. Another threat for IoT, is a general threat for wireless networks. The nature of the media and the unattended nature of wireless sensor networks make it extremely challenging to ensure authentication.
- Integrity: a malicious node present in the network can inject false data. Instability of wireless channel can cause damage or loss of data.
- Achieving a self-organizing and self-healing network in IoT is considered challenging since there is no fixed infrastructure to manage the network. This inherent feature brings another challenge as the damage resulting from an attack can be devastating.
- Localization in Wireless sensor network is essential as a compromised node can result for the attacker to manipulate data sending wrong location information by reporting false signal strengths and replaying signal.

Wireless sensor network limitations/weaknesses:

- Limited resources: for wireless sensor networks, the nodes will be limited in terms of memory, energy and processing power. Any of the security functions that will be applied on a WSN will need to take into consideration those issues as most of the available protocols and standards for encryption, decryption, data signatures, and signature verification consume memory, energy and computational power.
- Highly unreliable communication medium is another limitation for the wireless sensor networks as the nature of the communication medium can cause latency, multi-hop routing, network congestion or even conflicts such as collision. Unreliable transfers is another limitation where packets can become corrupted or even discarded which results in packet loss. This will force nodes to allocate more resources to error handling.
- On most wireless sensor networks applications, node will be left unattended and this can cause serious issues and limitation especially when nodes are exposed to physical attacks. The network is distributed thus if the design is not adequate, it can leave a network that is hard to manage, inefficient and fragile.

6.1 Security in RPL

Mayzaud et al. [65] identified three different categories of attacks on RPL that can violate one or more of the security goals defined in the previous section. The first category covers nodes resources such as energy, memory and processing power. The second category includes attacks on the topology of the RPL network and the third category corresponds to attacks against the network traffic. Attacks in the first category can damage the network since all nodes are constrained and this will shorten the lifetime of these nodes. Attacks in the second category will disrupt the normal operation of the network such as how RPL network converge and the third category of attacks will violate the confidentiality and integrity of data in the RPL network.

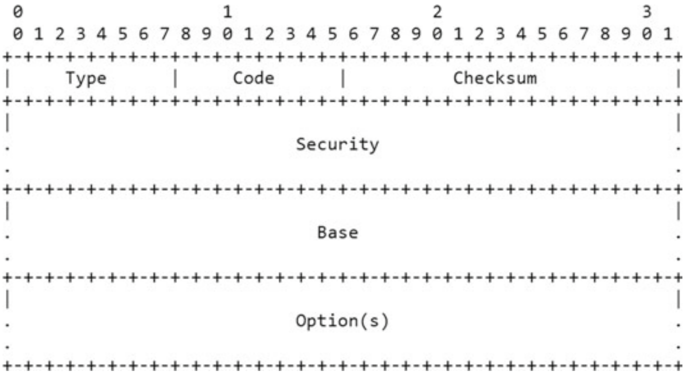
The main focus on this research is to mitigate attacks against traffic by preventing eavesdropping and passive sniffing.

RPL supports message confidentiality and integrity. It is designed as such that link-layer mechanisms can be used when available and appropriate and yet in their absence, RPL can use its own mechanisms. RPL supports three security modes defined in [53].

They are Unsecured, Pre-installed and Authenticated. Unsecured refers to the security mechanism that is provided in lower layers such as link layer security. Pre-installed and authenticated modes require the use of pre-installed shared keys on all motes prior to deploying the motes. Both modes provide security procedures and mechanisms at the conceptual level and are concerned with authentication, access control, data confidentiality, data integrity and non repudiation. This study focuses on the Pre-installed mode as a method of securing message transmission between motes in an RPL DAG instance. Authentication in the pre-installed mode involves the mutual authentication of the routing peers prior to exchanging route information (i.e., peer authentication) as well as ensuring that the source of the route data is from the peer (i.e., data origin authentication) [66]. The limitation of the pre-installed mode in its common form, is that it is assumed that a mote wishing to join a secured network is pre-configured with a shared key for communicating with all neighbours and the RPL root. This means that once this shared key is compromised, all network leaves in the RPL DODAG are compromised.

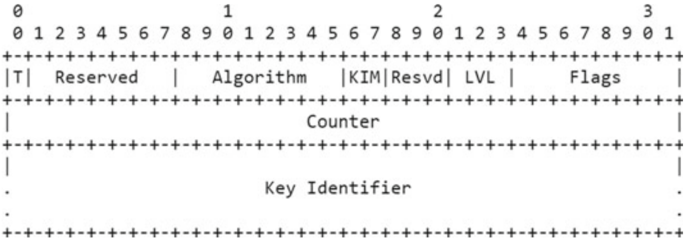
The process of distributing the keys is out of scope for the specification of the RPL request for comment document [53]. The document further assumes that in authenticated mode, the router will dynamically install new keys once they have joined a network as a host however how the router will distribute those keys is out of context for RPL specifications and is not defined.

The RPL control messages incorporated in [53] the secure field in the header contents as shown in Fig. 10. The secure field contains several subfields as shown in Fig. 11 and each of the subfields identify the level of security and the algorithms in use to protect RPL algorithms.



```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |     Code      |          Checksum             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
.                             Security                          .
.                                                               .
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
.                              Base                             .
.                                                               .
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
.                           Option(s)                           .
.                                                               .
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Fig. 10 Secure RPL control message as shown in [53]. The ICMPv6 information message with a type of 155. The code identifies the type of the RPL control messages (DIO, DAO, DIS, etc.), and the checksum computation field that is computed for each security message



```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|T|  Reserved   |   Algorithm   |KIM|Resvd| LVL |     Flags     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                            Counter                            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
.                        Key Identifier                         .
.                                                               .
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Fig. 11 Security section as shown in [53]. The level of security of the algorithm in use are indicated in the protocol message. The algorithm field specifies the encryption type, the MAC and signature scheme the network uses. The counter is time T that is a timestamp of security

The security variants provide integrity and replay protection as well as optional confidentiality and delay protection. The optional confidentiality variant is not defined in [53] however a security algorithm is proposed to specify the encryption algorithm to be used once keys are distributed.

The main security fields shown in Figs. 10 and 11 are the Message Authentication Codes (MAC) and signatures provide authentication over the entire unsecured ICMPv6 RPL control message, including the Security section with all fields defined but with the ICMPv6 checksum temporarily set to zero. Encryption algorithm provides confidentiality of the secured RPL ICMPv6 message that includes the cryptographic fields (MAC, signature, etc.). In other words, the security transformation itself (e.g., the Signature and/or Algorithm in use) will detail how to incorporate the cryptographic fields into the secured packet. The Security Algorithm field specifies the encryption, MAC and the signature scheme the network uses. The cryptographic mode of operation described in [53] (Algorithm = 0) is based on CCM and the block-cipher AES-128 defined in [67]. This mode of operation is widely supported by existing implementations.

6.2 Cryptography in IoT

The end-to-end principle argues that many functions can be implemented properly only on an end-to-end basis, such as ensuring the reliable delivery of data and the use of cryptography to provide confidentiality and message integrity. Adding a function to improve reliability on a particular link may provide some optimization, but can never ensure reliable delivery end-to-end. Similarly, security objectives that can only be met by protecting the conversation between two end-nodes are therefore best met by performing the cryptography at layer 3 or higher. There may even be security objectives that require protecting the data itself instead of the communication channel. However, this does not mean that all security objectives can be met end-to-end. In particular, achieving robust availability often requires protecting the subnetwork against attackers and more so for wireless networks. Adding a first line of defence at layer 2 may also increase robustness against attacks on confidentiality and integrity.

When combining encryption with authentication, some of the authenticated information may have to be sent in the clear. AES/CCM therefore encrypts a message (m) and authenticates that together with (possibly empty) additional authenticated data a, using a secret key K and a nonce N. A parameter L controls the number of bytes used for counting the AES blocks in the message; m must be shorter than 28L bytes. For IEEE 802.15.4 packets, the smallest value of L = 2 is plenty. Counter with CBC-MAC (Cipher Block Chaining Message Authentication Code) [CCM] is an authenticated encryption algorithm that provides at the same time confidentiality, authentication and integrity protection.

Even with the best link-layer security mechanisms, the data is no longer protected once it leaves the link. This makes the data vulnerable at any point that is responsible for forwarding it at the network layer, or on any link that has lesser security. Even worse, an attack on the network layer might be able to divert data onto a path that contains additional forwarding nodes controlled by the attacker. End-to-end security that protects the conversation along the entire path between two communicating nodes is therefore an important element of any robust security system, so much so, that this requirement became a banner feature in the development of IPv6 [45].

Security involves two main aspects, the Network access (authorization) and the key management during the device communication. Key management protocols can be classified according to the method the key is delivered (key transport or key agreement) and whether key exchanged are based on symmetric or asymmetric cryptography.

Symmetric techniques demand the communicating parties to possess the same key prior to message exchange. Standard online key exchange protocols involving public parameters or trusted authorities are generally avoided. Instead, as defined in [68] Key Pre-Distribution KPS techniques, involving the following steps are preferred: (i) Preloading of Keys into the sensors prior to deployment; (ii) Key establishment: this phase consists of (a) Shared key discovery: establishing shared key(s) among the nodes and (b) Path key establishment: establishing path via other node(s) between a given pair of nodes that do not share any common key.

All of key management or key agreement schemes follow one of the three general key agreement schemes: trusted-server scheme, self-enforcing scheme, and key pre-distribution scheme. Trusted server scheme is not suitable for wireless sensor network as usually there is no centralized infrastructure in sensor networks such as a centralized entity to manage Kerberos. The self-enforcing scheme depends on symmetric cryptography such as a key agreement using a public key certificate. Limited computation and energy resources of sensor nodes often make it undesirable to use public key algorithms such as Diffie-Hellman key agreement or RAS. Many implementation and evaluation proved this to be an unrealistic scheme for WSN [69]. To use Public Key Infrastructure (PKI) technology. For example, each endpoint must be able to store digital keys, run encryption and decryption algorithms and conduct sophisticated handshakes to establish secure SSL connections, etc. However, many IoT nodes like the passive RFID tags or sensors simply don't have the electrical power, storage, or processing power necessary to tackle even the simplest of PKI tasks.

The time to execute the main cryptographic operation of ECC, the scalar point multiplication has been reduced from 34 s in 2004 to less than 0.5 s in 2009. With ECC, any node can make use of digital signature schemes (ECDSA), key exchange protocols (ECDH), and public key encryption schemes (ECIES). However, PKC is still too expensive to be used by sensor nodes implementing web servers as the overhead of its software implementation (420 ms) is too high. Note that the use of other PKI primitives with extremely efficient encryption and verification is discouraged. However PKI is still too expensive to be used by sensor nodes implementing web servers, as the overhead of its software implementation (420 ms) is still too high [70].

IPsec was considered a serious contender for securing WSN and many methods of research were involved in creating a lightweight version of IPsec to be incorporated into the 6LoWPAN architecture. Authors in [71, 72] suggested compressing the IPsec and only looked at the authentication header part of the IPsec but suggested to use key pre distribution for the end to end communication. Other research suggested that the IPsec is unsuitable IAS t is designed for one-to-one communication. However, the dominant types of communication in WSNs are Many-to-one and One-to-many. This makes such protocols unsuitable for the usage in WSNs.

Sensors can use the 6LoWPAN protocol to interact with an IPv6 network as they are powerful enough to implement symmetric key cryptography standards such as AES-128 in [73].

Authors in [70] explain that even if assumptions were made that a WSN peer is protected by its own security mechanisms such as using the link layer security of IEEE 802.15.4, the public nature of the internet will require the existence of a secure communication protocol for protecting the communication between two peers. Key establishment is a fundamental security issue in wireless sensor networks (WSN). It is the basis to establish secure communication using cryptographic technologies between sensor nodes. Due to the current resource constraints on sensors, it is infeasible to use traditional key management techniques such as public key cryptography or key distribution centre based protocols. Therefore the key pre-distribution schemes are paid most attention in key management of WSN.

It was very important to understand how those networks utilize the available pre distribution techniques such as the mostly used one, proposed by Eschenauer and Giglor [1] to secure the Distributed Sensor Networks (DSN).

Authors in [69] modified E-G scheme by only increasing the number of keys that two random nodes share from at least 1 to at least q. It increased vulnerability in a large scale node compromise attack. They further extended this idea and developed two key pre-distribution techniques: a q-composite key pre-distribution scheme and a random pairwise keys scheme. The q-composite key pre-distribution also uses a key pool but requires two nodes compute a pairwise key from at least q-pre-distributed keys that they share. The random pairwise keys scheme randomly picks pairs of sensor nodes and assigns each pair a unique random key.

A framework was developed in [74] to be used to improve the performance of any existing key pre-distribution scheme using polynomial pairwise key. This framework does not require any prior knowledge of sensors' expected locations, and thus greatly simplifies the deployment of sensor networks.

It is now accepted to assume that the Key management scheme for distributed sensor networks developed by Eschenauer and Giglor is a standard to use for securing wireless sensor networks. However Eschenauer and Giglor only looked at the key pre-distribution schemes proposed for WSN and ZigBee as the main purpose of their research, our objective is to implement a Key distribution mechanism for the IoT to solve the problem of exchanging key between devices connected to the IoT without compromising the nodes or the validity of the Keys because of a Man in the Middle attack using the same scheme proposed by Eschenauer and Giglor [1]. Algorithm for the key management scheme for distributed sensor networks and how it will be used in the context of the IoT will be shown later on in this report.

6.3 Key Pre-distribution in DSN

In order to provide security between nodes communicating, encryption/decryption keys needs to be used for each and every communication link between devices. The main feature of key pre distribution and how it works is referred in the context of any Ad Hoc network as a challenge. The challenge simply lies in how the keys will be distributed beforehand and how to ensure that nodes communicating in an Ad-Hoc nature share a key and thus can provide secrecy and authentication by encrypting their communication channel.

The management of key is one of the key challenges to secure networks. We list below key pre distribution challenges when used in the context of the distributed sensor networks DSN.

- It is difficult to distribute keys and keying materials such as identifiers prior to deployment.
- Nodes in the networks are not authenticated and therefore obtaining a key does not guarantee that a node is trusted.
- Nodes in the distributed sensor networks are mostly battery operated low power devices, limited memory resources and computation power and the key pre distribution scheme chosen needs to have low overhead to ensure that the nodes can still operate efficiently.
- The nature of the distributed sensor networks and where nodes are located means that it is difficult to know where nodes. This can potentially result in the physical capture of the nodes and they become compromised and all credentials can be exposed.
- Note all nodes are implemented at the same time, for this reason the key pre distribution scheme needs to ensure that existing nodes in the network will work together securely with the newly added nodes.
- If node is compromised.

In addition the challenges to the key pre distribution presented above, the Internet of Things network present on top of those challenges other challenges unique to them. The main challenge related to this research is the nature of how nodes communicate in an IoT network which prevent nodes from creating more than one node and therefore if the key distribution scheme used does not produce enough keys not all nodes will participate in the IoT network.

In sensor networks, key distribution is usually combined with initial communication establishment to bootstrap a secure communication infrastructure from a collection of deployed sensor nodes. In the setting we study in this chapter, nodes have been pre-initialized with some secret information before deployment, but only after network setup will we know the location of nodes. The node location often determines which nodes need to establish a link with which other nodes, so we cannot set up these keys before deployment. In this chapter, we refer to the combined problem of key distribution and secure communications establishment as the security bootstrapping problem, or simply the bootstrapping problem. A bootstrapping protocol must not only enable a newly deployed sensor network to initiate a secure infrastructure, but it must also allow nodes deployed at a later time to join the network securely.

This is a challenging problem due to the many limitations of sensor network hardware and software. In this chapter, we discuss and evaluate several well-known methods of key distribution. Besides these, we present an in-depth study of random key pre distribution, a method that has recently attracted significant research attention and we have also worked on. However, the pairwise key establishment problem is still not solved. For the basic Probabilistic and the q-composite key pre-distribution schemes, as the number of compromised nodes increases, the fraction of affected pairwise keys increases quickly. As a result, a small number of compromised nodes may affect a large fraction of pairwise keys. While the random pairwise keys scheme doesn't suffer from the above security problem and given the memory constraint, the network size is strictly limited by the desired probability that two sensors share a pairwise key and the number of neighbour nodes that a sensor can communicate with.

The interest of this research is to look at the various methods of key distribution between various devices in the context of the IoT proposed and study their feasibility.

Pre-distribution of keys can follow one of three major approaches when used in the context of the IoT as explained in [75]. The probabilistic approach explained in Sect. 6.4, the deterministic approach explained in Sect. 6.5 or the hybrid approach that combines both as proposed in [76–79].

Paterson and Stinson mathematically investigated in [80] the metrics that should be used to assess the suitability of the various probabilistic and deterministic key pre distribution schemes and identified them as the network size, storage requirements, network connectivity and network resilience. When using those key pre-distributions schemes in the context of the IoT other metrics also needs to be evaluated as proposed in [81]. The metrics are scalability to identify if the scheme can support large networks, efficiency to evaluate how much storage and processing power the used scheme will use, storage complexity in term of the amount of memory required to store the security keys for large networks and processing complexity in order to computer the amount of processor cycles required to establish a key and communication complexity as in the number of messages exchanged during the key generation and distribution process. Resilience should also be considered in evaluating how resilient the network will be if a node is captured and keys need to be revoked. Finally the key connectivity metric will need to be evaluated as the number of keys will increase if the probability of two nodes to share a key is low and this will have a high impact on the other metrics.

6.4 Probabilistic Key Pre-distribution

Probabilistic schemes is where the secure link establishment is conditioned by the existence of shared pre-loaded keys and deterministic schemes which ensure total secure connectivity coverage. The idea behind the probabilistic scheme was proposed first by Eschenauer and Giglor [1]. A Random key pre-distribution (RKP) where each node is pre-loaded with a key ring of m keys randomly selected from a large pool. After the deployment step, each node exchanges with each of its neighbours the key identifiers that it maintains in order to identify the common keys. If two neighbours share at least one key, they establish a secure link and compute their session secret key which is one of the common keys. Otherwise, they should determine secure paths composed by successive secure links.

Traditional key exchange and key distribution protocols based on infrastructure using trusted third parties are impractical for large scale distributed sensor networks. There is no key distribution at the moment implemented on DSN other than key pre distribution. However the key pre distribution offers two inadequate solutions: Single mission key solution is inadequate because if one sensor node was compromised, this would lead to the compromise of all the DSN since selective key revocation is impossible upon sensor capture detection.

The other solution is pair wise private sharing of keys avoids compromise of the whole DSN since it allows selective key revocation. However, it requires pre distribution and storage of n − 1 keys in each sensor. This will mean that each node will require a large amount of memory to store the keys if for example a DSN contains 1000 nodes. In total there will be $n(n-1)/2$ keys per DSN. It will also render the communication between the devices complex and resources draining.

Eschenauer's and Giglor's approach was to propose a single key pre distribution scheme that requires memory storage for only a few tens to a couple of hundred keys, and yet has similar security and superior operational properties when compared to those of the pair wise private key sharing scheme.

Their scheme relies on Probabilistic key sharing among the nodes of a random graph and uses a simple shared key discovery protocol for key distribution, revocation and node re-keying.

This aim of this chapter is to identify how the Probabilistic key pre-distribution scheme can be applied in the context of the Internet of Things networks to allow keys to be distributed among nodes in the network so that only RPL nodes that share a pair-wise key can join the RPL DODAG and how the scheme will perform.

6.5 Deterministic Key Pre-distribution

Deterministic schemes ensure that each node is able to establish a pair-wise key with each of its neighbours. To guarantee determinism, LEAP make use of a common transitory key that is pre-loaded into all nodes prior to deployment. The transitory key is used to generate session keys between neighbouring nodes before being removed.

The scheme suggested by [2] divides the solution into three phases. In the first phase, each node attempts to discover which nodes are within its neighbourhood and to verify their identities. For this, each node will commit to each identity discovered in its neighbourhood and perform the fingerprinted mutual authentication protocol FMAP protocol with each neighbour it is supposed to share a key with. The FMAP protocol assumes that each node that is pre-loaded with the fingerprint of every other node. Each node that joins the network broadcast a simple HELLO message containing its fingerprint and its key list. Every node that receive this message can verify the fingerprint in order to confirm uniqueness. If a similar fingerprint exists, the node is not allowed to join. At the end of the first phase, each node will have a list of all its neighbours including identity and fingerprint and will have verified the identity with neighbours that it shares key with. At this stage, nodes have not decided whether to accept this identity or not. Each node will overhear all FMAP protocol messages in order to decide whether it accepts its identity or not. In Phase 1, each n_i has now established a path with all direct neighbours that it was able to identify their identity of the form $n_i \rightarrow n_j$.

In the second phase and since a node has already identified direct neighbours that it shares a key with, the next step is to identify if a path can be established further beyond neighbours by using them as hops—That is the neighbours that exist outside of n's neighbourhood in the form of $n_i \rightarrow n_j \rightarrow n_k$. Verifying a node that is not a direct neighbour is more difficult as FMAP protocol cannot be imitated on nodes that are not neighbours (Those nodes cannot respond to HELLO messages from neighbours of neighbours). For this n_i will have to rely on the trust issued by each of its direct neighbours to their corresponding neighbours. However it cannot assume that the process of identifying of its neighbours n_j assumption about the identity is correct. For this it applies a voting process in which if the majority of nodes that are direct neighbours identify n_k as their direct neighbours then it assumes that n_k is an honest node. Since n_k is trusted by the majority, it is now considered as a trusted device by n_i and thus a 2 hop path is established.

In Phase 1, each n_i learns paths of the form $n_i \rightarrow n_j$, and in Phase 2 each n_i learns paths of the form $n_i \rightarrow n_j \rightarrow n_k$. Just as nodes informed their neighbours of the results of Phase 1 so that the information could be utilized to construct 2-hop paths, each node broadcasts the results of Phase 2 so that nodes of their neighbourhood learn which 3-hop paths exist. More specifically, each n_j will broadcast all paths it has discovered of the form $n_j \rightarrow n_k \rightarrow n_l$. This way, in phase 3 each node increases its knowledge of the network by one hop by relying on the nodes that were verified during phase 1 and 3 of the protocol. In phase 3, n_i is not voting for the majority to decide whether to trust n_l and has to trust that n_j already has chosen n_l as it gained majority.

The aim of this chapter is to question how the Deterministic key pre-distribution scheme can be applied in the context of the Internet of Things networks to allow keys to be distributed among nodes in the network so that only RPL nodes that share a pair-wise key can join the RPL DODAG and how it will perform.

6.6 Threats Attacks Trees

Internet of Things networks are subject to several threats as discussed in Sect. 2.2 and identified which threats can be mitigated by using encrypted communication between nodes in the network.

In this section we will look at the different threats that can be carried by malicious actors and the attack surfaces that can be exploited in order to compromise the network. We categorized the threats identified in Sect. 2.2 into two different type of attacks. The first category of attacks explained in Sect. 6.6.1 assumes that the malicious actor is exploiting the link of nodes that are sending data in plain text and on the encryption algorithm used to protect the link. The second category investigated in Sect. 6.6.2 shows how a malicious actor can attempt to exploit the routing formation or the routing table.

6.6.1 Attack Tree on Confidentiality and Integrity of Data

The threat of having an insecure communication between IoT devices is now more tangible than a conventional threat for any other type of networks on the Internet. Plain text communication makes it easier for attackers to tamper with data as well. In another scenario where an attacker tampers with the communication between an IoT device sending regular measurement of a valve in a factory for another machine to switch off for example at a critical level and modifies the temperature data. This can potentially be disastrous for a factory and might even lead to loss of life. We present in Fig. 12 the attack tree that results in violation of confidentiality, integrity or availability of the RPL DODAG.

Man in the Middle (MiTM) attacks will allow a malicious actor to eavesdrop into the communication and sniff the data transmitted between nodes. This will reveal both the data information exchanged between nodes and the control messages between nodes such as routing table formation. Since MiTM is most of the time used to allow further attacks such as session replay where the attacker stores messages exchanged between nodes in order to replay them later on. This will potentially lead to repudiation of data as there will be no method to identify and validate if the data sent is correct and the malicious actor can tamper with the data.

The proposed solution can protect some of the attacks presented in Fig. 12. Traffic analysis can partly be prevented as the traffic is encrypted and the payload (data) is not sent in the clear text. Having the data sent in clear text will violate the confidentiality of the data. This will also lead to violation of the integrity if further attacks are carried out such as Man in the middle attacks that can easily be done if the traffic is sent in clear text. The different cryptanalytic attacks presented depends on the encryption algorithm used.

6.6.2 Attack Tree on the Routing Formation and the Routing Table

In Fig. 13 we present how the RPL routing table or the RPL topology maintenance can be attacked. We note that they all rely on the presence of one or more malicious nodes in the network. A malicious node can disrupt the RPL DODAG formation and results in one of the attacks shown in Fig. 12, however, if the nodes communicate using the proposed solution and form secure links they can prevented.

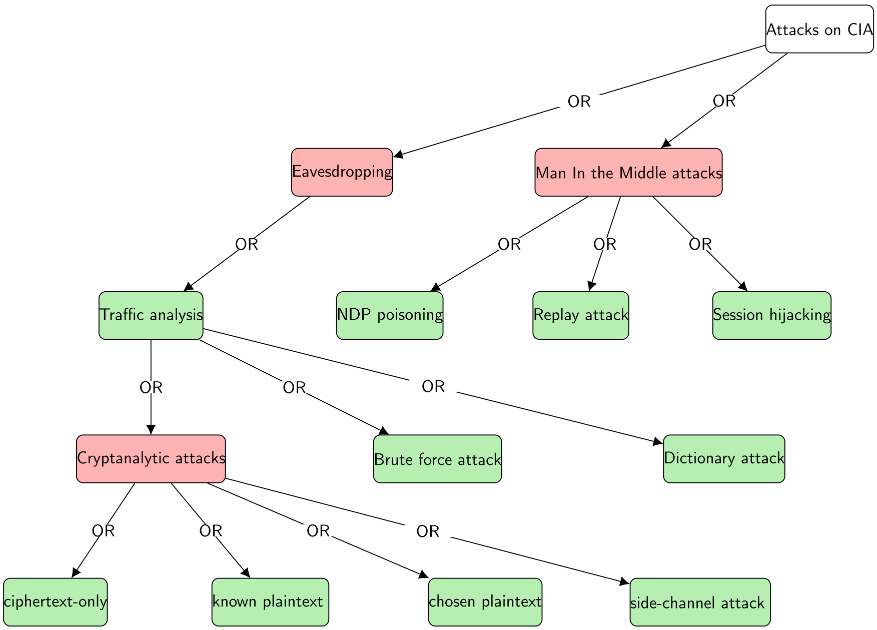


Fig. 12 Attack tree representation of all the attacks on the confidentiality, integrity and accountability that an Internet of Things network is vulnerable when all communications are sent in plain text

7 Summary

In this chapter, we defined the differences between the Wireless Sensor Networks WSN, the Distributed Sensor Networks DSN, and the Internet of Things IoT. The differences are mainly related to the link availability between nodes in the network since nodes between DSN and WSN are between each node and all its neighbours in comparison with the IoT networks where each node form a link only with one preferred neighbour based on certain variables.

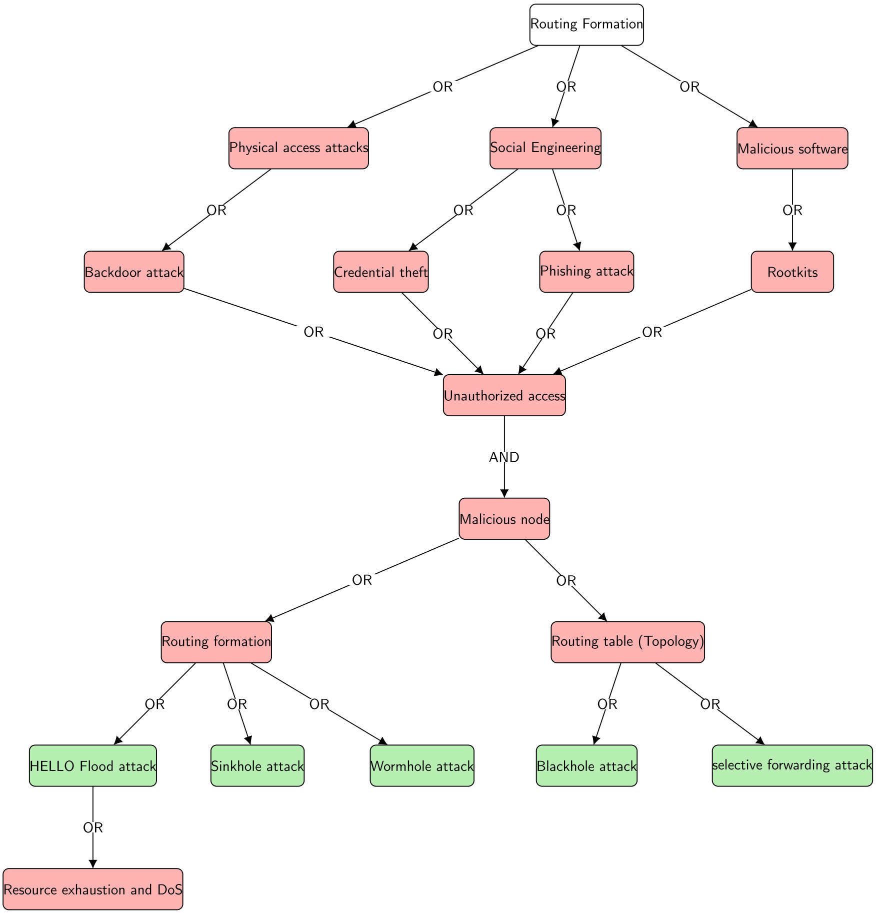


Fig. 13 Attack tree representation of all the attacks on the routing formation when all the routing control messages are sent in plain text

We introduced the IoT 6LoWPAN concept that defines how the Internet Protocol can be used in the context of the Internet of Things and researched the routing power for loss networks RPL and explained how it works and the various objective functions that can be used and the security measures that are incorporated within it.

We finally discussed the threats and vulnerabilities that IoT nodes and networks are vulnerable to and researched different key distribution schemes that are available and how each of them is used in the context of the IoT.

References

1. Eschenauer L, Gligor VD (2002) A key-management scheme for distributed sensor networks. In: Proceedings of the 9th ACM CCS. ACM, New York, USA, pp 41–47
2. Henry KJ (2015) Secure protocols for key pre-distribution, network discovery, and aggregation in wireless sensor networks
3. Mulligan G (2010) The 6LoWPAN architecture, p 78
4. IEEE Computer Society (2011) 802.15.4 low rate wireless personal area networks (LR-WPANs)
5. Siller M, Carlos-Mancilla M, López-Mellado E (2016) Wireless sensor networks formation: approaches and techniques. J Sens 2016
6. Bellavista P, Cardone G, Corradi A, Foschini L (2013) Convergence of MANET and WSN in IoT urban scenarios. IEEE Sens J 13(10):3558–3567
7. Joby PP, Sengottuvelan P (2015) A survey on threats and security schemes in wireless sensor networks
8. Makhdoom I, Abolhasan M, Lipman J, Liu RP, Ni W (2019) Anatomy of threats to the internet of things. IEEE Commun Surv Tutor 21(2):1636–1675
9. Grammatikis PIR, Sarigiannidis PG, Moscholios ID (2019) Securing the internet of things: challenges, threats and solutions. Internet Things 5:41–70
10. Borgohain T, Kumar U, Sanyal S (2015) Survey of security and privacy issues of internet of things
11. Poudel S (2016) Internet of things: underlying technologies, interoperability, and threats to privacy and security. Berkeley Technol Law J 31(2):997–1022
12. Drăgoi V, Richmond T, Bucerzan D, Legay A (2018) Survey on cryptanalysis of code-based cryptography: from theoretical to physical attacks. In: 2018 7th international conference on computers communications and control (ICCCC), pp 215–223
13. Surendran S, Nassef A, Beheshti BD (2018) A survey of cryptographic algorithms for IoT devices. In: 2018 IEEE long island systems, applications and technology conference (LISAT), pp 1–8
14. Abomhara M, Køien GM (2014) Security and privacy in the internet of things: current status and open issues. In: 2014 international conference on privacy and security in mobile systems (PRISMS), pp 1–8
15. Chen X, Makki K, Yen K, Pissinou N (2009) Sensor network security: a survey. IEEE Commun Surv Tutor 11(2):52–73
16. Bysani LK, Turuk AK (2011) A survey on selective forwarding attack in wireless sensor networks. In: 2011 international conference on devices and communications (ICDeCom), pp 1–5
17. Choudhary S, Kesswani N (2018) Detection and prevention of routing attacks in internet of things. In: 2018 17th IEEE international conference on trust, security and privacy in computing and communications/12th IEEE international conference on big data science and engineering (TrustCom/BigDataSE), pp 1537–1540
18. Raoof A, Matrawy A, Lung C (2019) Secure routing in IoT: Evaluation of RPL's secure mode under attacks. In: 2019 IEEE global communications conference (GLOBECOM), pp 1–6
19. Yang W, Wang Y, Lai Z, Wan Y, Cheng Z (2018) Security vulnerabilities and countermeasures in the RPL-based internet of things. In: 2018 international conference on cyber-enabled distributed computing and knowledge discovery (CyberC), pp 49–495
20. Wallgren L, Raza S, Voigt T (2013) Routing attacks and countermeasures in the RPL-based internet of things. Int J Distrib Sens Netw 9(8):794326
21. Mayzaud A, Badonnel R, Chrisment I (2016) A taxonomy of attacks in RPL-based internet of things. Int J Netw Secur 18(3):459–473
22. Le A, Loo J, Lasebae A, Vinel A, Chen Y, Chai M (2013) The impact of rank attack on network topology of routing protocol for low-power and lossy networks. IEEE Sens J 13(10):3685–3692

23. Rehman A, Khan MM, Lodhi MA, Hussain FB (2016) Rank attack using objective function in RPL for low power and lossy networks. In: 2016 international conference on industrial informatics and computer systems (CIICS), pp 1–5
24. Mosenia A, Jha NK (2017) A comprehensive study of security of internet-of-things. IEEE Trans Emerg Top Comput 5(4):586–602
25. Yang Y, Wu L, Yin G, Li L, Zhao H (2017) A survey on security and privacy issues in internet-of-things. IEEE Internet Things J 4(5):1250–1258
26. Nagrath P, Gupta B (2011) Wormhole attacks in wireless adhoc networks and their counter measurements: a survey. In: 2011 3rd international conference on electronics computer technology, vol 6, pp 245–250
27. Perazzo P, Vallati C, Varano D, Anastasi G, Dini G (2018) Implementation of a wormhole attack against a RPL network: challenges and effects. In: 2018 14th annual conference on wireless on-demand network systems and services (WONS), pp 95–102
28. Granjal J, Monteiro E, Sá Silva J (2015) Security for the internet of things: a survey of existing protocols and open research issues. IEEE Commun Surv Tutor 17(3):1294–1312
29. Nguyen KT, Laurent M, Oualha N (2015) Survey on secure communication protocols for the internet of things. Ad Hoc Netw 32:17–31. Internet of things security and privacy: design methods and optimization
30. Ahmed N, Sadiq A, Farooq A, Akram R (2017) Securing the neighbour discovery protocol in IPv6 stateful address auto-configuration. In: 2017 IEEE trustcom/BigDataSE/ICESS, pp 96–103
31. Ahmed ASAMS, Hassan R, Othman NE (2017) IPv6 neighbor discovery protocol specifications, threats and countermeasures: a survey. IEEE Access 5:18187–18210
32. Sudhakar, Aggarwal RK (2017) A survey on comparative analysis of tools for the detection of ARP poisoning. In: 2017 2nd international conference on telecommunication and networks (TEL-NET), pp 1–6
33. Chen B, Ho DWC, Hu G, Yu L (2018) Secure fusion estimation for bandwidth constrained cyber-physical systems under replay attacks. IEEE Trans Cybern 48(6):1862–1876
34. Hoehn A, Zhang P (2016) Detection of replay attacks in cyber-physical systems. In: 2016 American control conference (ACC), pp 290–295
35. Hu Q, Hancke GP (2017) A session hijacking attack on physical layer key generation agreement. In: 2017 IEEE international conference on industrial technology (ICIT), pp 1418–1423
36. Lu Z, Chen F, Cheng G, Li S (2017) The best defense strategy against session hijacking using security game in SDN. In: 2017 IEEE 19th international conference on high performance computing and communications; IEEE 15th international conference on smart city; IEEE 3rd international conference on data science and systems (HPCC/SmartCity/DSS), pp 419–426
37. Celebucki D, Lin MA, Graham S (2018) A security evaluation of popular internet of things protocols for manufacturers. In: 2018 IEEE international conference on consumer electronics (ICCE), pp 1–6
38. John R, Cherian JP, Kizhakkethottam JJ (2015) A survey of techniques to prevent Sybil attacks. In: 2015 international conference on soft-computing and networks security (ICSNS), pp 1–6
39. Zhang K, Liang X, Lu R, Shen X (2014) Sybil attacks and their defenses in the internet of things. IEEE Internet Things J 1(5):372–383
40. Genkin D, Valenta L, Yarom Y (2017) May the fourth be with you: a microarchitectural side channel attack on several real-world applications of curve25519. In: Proceedings of the 2017 ACM SIGSAC conference on computer and communications security, CCS'17. Association for Computing Machinery, New York, NY, USA, pp 845–858
41. Aggarwal R, Lal Das M (2012) RFID security in the context of "internet of things", pp 51–56
42. Special issue on "security and identity architecture for the future internet" (2013) Comput Netw 57(10):2215–2217
43. Ahmadi P, Islam K, Maco T, Katam M (2018) A survey on internet of things security issues and applications. In: 2018 international conference on computational science and computational intelligence (CSCI), pp 925–934

44. Miraz MH, Ali M, Excell PS, Picking R (2015) A review on internet of things (IoT), internet of everything (IoE) and internet of nano things (IoNT). In: 2015 internet technologies and applications (ITA), pp 219–224
45. Shelby Z, Bormann C (2007) 6LoWPAN: the wireless embedded internet, 1st edn. Wiley
46. Honggang Z, Chen S, Leyu Z (2018) Design and implementation of lightweight 6LoWPAN gateway based on contiki. In: 2018 IEEE international conference on signal processing, communications and computing (ICSPCC), pp 1–5
47. Kamma PK, Palla CR, Nelakuditi UR, Yarrabothu RS (2016) Design and implementation of 6LoWPAN border router. In: 2016 thirteenth international conference on wireless and optical communications networks (WOCN), pp 1–5
48. Janicijević N, Lukić M, Mezei I (2011) Routing protocol for low-power and lossy wireless sensor networks. In: 2011 19th telecommunications forum (TELFOR) proceedings of papers, pp 234–237
49. Montenegro G, Kushalnagar N et al (2007) Transmission of IPv6 packets over IEEE 802.15.4 networks. RFC 4944, Sept 2007
50. Conta A, Deering S, Gupta M (2006) Internet control message protocol (ICMPv6) for the internet protocol version 6 (IPv6) specification. RFC 4443
51. Deering SE, Hinden RM (1998) Internet protocol, version 6 (IPv6) specification. RFC 2460, Dec 1998
52. Hui J, Thubert P (2011) Compression format for IPv6 datagrams over IEEE 802.15.4-based networks. RFC 6282, Sept 2011
53. Winter T, Thubert P et al (2012) RPL: IPv6 routing protocol for low-power and lossy networks. RFC 6550, Mar 2012
54. Thubert P (2012) Objective function zero for the routing protocol for low-power and lossy networks (RPL). RFC 6552, Mar 2012
55. Vasseur JP, Kim M et al (2012) Routing metrics used for path calculation in low-power and lossy networks. RFC 6551, Mar 2012
56. Kushalnagar N, Montenegro G, Schumacher C (2007) IPv6 over low-power wireless personal area networks (6LoWPANs): overview, assumptions, problem statement, and goals. RFC 4919, Aug 2007
57. Gnawali O, Levis P (2012) The minimum rank with hysteresis objective function. RFC 6719, Sept 2012
58. Hui JW et al (2008) IP is dead, long live IP for wireless sensor networks. In: Proceedings of the 6th ACM conference SenSys. ACM, New York, USA, pp 15–28
59. Gnawali O, Levis P (2010) The ETX objective function for RPL. RFC 6719, May 2010
60. Qasem M, Al-Dubai A, Romdhani I, Ghaleb B, Gharibi W (2017) Load balancing objective function in RPL. Draft IETF
61. Qasem M, Al-Dubai A, Romdhani I, Ghaleb B, Gharibi W (2016) A new efficient objective function for routing in internet of things paradigm. In: 2016 IEEE conference on standards for communications and networking (CSCN), pp 1–6
62. Papadopoulos G, Dujovne D, Montavont N, Koutsiamanis R (2018) Traffic-aware objective function. Draft IETF
63. Ji C, Koutsiamanis R, Montavont N, Chatzimisios P, Dujovne D, Papadopoulos GZ (2018) TAOF: traffic aware objective function for RPL-based networks. In: 2018 global information infrastructure and networking symposium (GIIS), pp 1–5
64. Roman R, Lopez J (2009) Integrating wireless sensor networks and the internet: a security analysis. Internet Res 19:246–259
65. Mayzaud A, Badonnel R, Chrisment I (2016) A taxonomy of attacks in RPL-based internet of things. Int J Netw Secur 18(3):459–473
66. Tsao T, Alexander R, Dohler M, Daza V, Lozano A, Richardson M (2015) A security threat analysis for the routing protocol for low-power and lossy networks (RPLs). RFC 7416, Jan 2015
67. Housley R, Ferguson N, Whiting D (2003) Counter with CBC-MAC (CCM). RFC 3610, Sept 2003

68. Chan H, Perrig A, Song D (2004) Key distribution techniques for sensor networks. Springer US, Boston, MA, pp 277–303
69. Chan H, Perrig A, Song D (2003) Random key predistribution schemes for sensor networks. In: 2003 symposium on security and privacy, 2003, pp 197–213
70. Roman R, Zhou J, Lopez J (2013) On the features and challenges of security and privacy in distributed internet of things. Comput Netw 57(10):2266–2279
71. Raza S, Duquennoy S, Höglund J, Roedig U, Voigt T (2014) Secure communication for the internet of things—a comparison of link-layer security and IPsec for 6LoWPAN. Secur Commun Netw 7(12):2654–2668
72. Varadarajan P, Crosby G (2014) Implementing IPsec in wireless sensor networks. In: 2014 6th international conference on new technologies, mobility and security (NTMS), pp 1–5
73. Healy M, Newe T, Lewis E (2008) Analysis of hardware encryption versus software encryption on wireless sensor network motes. Springer Berlin Heidelberg, Berlin, Heidelberg, pp 3–14
74. Liu D, Ning P, Du W (2008) Group-based key pre-distribution in wireless sensor networks. ACM Trans Sens Netw (TOSN) 4(2):11–20
75. El Mouaatamid O, Lahmer M, Belkasmi M (2021) A review on key pre-distribution schemes based on combinatorial designs for internet of things security. Int J Eng Appl Phys 1(1):1–8
76. Camtepe SA, Yener B (2007) Combinatorial design of key distribution mechanisms for wireless sensor networks. IEEE/ACM Trans Netw 15(2):346–358
77. Huang Q, Cukier J, Kobayashi H, Liu B, Zhang J (2003) Fast authenticated key establishment protocols for self-organizing sensor networks. In: Proceedings of the 2nd ACM international conference on wireless sensor networks and applications, WSNA'03. Association for Computing Machinery, New York, NY, USA, pp 141–150
78. Lee J, Stinson DR (2005) Deterministic key predistribution schemes for distributed sensor networks. In: Handschuh H, Hasan MA (eds) Selected areas in cryptography. Springer Berlin Heidelberg, Berlin, Heidelberg, pp 294–307
79. Liu D, Ning P (2004) Multilevel tesla: broadcast authentication for distributed sensor networks. ACM Trans Embed Comput Syst 3(4):800–836
80. Paterson MB, Stinson DR (2011) A unified approach to combinatorial key predistribution schemes for sensor networks. Cryptology ePrint archive, report 2011/076
81. Yener B, Camtepe SA (2005) Key distribution mechanisms for wireless sensor networks: a survey. Technical report TR-05-07

Approaches and Methods for Regulation of Security Risks in 5G and 6G

Hamid Jahankhani, Stefan Kendzierskyj, and Osama Hussien

Abstract The proliferation of technology is now exponential. Developments in technology, the increase in computer power and the reduction of cost, has allowed for greater accessibility, use and implementation of this technology in all sectors and industries. The evolution of smart and autonomous technologies, such as artificial intelligence and machine learning, has enabled traditionally labour intensive data analytical tasks to be conducted, quickly and efficiently. Multiple datasets and data lakes that have been siloed, are now being utilised and interconnected. Digital twin, AI, metaverse, virtual technologies are being immersed into all sectors and more importantly merged into humans where the line between reality and virtual are seeming to be the same. However, in order to succeed utilising these amazing and emerging technologies, it means that there has to be an incredible backbone and capacity to carry data; and instantaneously delivery at high speed and securely. 5G is already in its rollout and has to achieve its objectives in order for 6G to be fully onboarded and implemented in a methodical manner. The European Commission has 5G objectives and is applying funding for strategic initiatives, such as Horizon 2020. There are huge benefits for all with 5G/6G but only if they are implemented in a manner that decreases the risk they can pose to security, privacy and trust, which are core pillars that must be maintained. Smart cities will mean the data that is being collected can be analysed and in the wrong hands it poses security risks to the data/individual/nation. With such an intertwining of technologies interacting with humans and the abundance of IoT and eIoT in smart cities, there has to be a clear governance plan in place and way to manage 5G/6G to ensure success. This chapter explains the 5G/6G background, risks, benefits and highlights the need for robust governance.

Keywords 5G · 6G · Wireless · Cyberattacks · Unmanned · Smart societies · Digital twin · Metaverse · AI · Supply chain

H. Jahankhani (✉) · S. Kendzierskyj · O. Hussien
Northumbria University London, London, UK
e-mail: Hamid.jahankhani@northumbria.ac.uk

H. Jahankhani and A. El Hajjar (eds.), *Wireless Networks*, Advanced Sciences
and Technologies for Security Applications,
https://doi.org/10.1007/978-3-031-33631-7_2

1 Introduction

It is imperative that with a foreseen utilisation and implementation of smart and automated systems within infrastructure and services, that consideration is taken to ensure the privacy and technology of these mechanisms and systems. Smart technologies, automated systems, and IoT are all dependant on data utilisation and with 5G/6G as the backbone of their functionality and being the carrier of the data. Securing both the communications mechanisms and the technologies themselves are key to their safe and secure implementation. It is also critical that such methodology, privacy and security frameworks are utilised to enable and instil trust in the use of these technologies, which whilst it will be critical in smart infrastructure, will also be pervasive in both nature and scope of use.

1.1 Fundamentals of Mobile Communication Technology

In 1983 almost all communications were wireless voice-centric, using analogue systems [1]. From 1983 until 2013 many generation type communications were introduced as follows:

- **First generation (1G)**: This was a mobile system and an integration of FM radios in analogue systems since manufacturing digital radio systems were expensive.
- **Second generation (2G)**: The former European GSM was transitioning from voice-centric wireless communication and changed into digital systems, such as EDGE, GPRS and GSM, where the code division multiple access (CDMA) system, was predominantly used in the USA with a bandwidth of 1.25 MHz.
- **Third generation (3G)**: From the end of 1990's, 3G was introduced into the market by connecting data and voice together.
- **3G to 4G migration**: Circa 2013, began a representative transgression from the internet at a lower data rate to the high-speed internet used for mobile videos and higher end multimedia. Both, LTE and WiMAX are part of fourth generation (4G) systems with a bandwidth of 20 MHz [1].

1.2 Technologies Behind the 5G and 6G Cellular Network

There are approximately six technologies that are collectively responsible for the existence and the function of the next generation network (NGN), the 5G cellular network. According to many specialists and researchers in this field, states that the innovative 5G is distinctive in three major features which shapes the technology to a positive extent, such as:

- Ability of multi-device connectivity
- Higher speeds

- Lower latency

More importantly the yearly subscription to mobile broadband systems showed a rapid increase in the number of individuals using it. In a 20-year global perspective, the number of devices connected to the internet demonstrate an exponential increase and by 2025 there will be around 75 billion internet-connected devices worldwide.

In order for the billions of IoT devices to interact with each other and with a base station as well as to respond to signals/requests faster and smoothly, it requires a faster and stable internet connection; which enables higher data rates for the purpose of information transfers. Therefore, 5G offers universal connectivity for machines, devices, and humans at various spectrum operating bands, because the goal is to develop a newly created network that can smoothly incorporate the fast growing number of devices into the new network [2].

5G Technology

5G is designed to be a cutting-edge technology and needed if the systems are to be smart enabled and undertake the range of emerging technologies. It is designed to allow long-distance coverage and stable connections as well as rapid data download and upload. As a result of 5G's wireless-based technology, the data migration enables a speed of 20 Gbps (Gigabyte per second) through wireless broadband connections, which simplifies the management of excessive data transmission via 5G.

However, the aspect of security and the overall intelligent connectivity system presents questions around social, technical and legal aspects. As a result, it is essential for the 5G/6G network to become a reliable and a well-developed technology, to assure safety against vicious cyberattacks and misuse of any kind.

One of the core parts of 5G networks is millimeter wave communication technology and offers wireless data transfer by settling for a higher bandwidth. However, the issue which arises from this technological concept is that the transmission distance of this particular wave is known to be limited to 100 m into the atmosphere, with regards to its deterioration, while the transmission is in progress. Ultimately, millimeter waves show a disadvantage in comparison to other wave types, which results in a fair transmission coverage.

The selection of frequency is essential in the sense that previous mobile technologies mainly used the lower frequency band. Therefore, 5G is expected to use higher frequencies within the frequency bands. However, higher frequencies decay faster than lower frequency and is comparatively more sensitive to signal losses.

If both, a lower frequency antenna and a higher frequency (HF) antenna were to transmit data at the same power/speed/data rate, the HF antenna would have a low area coverage, whereas lower frequency has not. As a result, users get higher data rates if the cell size is small. One essential part of 5G's architecture are small cells. Small cells are defined as *"low-power wireless access points that operate in licensed spectrum"* ([1], p. 64).

In order to serve high-dense urban locations with characteristic properties, such as number of users demanding high data rate capacities, small cells represent an alternative solution resulting in complementing the existing mobile network and densifying the network in crowded areas, such as hotspots (IZMF, n.d.). Also, Edfors et al. [3], support the general idea of deploying small cells to promote network densification, by overlooking numerous isolated base stations (BS) and achieve a non-homogeneous network architecture.

As a result, small cells are considered to satisfy the architectural requirements for the 5G cellular network. Ge et al. [4] state that in order for the 5G mobile network to be significantly reliant, the number of 5G base stations (BS) need to increase between 40 and 50 base stations per km^2, that is when Ge et al. ([4], p. 72) call 5G an "ultra-dense cellular network". Rodriguez [1] concluded that small cells offer an improvement in many applicative fields, such as in urban and rural areas and in applications for companies and homes, as well as an enrichment of provision in cellular capacity and coverage.

6G Technology

6G networks are the next generation of mobile communication technology, and will bring about significant improvements in terms of speed, capacity, and coverage, as well as a host of new capabilities such as immersive virtual and augmented reality experiences and ultra-reliable low-latency communication. But it also brings new challenges related to trust, security, and privacy. Trust is essential for ensuring the safety of the intertwined physical and digital worlds in 6G networks. Security is also crucial as the economy and society become more dependent on IT and networks. Privacy is a major concern as there is currently no way to determine when linked data becomes personally identifiable. These challenges are multidisciplinary, requiring solutions in technology, regulation, and ethics. Addressing these challenges are essential for the successful deployment and adoption of 6G networks [5]. Hence, a solid governance wide approach should be catered for both 5G and 6G.

The development of 6G technology also presents a number of technical challenges that need to be addressed in order to make it a reality. The following explains some of these key aspects of 6G technology:

Higher Frequency: One of the key aspects of 6G technology is the use of higher frequency bands, which have the potential to provide faster speeds and larger capacity. However, these higher frequency bands also present a number of challenges, including limited coverage and penetration, and the need for more sophisticated antenna and transmission technologies. Researchers are exploring a variety of solutions to these challenges, including the use of advanced antenna designs such as metamaterials and metasurfaces, as well as advanced modulation and multiplexing techniques [6].

Massive MIMO (multiple-input multiple-output): MIMO is expected to be used and involves the use of a large number of antennas at both the transmitter and receiver. This allows for the simultaneous transmission of multiple data streams, resulting in higher speeds and capacity. However, the implementation of massive MIMO presents a number of challenges, such as the need for high-precision calibration and the challenge of handling a large number of antennas [7]. Researchers are exploring a variety of solutions to these challenges, including the use of advanced algorithms and machine learning techniques [8].

Network slicing: Another key technology that is expected to be used in 6G is network slicing, which involves the virtual partitioning of the network into multiple independent logical networks, each with its own set of resources and characteristics. This allows for the customisation of the network for different types of applications and users, and enables the creation of new services and business models. However, the implementation of network slicing presents a number of challenges, such as the need for efficient resource allocation and the challenge of ensuring the security and isolation of different slices. Researchers are exploring a variety of solutions to these challenges, including the use of advanced optimisation techniques and blockchain technology [9].

Spatial multiplexing: Spatial multiplexing involves the use of multiple antennas at both the transmitter and receiver to transmit multiple data streams simultaneously. This allows for the increase of the data rate without increasing the transmission power, and is essential for applications such as URLLC (Ultra-Reliable Low Latency Communications). However, the implementation of spatial multiplexing presents a number of challenges, such as the need for accurate channel estimation [10] and the challenge of implementing the required signal processing algorithms [11]. Researchers are exploring a variety of solutions to these challenges, including the use of machine learning and deep learning algorithms [12].

Advanced error correction codes: Advanced error correction codes are essential for applications such as URLLC that require high reliability. These codes can significantly improve the reliability of the communication link by detecting and correcting errors that may occur during transmission. However, the implementation of advanced error correction codes presents a number of challenges, such as the need for low complexity and high decoding performance [13]. Researchers are exploring a variety of solutions to these challenges, including the use of advanced decoding algorithms and machine learning techniques.

Antenna design: This is essential for the successful implementation of technologies such as massive MIMO and spatial multiplexing. Researchers are exploring a variety of advanced antenna designs, including metamaterials and metasurfaces, which have the potential to significantly improve the performance of the communication system [6].

Wireless power transfer: Essential for a wide range of applications such as IoT, health monitoring, and wearable devices. Researchers are exploring a variety of wireless power transfer technologies, including near-field and far-field techniques, which have the potential to significantly improve the efficiency and convenience of wireless power transfer.

Overall, the goals and expectations for 6G technology are ambitious, and will require significant advances in a wide range of technical areas. However, if these goals can be achieved, 6G has the potential to revolutionise the way we communicate and interact with the world around us.

1.3 Strategic Directions from Government

The European Commission has been driving 5G technology opportunities since 2013 by establishing public–private partnerships. It was crucial, as to help seed research and accelerate innovation into 5G. To further assist the research initiatives, the European Commission committed public funding of €700 million through the Horizon 2020 Programme to support the initiatives and build an international plan for global 5G consensus.

In 2016, the Commission adopted a 5G action plan for the early deployment of 5G infrastructure across Europe with the idea being to launch 5G services in all EU Member States, by end of 2020 at the latest. Rolling further along on this plan, was to deploy a rapid uninterrupted 5G coverage in urban areas and along main transport paths, by 2025 [14].

According to the European Commission report, the EU has set its sights on additional targets to cover all populated areas with 5G by 2030 and is supporting the European 5G Observatory, so monitoring of the 5G Action Plan and Digital Decade strategy so that progress can be tracked, and reports created on preparatory actions taken by EU Member States.

Research and Innovation (R&I) initiatives on 6G technologies are now starting around the world, with the first products and infrastructures expected for the end of this decade and will transition from Gigabit to Terabit capacities and sub-millisecond response times. This will enable new applications such as real-time automation or extended reality sensing ('Internet of Senses), collecting data for a digital twin of the physical world. In Europe, a first set of 6G projects worth €60 million was launched under the 5G-PPP. The Hexa-X flagship is developing a first 6G system concept complemented by 8 projects investigating specific technologies for 6G.

The European Commission adopted its legislative proposal for a strategic European partnership on Smart Network and Services as a Joint Undertaking in February 2021, which entered into force on 30 November 2021. The Regulation includes a public R&I investment of €900 million over the period 2021–2027. In December, the newly created Joint Undertaking on Smart Networks and Services towards 6G, adopted its first Work Programme 2021–2022 with an earmarked public funding of approximately €240 million (European Commission). The SNS JU organised its launch event "*On the Road to 6G*" at the Mobile World Congress 2022, in Barcelona on 1 March 2022. The Joint Undertaking is coordinating research activities on 6G technology under Horizon Europe as well as 5G deployment initiatives under the Connecting Europe Facility Digital and other programmes.

It is clear that without this momentum, drive and structure to rollout 5G/6G there would be great uncertainty over utilising the emerging technologies such as digital twin, virtual, AI, etc., as those technologies rely on the bandwidth and other properties that 5G/6G offers.

1.4 Smart City Impacts and Interactions with Individuals

One of the strategic purposes of the 5G/6G mobile network is its implementation within the public and service sector, as well as in multimedia. The concept of smart cities relies heavily on the success of 5G/6G and prolific use of Internet of Things (IoT), enterprise IoT and eventually Internet of Senses, which will interact with individuals with and without their knowledge.

The general categorisation of IoT can be defined by their uses and implementations as follows:

- **Connected products**—From connected consumer-level coffeemakers to connected industrial pumps, this category enables end-to-end visibility into product-centric operations. It also promises improvements or even transformation around issues like regulatory compliance and product serviceability.
- **Connected assets**—In contrast with connected products, this category involves high-value, long-lived equipment such as aircraft and industrial machinery. Connected assets link production systems with manufacturing and maintenance processes to increase asset uptime and reduce operational and repair costs.
- **Connected fleets**—This category is all about tracking, monitoring, analysing, and maintaining any assets that move—from trucks to ships to construction equipment—wherever they appear in the network. Extracting data from mobile equipment has been difficult and expensive, so the promise here is immense.
- **Connected infrastructures**—From software networks to power grids to buildings, the majority of IoT sensors are likely to end up in connected infrastructures. This category will deliver new forms of digital operational intelligence to transformation physical systems. The goals will be to drive economic growth, improve service, and allow for more effective and efficient operations and risk mitigation.
- **Connected markets**—Markets apply to any activity that involves physical space, from retail centres to farms to cities. IoT can help cities, rural areas, and other markets to optimize use of assets and natural resources; reduce energy usage, emissions, and congestion; and improve efficiency and quality of life.
- **Connected people**—This category focuses on improving work, life, and health by linking people and communities, enabling organisations to evolve into new business models, and delivering better lifestyle experiences.

Another example of smart cities and interactions with individuals is autonomous driving, which is also a core requirement that needs to operate on the 5G network. As a result, smart cities and autonomous vehicles are connected to (massive) IoT devices, which ultimately creates the Vehicle-to-Everything (V2X) communication connection. Therefore, intelligent connectivity within cities could have a massive impact on communication overall.

City planners, public sector bodies and private entities are striving to utilise smart and automated technologies and IoT in a way to not only streamline services and maximise efficiency, but to improve the level of service to the citizen/consumer and to bring an additional convenience and ease in the delivery of services. To this end, AI is being used to bring together an analysis of captured data, that traditionally has been kept in silo, dependant on the agency or reason for the collection. The compute capabilities of AI and machine learning has enabled large amounts of collected data to not only to be unified and analysed, but look for predictable patterns and behaviours. This means that smarter, more accurate, strategic and operational decisions can be made. These capabilities also mean that data can be collected and analysed in real-time, having utilised captured historic data to train the algorithmic systems. In the construct of a smart city, an example of this would be to utilise traffic sensor information from traffic lights at junctions and intersections, to monitor the flow of traffic. The patterns learned in this instance can also govern and advise on future infrastructure improvements to the road network, or when maintenance and construction is required. Coupling this data with environmental data, pedestrian information, timetables for public transportation systems provide masses of valuable data in which resources and services can be effectively and appropriately managed. The real-time data analysis of traffic flow in a city could also help emergency services navigate through the less congested streets to minimise journey times.

Data transmission and storage are key points to control within smart cities. This of course, requires the proliferation and unification not only of the stored captured data, but also the data that is collected in real-time by IoT and smart devices. It is therefore imperative that the vulnerabilities and potential threat and attack vectors of these devices is considered before their implementation into a high impact system.

Possible attacks on an IoT infrastructure could include:

- Affecting target system behaviour by directly influencing deployed sensors to provide incorrect/faulty readings
- Create sensor impostor—Obtain IoT network access credentials and create (D)DoS attack on existing sensor to inject impostor(s)
- (D)DoS attack on sensor network to disable data collection
- Intelligence—Information collection and related analysis to observe typical patterns
- Disruptions on infrastructure—make grid elements to malfunction to cause either partial of full grid failure
- Modify water processing/ventilation to go outside of safety limits
- Get access to more secure networks/cloud through IoT infrastructure
- Modification of wearable/implanted health devices to cause bodily harm

Considerations need to be taken into the exploitation of the IoT infrastructure itself, whereby unsecured devices could be infected to form a BotNet, used to attack other remote systems, and to great effect, given the number of potential susceptible hosts on an IoT network. Also, individuals' data could be seriously compromised in both a malicious and passive way. Malicious threats are clearly understood but passive collation of data is more of an unknown impact. If we think of a smart city and how much data is being collated in the background on individuals. It raises all sorts of questions on who has access to the data, if it is passed onto third parties, and so on.

1.5 Ethics and Regulations

With the official introduction of 5G in 2020, ethical aspects need a predefined review with regards to user safety and public privacy. Furthermore, regulative agreements between government, network providers and public users are needed and shape and manage the overall degree of safety and security. IEEE's [15] globally developed standards and use cases covers areas that are being monitored within 5G, for instance enabling smart cities and the Internet-of-Things, interoperability of technology as well as autonomous driving, which are connected to the internet. IEEE ([15], p. 1) also addresses potential issues, such as:

- Convergence of fixed, mobile, and broadcast services
- Multi-tenancy models
- Sustainability, scalability, security, and privacy management
- Spectrum
- Software enablement for software-defined networking (SDN), network function virtualization (NFV), mobile edge, fog computing, and virtualization.

In a report of GSMA ([16], p. 4) the term "intelligent connectivity" is what is known as the potentially rising combination of 5G, IoT, smart landscapes and Artificial Intelligence (AI). Particularly, the ethics behind the junction of 5G and AI is of interest. Seeburn [17] highlights the positive and rising features of 5G as fast, reliable and providing a proficient quality of service, which itself shifts technology through a transformation process in a sense that the handling of internet seems to be changing. On the other hand, Seeburn [17] acknowledges the importance of finding an efficient solution for enclosing AI and 5G together. Also, recognizing that AI is intended to operate systems and machines with comparative human intelligence, while being reliable and faster because systems executing tasks and analysing data are trained to eventually perform autonomously whilst acting cost-efficient. Merging speed, dependability and human-like intelligence levels, while factoring the technical aspect, rises both safety and ethical concerns [17].

However, the Internet of Things as well as AI are exposed to significant penetration attacks. Especially with the migration from current 4G/LTE-network to the 5G, the threat impact and its probability increases.

2 The Age of Digital Transformation Moving to 5G/6G

The age of digital transformation has urged the adoption of 5G/6G networks, for the demand and significant advancements in connectivity, speed, and capacity; enabling new use cases and further driving digital transformation. In the context of 5G/6G, digital leaders will also need to understand the implications and potential of these technologies, and how to leverage them to drive business value and stay competitive. Organisations can ensure that their digital transformation efforts are aligned by staying informed about the latest technological developments and trends, conducting regular technology assessments, investing in research and development, building strong partnerships with technology providers and industry experts, and encouraging a culture of innovation and experimentation within the organisation. It can also be said that the digital transformation needs to have certain key elements in order to be successful such as:

- Clear and well-defined strategies
- Strong leadership and alignment
- Effectively manage and analyse data
- Adapt to changing market conditions and consumer expectations
- Focus on continuous improvement and innovation
- Ethical and societal implications of digital transformation enabled by 5G and 6G.

The current state of digital transformation is characterised by the widespread adoption of digital technologies across various industries and the IT belief across the world [18]. This has led to a significant increase in the amount of data being generated and used, as well as the development of new business models and the automation of many processes. So, it can be said that the adoption of 5G/6G technology is expected to play a key role in driving the next phase of digital transformation by enabling new use cases and technologies, and further increasing the speed, reliability, and capacity of communications networks. The next phase of digital transformation contain several key factors (Fig. 1) that contribute to its development and realisation [19], that businesses need to achieve and enhance, while coping with the transformation procedure in order for it to be efficient as well as produce favourable results.

These requirements include adoption of new technologies such as:

- Cloud computing
- Big data analytics
- Artificial intelligence
- Quantum computing.

These technologies are driving digital transformation by enabling organisations to process and analyse large amounts of data, automate processes, and improve decision making. A key factor in the digital transformation is the current business pressures as the increasing competition and changing market conditions are driving organisations to adopt digital technologies to improve efficiency, reduce costs, and gain a

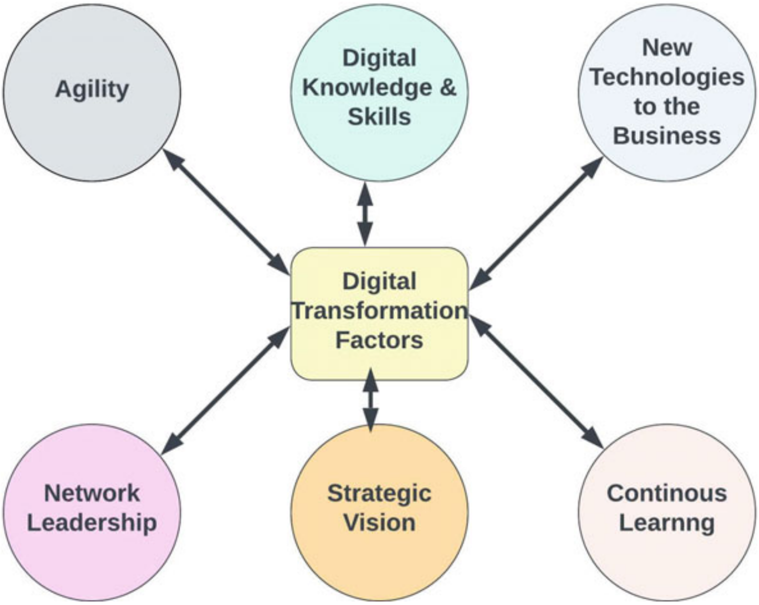

Agility
Digital Knowledge & Skills
New Technologies to the Business
Digital Transformation Factors
Network Leadership
Strategic Vision
Continous Learnng

Fig. 1 Key factors for digital transformation

competitive advantage; which in turn serves the consumer expectations for personalised, convenient, and always-on experiences. 6G networks enable organisations to support new business models and services, such as edge computing, which can help them to increase efficiency, reduce costs, and gain a competitive advantage which also enable organisations and businesses to provide faster, more reliable, and more personalised experiences for consumers. Another factor which plays a huge part in the digital transformation is the new and ongoing government regulations and policies [20]. Particularly in industries such as healthcare, finance, and energy, where there are stringent regulations around data privacy and security such as GDPR (EU, 2016).

2.1 Digital Identity and Emerging Technologies Relationship with Data Protection of Societies

Digital identity (DID), Self-sovereign identity (SSI), digital twin, blockchain and AI are all technologies that have the potential to play a significant role in protecting privacy and data in societies and below are explanations of these main technologies.

Digital identity (DID): DID refers to the unique digital representation of an individual, which is used to verify the identity of a person and grant them access to various online services. Digital identities are becoming increasingly important as more and more of our daily interactions take place online, and when combined with Self-sovereign Identity (SSI), which is an approach to digital identity that gives individuals control over their own personal data. Individuals can choose which personal information to share with others and who can access it and is seen as a way to empower individuals and give them more control over their personal data [21]. It can be used to protect privacy by ensuring that only authorised individuals have access to sensitive information (Ferdous et al. 2019).

Digital twin (DT): DT is a digital replica of a physical object or system. Digital twin can be used to model the behaviour of physical systems, such as buildings or power grids, in order to optimise their performance. In the context of privacy and data protection, digital twins can be used to analyse and protect sensitive information without exposing the actual data [22].

Blockchain technology: Blockchain is a distributed ledger system that uses cryptography to secure transactions. Blockchain can be used to create a tamper-proof record of digital transactions [23], making it useful for protecting sensitive information. Blockchain can also be used to create a secure and decentralized digital identity system [24].

Artificial intelligence (AI): AI can be used to analyse large amounts of data and identify patterns that can be used to improve privacy and data protection.

Monitoring manufacturing structure, assuring routine maintenance, and creating effective items and services are all made possible by digital twins and blockchains. They can aid in the quick and effective resolution of operational problems since they are based on dispersed network infrastructures. Nevertheless, without sufficient security, the data they contain may be susceptible to theft or misuse, possibly disclosing private company data. These technologies are anticipated to take over some occupations currently performed by people, and might have devastating impacts on some industries.

For decision-making operations, maintaining data integrity is essential, hence strict security measures are required to safeguard DTs and uphold public confidence in their usage. Although blockchains might possess the ability to improve security, there are still issues with implementation that need to be resolved [25].

AI can be used to detect and prevent data breaches, and to monitor and analyse the behaviour of individuals and systems to identify potential threats such as in SIEM and SOAR tools. AI can also be used to create personalised privacy settings and make recommendations to individuals about how to protect their personal data [26]. By giving individuals control over their own personal data, analysing and protecting sensitive information without exposing the actual data, creating tamper-proof records of digital transactions, creating a secure and decentralized digital identity system and using AI to detect and prevent data breaches, these technologies can help protect the privacy.

2.2 Current Infrastructure Weakness and Cyberattack Manipulations

When using technologies of different kinds, for instance, mobile phones, laptops, or IP-based/public networks, there is always a danger of personal data being unprotected due to a lack of proper network security and increased attack surface with the abundance of IoT devices. To add to this risk, 5G's technological specification includes the coverage of 3G and 4G/LTE. Therefore, a vast number of risk components mark critical security challenges for the 5G network.

Power supply depicts a crucial point when assessing risks, the 5G network has on users and the security structure of a nation. Ahmad [27] mentioned the tremendous criticality a collapse of wired power supply systems might have on affecting systems within the network chain, such as data handling and electrical systems, which are integrated into society and were occurred by a security breach.

With consideration of existing mobile communication networks and their specific technical protocols, for instance, HSPDA/HSPA+, GSM and LTE, individuals were gradually introduced to the power and the ability of today's technology. Telecommunication providers are eager to provide profitable services designed around maintaining customers privacy by also fulfilling information security requirements when offering Voice-IP (VoIP), national and international services, such as PABX, call and messaging services as well as roaming [28]. Therefore, the Internet of Things is exposed to a number of security threats and vulnerabilities. Ahmad et al. ([27], p. 2) point out a number of major security issues:

i. **Flash network traffic**: High number of end-user devices and new things (IoT).
ii. **Security of radio interfaces**: Radio interface encryption keys sent over insecure channels.
iii. **User plane integrity**: No cryptographic integrity protection for the user data plane.
iv. **Mandated security in the network**: Service-driven constraints on the security architecture leading to the optional use of security measures.
v. **Roaming security**: User-security parameters are not updated with roaming from one operator network to another, leading to security compromises with roaming.
vi. **Denial of Service (DoS)** attacks on the infrastructure: Visible nature of network control elements, and unencrypted control channels.
vii. **Signalling storms**: Distributed control systems requiring coordination, e.g. Non-Access Stratum (NAS) layer of Third Generation Partnership Project (3GPP) protocols.
viii. **DoS attacks on end-user devices**: No security measures for operating systems, applications, and configuration data on user devices.

One of the most significant weaknesses of current infrastructure is the lack of proper security measures in place. Many organisations fail to implement basic security measures, such as firewalls, intrusion detection and prevention systems, and encryption. This leaves them vulnerable to attacks that exploit known vulnerabilities in their systems. For example, in 2017, the WannaCry ransomware attack affected more than 200,000 computers in 150 countries [29], exploiting a vulnerability in older versions of the Microsoft Windows operating system. This attack caused widespread disruption to businesses and organisations, highlighting the importance of keeping systems updated and patched to prevent known vulnerabilities from being exploited.

Another weakness is the use of outdated software. Many organisations continue to use older versions of software, such as operating systems and applications, that are no longer supported by their vendors. This makes it easier for hackers to exploit known vulnerabilities in these systems, as vendors typically release security updates and patches for the latest versions of their products. An example of this is the Equifax data breach in 2017 where hackers exploited a known vulnerability in an older version of the Apache Struts web application framework. This breach resulted in the personal information of over 143 million individuals being compromised [30].

The widespread use of mobile devices and cloud computing has also created new opportunities for hackers. These technologies have made it easier for hackers to gain access to sensitive information and disrupt operations. For example, a hacker could use a malware-infected mobile device to gain access to a company's network or they could use a cloud-based service to launch a distributed denial-of-service (DDoS) attack. In 2016, a DDoS attack on DNS provider Dyn used a botnet of Internet of Things (IoT) devices, such as security cameras and routers, to flood the company's servers with traffic, resulting in a widespread internet disruption.

Another example of a weakness in current infrastructure is the lack of security on the Internet of Things (IoT) devices. Many IoT devices are designed with little to no security built-in, making them easy targets for attackers. In 2018, a vulnerability in a popular IoT device, the Nest Cam, was discovered, allowing an attacker to gain access to the device's live video feed and microphone [31]. This highlights the need for manufacturers to prioritise security when designing IoT devices.

One of the main reasons why many organisations have weak infrastructure is due to a lack of investment in security and this is due to a lack of understanding of the importance of security.

The implications of weak infrastructure can be severe, including:

- Financial losses
- Damage to reputation
- Legal and regulatory penalties.

Many organisations prioritise cost-saving measures over security, and as a result, they may not allocate sufficient resources to implement and maintain robust security measures. It can lead to outdated software and hardware, which are vulnerable to known security risks and exploits. One example of this is the Target data breach in 2013, where hackers were able to gain access to the company's network by exploiting a weakness in the security of a third-party vendor. This breach resulted in the theft of 40 million credit and debit card numbers and the personal information of 70 million individuals. Target was later found to have not implemented basic security measures, such as network segmentation, and had not adequately monitored network activity [32]. This incident resulted in significant financial losses for the company and damage to its reputation.

Another example is the Sony Pictures hack in 2014, where hackers gained access to the company's network and stole a large amount of sensitive data, including personal information of employees and confidential information about upcoming films [33]. This hack resulted in significant financial losses for the company and damage to its reputation. In addition to these tangible consequences, weak security can also lead to a loss of trust from customers, partners, and other stakeholders. Organisations must take steps to address these weaknesses by implementing security measures and updating their systems to the latest versions to minimize their exposure to cyber-attacks. This includes keeping software updated and patched, implementing firewalls and intrusion detection systems, and ensuring that all devices connected to the network, including IoT devices, are secure.

New network architectures and other use cases establish fundamental concerns for 5G's security. So called "new cloud virtualization technologies such as software-defined networking (SDN) and network functions virtualization (NFV) are thought to create loopholes for vulnerabilities, which undermine the overall security of the 5G network although these network architectures excel flexibility, programmability and openness. SD × Central [34] goes further by demonstrating system downfalls due to the misuse of management interfaces of an SDN partition to attack either the overall management system or the SDN controller, which ultimately results in a security breach.

In contrary, SDN networks mainly focus on the separation of control plane from data plane by centralising control instead of standardising network protocols, whereas NFV networks focus on the replacement of certain network functions with software by using cloud computing services [35], which show a significant potential to mitigate CAPEX and OPEX, known as Capital and Operational Expenditures [27]. Lowering these expenditures show a positive benefit in the heterogeneity of 5G services, such as its functionalities and architecture because flexibility of the 5G network is, amongst other things, a key component of the divergent requirements of 5G driven applications [36].

Furthermore, the deployment of cloud services is purely based on network preferences [37]. Efficiency is an advantage feature of cloud computing because it does not own physical infrastructure for the maintenance of services, data and application ran by operators [27].

2.3 Data Privacy and Security Challenges

Data privacy and security are of paramount importance in today's digital age. With the increasing amount of personal and sensitive information being collected, stored, and shared online, organisations and individuals must take steps to protect this data from potential breaches, misuse, and lack of regulation.

One of the significant features of 5G to consider, are data handling and storing solutions. Huawei [37] points out that *'security'* as such, remains an indispensable factor for business continuity. Furthermore, Huawei [37] suggests the consideration of applying privacy and security properties from former generations of mobile network to the upcoming mobile networks, so that business continuity can be provided. By enormously mitigating the impact of security breaches and understanding the influence that risk factors have, business continuity can be subject to audit through consistent safeguarding [38].

There are essential parts of the 5G network that could lead to a higher probability of network vulnerability. Even the current network (4G/LTE) and also 5G, consist of different properties catering to different services. IoT can create exposure to numerous vulnerabilities because the technological structure exhibits potential weak spots, although it was developed based on core objectives, such as reliable network connection. Miller [39] categorically classifies "Theft", "Privacy", "Safety" as well as "Productivity" as the most significant attack types and ultimate risk factors for IoT landscapes (system, network, infrastructure). With the 5G network adding function and enhancement to the reliability and availability of faster wireless service to applications, appliances and other 5G driven technologies, the security issue gains importance and further highlight to 5G.

Although, 5G will be capable to cover high numbers of devices, machines and other appliances, the amount of data retrieved and processed will increase enormously.

That is when the confidentiality of vulnerable information may get violated and the risk for users may be immense. As Miller [39] explains, the risk of being affected of theft is especially high with the use of autonomous vehicles because hackers can get access to the vehicle's remote keyless entry system but the possibility of unauthorized access to homes are almost as high.

Huawei [37] explained that the 4G network provides an insufficient trust model because it already covers an established and bidirectional trust-relationship between *"Users"* and a *"Network",* but it does not exhibit a link between *"Users"* and the specific *"Service"* technologies (in this case the 4G mobile network) must provide (see Fig. 2).

This view is also supported by Blum et al. [40] who states that critical tasks, such as security issues arising from the verification process of computer-based systems, diminishes other arrays of problems, for instance, the reliability of a computer-based technology as well as its usability.

With the introduction of the 5G network technology into the mobile communication market there is a mutual but distinct expectation of trust on both the public and private side. Fogg and Tseng [41] state that the usability of technology is a crucial factor of trust by which a user's degree of trust is measured by. Moreover, Blum et al. [40] describe 'Trust' as an accumulation of key elements of trust, which comprise factors, such as availability, reliability and privacy, into the definition of trust with regards to the field of technology.

One of the major challenges in data privacy and security is the prevalence of data breaches. Cybercriminals are constantly devising new methods to gain unauthorised

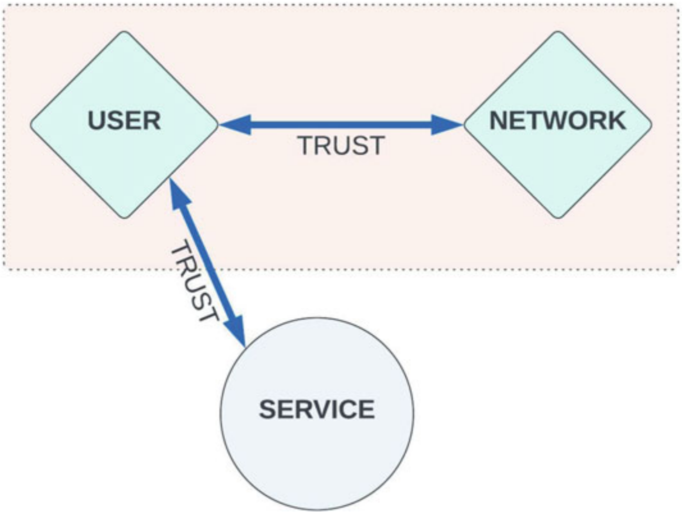


Fig. 2 Trust model of the 4G network

access to sensitive information, such as through phishing scams, malware, and other malicious techniques, according to [42]. Phishing attacks accounted for 83% of all of the attacks against business organisations and 87% for charities organisation, followed by impersonation attacks (27% and 26% respectively) and viruses and malwares (12 and 11%), and according to the same survey, there is a huge number of micro and small to medium organisation affected with data breaches in compared to large organisations, this may be the fact due to the less security measures and controls and security mentality over this organisations and businesses. These breaches can have severe consequences, including financial loss, reputational damage, and loss of trust from customers. For example, the high-profile data breaches of companies like Yahoo (NCSC, 2016) and Marriott, [42] have resulted in the compromise of millions of customers' personal information.

Another major challenge is data misuse. Even when data is not stolen, it can still be misused by companies, governments, and other organisations. This can include using personal information for targeted advertising, or sharing data with third parties without proper consent. This not only violates individuals' privacy rights but can also cause harm to the individuals in case of sensitive information. One example of this is the Cambridge Analytica scandal, in which the personal data of millions of Facebook users was harvested without their consent and used for political advertising [43]. This data can be used later for many reasons including identity thefts, which has become one of the fastest growing crimes [44]. Most people are unaware of the amount of data they disclose over the Internet. This data can be easily aggregated, data-mined and linked together.

Another challenge is the lack of regulation for data privacy and security. In many countries, there are few laws in place to protect personal data, and even where regulations do exist, they can be difficult to enforce [45]. This lack of accountability can make it easier for organisations to mishandle personal data. For example, the General Data Protection Regulation (GDPR) which was implemented in the European Union in 2018, provides strict guidelines for organisations handling EU citizens' personal data but still, there are many organisations which are not compliant with it.

Inadequate security measures are another challenge faced by organisations. Many organisations do not have the proper security measures in place to protect personal data, such as encryption or strong password policies. With the increasing use of new technologies like NFC, 5G, and the proliferation of devices, it is crucial that organisations keep their security measures up-to-date and adapt to the new challenges. For instance, with the integration of 5G networks, there will be an increase in the amount of data that can be transmitted, and the number of devices that can be connected, which will open up new attack surfaces for cybercriminals. The use of wireless networks and devices also present significant cybersecurity risks. As the number of connected devices increases, the surface area for potential security breaches expands. It is crucial that cybersecurity measures are integrated at all stages of the development and deployment of these technologies to mitigate the potential risks.

There needs to be a multifaceted approach involving both individuals and organisations. Individuals must take responsibility for protecting their personal information online by being cautious when sharing personal information online, using strong passwords, and keeping their software and devices updated. Organisations must also take necessary measures to protect personal data, including implementing robust security measures, ensuring compliance with regulations, and promoting a culture of data privacy and security.

3 Governance and Adopting Methodologies for Managing Standardisation and Interoperability

The emergence of 6G networks is set to revolutionise the way we communicate and interact with technology. With ultra-low latency and high data rate communication, 6G networks will enable new use cases and applications, such as the deployment of autonomous vehicles, intelligent transportation systems, and the internet of things at a massive scale, as well as support for advanced artificial intelligence and machine learning applications. This level of technological advancements, however, also brings new challenges, especially in terms of information governance.

Information governance (IG), as defined by the International Association for Information Governance Professionals (IAIGP), is the processes and standards that ensure the availability, integrity, and security of the data an organisation relies on to achieve its goals. It involves a wide range of issues such as security, privacy, data sharing, and regulatory compliance. As 6G networks will generate, transmit, and store a tremendous amount of data, it is crucial to have a well-defined governance framework in place to ensure the protection and safe management of this data. However, standardising IG for 6G networks poses several challenges, such as the fast-changing technology and the need for flexible standardisation approach. Additionally, there is a lack of international standards or best practices for information governance in 6G networks.

As the world becomes increasingly dependent on technology and mobile networks, the next generation of wireless communication, 6G, is being developed to address the needs of an increasingly connected society. However, the development and deployment of 6G also raises a number of governance challenges related to spectrum allocation, network security and privacy, international coordination, and the impact of emerging technologies such as artificial intelligence and the Internet of Things.

Spectrum allocation is a critical component of wireless communication and will be even more crucial for 6G networks. 6G networks will require new spectrum bands that have not been used for mobile communication before, and this will require new governance models for spectrum management. Dynamic and flexible spectrum access is also needed in 6G networks to ensure that the available spectrum is used in an efficient way.

Network security and privacy are also key considerations for 6G. With the vast amount of data generated, transmitted and stored by 6G networks, it is crucial to have robust security and privacy measures in place. 6G networks must be designed to protect sensitive information and prevent unauthorised access to the network. The governance of 6G networks must also consider the potential impact of emerging technologies such as artificial intelligence and the Internet of Things on security and privacy. International coordination is also essential for the governance of 6G. With 6G networks spanning borders, it is important to have international agreements in place to ensure that different countries' networks can interoperate. This will require cooperation between governments, the private sector, and academia.

3.1 Enabling Secure and Resilient Societies

Enabling secure and resilient societies is a critical goal for governments, organisations, and individuals around the world. The ability to protect citizens and infrastructure from natural disasters, cyberattacks, and other forms of disruption is essential for maintaining social and economic stability. In recent years, the frequency and severity of these types of incidents have increased, highlighting the need for effective and comprehensive strategies for building secure and resilient societies. One key aspect of building secure and resilient societies is the use of technology. Advanced sensors, communication systems, and analytical tools can provide early warning of potential threats and help decision-makers respond quickly and effectively.

For example, predictive analytics can be used to identify patterns of behaviour that may indicate an imminent cyberattack when coupled with artificial intelligence (AI), while advanced communication systems can enable rapid response and recovery in the event of a natural disaster. A research conducted by Masombuka et al. [46] highlight *'The Application of AI'* techniques to constantly guard the network and discuss the necessity to employ novel strategies, for instance the use of versatile, adaptive, growing, and analysis-driven AI technologies.

The worldwide industrial operations of today have more demanding needs than ever. The appropriate components for incident management choices and operations virtualisation appears to be a sensor-packed production system that ensures that every procedure or equipment component renders events and the monitoring is accessible. Also, the use of technology in building secure and resilient societies by using Internet of Things (IoT) devices. These devices can be used to monitor critical infrastructure, such as power grids, water systems, and transportation networks, and to provide early warning of potential failures or disruptions. Additionally, IoT devices can be used to track the location of emergency responders and other personnel, allowing them to coordinate their efforts more effectively. Which can be incorporated into the next industrial revolution for the cyber-physical systems [47].

Blockchain technology is another example being used to enable secure and resilient societies. It is a decentralized, distributed ledger that can be used to record transactions and other data in a way that is secure, transparent, and tamper-proof. This makes it an ideal technology for a variety of applications related to security and resilience, such as supply chain management, digital identity verification, and emergency response coordination.

Citizen engagement is another important aspect of building secure and resilient societies. This can involve educating the public about potential threats and how to prepare for them, as well as encouraging active participation in emergency management and recovery efforts. Community-based organisations, for example, can play a vital role in helping to mobilize and coordinate local response efforts [48]. Citizen science is an example of this method of scientific research. It involves the participation of citizens, who can help to collect data, report observations, and provide insights about potential hazards and vulnerabilities. Citizens can use mobile apps to report information about flood-prone areas, bushfires, or other hazards, which can help to improve the accuracy of flood and fire maps and support emergency management efforts [48].

While technology and community engagement are both important, they must be balanced with the need to maintain civil liberties and protect privacy. Governments must be transparent about the data they collect and how it is used, and they must also take steps to protect citizens from overreach and abuse of power. This can include implementing strict data protection and privacy regulations, as well as creating oversight mechanisms to ensure that these regulations are being followed.

Overall, building secure and resilient societies is a complex and ongoing process that requires the cooperation of governments, organisations, and individuals. While technology and community engagement can play a critical role, it is ultimately up to humans to manage and control these efforts to ensure that they are effective and ethical. This includes implementing effective governance, risk management, and incident response frameworks, as well as ensuring that the needs and perspectives of all stakeholders are considered. When it comes to building secure and resilient societies, there are a number of technical standards and guidelines that organisations and governments can follow to ensure that their efforts are effective and aligned with industry best practices.

One widely used standard for information security is ISO/IEC 27,001 as it provides a framework for implementing, maintaining, and continually improving an information security management system (ISMS). It covers all aspects of information security, including the management of risks, incident management, and compliance with legal and regulatory requirements. Organisations can use this standard as a guide for developing their own information security policies and procedures, and can also seek certification to demonstrate their compliance with the standard [49].

Another important standard for building secure and resilient societies is the National Institute of Standards and Technology's (NIST) Cybersecurity Framework (CSF). This framework provides a flexible and adaptive approach for managing cybersecurity risks, and it is widely adopted by organisations in both the public and private sectors. The CSF includes a set of best practices for identifying and assessing cybersecurity risks, protecting against threats, detecting and responding to incidents, and recovering from disruptions [50] (Fig. 3).

For disaster recovery and business continuity, organisations can refer to standards such as ISO 22301 and BS 25,999. These standards provide guidelines for developing and implementing effective continuity management plans, including risk assessments, incident response procedures, and recovery strategies [51, 52].

3.2 Disaster Resilience and Managing the Risks

The rise of cyber threats has become a major concern for organisations, as cyber security incidents can cause severe damage to an organisation's reputation, financial losses, and even loss of lives. Disaster resilience refers to the ability of organisations to prepare for, withstand, and recover from the impacts of disasters and security incidents. The implementation of risk management frameworks, incident response plans, and early warning systems can be effective in improving disaster resilience and reducing the impact of cyber security incidents.

It was revealed that the current state of cyber security in relation to disaster resilience is a matter of concern, as cyber threats have become more sophisticated and frequent [53]. The results from different surveys conducted revealed that many organisations are not adequately prepared to handle cyber security incidents [54]. In addition, there is a shortage of skilled individuals in the cyber security fields in Europe and due to the severe scarcity of experienced security specialists, which has been observed, the industry has been struggling to keep up with demand, which has been growing over the last few years as a result of the culture's extensive digitalisation [55].

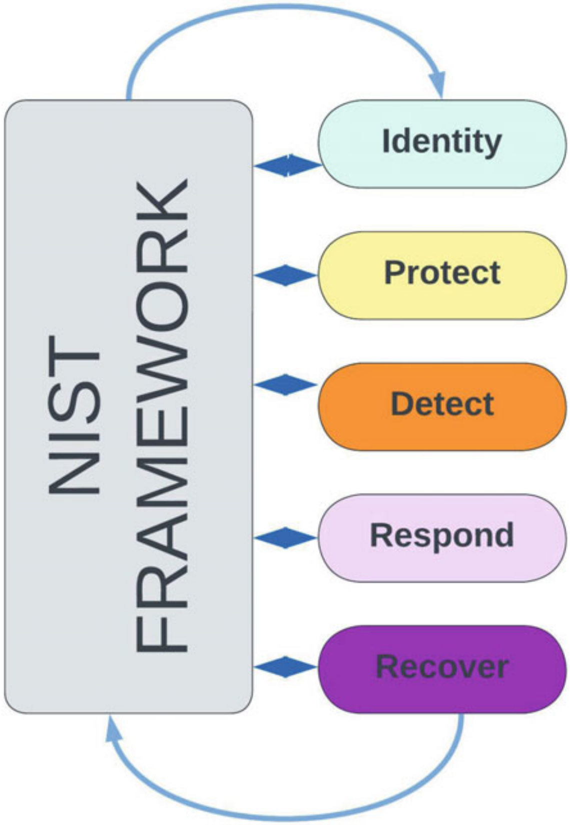


Fig. 3 NIST Framework—key factors

It can be concluded that the risk assessment and mitigation strategies such as the use of risk management frameworks, incident response plans and early warning systems are crucial for ensuring disaster resilience, and universities should focus on ensuring that they produce more experienced individuals who are ready to take on the job market in the Cyber Security Field and fill the current shortages.

The importance of incident response plans and risk management frameworks in improving disaster resilience is emphasized by many researchers [56, 57], as well as the need for organisations to regularly test and update their incident response plans to ensure that they are effective in the event of a cyber security incident [58, 58].

The EU has made significant progress in improving its readiness against cyber threats and has established a comprehensive framework for cyber security, which includes legislation, policies, and initiatives aimed at improving the EU's cyber security posture. The EU's cyber security strategy, which was updated in 2020, sets out a clear vision for the EU's cyber security efforts and provides a framework for the EU's cyber security initiatives. The EU's cyber security agency, ENISA, plays an important role in supporting the EU's cyber security efforts, and has been instrumental in the development of the EU's cyber security framework.

4 Strengthening Trust in Complex Private and Public Supply Chains

The growing intricacy of supply chains, be it private or public, has made it challenging for organisations to gain the confidence of their customers, vendors, and other stakeholders. To overcome this challenge, companies should adopt a multifaceted approach that includes increased oversight, responsibility, transparency, robust partnerships, and a proactive approach to addressing societal issues. By implementing technologies like RFID, GPS tracking, and blockchain, companies can achieve real-time tracking of goods, evaluation of suppliers' performance and identification of potential risks. Independent verifications such as certifications and third-party audits can assure compliance with established standards, laws and regulations. Building strong relationships through regular communication and sharing of information can help identify and mitigate supply chain risks. Furthermore, addressing societal concerns such as fair labour practices, environmental sustainability and ethical business behaviour can help companies to build trust with stakeholders who are increasingly concerned about the impact of business on society.

Researchers contend that businesses may not always detect and prioritise these risks appropriately, leaving them unprepared for dangers with low likelihood but significant consequences. Trust and maintaining credibility is another factor that businesses may struggle to display. One way to tackle the issue of establishing trust in complex dependencies on public and private service providers and supply chains is through increased transparency. This can be achieved by implementing systems that provide real-time visibility into supply chain activities. For example, using technologies like RFID (Radio-Frequency Identification) tags, GPS tracking, and blockchain can help companies track the movement of goods, monitor supplier performance, and detect potential risks in their supply chains. This real-time visibility can help companies to quickly identify and respond to issues as they arise, which can help to build trust with customers, suppliers, and other stakeholders. The adoption of blockchain in supply chains is still in its early stages, as there are several technical, regulatory, and new organisational challenges that need to be overcome. These challenges include scalability, interoperability, data privacy, and regulatory compliance (looking at different geographical jurisdictions). A successful implementation of blockchain requires a collaborative approach involving all stakeholders in the supply chain, including suppliers, manufacturers, logistics providers, and customers [60].

Proactivity identifying and addressing societal issues such as labour rights, environmental sustainability, and ethical business practices is also a key aspect of building trust in the complex private and public supply chains. Companies can create and implement policies, procedures, and standards to ensure that their suppliers adhere to such societal issues. In January 2012, the California Transparency in Supply Chains Act (Senate Bill 657) (CTSCA) was enacted. The CTSCA requires that retailers and manufacturers doing business in California, with annual worldwide gross receipts of $100 million or more, must explicitly disclose their efforts to eradicate slavery and human trafficking. Companies have moved quickly to update their auditing mechanisms to ensure all supplier factories meet the requirements of the Act [61].

Cybersecurity is also a critical aspect that must be considered when strengthening trust in complex private and public supply chains, it can be said that cybersecurity in logistics and supply chain management is a growing area of concern [62]. With the increasing use of technology and digital systems in supply chain management, there is a growing risk of cyberattacks that can compromise the integrity and security of sensitive information and disrupt supply chain operations. There are many activities organisations should do to mitigate these risks and all fall into the information governance and how that is managed across all the stakeholders. Another type of model suggested is to build trust within the supply chain through a cyber security maturity model (CSMM) and combine the model with blockchain. The framework assists in an end-to-end supply chain that ensures all those that sign up to the supply chain follow the CSMM framework requirements and utilises some form of industry methodology (e.g. CMMi, ITiL, etc.) to ensure monitoring, training, compliance, etc., are adhered to on an ongoing basis. Blockchain can then be the mechanism to enhance security that allows tracking from origin all the way through the supply chain, from raw materials, manufacturing/distribution; using smart contracts, to offset criminality, counterfeiting, falsification and tampering [63].

With the importance that 5G/6G brings to both organisations and individuals it is imperative that societal and ethical impacts are taken into consideration especially as these technologies continue to advance. It will become even more crucial to ensure that they are secure, and that sensitive data is protected. Additionally, it is essential to establish transparency and trust in the decision-making processes of these systems and that they are aligned with societal issues. Organisations will need to continue to implement robust cybersecurity measures, build strong partnerships, and address societal issues in order to establish trust and ensure the success and sustainability of their operations.

5 Conclusion

Since the introduction of mobile/wireless communications, internet, devices and IoT, the need for 5G/6G adoption and its roll-out in a safe and secure manner, is becoming increasingly important. Humans are now experiencing very high levels of interaction with technology that has not been seen before and it is only set to increase and be further connected; in a way that presents more humanoid interconnected interactions. Both organisations and individuals know that data is extremely important and safeguarding it needs to have very disciplined controls and governance that has the monitoring and checks that would be expected. Whilst the use of AI, digital twin, virtual reality and other tools are there to assist and support analysing these huge data sets, they also have the capacity to allow data to fall into the wrong hands or be passed onto third parties that may make prejudgements on individuals without their knowledge. It can be further complicated with recent acceleration of satellite communications, technologies and its interaction with all other traditional systems (of which 5G/^G will be part of). What was once more military/government controlled launching of satellites into high earth orbit (HEO) is now experiencing thousands of satellites being launched by commercial companies into low earth orbit (LEO). That raises very concerning questions on how these will interact with 6G networks, and where the data will be located. If we consider what governance method is being applied here, and presents a rather large question mark on where the control, access, monitoring and security responsibilities lie.

Clearly the acceleration of emerging technologies is needed as to help support humans living now and in the future, with increasing population size and diminishing resources. We will need these 'smart' technologies and its computational power. But what is also needed is that sense of traditional discipline and governance frameworks that encompasses end-to-end the activity on 6G networks and how the data is treated and ensure it is secure, respect its privacy but not hinder the advancement of the benefits 6G will bring to all. A difficult balance to maintain, but necessary.

References

1. Rodriguez J (2015) Fundamentals of 5G mobile networks, 1st edn. Wiley, Chichester/West Sussex
2. Al-Dulaimi A, Chih-Lin I, Wang X (2018) 5G networks: fundamental requirements, enabling technologies, and operations management. 1st edn. New Jersey: Wiley
3. Edfors O, Larsson E-G, Marzetta T-L, Tufvesson F (2014) Massive MIMO for next generation wireless systems. IEEE Commun Mag, pp 186–195
4. Ge X, Mao G, Han T, Tu S, Wang C-X (2016) 5G ultra-dense cellular networks. In: IEEE wireless communications. 23(1):72–79
5. Ylianttila M et al 6g white paper: research challenges for trust, security and privacy. arXiv: 2004.11665
6. Shlezinger N et al (2021) Dynamic metasurface antennas for 6G extreme massive MIMO communications. IEEE Wirel Commun 28(2):106–113
7. Rajatheva et al (2020) White paper on broadband connectivity in 6G. arXiv:2004.14247v1[eess.SP]. https://arxiv.org/abs/2004.14247
8. Chen M et al (2019) Artificial neural networks-based machine learning for wireless networks: a tutorial. IEEE Commun Surv Tutorials 21(4):3039–3071
9. Khan LU et al (2020) Network slicing: recent advances, taxonomy, requirements, and open research challenges. IEEE Access 8:36009–36028. https://doi.org/10.1109/ACCESS.2020.2975072
10. Giordani M et al (2020) Toward 6G networks: use cases and technologies. In: IEEE communications magazine 58(3):55–61. https://doi.org/10.1109/MCOM.001.1900411
11. Nayak S, Patgiri R (2020) 6G communication: envisioning the key issues and challenges. arXiv: 2004.04024
12. Jagannath A, Jagannath J, Melodia T (2021) Redefining wireless communication for 6G: signal processing meets deep learning with deep unfolding. IEEE Trans Artif Intell 2(6):528–536. https://doi.org/10.1109/TAI.2021.3108129
13. Yue C et al (2022) Efficient decoders for short block length codes in 6G URLLC. arXiv:2206.09572
14. European Commission (2021) Shaping Europe's digital future: 5G. https://digital-strategy.ec.europa.eu/en/policies/5g. Accessed 19 Jan 2023

15. IEEE (2018) IEEE standards association: IEEE standards activities in 5G". Available at https://standards.ieee.org/content/dam/ieee-standards/standards/web/documents/other/5G.pdf. Accessed 18 Aug 2019
16. GSMA (2019) Intelligent connectivity: how the combination of 5G, AI, big data and IoT is set to change everything. Available at https://www.gsma.com/IC/wp-content/uploads/2019/02/22209-Intelligent-connectivity-report.pdf. Accessed 19 Jan 2023
17. Seeburn K (2019) 5G and AI: a potentially potent combination. Available at http://www.isaca.org/Knowledge-Center/Blog/Lists/Posts/Post.aspx?ID=1146#Comments. Accessed 20 Jan 2023
18. Drechsler et al (2020) At the crossroads between digital innovation and digital transformation. https://www.researchgate.net/publication/341412594_At_the_Crossroads_between_Digital_Innovation_and_Digital_Transformation. Accessed 20 Jan 2023
19. Kokolek et al (2019) Data protection in the EU. https://commission.europa.eu/law/law-topic/data-protection/data-protection-eu_en https://commission.europa.eu/law/law-topic/data-protection/data-protection-eu_en
20. Forradellas R, Gallastegui L (2021) Digital transformation and artificial intelligence applied to business: legal regulations, economic impact and perspective. https://www.mdpi.com/2075-471X/10/3/70. Accessed 19 Jan 2023
21. Fedrecheski G et al (2020) Self-sovereign identity for IoT environments: a perspective. In: 2020 global internet of things summit (GIoTS). IEEE
22. Harper KE, Ganz C, Malakuti S (2019) Digital twin architecture and standards. IIC J Innov 12(2019):72–83
23. Bhowmik D, Feng T (2017) The multimedia blockchain: a distributed and tamper-proof media transaction framework. In: 2017 22nd international conference on digital signal processing (DSP). IEEE
24. Bakre A, Patil N, Gupta S (2017) Implementing decentralized digital identity using blockchain. Int J Eng Technol Sci Res 4(10):379–385
25. Yaqoob I et al (2020) Blockchain for digital twins: recent advances and future research challenges. IEEE Netw 34(5):290–298
26. Vast R et al (2021) Artificial intelligence based security orchestration, automation and response system. In: 2021 6th international conference for convergence in technology (I2CT). IEEE
27. Ahmad I, Gurtov A, Kumar T, Liyanage M, Okwuibe J, Ylianttila M (2017) [online] Available at http://jultika.oulu.fi/files/nbnfi-fe201902124647.pdf. Accessed 23 Jan 2023
28. Yesuf AS (2017) A review of risk identification approaches in the telecommunication domain. https://www.researchgate.net/publication/314392917_A_Review_of_Risk_Identification_Approaches_in_the_Telecommunication_Domain [PDF] In: Conference paper. Conference: the 3rd international conference on information systems security and privacy—ICISSP. Accessed 20 Jan 2023
29. Reuters (2017) Cyberattack hits 200,000 in at least 150 countries: Europol https://www.reuters.com/article/us-cyber-attack-europol-idUSKCN18A0FX. Accessed 20 Jan 2023
30. Brewster T (2017) How hackers broke equifax: exploiting a patchable vulnerability. forbes. https://www.forbes.com/sites/thomasbrewster/2017/09/14/equifax-hack-the-result-of-patched-vulnerability/?sh=ce0ddce5cda4. Accessed 20 Jan 2023
31. Wang A (2018) 'I'm in your baby's room': a hacker took over a baby monitor and broadcast threats, parents say. Washington Post. https://www.washingtonpost.com/technology/2018/12/20/nest-cam-baby-monitor-hacked-kidnap-threat-came-device-parents-say/
32. Shu X et al (2017) Breaking the target: an analysis of target data breach and lessons learned. arXiv preprint. https://arxiv.org/pdf/1701.04940.pdf. Accessed 20 Jan 2023
33. Gara T, Warzel C (2014) A look through the sony pictures data hack: this is as bad as it gets. BuzzfeedNews. https://www.docketalarm.com/cases/PTAB/CBM2015-00030/Covered_Business_Method_Patent_Review_of_U.S._Pat._6321201/03-10-2015-Patent_Owner/Exhibit-2002-Exhibit_2002___A_Look_Through_The_Sony_Pictures_Data_Hack___BuzzFeed_News/

34. SDxCentral (2019) What are the top 5G security. Challenges". Available at https://www.sdxcentral.com/5g/definitions/top-5g-security-challenges/. Accessed 17 Aug 2019
35. Zhang Y (2018) Network function virtualization concepts and applicability in 5G networks, 1st edn. Wiley, New Jersey
36. Condoluci M, Mahmoodi T (2018) Softwarization and virtualization in 5G mobile networks: benefits, trends and challenges. Comput Netw 146(1):65–84
37. Huawei (2018) 5G security: forward thinking Huawei white paper. Available at https://www.huawei.com/minisite/5g/img/5G_Security_Whitepaper_en.pdf. Accessed 19 Jan 2023
38. Calder A, Watkins S (2015) IT governance: an international guide to data security and ISO27001/ISO27002, 6th edn. Kogan Page, London
39. Miller L (2016) IoT security for dummies, inside secure edition, 1st edn. John Wiley & Sons, Chichester/West Sussex
40. Blum JJ, Lawson-Jenkins K, Hoffman L-J (2006) Trust beyond security: An expanded trust model. Commun ACM 49(7):95–101
41. Fogg BJ, Tseng S (1999) Credibility and computing technology. Commun ACM 42(5):39–44
42. GOV.UK (2022) Cyber Security Breaches Survey 2022. https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2022/cyber-security-breaches-survey-2022#chapter-5-incidence-and-impact-of-breaches-or-attacks https://www.ncsc.gov.uk/news/data-breach-500m-yahoo-accounts https://hoteltechreport.com/news/marriott-data-breach. Accessed 19 Jan 2023
43. Confessore N (2018) Cambridge analytica and facebook: the scandal and the fallout so far https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html. Accessed 19 Jan 2023
44. Aïmeur E, Schőnfeld D (2011) The ultimate invasion of privacy: identity theft. In: 2011 ninth annual international conference on privacy, security and trust. IEEE. https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html Accessed 23 Jan 2023
45. Privacy International (2017) 101: data protection. https://privacyinternational.org/explainer/41/101-data-protection. Accessed 23 Jan 2023
46. Masombuka M, Grobler M, Watson B (2018) Towards an artificial intelligence framework to actively defend cyberspace. In: European conference on cyber warfare and security. Academic conferences international limited. https://search.proquest.com/openview/f6ccddd62973bd89da756a6c4f7272f0/1?pq-origsite=gscholar&cbl=396497&casa_token=fefF24OzjlcAAAAA:lW8TZptX9KGeshqbVXXBk1MBmrm0zyKHj5mmY62oPWdizJiYTe0WcDk4RMFtG2P0ZsuzdvAtZBo
47. Babiceanu RF, Seker R (2023) Big data and virtualization for manufacturing cyber-physical systems: a survey of the current status and future outlook. Computers in industry 81:128–137. https://www.sciencedirect.com/science/article/pii/S0166361516300471?casa_token=S59wxZXqps8AAAAA:SudkZGNExVlneS0cwzOiJPq3T6peQI63_K3I1fFNKuIkNz4hhlaAt4IKbxWnjFT9WBwX37vxlII. Accessed 22 Jan 2023
48. Hicks A et al (2019) Global mapping of citizen science projects for disaster risk reduction. Frontiers Earth Sci 7:226. https://doi.org/10.3389/feart.2019.00226/full. Accessed 19 Jan 2023
49. ISO/IEC (2022) https://www.iso.org/standard/82875.html
50. NIST (2018) https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf
51. ISO (2019) https://www.iso.org/standard/75106.html
52. BS (2007) https://knowledge.bsigroup.com/products/business-continuity-management-specification-1/standard
53. Schlehahn E (2020) Cybersecurity and the state. The ethics of cybersecurity. Springer, Cham, 205–225
54. Eltringham M (2017) UK organisations remain unprepared to deal with effects of cyber attack. UK organisations remain unprepared to deal with effects of cyber attack—Workplace Insight. Accessed 19 Jan 2023
55. Caulkins B, Marlowe T, Reardon A (2018) Cybersecurity skills to address today's threats. In: Ahram T, Nicholson D (eds) Advances in human factors in cybersecurity, AHFE 2018. Advances in intelligent systems and computing, pp 782–788. https://doi.org/10.1007/978-3-319-94782-2_18

56. Panda A, Bower A (2020) Cyber security and the disaster resilience framework. Int J Disaster Resilience Built Environ 11(4):507–518
57. Goodwin C et al (2015) A framework for cybersecurity information sharing and risk reduction. Microsoft
58. Landry BJL, Koger MS (2006) Dispelling 10 common disaster recovery myths: Lessons learned from hurricane katrina and other disasters. J Educ Resour Comput (JERIC) 6(4):6-es
59. Hyslop M (2007) Comments on standards in information security, disaster recovery, business continuity and business resilience. Crit Inf Infrastruct Resilience Prot (2007):94–144
60. Schmidt CG, Wagner SM (2019) Blockchain and supply chain relations: a transaction cost theory perspective. J Purch Supply Manag 25(4):100552
61. Pickles J, Zhu S (2013) The California transparency in supply chains act. SSRN Electron J. https://doi.org/10.2139/ssrn.2237437
62. Cheung K-F, Bell MGH, Bhattacharjya J (2021) Cybersecurity in logistics and supply chain management: an overview and future research directions. Transp Res Part E Logistics Transp Rev 146:102217. https://doi.org/10.1016/j.tre.2020.102217
63. Kendzierskyj et al (2021) Cyber security and supply chain management, pp 147–174. https://doi.org/10.1142/9789811233128_0007. Accessed 22 Jan 2023

Investigating Gesture Control of Robotic Arm via Lora Technology for Smart Cities

Amaechi Stanley Okoro, Sufian Yousef, and Akram Qashou

Abstract This paper aim to establish gesture control of robotic arm utilizing long range (LoRa) technology to enhance the signal's range while facilitating low power consumption which is achievable because the device is in continuous sleep mode and only activates when it needs to send a message. This paper was carried out by constructing a hand sensing glove with sensors and accelerometer to send signals to the robotic arm, incorporating the LoRa technology as the transmission module for transferring the signal and programming a microcontroller that processes sensor data and direct robotics arm movement. This technology has been adopted in IoT applications and found relevance when facilitating long range, low power consumption, and low cost. Notwithstanding, the shortcomings of this technology is discussed briefly in this paper. The goal of this study is to build gesture control of a robotic arm using long range (LoRa) technology to increase signal range while allowing for low power consumption, which is possible because the device is in continuous sleep mode and only activates when a message needs to be sent. This paper was completed by building a hand sensing glove with sensors and an accelerometer to deliver signals to a robotic arm, using LoRa technology as the signal transmission module, and developing a microcontroller that interprets sensor data and directs robotic arm movement. This technology has been used in IoT applications and has proven useful in enabling extended range, low power consumption, and low cost. Nonetheless, the drawbacks of this technique are briefly highlighted in this paper.

Keywords LoRa · Sensors · MPU6050 · Hand gesture · ESP32 · Robotics

A. S. Okoro · S. Yousef (✉) · A. Qashou
Anglia Ruskin University, Cambridge, UK
e-mail: Sufian.Yousef@aru.ac.uk

H. Jahankhani and A. El Hajjar (eds.), *Wireless Networks*, Advanced Sciences
and Technologies for Security Applications,
https://doi.org/10.1007/978-3-031-33631-7_3

1 Introduction

The human way of doing things has been made simpler by technological advancements, which has greatly accelerated and improved productivity. The creation of the robotic arm is one instance where this has been demonstrated to be true. Robotic arms have been utilized extensively to accomplish more work in a given amount of time or in circumstances where human life may be at danger [31].

One method of controlling a robotic arm is by using gestures [7]. A gesture controlled robotic arm is a type of robot that works based on signals supplied by human hand gestures. It moves and executes a task based on human hand gestures, thus mimicking the motion of the human hand [31, 37]. Gesture controlled robotic arms are currently being used in military operations and industrial processes. With the development of IoT, they have found use in the medical field, allowing surgeons to do procedures from a distance by wirelessly directing a robotic arm [34, 39].

A transceiver system, which allows a transmitter from the human operator end to transmit a signal and a receiver linked to the robotic arm to receive it, is used to control a robotic arm via gestures. At the transmitting end, the human operator dons a sensor glove equipped with an accelerometer that picks up the hand's pattern of motion and sends the signals to the robotic arm's receiver. Depending on the user's motion, a microprocessor at the receiving end interprets the transmitted sensors signals from the glove and instructs the servos on the robotic arm to respond appropriately [37]. Wireless communication is utilised in the exchange of information between the transmitting and receiving systems.

Several wireless transmission technologies have been utilized to enable transmission and reception of information between the transmitting and receiving systems in order to achieve gesture control of a robotic arm. For instance, wireless communication technologies like infrared, Bluetooth, WiFi, and Zigbee have been used. However, these communication technologies are limited to short-range communication, with their maximum range being less than 100 m [21, 25, 33]. They also require considerable amount of power to be able to operate (within the range of 10–100 mW) [25]. But there are some operations that involve long-range activities requiring a significantly wider range of control. Activities such as bomb defusing, painting and welding in hazardous environments and rescue operation from disastrous occurrences (e.g. fire, collapsed buildings, natural disasters, floods, etc.) require more distance between the operator and the robotic arm to ensure safety. There are also certain operations that require long-range transmission in areas where consistent access to power will not be possible and in areas with no power supply. Therefore, how can long-range communication be carried out with minimal power consumption in such situations?

The LoRa transceiver is a system that incorporates a wireless transmission with a longer range spanning over 15 km in the countryside and up to 5 km in the city than the aforementioned communication technologies and requires very minimal power consumption. As a result, it is a great choice for long-distance activities [3], Semtech [28, 35]. A typical LoRa transceiver requires a maximum transmitting power of

+ 14 dBm [25]. Hence, the LoRa technology will be very useful in situations that require a long-range transmission with a limited power supply.

1.1 Significance of Study

This project work is carried out to ensure that gestures can be used to operate a robotic arm from a long distance in situations where close contact will be harmful or dangerous, thus ensuring maximum safety. Also, since the LoRa technology facilitates low power consumption, this project work will be useful in certain operations where consistent access to power will not be possible and even in areas with no power supply.

1.2 Scope of Research

This paper work is limited to the deployment of the LoRa communication protocol in achieving gesture control of a robotic arm. Also, this paper work does not consider the design and construction of the robotic arm itself.

1.3 Applications

The project can be applied in:

- Bomb defusing
- Painting in hazardous environments
- Military applications
- Rescue operation from disastrous occurrences (e.g. fire, collapsed buildings, natural disasters, floods, etc.)
- Industrial applications like lifting of heavy objects
- Fireworks production
- Welding in hazardous environments.

2 Literature Review

2.1 Gesture Control of Robotic Arm Using Infrared

On the subject of "Controlling a Robotic Arm via gesture using Leap Motion," [20] published an article in the "Indian Journal of Science and Technology." To detect the movement of a human hand, the device uses a leap motion controller. The sensor, leap motion can recognize a human hand within a 1 mm range in 300 s using 3D coordinates (X, Y, and Z). Two monochromatic infrared (IR) cameras that detect heat emitted by human hands and three IR LEDs that identify the hand's structure were used by the authors to build their system. The three IR LEDs emit light with an 850 nm wavelength as soon as human hand movements are detected. The data that was received from the leap mot on is then transmitted to a controller, which transforms the data into coordinates that may be used to move the robotic ar.m. The range of a common jump motion controller is 1 m, while the maximum line-of-sight distance for IR transmission is roughly 5 m [19].

2.2 Wireless Gesture Controlled Robot via Bluetooth Wireless Connectivity

Using Bluetooth wireless communication, Chanda et al. [9] created and developed a wireless gesture controlled robot. They put their design into practice using an Android smart phone Java-based mobile application, an Arduino ATMEGA 328 microcontroller that processes the signals depending on the gestures, and an HC-05 Bluetooth module to communicate the signals to the robot in order to control it remotely. The ISM band between 2.400 and 2.485 GHz is where Bluetooth technology operates. The range of transmission is between 15 and 30 m, and the maximum broadcast power is 10 mw (100 mw with Bluetooth 5) [6, 25].

2.3 Gesture Control of Robotic Arm Using Zigbee Technology

Keder et al. [22] implemented gesture control of a robotic arm using Zigbee wireless communication technology in their paper "Development of Zigbee Based Tele Operated Multipurpose Robotic Arm With Hand Gesture Recognition" published in "International Journal of Mechanical Engineering and Technology" in August 2017. To wirelessly operate the robotic arm with hand gestures utilizing Zigbee transmitter and receiver modules, they use the high-end microprocessor AVR328 along with the Arduino Uno platform, precise accelerometers, flex sensors, and rover platform.

Zigbee technology was also employed by Rakesh and Shivashankara [30] to operate a robot with hand gestures. Wearing a transmitting device that sends commands to the robot to carry out the intended operation is part of the technology they designed. An analog-to-digital converter (ADC) in the transmitting unit turns the analog data into digital data, which is then sent to the microcontroller for encoding the four pieces of information before being sent to the Zigbee transmitter module to be transmitted to the receiver. A second microcontroller at the receiver end decodes the information after it has been gathered by the robot's Zigbee receiver module and used for proper operation.

The highest transmit power of the Zigbee communication protocol is 22 dB, and its transmission range is 10–100 m [6, 25].

2.4 Gesture Based Wireless Mobile Robotic Arm via WiFi Connection

Shifas et al. [36] developed a "Gesture Based Wireless Mobile Robotic Arm Using Flux Sensor". The system uses the WiFi communication technology for signal transmission. The researchers make use of a flex sensor which is fitted to a glove worn by the user and which senses the movement of each finger. The digital signals from the ADC are passed on to the ESP8266 Arduino Wi-Fi module for transmission to the receiver section. At the receiver section, the Arduino Uno microcontroller receives the transmitted signals, processes and converts them into the required pulses which are then utilised as input by the servo motors. This supplies the energy needed by the servo motors to generate motion. WiFi communication Technology has a transmission range of 100–1000 m while the maximum transmit power of the WiFi module is 28 dBm [25].

2.5 Gesture Controlled Robotic Arm Using 433 MHz RF Module

Gesture-Controlled Robotic Arm Design and Implementation for Industrial Applications was the subject of a study written by Pradeep and Paul and published in the "International Journal of Advanced Scientific Research and Development" in December 2016. For the wireless communication between the transmitter and the receiver sections, the authors made use of an RF transceiver module. The RF transceiver module works on a frequency of 433 MHz. Garg et al. [18] also developed a gesture-based robot with a robotic arm for pick and place operations using RF module. The RF module has a limited range of 3 m, but with special antenna and appropriate power supply the range can be increased to about 30–35 m [27].

This project work focuses on the use of the LoRa technology interfaced with ESP 32 microcontroller to achieve gesture control of a robotic arm as it will be very useful in situations that require a long-range transmission with a limited power supply.

2.6 An Overview of Lora Technology

LoRa, which is an acronym that stands for “Long Range,” is a non-cellular wireless technology that has a long range and uses very little power. It is being supported by the LoRa Alliance. It belongs to the group of low-power wide-area (LPWA) network technologies and is a radio modulation technology for wireless local area networks (WLANs). A LoRa-based network protocol is called LoRaWAN [17, 25].

The LoRa protocol is optimised for low-power (battery-operated) end devices that need to send only a small quantity of data at a time during deployment and where end devices can either start data traffic on their own (when the end device is a sensor, for instance) or independently (when the end device is an actuator), with the aid of a third party desiring to connect with the end device [23].

2.7 Lora Transceiver

LoRa transceiver module is a communication module used to send and receive data from LoRa sensors. It offers a simple, low-power alternative for wireless data transfer across vast distances [1, 12]. An RFM95 LoRa transceiver module is shown in Fig. 1.

A LoRa transceiver chip’s typical components are shown in Fig. 1. The UART, GPIOs, LoRa Radio layer, LoRa protocol stack, processor, interface buses (such I2C, SPI), and other components make up this device. UART is used to connect the microcontroller unit to the LoRa transceiver for monitoring and controlling applications. Any user-defined hardware elements, like LEDs, switches, etc., are interfaced using GPIOs. The LoRa RF layer interfaces with antennas operating in many frequency ranges, including 433 and 868 MHz. Crystal is necessary to run the LoRa transceiver’s CPU and real-time clock [32].

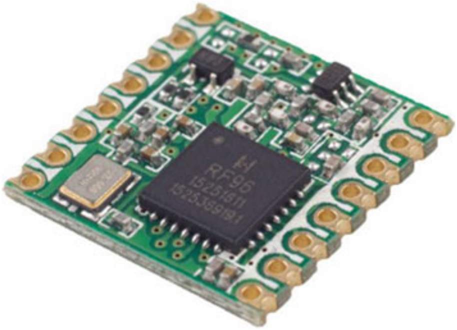


Fig. 1 RFM95 LoRa transceiver module [14]

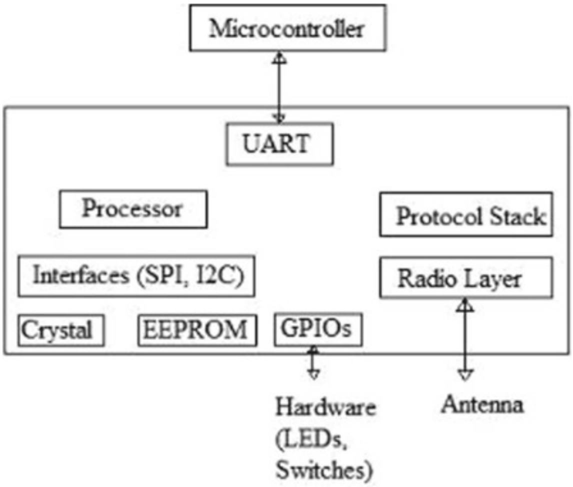


Fig. 2 Typical components in a LoRa transceiver chip [32]

2.8 Lora Protocol Stack

With a focus on reducing energy consumption, the LoRa wireless communications system aims to be practical for use in long-lasting battery-powered devices [4]. LoRa is frequently used to describe two separate layers, namely:

A physical layer employing the radio modulation method of the Chirp Spread Spectrum (CSS) [24].

LoRaWAN, a MAC layer protocol although a particular access network architecture is advocated by the LoRa communications system [4].

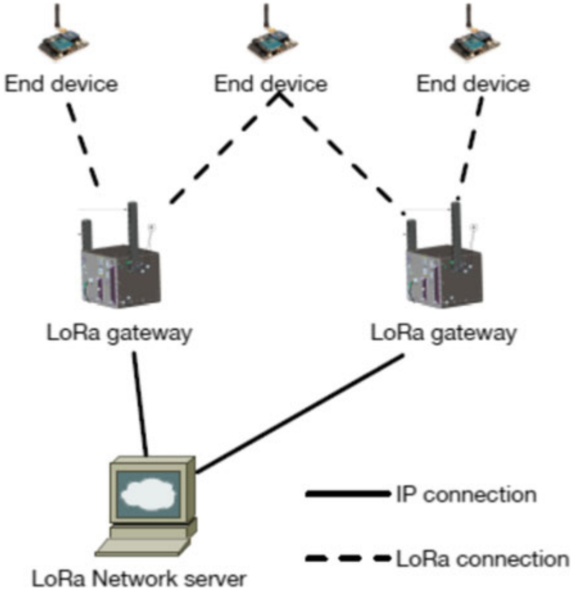
Long-distance communications that use little energy and have a slow throughput are feasible, thanks to the Semtech-developed LoRa physical layer. Depending on the area where it is deployed, it uses the ISM bands at 433, 868, or 915 MHzT of each transmission payload may contain anywhere from two to 255 octets when channel aggregation is employed and the data rate can be as high as 50 kbps. Semtech's unique technology underlies the modulation method [35].

Since LoRaWAN provides a medium access control mechanism, many LoRa-modulated end devices can communicate with a single gateway and despite LoRa modulation being an exclusive technology, the LoRa Alliance is working to produce the open standard LoRaWAN [23].

2.9 Lora Network Architecture

"Star-of-stars topology" of a typical LoRa network as seen in Fig. 3, which consists of three different kinds of devices.

Fig. 3 LoRa network architecture [4]



The fundamental components of a LoRaWAN network include: LoRaWAN is the protocol used by end devices to communicate with gateways. Unprocessed LoRaWAN packets are forwarded from devices to a network server via gateways using a backhaul interface that has a higher throughput. This interface is often Ethernet or 3G. Due to the fact that the network server is in responsible of decoding the packets that are provided by the devices and constructing the packets that are supposed to be sent back to the devices, gateways are just bidirectional relays or protocol converters [4].

2.9.1 How Lora Sensor Transmits and Receives Data

A LoRa network employs the LoRaWAN protocol in order to transmit and receive data from LoRa sensors. Despite the fact that LoRaWAN primarily acts as a network layer protocol, it is also a cloud-based media access control (MAC) layer protocol. We use LoRaWAN to govern communication between LoRa gateways and LoRa devices. As a protocol for routing, it is maintained by the LoRa Alliance. LoRaWAN describes the LoRa network's system architecture and communication protocol. It offers a secure and reliable long-distance communication connection. The power optimization, communication frequencies, and data rates of all LoRa devices are controlled by LoRaWAN [40].

Within a LoRa network, LoRa nodes communicate asynchronously and start broadcasting as soon as they have data to broadcast. A LoRa network can thus compromise between sensitivity and data rate while preserving a predetermined channel bandwidth. The most important factor is selecting the amount of spread to employ, which is a customizable quantity between 7 and 12. The sensitivity and data rate of a LoRa node are determined by this spreading factor. A number of LoRa gateways receive the data packets that a LoRa node transmits and send them to a central network server (IoT server). The IoT server controls the network, removes duplicate packets and performs security checks. The server then distributes this information to the associated smart devices, control panels, or application modules. In this manner, the LoRaWAN protocol exhibits good accuracy and dependability under moderate load. Forward Error Correction coding is also employed by the LoRa protocol. This improves the LoRa network's tolerance to any sort of interference with a high interference level. The very high wireless link budgets of a LoRa network, which vary from 155 to 170 dB, are what give it its tremendous range [40].

2.9.2 Lora Range and Power Requirements

LoRa technology guarantees long-range communication at distances up to 5 km in urban areas and over 15 km in rural areas. Ultra-low power needs, which enable the development of battery-operated devices with a 10-year lifetime, are unique features of systems based on LoRa. Maximum transmission power of a common LoRa transceiver is + 14 dBm. A network built on the open LoRaWAN protocol and set up in a star topology is great for applications that need a lot of small, low-power data collection devices to talk to each other over a long distance or deep inside a building [3, 25, 28, 35].

2.9.3 Motivation

After comparing the characteristics of IR, Bluetooth, Zigbee, 433 MHz RF, WiFi, and LoRa technologies for wireless communication, LoRa has shown to be the optimal solution for implementing gesture control of a robotic arm because of its low power usage and extensive range of communication as seen in the works of [3, 25], Semtech [28, 35]. Hence, this paper work focuses on the use of the LoRa technology to achieve gesture control of a robotic arm as it will be very useful in situations that require a long-range transmission with a limited power supply.

2.9.4 Review of Principles Relevant to This Project

The following sections contain a review of the principles applied and main components used in investigating gesture control of robotic arm via LoRa.

3 Flex Sensors

3.1 What is a Flex Sensor?

Flex sensors measures how much deflection or bending has occurred. Materials like plastic and carbon can be used to build this sensor. The sensor's resistance will change as the plastic strip holding the carbon surface is flipped aside. The amount of turn can be directly proportional to its fluctuating resistance [15]. A typical flex sensor is shown in Fig. 4.

3.1.1 Pin Configuration

Figure 5 illustrates the flex sensor's pin layout. The device has two terminals, which are designated P1 and P2. The positive terminal of the power source is typically linked to pin P1, while the negative terminal (GND pin) of the power source is typically attached to pin P2. In contrast to a diode or a capacitor, this sensor does not have a polarized terminal present, hence there is no positive or negative terminal. Any sort of interfacing can provide the 3.3–5 V DC required for the sensor to be activated [15].

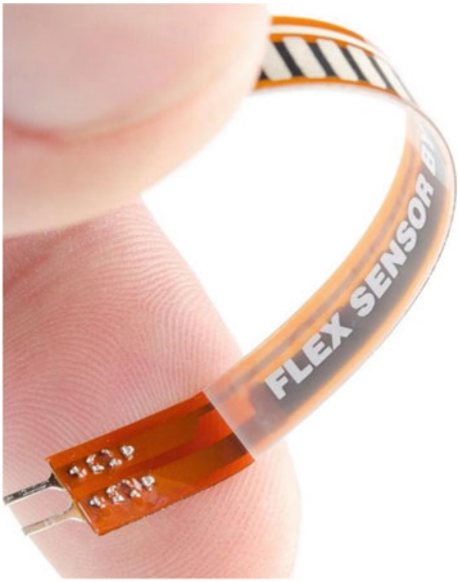


Fig. 4 A typical flex sensor [15]

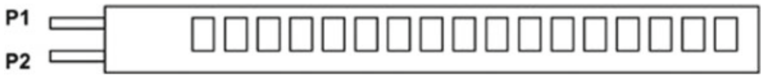
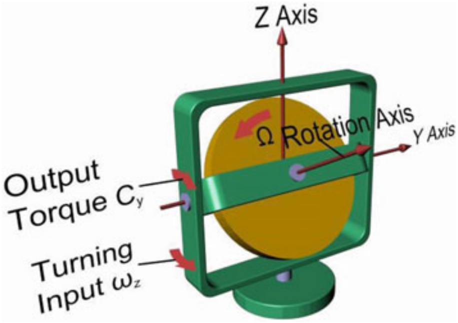


Fig. 5 Pin layout of the flex sensor [11]

Fig. 6 A mechanical gyroscope [29]



3.1.2 Gyroscopes

Gyroscopes are basically device that has the ability, when embedded on a frame to detect the angular velocity when the frame is rotating. Gyroscopes are useful independently as a standalone system and as a component to more complex systems such as the Inertia navigation system, Inertia Measurement, Gyrocompass, Attitude Heading Reference System [29]. The main parameters of a mechanical gyroscope is seen in Fig. 6.

A gyroscope has the ability to detect the rotation of an object around a set of axes by using the gravity of the earth to figure out how the object is oriented around the axes. This makes it possible for gyroscopes to be used to control, direct, and measure how an object rotate around the axes. The gyroscope can act as a motion sensor by using these features to measure an object's overall motion [26].

3.1.3 Gyroscope Angular Velocity

A gyroscope can detect an object's motion and determine its angular velocity. Angular velocity can be broken down into three different types: yaw, pitch, and roll as seen in Fig. 7. Yaw is referred to the horizontal rotation when viewing an object from above on a flat surface. When viewing the object from the front, the vertical rotation is referred to as pitch while the horizontal rotation is known as roll [26].

A typical gyroscope sensor is shown in Fig. 8. Gyroscope sensors are more sophisticated than accelerometers. While accelerometers can only detect linear motion, gyroscope sensors can measure both the inclination and horizontal position of the object. Gyroscope sensors are also known as angular velocity sensors and angular

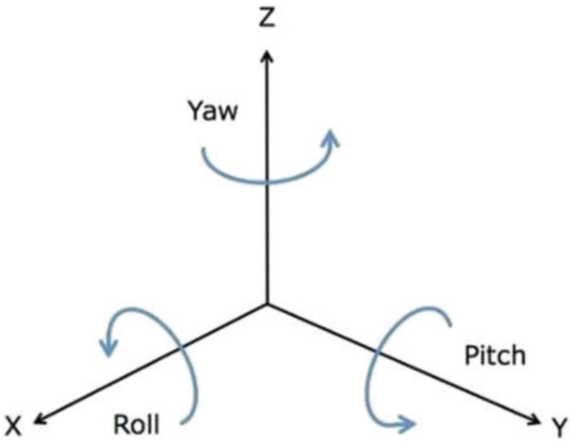


Fig. 7 Types of angular velocity [26]

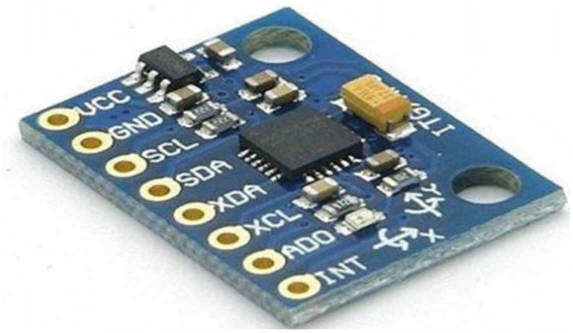


Fig. 8 Gyroscope sensor [16]

rate sensors. These sensors are utilised in situations where it is difficult for humans to discern the orientation of an object [16].

4 Servo Motors

4.1 What is a Servomotor?

A servomotor is an actuator that lets you control position, acceleration, and speed in a linear or angular way. It is made up of a motor that is hooked up to a position feedback sensor. In addition to this, it requires a very complicated controller, which is typically a unique module designed specifically for use with servomotors [13]. It is shown in Fig. 9.

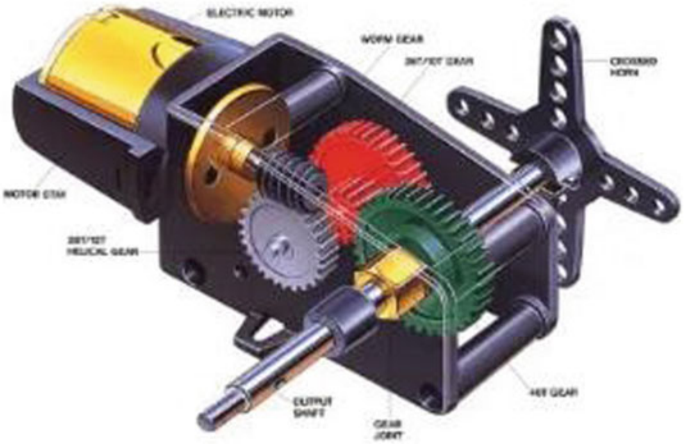


Fig. 9 A servomotor [13]

4.1.1 ESP32 Microcontroller

In this paper, the ESP32 microcontroller is used both in the transmitter and the receiver sections. ESP32 is a well-known and low-cost System on Chip (SoC) microcontroller created by Espressif Systems Company, the company behind the ESP8266 SoC. It is available in both single-core and dual-core versions of the 32-bit Xtensa LX6 microprocessor from Tensilica, and it has Wi-Fi and Bluetooth integrated. The ESP32 microcontroller's inbuilt RF components consisting the, Antenna switch, RF Balun, Power Amplifier, Filters and Low-Noise Receive Amplifier are a key feature. These components make it simple to construct hardware around the microcontroller because so few external components are needed. The ESP32 is particularly user-friendly since it supports multiple programming environments, including the PlatformIO IDE (VS Code), Arduino IDE, JavaScript, MicroPython, Espressif IDF (IoT Development Framework) and LUA [38].

4.1.2 Lora Transceiver

LoRa transceiver module is a communication module used to send and receive data from LoRa sensors. It offers a simple, low-power alternative for wireless data transfer across vast distances [1, 12]. An RFM95 LoRa transceiver module is shown in Fig. 2.

A LoRa transceiver chip's typical components are shown in Fig. 1. The UART, GPIOs, LoRa Radio layer, LoRa protocol stack, processor, interface buses (such I2C, SPI), and other components make up this device. UART is used to connect the microcontroller unit to the LoRa transceiver for monitoring and controlling applications. Any user-defined hardware elements, like LEDs, switches, etc., are interfaced using GPIOs. The LoRa RF layer interfaces with antennas operating in many frequency ranges, including 433 and 868 MHz. Crystal is necessary to run the LoRa transceiver's CPU and real-time clock [32].

4.1.3 How Lora Sensor Transmits and Receives Data

A LoRa network employs the LoRaWAN protocol in order to transmit and receive data from LoRa sensors. Despite the fact that LoRaWAN primarily acts as a network layer protocol, it is also a cloud-based media access control (MAC) layer protocol. We use LoRaWAN to govern communication between LoRa gateways and LoRa devices. As a protocol for routing, it is maintained by the LoRa Alliance. LoRaWAN describes the LoRa network's system architecture and communication protocol. It offers a secure and reliable long-distance communication connection. The power optimization, communication frequencies, and data rates of all LoRa devices are controlled by LoRaWAN [40].

Within a LoRa network, LoRa nodes communicate asynchronously and start broadcasting as soon as they have data to broadcast. A LoRa network can thus compromise between sensitivity and data rate while preserving a predetermined channel bandwidth. The most important factor is selecting the amount of spread to employ, which is a customizable quantity between 7 and 12. The sensitivity and data rate of a LoRa node are determined by this spreading factor. A number of LoRa gateways receive the data packets that a LoRa node transmits and send them to a central network server (IoT server). The IoT server controls the network, removes duplicate packets and performs security checks. The server then distributes this information to the associated smart devices, control panels, or application modules. In this manner, the LoRaWAN protocol exhibits good accuracy and dependability under moderate load. Forward Error Correction coding is also employed by the LoRa protocol. This improves the LoRa network's tolerance to any sort of interference with a high interference level. The very high wireless link budgets of a LoRa network, which vary from 155 to 170 dB, are what give it its tremendous range [40].

5 System Design

The system involves two parts: Hardware design and Software design. The hardware is the physical part of the system while the software part consists of codes written to control the operation of the system and the components required for the efficient functioning of this systems are as follows:

5.1 Microcontroller

The ESP32 microcontroller is used both in the transmitter and the receiver end. This is the heartbeat of the system and serves as the platform to which other sensors (LoRa Module, Gyroscope, Flex sensor etc.) necessary for this system is interfaced.

5.2 Hardware Design Analysis

This transmitter and receiver system was divided into various units consisting of the input unit, processing unit and output unit.

5.2.1 Input Unit

The input unit consists of the flex sensor and gyroscope.

Flex sensor: The flex sensor, as explained in chapter two of this paper work is used in this design to measure the rate at which the finger the sensor is attached to bends, after which it sends a high signal to the D34 pin of the microcontroller.

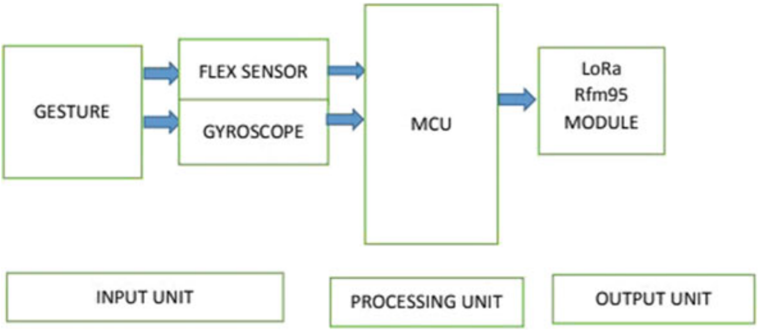


Fig. 10 Transmitter system

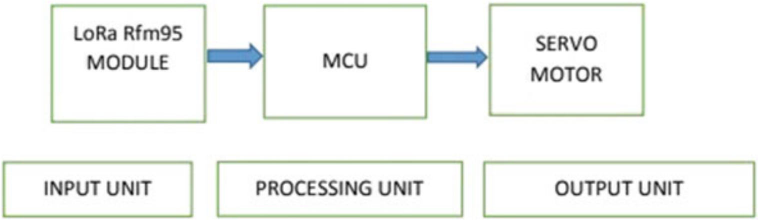


Fig. 11 Receiver system

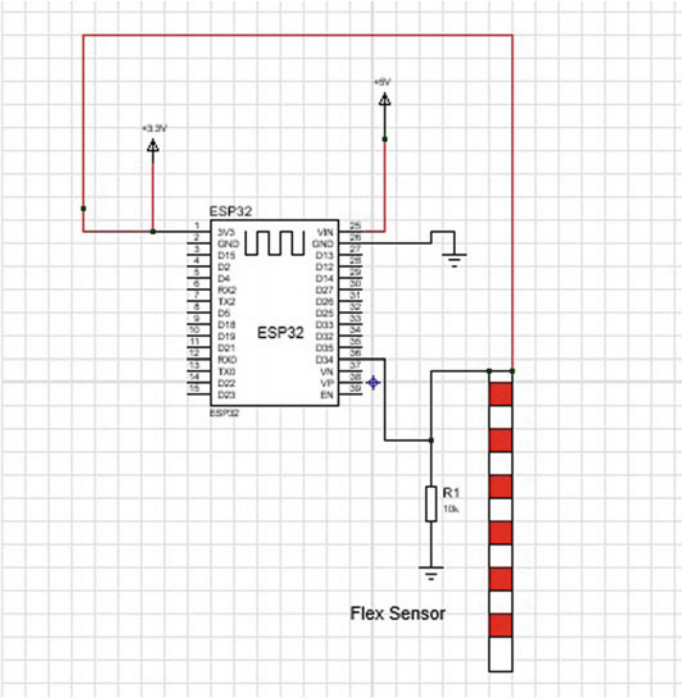


Fig. 12 Connection of the flex sensor to the ESP32 MCU

Gyroscope: The MPU6050 accelerometer and gyroscope is used in this paper to get the wrist motion in the three coordinates x, y and z, each axis represented as pitch, roll and yaw. Each representing a separate degree of freedom labelled as 3 DOF. In this paper, only 2 axes namely x and y—pitch and roll are used. The pin connection of the accelerometer and gyroscope to the ESP32 MCU is:

SDA – D24
SCL – D23
GND – GND
VCC – 3v3

5.3 Lora Transceiver

The LoRa communication module is a transceiver used at the transmitting and receiving ends of the system. The LoRa module at the transmitting end sends the data of the flex sensor and gyroscope received from the MCU at the transmitting end to the LoRa module at the receiving end, and the MCU at the receiving end outputs the result to the servo motors on the robotic arm.

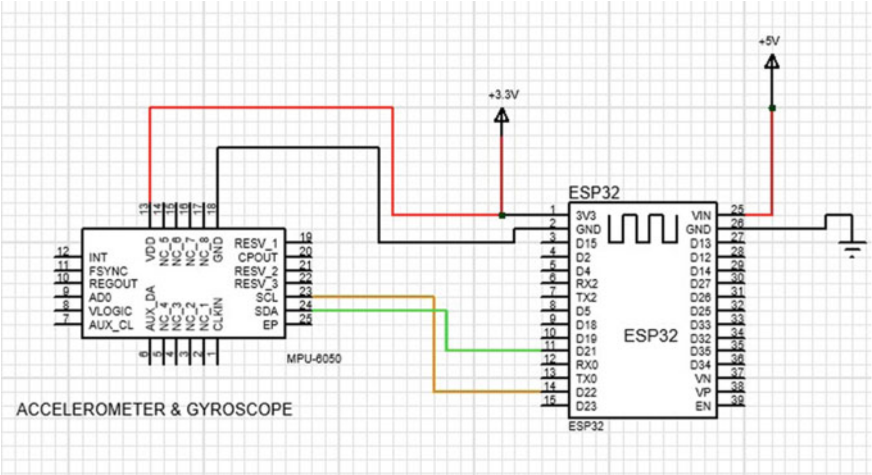


Fig. 13 Connection of the accelerometer and gyroscope to the ESP32 MCU

The pin connection of the LoRa transceiver to the ESP32 MCU is:

DI00 – GPIO 2
RESET – GPIO 4
NSS – GPIO 14
SCK – GPIO 18
MOSI – GPIO 23
MISO – GPIO 19

5.4 Output Unit

The output unit consists of the servo motors.

Robotic Arm: The robotic arm is the vital part of the system which outputs the signals received from the transmitter through the servo embedded on it allowing it move in different axes and also picking and placing object. The servo motor is responsible for the motion of the 2 DOF robot and this motion depends on the signal from the transmitter to the receiver system.

Servos have three terminals which are power, ground and signal terminal. The signal pin is the input pin and works depending on the pulse width modulation from the input signal from 0 to 180° which represents its minimum and maximum angle. The servo pin connections to the ESP32 MCU are:

Red (VCC) = +5 V
Brown (GND) = GND
Orange (PWM) = D27

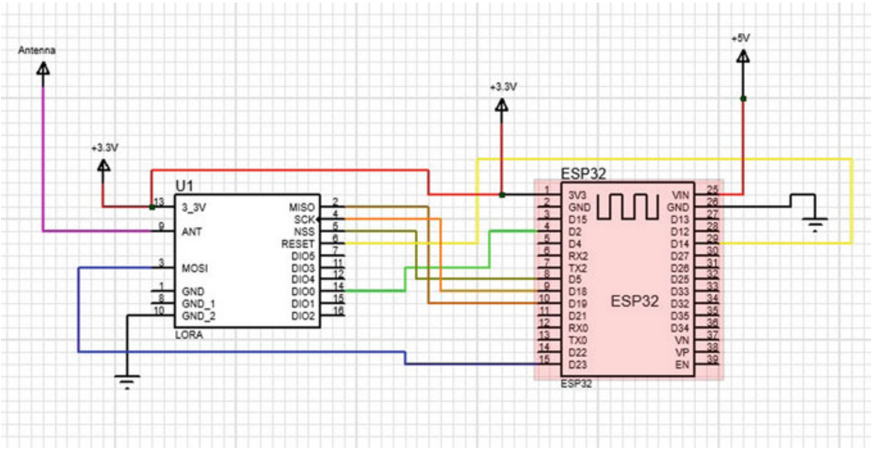


Fig. 14 Connection of the LoRa transceiver to the ESP32 MCU

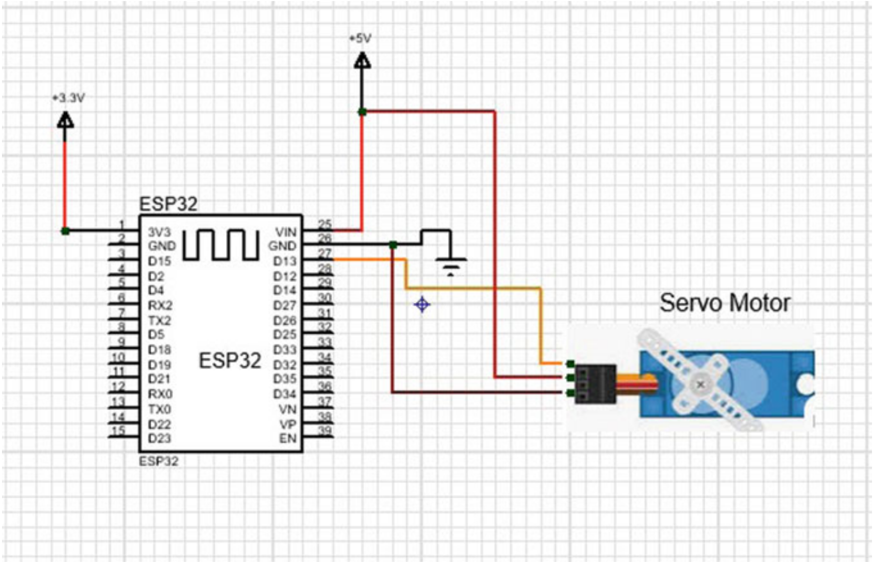


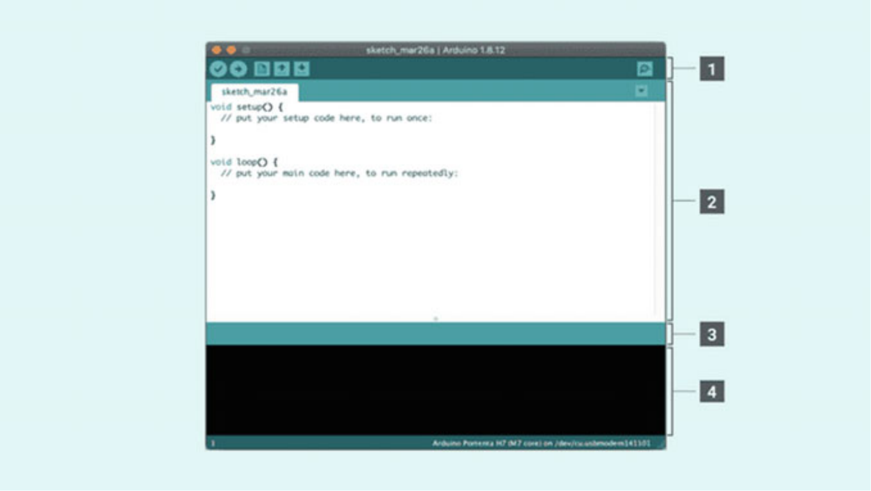
Fig. 15 The connection of the servo motor to the ESP32 MCU

5.5 *Software Design Analysis*

Software implementation is the brain behind this system functionality and operation. Without a program installed in the hardware device, it is impossible to implement the intended operation. An algorithm is generated on how the system should operate and a program is written with respect to this algorithm. This software algorithm was implemented with the aid of the C programming language using the Arduino IDE compiler.

5.5.1 Arduino Integrated Development Environment (IDE)

The Java-based Arduino Integrated Development Environment (IDE) is used to create software for microcontrollers. Although the ESP32 supports a variety of programming environments, using the Arduino platform is the simplest method to begin creating code for the ESP32 platform, hence it is used in this project work. The Arduino platform is an open-source platform built around Atmel microcontrollers and intended for quick prototyping. For the ESP32 Wi-Fi chip, a plugin known as the Arduino core is developed. The plugin installs support for ESP32 microcontroller development in the Arduino IDE environment. The Arduino core extension for the ESP32 Wi-Fi chip is made available as open-source project [5]. Figure 16 shows the interface of the Arduino IDE where Sect. 1 represents the toolbar where we have access to the software features. The serial monitor and serial plot which are one of the features of this software allow us to see the results and how our program functions which gives us room for testing and debugging before the actual hardware device is implemented. Section 2 represents the test editor where we write our code. Section 3 is the status bar which helps to know if our code compiled and uploaded successfully. Section 4 represents program notification area to know if our code is successful or if there is an error and what could be the cause.


sketch_mar26a | Arduino 1.8.12
sketch_mar26a
Arduino Portenta H7 (M7 core) on /dev/cu.usbmodem141101
1
2
3
4

```
void setup() {
  // put your setup code here, to run once:

}

void loop() {
  // put your main code here, to run repeatedly:

}
```

Fig. 16 Arduino IDE interface [2]

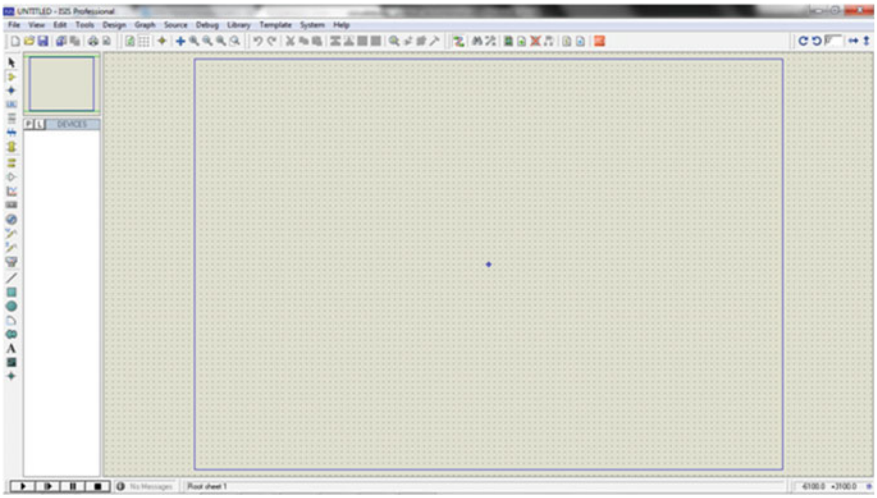


Fig. 17 Proteus design interface [10]

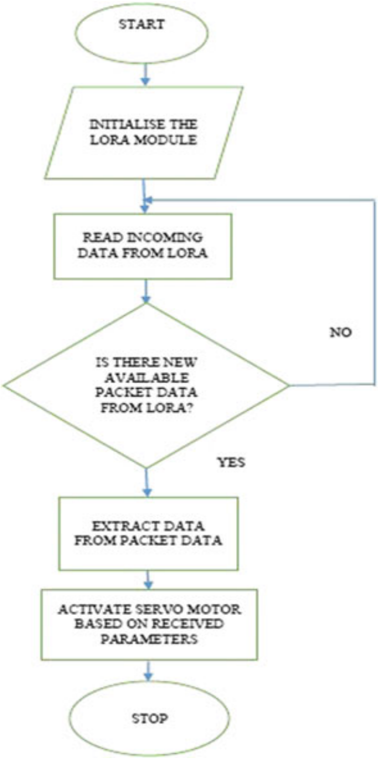
5.5.2 Proteus Simulation

The design of this project is simulated using Proteus design suite version 8, which is a simulation and design software programme developed for Electrical and Electronic circuit design by Labcenter Electronics. Proteus is a software package that includes schematic, simulation, and PCB design tools. The Proteus design suite's ISIS program is used to create schematics and do real-time circuit simulations. The programme delivers simulation in real time by permitting user input while it is running. A debug file or a hex file is applied to the microcontroller portion on the schematic in Proteus to simulate microcontrollers. It is then co-simulated with any attached analog and digital circuits [10]. The Proteus design interface is shown in Fig. 17.

5.6 Flow Chart of the System

The working algorithms of both the transmitter and the receiver of the gesture control of robotic arm via LoRa technology are represented by the flow charts shown in Figs. 18 and 19.

Fig. 18 Transmitter system


START
INITIALISE THE LORA MODULE
READ INCOMING DATA FROM LORA
IS THERE NEW AVAILABLE PACKET DATA FROM LORA?
NO
YES
EXTRACT DATA FROM PACKET DATA
ACTIVATE SERVO MOTOR BASED ON RECEIVED PARAMETERS
STOP

5.7 Circuit Diagram of the System

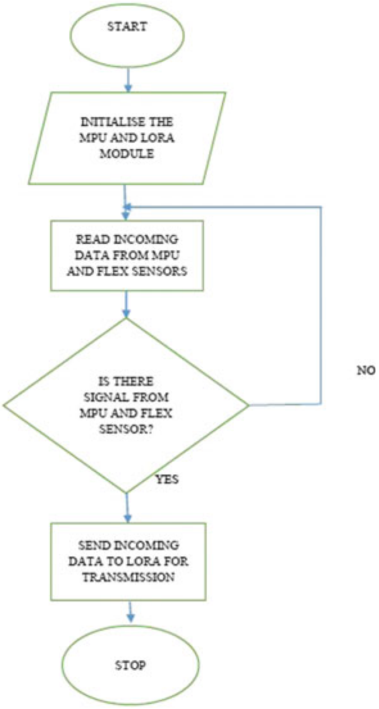
The complete circuit diagram of the gesture control of robotic arm via LoRa technology showing both the transmitter end and the receiver end is seen in Figs. 20 and 21.

6 Results, Analysis and Findings

6.1 Breadboarding

After simulating the circuit on the Proteus simulation workbench, the complete design was implemented using breadboard as shown in Figs. 22 and 23. This was done to provide real life problems scenarios that may not have occurred during simulation and to ensure that the circuit works as desired from the circuit diagram. The main purpose of breadboard testing is to ensure that all problems which may be encountered

Fig. 19 Receiver system


START
INITIALISE THE MPU AND LORA MODULE
READ INCOMING DATA FROM MPU AND FLEX SENSORS
IS THERE SIGNAL FROM MPU AND FLEX SENSOR?
NO
YES
SEND INCOMING DATA TO LORA FOR TRANSMISSION
STOP

during the final build of the project are identified and solved before embarking on final construction.

6.2 Serial Plot

The graphical representations of the serial monitor of the mpu6050 accelerometer and gyroscope module is seen below depicting the yaw, pitch, and roll at default state and also the serial plot of the pitch angle.

6.3 Servo Motors Calibration of Prototype

The servo motors used to control the movement of the robotic arm are calibrated using a potentiometer. This is necessary as we need to centre the servo motors in a certain position and this position’s angles are taken into consideration when writing the code.

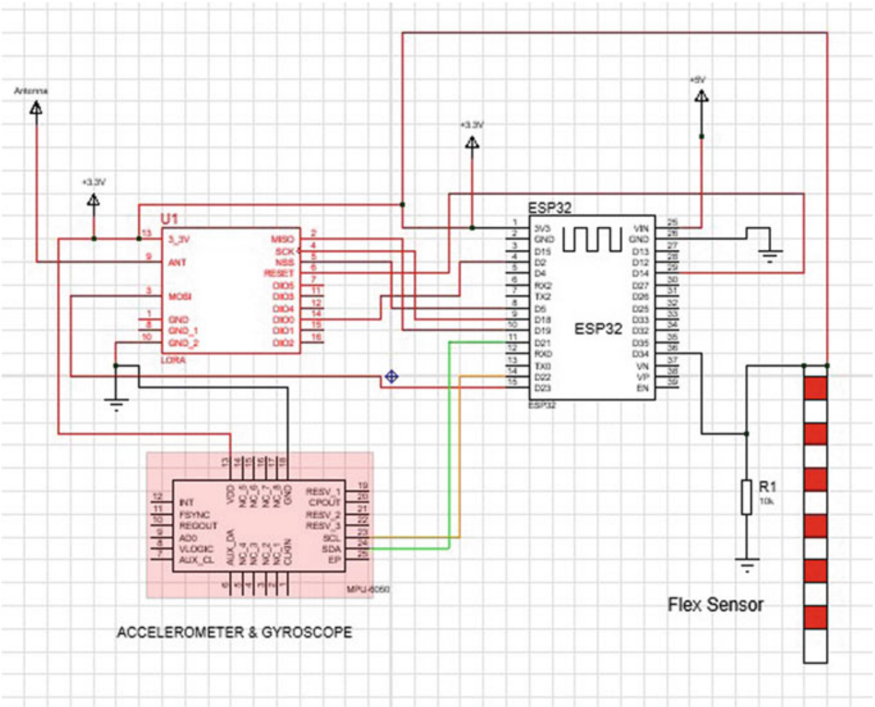


Fig. 20 Circuit diagram of the transmitter for the gesture control of robotic arm via LoRa technology

6.4 Flex Sensor Calibration and Calculation

Figure 27 shows the flex sensor resistance on the multimeter at its default state and when it is bent ranging from 6 to 10 kΩ.

6.5 Transmitter System

Several angles of the hand gesture of transmitter system are shown below consisting of the flex sensor, LoRa module, ESP32, MPU6050 accelerometer and gyroscope.

6.6 Receiver System

The receiver system shows several angles of the arm replicating the gestures made at the transmitter end as shown below.

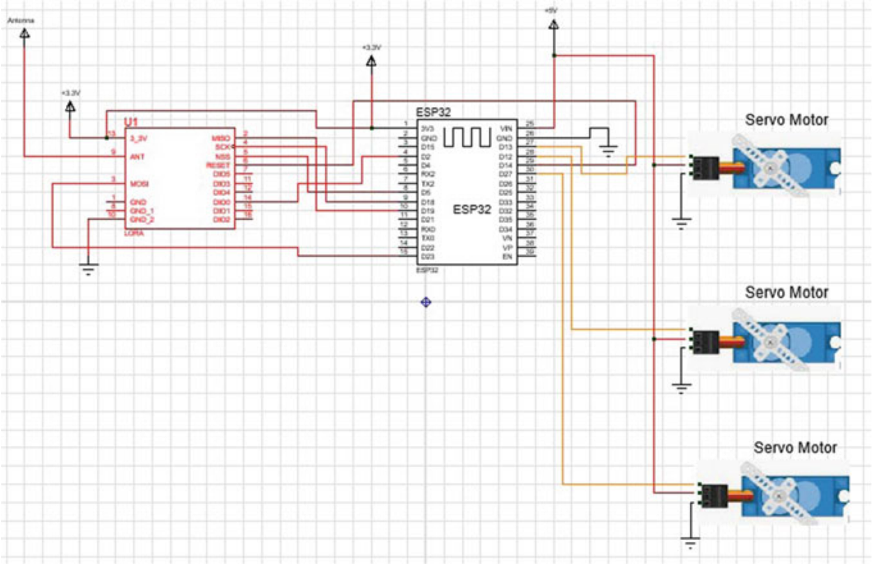
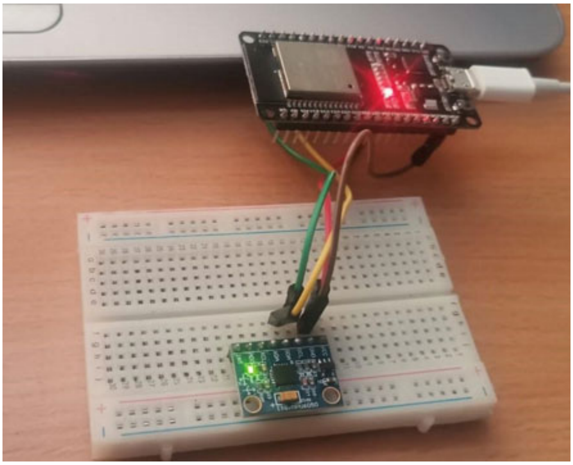


Fig. 21 Circuit diagram of the receiver of the gesture control of robotic arm via LoRa technology

Fig. 22 Breadboard simulation of mpu6050 with ESP32



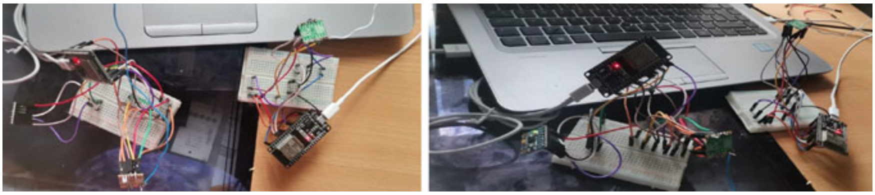
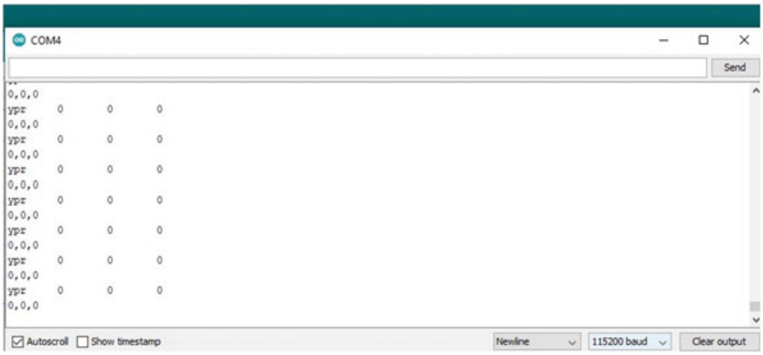


Fig. 23 Breadboard simulation of the LoRa (transmitter and receiver) interfaced with mpu6050 accelerometer and gyroscope



```
0,0,0
ypr     0       0       0
0,0,0
ypr     0       0       0
0,0,0
ypr     0       0       0
0,0,0
ypr     0       0       0
0,0,0
ypr     0       0       0
0,0,0
ypr     0       0       0
0,0,0
ypr     0       0       0
0,0,0
```

Fig. 24 Serial monitor of mpu6050 at default state

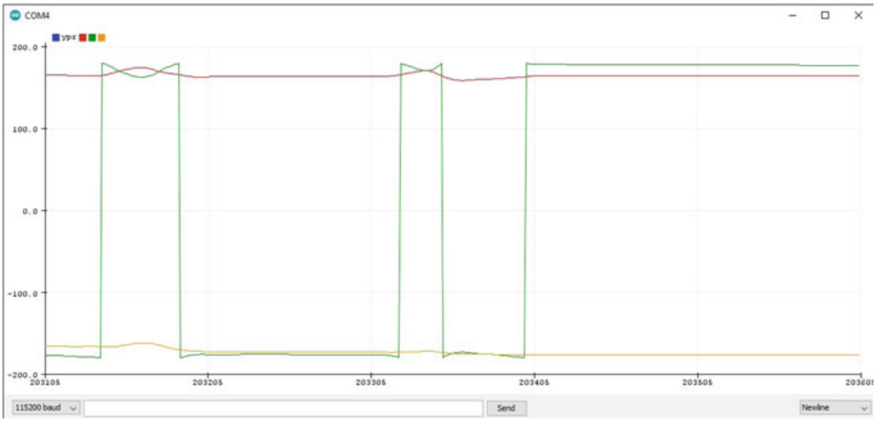


Fig. 25 Serial plot of mpu6050 tilted in the pitch axis

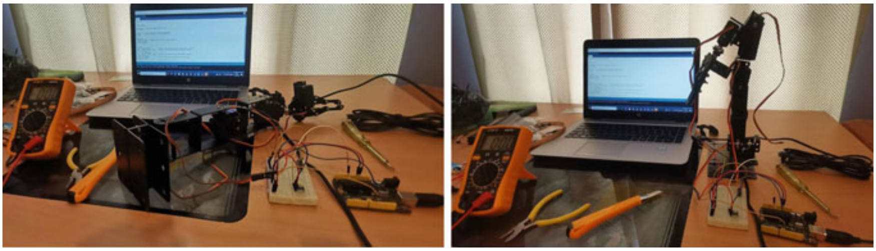


Fig. 26 Servo calibration of prototype using potentiometer

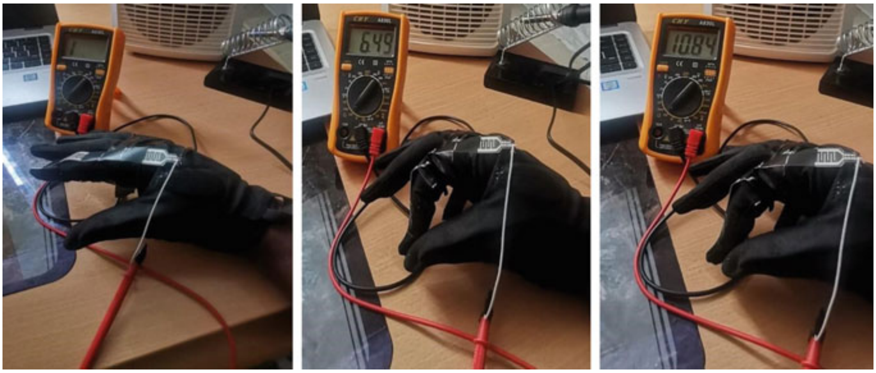


Fig. 27 Flex sensor resistivity on multimeter

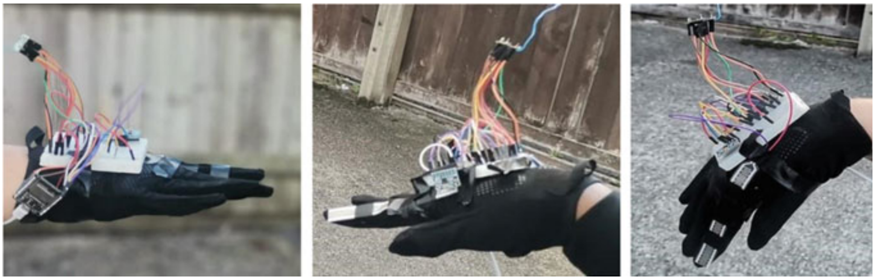


Fig. 28 Transmitter system showing different angles of hand gestures

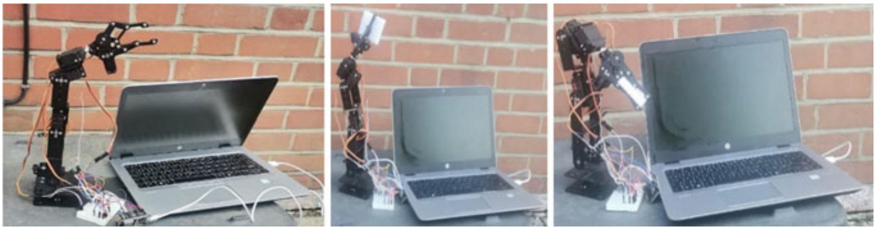


Fig. 29 Receiver systems showing different angles of the robotic arm

6.7 Transmitter and Receiver System

Figure 30 shows both the transmitter and receiver systems with the receiver replicating several arm movements of the gesture being made on the transmitter.

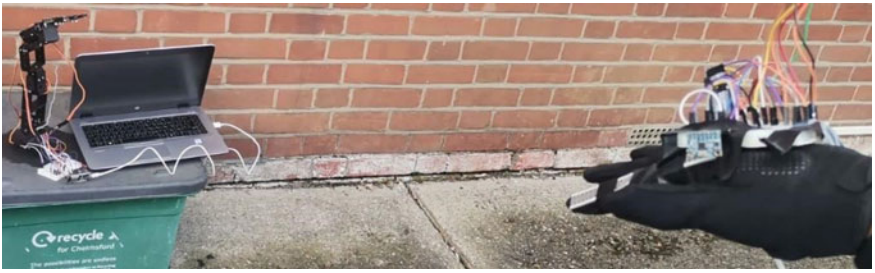


Fig. 30 Transmitter and receiver systems showing different angles of gestures

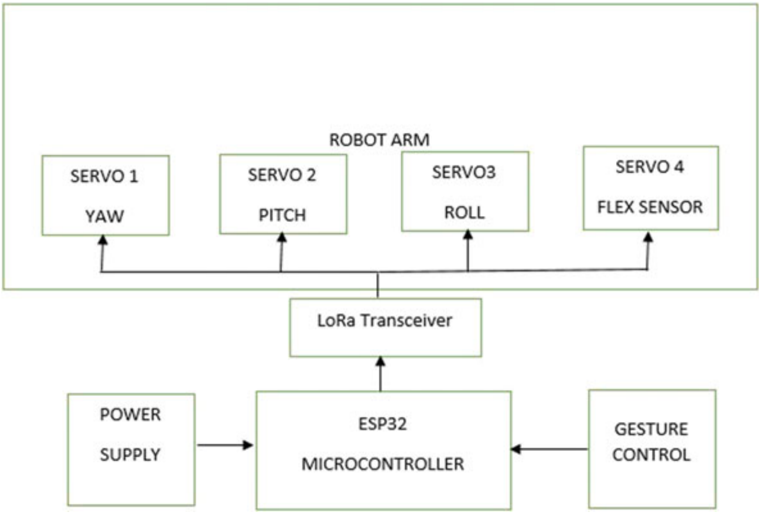


Fig. 31 Block diagram of the microelectronic unit and the servo motors embedded in the robotic arm

6.8 LoRa Spread Factor, Bit Rate and Data Range

LoRa technology is based on Chirp Spread Spectrum (CSS) technology. The chirps known as symbols are the carrier of data. The chirp rate is governed by the spreading factor, which also governs the data transmission speed. A higher data transmission rate results from faster chirps, which are caused by lower spreading factors. Spread factors used by LoRa range from 7 to 12. The time on air for SF7 is the shortest; SF12 will be the longest. Each increase in spreading factor doubles the length of time required to transmit a certain quantity of data while also expanding the possible receiving area. Even with relatively little data sent, a spreading factor of 12 already extends the broadcast beyond one second, increasing energy usage. Consequently, sending regularly must be carefully evaluated, and the amount of data sent should be kept to a minimum.

Depending on where you are in the world, LoRA employ one of three frequency bands: 433, 868, or 915, which are unlicensed but subject to strict regulation. 868 MHz is rather popular across Europe and was used in this paper. Even though the frequency is unlicensed, it is strictly regulated in terms of power and duty cycle (how much time is allowed to be spent "on air") [8].

6.9 Mode of Operation

The mode of operation of the gesture control of robotic arm via LoRa technology is basically grouped into two units—the transmitter and the receiver units. The transmitter unit consists of the mpu6050 accelerometer and gyroscope, flex sensor, LoRa module and the esp32 microcontroller while the receiver unit consists of the LoRa, the robotic arm which is made up of servos and the esp32 microcontroller. When a gesture is made on the wrist, the wrist orientation is captured by the gyroscope in the direction of yaw, pitch and roll while the finger movement is captured by the flex sensor that is attached to that particular finger. The mpu6050 and flex sensor replicate the hand movement and the mpu6050 is integrated to the MCU using inter-integrated circuit, I2C. The two parameters from the MCU which are pitch and roll are responsible for the control of the servos. These parameters (wrist orientation and finger movement) which are been sent from the transmitter are to control the robot arm in which two of the servos will be working in the direction pitch and roll in degrees, while the last servo will be controlled by the flex sensor which is responsible for picking an object. The flex sensor works in such a way that increase in voltage will cause an increase in resistance which activates the microcontroller at the transmitter unit to send a signal to the microcontroller at the receiver end via LoRa, thus activating the servo to grab an object based on the change in resistance associated with the degree at which the finger bends. This change in resistance is represented as a voltage but will be marked in angles at the receiver end because servo motors works in angles, 0–180°. LoRa communicates with the esp32 via serial peripheral interface, SPI. LoRa has channels whereby they can broadcast at a particular frequency for effective communication between the transmitter and the receiver. For this research, the transmitter and receiver frequency was set to 868 MHz which is the LoRa frequency for United Kingdom.

7 Conclusion

This study investigates a LoRa-based gesture control of a robotic arm created and developed for remote robot control. This approach has proven beneficial in terms of cost, range, and battery longevity in low- and lower-middle-income countries where internet connectivity is still patchy, particularly in rural areas with no power supply. It was observed that for LoRa to work effectively, the transmitter and receiver antennas must communicate at a line of sight. For the antennas to communicate over a long distance, their frequencies must match or be in sync with the frequency of the LoRa module. One of the problems encountered during the course of this project was "latency". LoRa has a very tiny data bandwidth, allowing only very short data transfers, and because of its low bit rate, LoRa will function more efficiently in transmitting data to a node or end point with a long time interval, as it cannot be utilised for real-time applications. This limitations of LoRa should be addressed and considered to match various use cases for LoRa before it can be adopted and if LoRa must be used, then a very high clocking microcontroller must be used to minimise latency as much as possible. Hence, a high frequency microcontroller is needed to handle it such as a 32–64 bit architecture with a high processor. The MPU6050 accelerometer and gyroscope used in this paper has a very high clock rating with a baud rate of 11,520 bits per seconds which needs a microcontroller with a high processing speed hence the choice of ESP32 which has a processing speed is 240 MHz. LoRa would function better in battery operated systems and thus the choice of LoRa in any wireless communication should be carefully selected in along with 4G, 5G, and other wireless modules that can transmit at a larger bandwidth and bitrate.

References

1. Ahmad KA, Segaran JD, Hashim FR, Jusoh MT (2018) LoRa propagation at 433 MHz in tropical climate environment. J Fund Appl Sci 9(3S):384–394. https://doi.org/10.4314/jfas.v9i3s.31
2. Aljundi L (2022) Using the Arduino software (IDE). [online] Available at: https://docs.arduino.cc/learn/starting-guide/the-arduino-software-ide [Accessed 1 Sep 2022]
3. Andrade RO, Yoo SG (2019) A comprehensive study of the use of LoRa in the development of smart cities. Appl Sci 9(22):4753. https://doi.org/10.3390/app9224753
4. Augustin A, Yi J, Clausen TH, Townsley WM (2016) A study of LoRa: long range & low power networks for the internet of things. Sensors MDPI 16(9):1466–1483
5. Babiuch M, Foltynek P, Smutny P (2019) Using the ESP32 microcontroller for data processing. In: Proceedings of 20th international carpathian control conference (ICCC) 2019. Krakow – Wieliczka, Poland, pp 88–93. https://doi.org/10.1109/carpathiancc.2019.8765944
6. Bahashwan AA, Anbar M, Abdullah N, Al-Hadhrami T, Hanshi SM (2020) Review on common IoT communication technologies for both long-range network (LPWAN) and short-range network. In: Saeed F et al (eds) Advances in Intelligent Systems and Computing. Springer, Singapore, pp 341–353
7. Bouteraa Y, Ben Abdallah I (2017) A gesture-based telemanipulation control for a robotic arm with biofeedback-based grasp. Indust Rob: Int J 44(5):575–587. https://doi.org/10.1108/ir-12-2016-0356
8. Brink H, van den (2019) Low power IoT devices and the possible use case in the grid. [online] Medium. Available at: https://harmvandenbrink.medium.com/low-power-iot-devices-and-the-possible-use-case-in-the-grid-4c3261527afb [Accessed 6 Jan 2023]
9. Chanda P, Mukherjee PK, Modak S, Nath A (2016) Gesture controlled robot using Arduino and Android. Int J Adv Res Comput Sci Softw Eng 6(6):227–234

10. Circuits Today (2016) Proteus PCB design and simulation software – introduction. [online] Available at: https://www.circuitstoday.com/proteus-software-introduction [Accessed 1 Sep 2022]
11. Components101 (2018) Flex sensor. [online] Available at: https://components101.com/sensors/flex-sensor-working-circuit-datasheet [Accessed 19 Jul. 2022]
12. Daud S, Yang TS, Romli MA, Ahmad ZA, Mahrom N, Raof RAA (2018) Performance evaluation of low cost LoRa modules in IoT applications. IOP Conf Ser: Mater Sci Eng 318(012053):1–11. https://doi.org/10.1088/1757-899x/318/1/012053
13. Electrical4U (2020) What is a Servomotor? [online] Available at: https://www.electrical4u.com/what-is-servo-motor/ [Accessed 22 Jul 2022]
14. Elektor Store (n.d.) RFM95 Ultra-long LoRa transceiver module (EU868). [online] Available at: https://www.elektor.com/seeed-studio-rfm95-ultra-long-lora-transceiver-module-eu868 [Accessed 23 Jul. 2022]
15. ElProCus (2019a) Flex sensor: pin configuration, working, types & its applications. [online] Available at: https://www.elprocus.com/flex-sensor-working-and-its-applications/ [Accessed 19 Jul. 2022]
16. ElProCus (2019b) Gyroscope sensor-working, types & applications. [online] Available at: https://www.elprocus.com/gyroscope-sensor/ [Accessed 20 Jul 2022]
17. Feng X, Yan F, Liu X (2019) Study of wireless communication technologies on internet of things for precision agriculture. Wirel Pers Commun 108(3):1785–1802. https://doi.org/10.1007/s11277-019-06496-7
18. Garg P, Patel M, Verma H (2022) Gesture controlled robot with robotic arm. Int J Res Appl Sci Eng Technol 10(5):2139–2146. https://doi.org/10.22214/ijraset.2022.42767
19. Gunawardane H, Medagedara N, Madhusanka A (2017) Control of robot arm based on hand gestures using leap motion sensor technology. Int J Rob Mech 3(1):7–14. https://doi.org/10.21535/ijrm.v3i1.930
20. Hameed S, Ahson Khan M, Kumar B, Arain Z, Hasan M (2017) Gesture controlled robotic arm using leap motion. Indian J Sci Technol 10(45):1–7. https://doi.org/10.17485/ijst/2017/v10i45/120630
21. Kazeem OO, Akintade OO, Kehinde LO (2017) Comparative study of communication interfaces for sensors and actuators in the cloud of internet of things. Int J Internet of Things 6(1):9–13. https://doi.org/10.5923/j.ijit.20170601.02
22. Kedar SF, Abdullah Sudhindra F, Annarao SJ, Vani RM, Motgi BS (2017) Development of Zigbee based tele operated multipurpose robotic arm with hand gesture recognition. Int J Mech Eng Technol 8(8):1275–1286. [online] Available at: http://iaeme.com/Home/issue/IJMET?Volume=8&Issue=8
23. LoRa Alliance (2015) White Paper: a technical overview of Lora and Lorawan. San Ramon, CA, USA: The LoRa Alliance
24. Madaan A, Bansal S, Sahu A, Kidwai F (2020) Peer to peer communication in GUI interface using Lora technology. Proc Comput Sci 173:299–304. https://doi.org/10.1016/j.procs.2020.06.035
25. Mahmoud MS, Mohamad AAH (2016) A study of efficient power consumption wireless communication techniques/modules for internet of things (IoT) applications. Adv Internet of Things 06(02):19–29. https://doi.org/10.4236/ait.2016.62002
26. Meyer A (2020) Using gyroscopes to enhance motion detection. Valparaiso Univ College Eng Student Trade J. [online] Available at: https://scholar.valpo.edu/cgi/viewcontent.cgi?article=1013&context=stja [Accessed 20 Jul. 2022].
27. Mohan A, Priyadarshinhini R (2020) Gesture controlled robot using accelerometer. Int J Eng Adv Technol 9(5):1241–1245. https://doi.org/10.35940/ijeat.e1057.069520
28. Ould S, Bennett NS (2021) Energy performance analysis and modelling of LoRa prototyping boards. Sensors 21(23):7992. https://doi.org/10.3390/s21237992
29. Passaro VMN, Cuccovillo A, Vaiani L, De Carlo M, Campanella CE (2017) Gyroscope technology and applications: a review in the industrial perspective. Sensors 17(10):2284. [online] https://doi.org/10.3390/s17102284

30. Rakesh HK, Shivashankara BS (2016) Wireless robot control with robotic ARM using MEMS and Zigbee. Int J Adv Netw Appl Spec Issue 205–209
31. Rathika PD, Jai Gowtham S, Aravinth Kumar T, Shri Ram S (2021) Gesture based robot arm control. Nat Volatiles Essent Oils 8(5):3133–3143. [online] Available at: https://www.nveo.org/index.php/journal/article/view/893/819 [Accessed 17 Jun 2022]
32. RF Wireless World. (n.d.) LoRa wireless transceiver. [online] Available at: https://www.rfwireless-world.com/ApplicationNotes/LoRa-transceiver.html [Accessed 23 Jul 2022]
33. Rogalski A (2019) Infrared and terahertz detectors, 3rd edn. CRC Press, Taylor & Francis Group, Boca Raton, Fl, p 929
34. Satheeshkumar R (2020) Real time robotic arm control using human hand gesture measurement. J Adv Res Dyn Control Syst 12(SP4):984–996. https://doi.org/10.5373/jardcs/v12sp4/20201571
35. Semtech Corporation (2019) LoRa® and LoRaWAN®: a Technical overview. [online] Semtech, Camarillo, CA, USA: Semtech Corporation, pp 1–26. [online] Available at: https://lora-developers.semtech.com/uploads/documents/files/LoRa_and_LoRaWAN-A_Tech_Overview-Downloadable.pdf [Accessed 23 Jun 2022]
36. Shifas PS, Sharmishta PK, Sravan Sankar PP, Shereena ER, Binish MC (2020) Gesture based wireless mobile robotic arm using flux sensor. Int J Adv Res Innov Ideas Educ 6(3):243–247
37. Sreeharsha D (2020) Gesture control robotic arm. Mech Eng Res 9(2):51. https://doi.org/10.5539/mer.v9n2p51
38. Teja R (2021) Introduction to ESP32 microcontroller. [online] Available at: https://www.electronicshub.org/getting-started-with-esp32/ [Accessed 13 Aug 2022]
39. Ugale A, Chandwadkar DM (2016) Overview on latest gesture controlled systems for robotic arm. Int J Comput Appl 135(1):29–31. https://doi.org/10.5120/ijca2016908309
40. Yang (2019) How does lora sensor send and receive data. [online] Available at: https://www.mokosmart.com/how-does-lora-sensor-send-and-receive-data/ [Accessed 23 Jul 2022]

Safety and Security Issues in Employing Drones

Durga Prasad Srirangam, K. Hemalatha, Ashok Vajravelu, and N. Ashok Kumar

Abstract The use of drones has been steadily growing over the past few years, not only in a variety of businesses and governmental organizations but also among private individuals. This is due to the rapid deployment of drones for a variety of applications, which can be accomplished by merely attaching the application-specific devices to drones, which are typically controlled by a remote or a smartphone. However, the breakthroughs that have been made in the use of drones have also opened up security challenges. In many applications, the orders that are sent to the drones and the data that is transmitted from the drones are not encrypted. As a result of the fact that drones are also used for illegal and criminal activities by bad actors, it is necessary to add technology for attack detection, protection, and preventive countermeasures in drones, in addition to regulation on the usage of drones through law enforcement by the government agencies. In this chapter, we will analyze the exploiting of drone vulnerabilities such as GPS spoofing, Downlink intercept, and Data exploitation. Additionally, we will examine how to neutralize threats and countermeasures that should be addressed for the safety of the drones.

D. P. Srirangam
Department of CSE, Baba Institute of Technology and Sciences, Visakhapatnam, Andhra Pradesh, India
e-mail: prof.srirangam@gmail.com

K. Hemalatha
Department of Electronics and Communication Engineering, Kongu Engineering College, Erode, India
e-mail: khemalatha.ece@kongu.edu

A. Vajravelu (✉)
Department of Electronics, Faculty of Electrical Engineering, Universiti Tun Hussein Onn Malaysia, Johor, Malaysia
e-mail: ashok@uthm.edu.my

N. Ashok Kumar
Department of ECE, Mohan Babu University (Erstwhile of Sree Vidaynikethan Engineering College), Tirupati, Andra Pradesh 517102, India
e-mail: ashoknoc@gmail.com

H. Jahankhani and A. El Hajjar (eds.), *Wireless Networks*, Advanced Sciences
and Technologies for Security Applications,
https://doi.org/10.1007/978-3-031-33631-7_4

Keywords Drones · Security · Unmanned aerial vehicle (UAV) · Jamming attack · Spoofing attack · Data interception attack · KeyLogging attack · MSG injection attack · Eavesdropping attack

1 Introduction

UAVs Security Issues

As a result of recent improvements in technology, unmanned aerial vehicles (UAVs) are now capable of carrying out critical, difficult, and intricate missions. Because of this, they have a lot of security problems, which leaves them vulnerable to attacks that might be quite damaging. Additional attacks are carried out in an effort to gain control of the UAV or to destroy it. The severity of the repercussions is proportional to the nature of the attack. There are not many tools that might be used as hacking tools [1]. As an element of the Internet of Things ecosystem, researchers began beefing up the security of unmanned aerial vehicles (UAVs). In general, it necessitates the efficient construction of a variety of approaches connected to the many IoT deployment and connection regions. In this part, we focus on security and privacy concerns associated with UAVs, as well as attacks carried out by UAVs. This section discusses the use of unmanned aerial vehicles (UAVs) to launch system attacks as well as UAVs charging system attacks. In this section, we also explain the reasons that led to our work on battery depletion attacks against UAVs. The research findings that were discussed before, which will be used in the next subsections, indicate a variety of worries and problems with UAVs. These study studies evaluated a variety of distinct forms of attacks, in addition to several outcomes.

UAVs Security Concerns

When dealing with any form of digital technology, the most important thing you can focus on is keeping yourself safe. To ensure the safety of the UAV system, it is essential to perform the necessary preventative measures. UAV systems are vulnerable to cyberattacks and the deterioration of their functions, both of which have a direct impact on the key contributor. Therefore, attacks on the system or failures in the system lead to significant problems. Park et al. [2] discusses a variety of security concerns in further detail. In these kinds of situations, the attacker causes disruption to the availability, integrity, and confidentiality of the drone. Due to the fact that private information has been revealed, it is now quite easy for a competitor to establish the sensitive information that pertains to the UAV. In addition, the authors in [3] demonstrated that UAV networks are vulnerable to attacks and sensor flaws, proving that UAV networks are sensitive. It is possible for the adversaries to gain access to the communication lines of the UAV, which would then enable them to connect and take control of the UAV. Canis [4] highlighted a variety of different kinds of attacks and categorized them into two broad sectors based on the components of UAVs that were targeted and the attack route. Canis [4] also highlighted a number of different kinds of attacks. There are two types of vector attacks: those that are carried out physically and those that are carried out remotely. A swarm of unmanned aerial vehicles (UAVs) was disrupted during strikes staged at Russia's Hmeimim airfield in 2019. This is only one example of the myriad effects that might result from security flaws. 13 hostile fixed-wing unmanned aerial vehicles (UAVs) were sent to attack the airbase itself. It has expanded throughout a broad variety of areas in Syria, including the Latakia Governorate, the town of Hmeimim, which is located close to Latakia, and a range of 250 km. Despite this, the vulnerabilities that are already there allow attackers the opportunity to become more skilled and proactive in their activities.

1.1 Attacks on UAVs-Based Systems

The systems that are used by UAVs are comparable to those that are used by other IoT systems that are currently in use. They must utilize a centralized server in order to store data and connect to a network in order to carry out wireless communication. In the event that the system is attacked, the mission of the UAV will be terminated, which is a vulnerability in the security. The primary purpose of attacks against systems based on UAVs is to either crash the system or modify the data that is stored on the system. There are a variety of cyberattacks that may target systems based on UAVs, including the following:

Jamming attack: GPS Jamming, Control Stream Jamming, and Data Stream Jamming are the three forms of jamming that are associated to this attack, which comes in at number two on the list of most prevalent attacks [1, 4–8]. The opponents look for Radio Frequency (RF) signals broadcasting in the same frequency range as the drone that is being attacked, and then transmit transmissions that are incompatible with those signals. The attack is organized utilizing nodes that are based on a wireless channel concept in order to accomplish range-based localization. The antenna on the jammer may receive signals coming from any direction. This antenna will transmit radio frequency signals in a manner that is uniformly radiated in all azimuthal directions. An research that was reported in shows that it is not always safe to utilize specific transmitters in order to intercept remote control signals. This is the case even if the jammer is located far closer to the UAV than the operator who is in charge of commanding it using the remote controller. An anonymous individual performed a GPS Jamming attack on May 10, 2012, in South Korea, while testing [4]. This attack was reported to have taken place. During the attack, a rotor based on an Austrian unmanned aerial vehicle known as the Schiebel Camcopter S-100 collided with the ground control station, causing two remote pilots to sustain injuries.

Spoofing attack: The [9] attack is comparable to the jamming attack; however, it has a greater degree of intricacy. Instead of seeking to disrupt existing signals, the adversary will generate false signals in a random but controlled fashion. These signals will then counterfeit and fake the GPS position. As a result, the drone's behavior will be altered as a result of these phony signals, and it will be guided to a destination that is distinct from the primary course that was planned. It culminates in the victim being bound with bogus data for their latitude and longitude. The process is carried out invisibly, without causing any disruption to the normal functioning of the GPS.

Data Interception attack: The [10] Intercept Data attacks constitute a breach of confidentiality and may have far-reaching repercussions for the drone in question. The exploit gives unauthorized attackers the ability to access data via an unauthorized file reader when the system is in contact, while it is in flight, or while it is at rest. A video containing the stolen information was found by the American military defense in Iraq on the laptop of an activist who had been taken into custody. This led to the identification of a data interception attack in [4]. According to this information, the footage was obtained by utilizing SkyGrabber to intercept the unencrypted communication lines that existed between the several flying UAVs. Consequently, data interception attempts will be carried out whenever a non-secure and easily accessible wireless transmission is used. It is difficult to spot an attack of this kind.

KeyLogging attack: A form of monitoring software is designed to record keystrokes and steal data from a computer. Malicious software that logs keystrokes has emerged on the scene as a form of tracking spyware that collaborates with legitimate software to share resources. Creech Air Force Base in Nevada was the location where [11] discovered a keylogging attack that was carried out against US Predator. It was launched once a connection had been made between the Predator and Reaper ground control stations and a removable hard drive. This will result in the capture and transmission of sensitive information.

MSG Injection attack: This type of attack is known as an integrity attack, and it can be carried out through remote access if the targets are [5, 10]. The process of immunizing genuine faux communications with malicious payloads is known as injecting a malicious payload. The messages are backed by a structure that is an exact replica of the structure of the authentic message. They use a second phony UAV to divert the attention of the GS system as well as the UAV. According to this, the process of deleting messages and the process of modifying messages both use the same injection technique. Injecting malicious software, such as viruses, worms, or Trojan horses, will therefore result in the modification of sensitive data. Specific system technologies, such as StackGuard and StackOFFence, are used to protect unmanned aerial vehicles (UAVs). The first instrument is an automatic adaptive detection and prevention technique, while the second instrument is an attack mitigation mechanism. Both instruments work together to protect against attacks.

Eavesdropping attack: A stealthy and unobtrusive attack on the secrecy of the UAV is represented by the coordinates [5, 7, 12, 90]. It is being construed as an illegal real-time eavesdropping of the communication channels being conducted by the party. Without disrupting the transmission of the network, a hostile vehicle eavesdrops on the conversations taking place between the UAV entities. During this attack, sensitive data is gathered without compromising the quality of the signal received by a genuine receiver. Therefore, listening in on a private network is a breach of privacy. Eavesdropping is referred to as a sort of man-in-the-middle attack. On the other hand, the attacker creates a second network that is associated with the victim and sends messages as if they are chatting with a legitimate person. This makes it seem as if the victim is communicating with a third party.

Distributed denial of service (DDoS) attack: Sending an excessive number of requests during the mission [5, 13] is a popular kind of direct attack that might hinder the availability of the UAV. Through the use of data connections, the adversary might provide erroneous data in the form of continuous requests. As a consequence of this, the ever-increasing volume of network traffic will result in the communication channel becoming overloaded, which will prevent the connection from being established.

Sybil attack: The condition arises when an adversary builds several nodes in the network that are distinct from one another using either stolen or manufactured identities. This action will increase the likelihood that a hostile entity will be able to intercept a routing message and manage the Peer to Peer (P2P) overlay network. Through the use of threats, the adversary may achieve an excessive amount of authority and exert control over the system's performance in all aspects.

Blackhole attack: The sort of attack that [14] falls under is referred to as a denial of service attack, and it is classified as a form of lethal attack. In order to get a route that will continue to flow to the target node, a malicious node will pull all data packets by offering incorrect information in order to gain the route. The information packets are sent to the black hole by the source node, rather than being sent to the node that is designated as the destination. If the nodes are given inaccurate information on the routing data, the protocol for determining routes will be significantly disrupted. As a consequence of this, the adversary will access these packets while the data is being sent via the black hole. The attacker will advertise a large number of false paths in the hope of attracting data traffic. During this specific attack, a directed pull attack will be initiated, and all routing data will undergo a full transformation.

Grey hole attack: The [15] may change their mindset from one of authenticity to one of a sinkhole. A similar idea has been proposed for the grey hole, in which malevolent nodes block the transit of data across the network by broadcasting incorrect routing information. Because of this, it is an expansion of the attack on the black hole. The node might function in either a harmful or a regular state depending on how it was configured.

Fake information dissemination (FID) attack: This event [5] takes place anytime the intruder sends out a bogus GPS signal in order to change the course of the UAV and get data via impersonating. An attacker may carry out a FID attack on a network by creating forged authentication messages by making use of legitimate routing packets that have been obtained from malicious devices. The malicious node's fake injection will result in the destruction of the routing table used by the other nodes. As a direct result of this, the nodes will suffer a loss of packets due to an error in the routing. In addition to that, the pace at which packets are sent will slow down.

Replay attack: A [10, 13] attack is a kind of cyber warfare that is analogous to a denial of service attack and involves either eavesdropping on legitimate data transmissions or slowing them down in order to retransmit altered data in lieu of an intercepted message without first decrypting it. Eavesdropping, keylogging, and notably Sybil attacks are examples of the kind of cyberattacks that have the potential to completely ruin the availability of data throughout the whole system.

Attacks on the UAVs-Charging Systems

A comparable embedded power mechanism is the UAVs charging system [16]. The charging mechanism of the UAV is susceptible to attacks, which might result in the destruction of the whole UAV. These kinds of problems have the potential to halt the functioning of the UAV. Recently, experts have been working toward the goal of improving the safety of the UAV charging system. The author of the work cited in [17] constructed a model that includes an analysis of energy requirements. The algorithm will make an accurate projection of the demands that will be made on the drone based on the amount of energy that will be required to complete the permitted mission. A direct result of this is that this model will be aware of attacks, which will have the effect of lessening the vulnerability of the charging system. Temperature and actual discharge rate are only two of the many factors that have a substantial influence on the operation of the charging system. Because of this, the resistance of the battery as well as the power supply will be altered. In addition, this typical system is vulnerable to a variety of attack patterns, which presents a danger. In addition, defects in voltage control [18] may generate a wide variety of problems for the charging systems of UAVs. Because of this vulnerability, customers might be overcharged or undercharged.

Additionally, it shortens the lifespan of the battery and causes harm to the contributing unit. The unmanned aerial vehicle (UAV) was the victim of an attack in [8], during which the attacker created bogus requests that caused damage to the charging system. It led to a problem with an excessive amount of energy as well as an excessive decrease in voltage. The charger control unit could need to be tampered with, or the data sources might need to be manipulated, in order to achieve this goal. For instance, [8] uncovered a variety of charging system potential concerns, including as the WPT's ineffective functioning. In addition, the authors investigate the attacks that are designed to control the charging process in [19]. The malicious software takes over and changes the software that is utilized by the rapid-charging station when an unmanned aerial vehicle (UAV) is linked to the station. The attack will transform the unmanned aerial vehicles into high-speed chargers and will cause damage to the charging infrastructure. This malicious power strike is sneaky and swift, with little warning or opportunity for resistance. It has the potential to alter the configuration and add more work up to the point where it causes harm to the whole system. As a result, any unmanned aerial vehicle (UAV) that is attached to or linked to the charging station will constitute a threat.

Attacks that Result in UAV Battery Depletion

Depletion of Battery (DoB) [20] is a particular kind of attack that might be used to target UAVs and induce increased power consumption on a variety of different levels. Because of this, failure is difficult to anticipate, and when it does happen, the damage may not be able to be repaired due to the complexity of the situation. According to the first notification, rapid battery depletion may be identified if it was found that there was an unanticipated drop in the amount of remaining battery capacity that was observed between follow-up visits. As a consequence of this, these types of attacks are the most typical reasons for the failure of a mission, and they have the ability to cause a loss of connection as well as a crash. During the course of the attack, many sensors will fail, and several functionality will become less effective until they are completely disabled. The DoB has a much increased risk of an electrical component failing, which will result in a rapid discharge of the battery. UAVs are particularly susceptible to DoB attacks due to the fact that these attacks may take advantage of the UAV's autonomy, its physical motions in the surroundings, its wired and wireless communication channels, or all of these things concurrently. DoB allows the attacker to reveal the software and hardware computing units, as well as the data and physical architecture of the target unmanned aerial vehicle (UAV). Attacks that deprive the target of energy are similar to those that disrupt service (DoS) [21]. Attacks that use denial of service may hasten the discharge of a battery by up to 18.5% [21]. In addition, there is an attack known as Denial of Sleep (DoS) [13] that seeks to accomplish the same thing. It is predicated on limiting the amount of time the UAV spends in sleep mode in order to increase the amount of power consumption until the battery is completely depleted. In addition, the adversary modifies the charge parameter in order to carry out cross-layer attacks [13] in order to drain the UAV battery in an indirect manner. However, there are two different kinds of attacks that drain the battery:

Attacks without physical contact: This first kind encompasses attacks that do not need to have any kind of direct physical contact with the device. These are examples of attacks against wireless channels. Recent attacks are made up of two-channel kinds of energy crisis control systems each. They are known as the control data transmission channel and the GPS data transfer channel respectively. The transmission of GPS data is used in order to ascertain the geographical position of the UAV. As a result, the GPS channel is the focus of the attacker, who uses an Omni antenna to cause interference. The purpose of the attack is to either prevent the signals from reaching the receiving side entirely or to send them with incorrect locations. Additionally, when the UAV gets many commands, it may travel in a haphazard manner, which causes additional drain on the battery. The second channel is used to synchronize instructions with the UAV. These instructions may concern GPS data, network settings, or the overall state of the UAV.

Attacks with physical contact: This kind is discharged when the unmanned aerial vehicle (UAV) is in the standby state. The attack begins from several different entries based on this information, including the physical component, the USB interface, and the microcircuit. Additionally, the invader will compel the main rotors of the UAV to operate at full power and use more charge if they attach a physically enormous weight to the UAV in order to create an imbalance. Finn et al. [22] conducted an experimental investigation to investigate the effect that weight has on the amount of electricity used by UAVs. The first of two unmanned aerial vehicles (UAVs) utilized in the experimental setup had a total weight of 30 kg and 8 motors; the second UAV had extra payloads that brought the total weight up to 35 kg while maintaining the same number of motors. For each test, notes were taken on the movement sets of lifting, hovering, and landing that required the most power. The amount of electricity used is calculated depending on the rotational speed (RPM). According to the findings of this research, the values improved across the board in the subsequent test.

According to [23], there are two different methods that a UAV may be used to launch a denial of service attack:

- The attacker is continually sending requests by providing bogus communication packets in order to fool the target. As a consequence of this, the unmanned aerial vehicle (UAV) will need a percentage of additional energy for the authentication process in order to analyze each request, which will cause the battery to run down.
- By producing electromagnetic (EM) noise with the intention of causing a high mistake rate at the UAV. Because of this, there will be a rise in the total amount of retransmissions, which will result in an increase in energy usage. Because of the increasing noise, the UAV could be compelled to boost its transmission power, which would shorten the battery's lifespan.

There are many different things that may go wrong with a UAV's battery, including overcharging, which can cause the battery to boil, draining, leaking, improper setup, and using up all of the available energy. In addition, there are other contributors to the depletion of energy. For example, the research presented in [17, 24] analyzes the impact that elements such as payload, movement, hovering, communication, and speed have on the amount of energy that is expended. Last but not least, unless the battery of the vehicle is totally drained during the trip, there is a possibility that it will not have enough time to return to the base and efficiently perform its mission. As a result, the logistical operations of the infrastructure can experience a large amount of disruption.

Attacks Assessments of UAVs-Based Systems

A classification system for attacks using UAV-based systems is going to be presented in this part. These attacks are organized into four distinct groups, which are as follows:

1. Attacks directed against the fundamental software
2. Attacks on the monitoring systems
3. Attacks on the various avenues of communication
4. Incursions against the GPS channel.

Proposed taxonomy: The majority of UAV attack types may be categorized according to the kind of attacker, the offenses committed, and the aims of the attack. The modeled chain is an illustration of the series of attacks that are based on UAVs.

The actual act of attacking may be broken down into four distinct steps. An adversary equipped with a relative goal, attack vector, and the ability to define the attack entry. After then, it reaches an attack depth that was previously determined. Last but not least is the attack's effect, often known as the damage it does. This sequence lends credence to the taxonomy that was suggested. The taxonomy provides an overview of all the different types of attacks that may be mounted against the UAV-based system. Every strike is equipped with a unique set of behavior characteristics that are realized to target one or more layers. In particular, the attacker may take advantage of one or more vectors in order to carry out further attacks. These attacks have been categorized according to the preceding chain in order to provide answers to the following questions about their purposes:

- Attacker: Who exactly is the one doing the attacking?
- Attack Vector: What causes it to be activated? Which layer has it established a presence on? What really is the danger? Is it a direct attack, or is it being carried out by a distant auxiliary? Who or what exactly are the targets of the UAV's attacks?
- Attack Type: Describe the characteristics of the attack being made. Are there some attacks that are more specialized than others?
- Attack Offenses: Identifying Vulnerabilities That Were Targeted What were the weaknesses that were exploited? What kind of fallout will there be from the attack? In a manner that is more formal, each dimension of the taxonomy is defined as follows:

Attacker: Attacks may be carried out by a variety of persons or organizations, including terrorists, spies, thieves, and hacktivists, with the intention of achieving a variety of other objectives in a variety of attack locations and positions. Researchers looked at a variety of potential attacker situations for unmanned aerial vehicles (UAVs), including terrorist airstrikes, hijacking, and surveillance. Their findings may be found in [10]. In addition, the report disclosed that UAV thieves were responsible for a recent incident in which Iranian troops stole a US RQ-170 Sentinel. Hacking into unmanned aerial vehicles (UAVs) was done with the use of a software system called SkyGrabber [9]. There are several different UAVs hijacking software programs, such as SkyJack, which were designed to hack and operate the UAV wirelessly by using an autonomous middleware. In addition, the word "Terror by Joystick" that was thrown into the flight path of the airplane sheds light on the nefarious acts that terrorists have carried out using UAVs. As a result, criminals pose a risk that justifies the employment of UAVs to wreak havoc on society.

Attack Vector: Attacks may be conducted using a variety of vectors, such as a direct attack or a distant attack via medium entries. Attacks from a distance intercept data using an auxiliary tool, allowing them to be compromised by questionable internal processes. The control software, the sensors, the communication channels, and the GPS channel are the auxiliary that are being referred to here. These four are the primary targets that attackers aim at most of the time. The entities that are being attacked are the surface, also known as the element that is being targeted by an attack. This component is part of the basic system that the physical vehicle utilizes. Unmanned Aerial Vehicles (UAVs) have a dialogue with the world around them. As a consequence of this, it could take the form of an intrinsic component, a virtual or physical environment, or both.

Attack Depth: The severity of these dangers is determined by their characteristics, which place them into one of four distinct categories of attacks. The opponent intends to get intelligence by infecting the UAV with malware, exploiting it for the aim of acquiring information or anything familiar, intercepting its transmissions in order to break them, and authenticating itself. Threats to computer network security may use data in clandestine ways to accomplish their objectives without the awareness of system operators. The nature of the exploitation, such as injection or modification, may be used to categorize the different types of attacks [11]. In addition, fabrication is included as one of the typical specified methods of attacking authentication [10]. The most recent attack is a bait for the unmanned aerial vehicle (UAV) authenticity, which enables the attacker to get privileged access to the components in order to fabricate bogus information and deliver it to them. There are several various forms of attacks that may modify the content of the UAV or alter its decision-making in the event of specialized attacks.

Attack Offences: As a direct consequence of this, their data will be pilfered, altered, and corrupted. Other crimes can be committed as a result of these attacks, such as data theft, an authentication crime that involves cracking and stealing, and fuzzing, which is when criminals try to find zero-day exploits by using a technique called fuzzing. Because of this, they have the potential to cause fuzzing in the system by interfering with the process, the communication, and the functionalities. As a result, attacks based on UAVs are able to sneak up on targets through a variety of channels by utilizing a planned entry and fixed damage for exit.

Software-based attacks: The processing of data for a decision-making system is the responsibility of software based on UAVs [11]. It is in charge of regulating the sensors, as well as the protocols for navigation and communication, as well as connecting the various components. To a large extent, the base program is the one that is in charge of establishing the flight parameters. Attacks may easily be launched against these components. As a consequence of this, the software that runs the drone base does not have any stringent security features that prevent hostile applications from changing the data. There are many different kinds of software that may be used in attacks, such as the buffer overflow. It is software designed to target the operating systems of UAVs. The attacker searches for memory blocks and then populates those blocks with unnecessary data in order to squander the space that has been allotted for data. Because of this, the system will be forced to execute random codes, which will make it possible to manage and monitor these systems. In addition, other sophisticated attacks on the core program might potentially get critical data. For example, a Structured Query Language Injection, sometimes known as a SQL injection attack, is used against data-driven applications. In addition, some malicious actors choose to begin their attack on the embedded Software Defined Radio (SDR) boards because of the ease with which they may get access to these boards and the lack of protection they provide. In the end, foundation Software security flaws are continuously maintained owing to faults in the microcontroller system, with suitable authentication and permission assessment.

Attacks on the Sensors

The drone is equipped with a variety of sensors that are capable of carrying data and providing readings. Because of this, attackers see sensors as a potential target for their activities. They are using them as the attack surface in order to intercept from them. The data that is being delivered to these sensors is being corrupted as a result of these attacks. "Sensor input spoofing attack" was the name given by the intruders to the attack that they developed in and carried out using sensors. This exemplified the efficacy of attacks mounted against UAVs using the sensors. Additionally, Nichols et al. suggested a method through which the adversary sends bogus data to the drone by means of an onboard sensor in order to throw it off. In addition, in [13], the adversary interferes physically with the UAV sensors in order to disrupt their availability, and then they conduct a DDOS attack. Against the other hand, there have been no recorded attacks on sensors in the form of connected cameras to UAV [4]. However, research such as [11] has shown that the sensor may be protected to protect the data transfer inside the network.

Attacks the communication protocols: In most cases, ground control stations and unmanned aerial vehicles use distinct communication protocols. Micro Air Vehicle Link (MAVLink) protocol, UranusLink, and UAVCAN are the most important communication protocols. The following is a list of the vulnerabilities and failures that are associated with these protocols:

MAVLink: A library for marshalling data that was developed with the intention of establishing a lightweight message serialization mechanism. It has the highest level of support among its contemporaries. In addition to the fundamental ideas, this protocol suffers from a striking deficiency in the presence of structured references. In spite of the fact that certain dangers are there, there is no safeguard in place to ensure that the communications that are sent are accurate. In addition, the security surrounding the transmission of the communications is subpar. Because of this, it is necessary to strengthen the security of the end-to-end connection between the GCS and the UAVs.

UranusLink: Is a protocol that handles data in packets and can produce both unreliable and reliable services. This protocol is very different from the other protocols already in use for interacting with UAVs. It includes the checksum that can be used to verify that the original message was transmitted successfully and that it was received. However, it was unable to check whether the message had been altered in any way. As a consequence of this, a straightforward checksum does not guarantee the secrecy or integrity of the data. On the other hand, there is a lack of sufficient experimental evidence to support the UranusLink hypothesis.

UAVCAN: Is a protocol for controller area network that is based on the CAN bus and is available as open source. Its purpose is to provide private communication while using reliable car networks. Due to the lack of shielding that the protocol offers, it is not advised for use in sensitive missions or on the system. 6.5. Attacks made against the GPS channels are used to carry out attacks on wireless networks, including GPS Jamming and GPS Spoofing. Emulators of computers were used in each of these most recent attacks. There is a variety of jammers available. First, there is the basic constant jammer, which sends out a signal of continual interference using the default amount of power. Additionally, a straightforward regular jammer that has a high-power transmission that is distributed in packets. The continual transmission may provide the impression of a higher capacity than it really has. The random jammer only makes sporadic transmissions, which brings us to our second point. Both high power and moderate power appraisals are problematic in their own ways. In addition, the complex jammer may be used to describe a reactive jammer. In this particular type of jammer, the signal won't be transmitted until the transmission target has first been established and then identified. In addition, the intelligent jammer is one that possesses prior knowledge of the leverage protocols and modulation that are currently being used. In conclusion, ensuring the safety of the GPS channels is very necessary for the UAVs to successfully complete the task.

GPS-Spoofing Attack Detection Technology

For Guidance, Navigation, and Control, Unmanned Aerial Vehicles (UAVs) of today mainly depend on the Global Navigation Satellite System (GNSS) (GNC). When it comes to the GNSS choices that are now accessible, the Global Positioning System (GPS) is the satellite navigation system that is most extensively adopted and used. Autonomous unmanned aerial vehicles (UAVs) are even more reliant on flying aids such as autopilots, navigational systems, and dynamic positioning systems than traditional UAVs. In addition to its well-known precise location function, the Global Positioning System (GPS) also provides time synchronization to an accuracy of around 10 billionths of a second by making use of the atomic clocks that are carried by the satellites themselves (Wei and Sikdar 2019). Time-sensitive systems, like synchrophasors found in power grid systems, use GPS time in order to conduct offline engineering assessments and synchronous state estimations [25]. All of these technologies have been developed with the presumption that the GPS services may be trusted (Bhatti and Humphreys 2017).

In order for unmanned aerial vehicles (UAVs) that rely on GPS to operate safely, the location information they receive must be precise, reliable, and continuous. However, a number of studies have demonstrated that it is possible to fake or disrupt GPS signals due to the inherent flaws and weaknesses that are present in the system. It is simple to interfere with GPS services by transmitting high-power jamming signals in the direction of the victim platform due to the low signal strength, which is approximately − 130 dBm. Because the civil GPS services do not have encryption or authentication mechanisms, it is simple to replicate or fabricate the satellite signals, which can then be used for the launch of sophisticated GPS spoofing attacks. This is because the signals can be easily replicated. In addition to this, the civil GPS services do not have any authentication mechanisms.

GPS spoofing is the process of recreating or falsifying the creation of the GPS signals in order to trick a particular GPS device or receiver by altering its Position, Velocity, and Timing (PVT) characteristics. This is done in order to mislead the device or receiver. This is done with the intention of tricking the GPS device or receiver that is in issue (Psiaki and Humphreys 2016). As a result of the spread of low-cost, user-tunable Software Defined Radios (SDRs) and online open source projects and tutorials for hobbyists and newcomers, it is now possible to launch GPS spoofing attacks against UAVs. This begs for more robust spoof-resilient safeguards to be included in from the beginning, especially for the sake of the safety of mission-critical aerial applications (Huang and Yang 2015).

If an attempt to spoof a drone's GPS coordinates is successful, the attack could result in the drone crashing or the flight path being altered, both of which are potentially disastrous outcomes. According to the findings of a number of studies, an adversary can force a GPS-guided drone to deviate from its course or even hijack it if the adversary is aware of the drone's current position and intended travel path (Noh et al. 2019). These findings were reached by Seo et al. and Noh et al., respectively. By using spoofing, it is possible to circumvent the safety feature known as "Geofencing," and as a result, the targeted drone may be coerced into flying in restricted airspace (Schmidt 2015). This weakness may be used by drug smugglers and others in order to violate regulated boundaries between prisons for the purpose of selling drugs and conducting unlawful surveillance (US National PNT Advisory Board 2018). If a military-grade unmanned aerial vehicle (UAV) that is armed is somehow stolen and then utilized by a terrorist group, the resulting devastation might be catastrophic (Fig. 1).

The Department of Homeland Security (DHS) carried out an unclassified test exercise on June 19, 2012 at White Sands Missile Range (WSMR) under the codename "GYPSY". This was the first time that it was proven that civil GPS systems are susceptible to spoofing attacks, and it was the first time that this vulnerability was demonstrated [25]. During that particular exercise, a GPS spoofing attack was carried out at a height of forty feet against the mini-drone known as "Hornet," which resulted in the manipulation of "Hornet's" perceived position and time. This attack was carried out at a height of forty feet. When an American RQ-170 Sentinel drone was successfully seized by the Iranian Army (Hartmann and Steup 2013), another significant GPS spoofing allegation was made against a military-grade UAV by the Iranian Army. On the other hand, the veracity of the allegation as well as the specifics of how the UAV was taken are not confirmed and are a source of controversy. In 2016, it was claimed that Mexican drug dealers and traffickers had deceived an unmanned aerial vehicle (UAV) belonging to the United States Customs and Border Protection agency via a spoofing attack on its GPS signal (Khan 2020). Additionally, comparable GPS-based spoofing attacks have also been proven in a number of other publications (Zheng and Sun 2020) against Hornet Mini, DJI's Matrice 100.

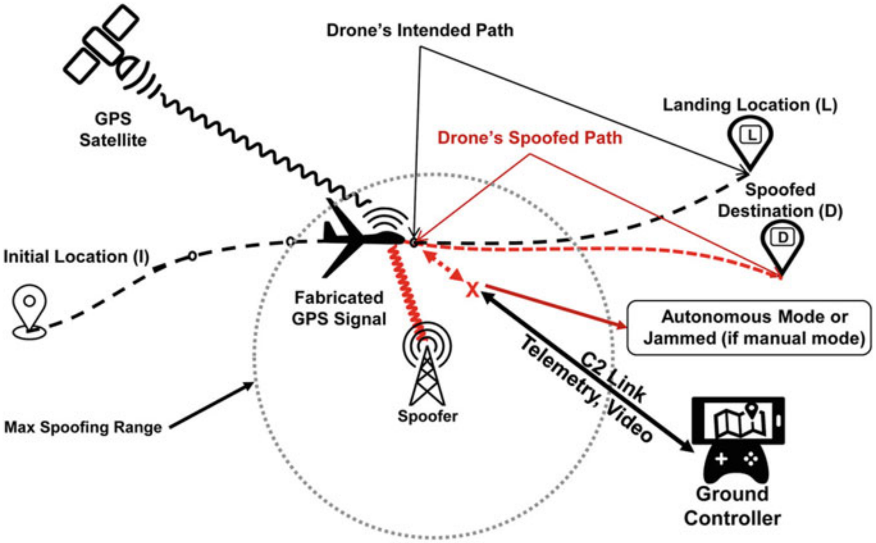


Fig. 1 GPS spoofing

1.2 Development of GPS Anti-Spoofing Technology Components for UAVs

In this section, we will talk about the internal architecture of a software package that is able to put our GPS anti-spoofing solution into action. This software package is capable of preventing spoofing by using our approach. The internal architecture is comprised on two primary parts, both of which were discussed before. They are a piece of software that can simulate attacks and another piece of software that can detect attacks (analyzer).

To begin, let's have a look at the overarching structure of the software application, which can be shown in Fig. 2.

The attack simulation software module on the left provides, as can be seen from the picture, the entire capability that enables an interchange of data with other modules. This is made possible by the module's provision of the leftmost slot. A database is also used to store the information that was obtained from the navigation system. The provision of extra redundancy requires that this step be taken. The data are not lost in the event that there are issues with communication between the attack simulation software module and the attack detection module (analyzer). The green square represents the interface that allows data to be transmitted from the module that analyzes attacks to the module that simulates attacks. The module for updating publications, which can be identified by the presence of a gray rectangle, is designed to transmit information on the attack to the control system. The updated subscriber (shown by a rectangle in orange), which is responsible for receiving data from the field controller, then sends that data to the raw data processing module (indicated

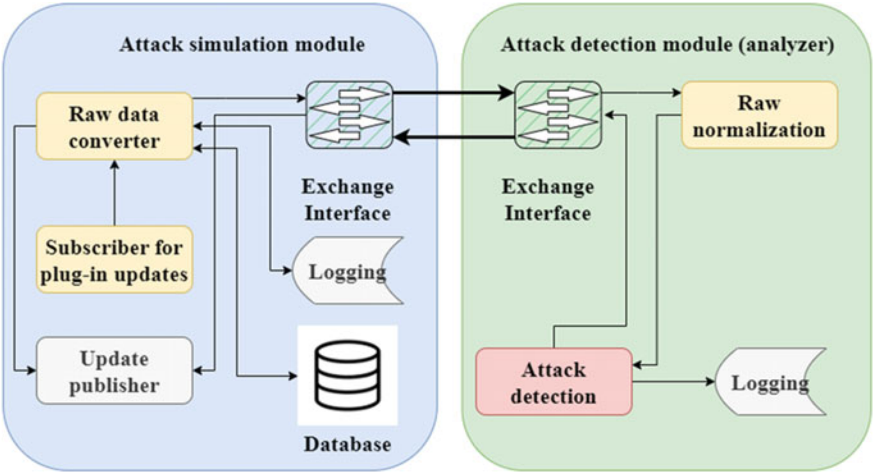


Fig. 2 Software application of attack simulation module

by a rectangle in yellow), which is responsible for normalizing the data. After the raw data have been translated, they are then transferred to the analyzer module via the interface (which is represented by a green square). At this point, the data are either normalized or communicated to the attack detection module, depending on which module is highlighted with a yellow rectangle (pink rectangle). A logging log is maintained by the attack detection module, which is required for the debugging process. The data are sent over the interface to the publishing module in order to alert the control system about the present status of the unmanned aerial vehicle (UAV), which occurs either when an attack is detected or when the behavior is normal.

Because the attack detection module is independent from the attack simulation software module, and because there is a client/server connection between the two, it is essential to anticipate any dangers that may be caused by this link. Even if the interaction is programmed at the software level, every external contact between modules carries with it the risk of a connection failure, delays, data loss, blockage of communication, or a break in the channel. This is true even if the interaction is implemented at the software level. For the purpose of gathering data and issuing control directives, ROS2 was selected to serve as an interlayer between the flight controller and the control board. The flight controller is responsible for providing the GPS spoofing attack simulation software module with any new information. The attack simulation module is a subscriber to the control module and receives instructions for establishing or altering parameters from it. These commands come from the control module. Tabular representation of the parameters received from other systems for use in analysis may be found in Table 1. As soon as it has an update, the attack simulation module immediately begins sending data to the analyzer in a sequential fashion. In this scenario, the attack simulation module will continually keep waiting for the analyzer to provide a response to the data that it has received.

Table 1 The set of parameters for analysis

Number	Description	Range of values
1	The speed after GPS satellite positioning	(0; 40), 0.1 m/s
2	GPS track angle	(−180, 180), degrees
3	GPS satellite number	(0; 34)
4	GPS altitude	(0;1000), unit 0.1 m
5	Integrated navigation latitude	(−90;90), 0.0000001 degree
6	Integrated navigation longitude	(−180;180), 0.0000001 degree

As a result, the attack simulation module not only manipulates the data, but it also functions as a layer between ROS2, external UAV modules, and the attack analyzer. This technique lessens the strain placed on the attack analyzer while simultaneously boosting the processing speed necessary to identify an attack.

As a result, the primary information that is received from the flight controller will be moved to its own subject that is specifically designed for subscribers, and information on the pace of the flight will also form its own topic. Both of these subjects are followed by the software component that simulates an attack using GPS spoofing.

The module of the attack simulation program allows for the generation of datasets based on various factors. At the same time, the module may switch between three distinct modes of operation, each of which is determined by the level of strength of the attack. The state of having no enemy attacking you is referred to as the initial mode. In this setting, no data will be created at all. The attack simulation may be canceled out completely by activating this option. The second mode is one that does significant damage. This mode represents a circumstance in which the values of every parameter, with a few notable exceptions, are liable to change. A mild attack constitutes the third mode. This mode is equivalent to a scenario in which data for just the most fundamental characteristics, such as the GPS noise level, the number of GPS satellites, and the GPS flight altitude, are fabricated (Fig. 3).

1.3 Experimental Research Methodology

The following are some of the most important and desirable qualities that should be present in a system that can defend against GPS spoofing attacks by simulating their impact on an unmanned aerial vehicle (UAV):

- Timely notification of the beginning of an attack;
- Accuracy of attack detection;

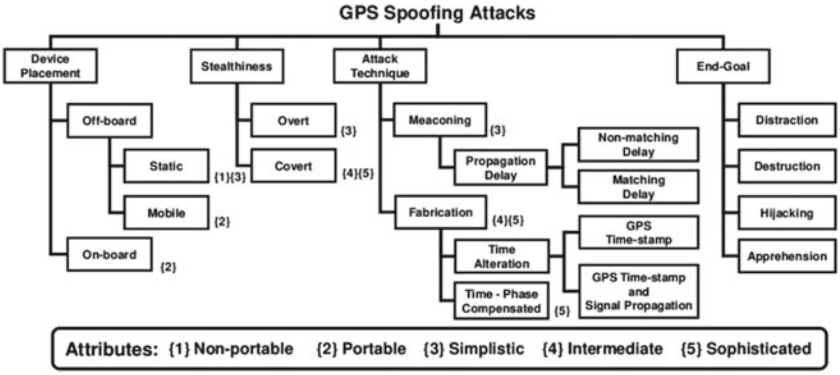


Fig. 3 Taxonomy of GPS spoofing attacks

- The plausibility of the forged attack data;
- The amount of time spent simulating the data.

The time relative to the beginning of the attack and the time the notice was sent to the operator are taken into consideration to decide whether or not the notification was delivered in a timely manner. In addition, there shouldn't be any dire effects for the unmanned aerial vehicle (UAV) itself for a certain amount of time. Using mistakes of the first and second type, estimations of the confidence interval, and testing hypotheses against confidence intervals, the accuracy of attack detection may be evaluated and improved.

The likelihood of making a type I mistake refers to the wrong rejection of the null hypothesis, sometimes known as a "false alarm". Type I errors occur when researchers incorrectly reject the null hypothesis. In this particular scenario, we are discussing the process of notifying an attack while simultaneously seeing no changes related with the attack itself. The possibility of staying within the bounds of the null hypothesis even when it is demonstrably false is an example of type II mistake (also known as "missing a goal"). In the context of this discussion, we are referring to a scenario in which an attack is carried out, but the system views the condition as being entirely normal.

The following accomplishments were made toward the goal of tackling the challenge of building a GPS spoofing detection mechanism for unmanned aerial vehicles (UAVs):

- An initial investigation was carried out, which paved the way for the development of a mathematical framework for the purpose of resolving the issue.
- A set of cyber-physical parameters that may be used to identify an attack was established as a consequence of conducting an analysis of parameters and techniques of data normalization. This set of parameters can be used to determine whether or not an attack has occurred.

- An investigation of the Kullback–Leibler divergence measure, which was used in the search for anomalies, was carried out. As a result, the quality of anomaly identification has been made much better.
- A novel technique for detecting attacks based on the characteristics of the sensor system of an unmanned vehicle has been presented. This technique enables the UAV to identify an attack in real time and independently without the requirement for previous information about the reference change of sensor values. The value of entropy, which may be thought of as the difference in the probability distributions of cyber-physical characteristics, is what serves as the foundation for this approach to problem solving.

As a part of the process of finding a solution to the problem of developing the architecture of anti-spoofing technology, the architecture of anti-spoofing technology for OS ROS2 was developed and described. It was constructed as a result of the publisher-subscriber concept, and it can be distinguished by the following characteristics:

- The use of this technology should allow for the detection of an attack, as well as the notification of the operator and any essential subsystems of the UAV about the fact that an attack has occurred. After receiving word of an attack, UAV control systems have the responsibility of ensuring that countermeasures are put into effect.
- It is not necessary to establish and record changes in indicators during normal operation in order to detect an attack using this technology. Instead, the system must ensure the recording of anomalies in real time by analyzing the degree of change in indicators obtained over the course of the previous period of time and for the period of time that is currently being measured. This is one of the features of this technology.
- The following activities need to be completed before the technology may be implemented: an interface has been developed for the purpose of collecting data on the state of the navigation system, which is required to detect a change in its state, from the flight controller or any other subsystem that can provide the required data set, the format and types of values transmitted parameters, the possibility of implementing a GPS spoofing attack on the simulation model is provided, and its effective parameters are determined; the possibility of transmitting a signal about the fact that the navigation system has been compromised; and the possibility of transmitting a signal about When compared to other methods, our approach provides a better level of accuracy in the detection of attacks. In addition to this, it is simpler to put into action, and one does not need a significant quantity of data in order to construct a decision-making system or train a neural network. Support Vector Machines, for instance, provide detection accuracy of up to 80%. A detection accuracy of up to 90% may be achieved using the deep learning approach in conjunction with the support vector machine [8]. The accuracy of our attack detection approach for a fleet of UAVs may reach as high as 96%, but at the same time, it has a false positive rate of 3.5%. Additionally, in our plan, unmanned aerial vehicles (UAVs) do not function independently, and the

system operates at the level of both UAVs and base stations to identify potentially dangerous deviations.

1.4 Secure Communication in UAVs

There is no need for extra assistance from the network infrastructure to use UAVs for the purpose of conducting surveillance over a vast region. Communication between the UAVs and the GCS allows for the continuous transmission of vital information while the UAVs are in flight. The dynamic topology brings forth additional difficulties as a result of the information that is being exchanged. The transfer of data from one node to the GCS is often handled by unmanned aerial vehicles (UAVs). The data that is being transferred is susceptible to several types of attacks. The majority of sensitive information in military applications is sent between two authorized users through wireless communication channels. This occurs in the majority of military applications. Due to the fact that the wireless channel is an unsecured medium, it is quite feasible to access the information by means of launching cyberattacks such as those targeting the integrity, availability, and confidentiality of the data. Multiple kinds of security protocols are used to encrypt the data transfer and verify the identities of the users in order to shield it from the prying eyes of potential adversaries. For instance, symmetric and asymmetric security protocols are used in order to ensure the confidentiality of the communication that takes place between the UAV and the GCS.

The encryption and decryption processes can only be carried out successfully with the usage of a single private shared key when using symmetric security protocols. While utilizing asymmetric security protocols, two distinct keys, one of which is kept secret and the other of which is kept public, are used. When anything is encrypted, a public key is used, whereas a private key is necessary for decoding. In sections II-A1 and II-A2, respectively, more coverage is given to these two distinct categories of security procedures. The authentication methods that are used to verify the identity of the transmitter are also discussed in Section IIA2 of the document. This is done to assure that the message that was received is genuine and was not delivered by an adversary. Lightweight authentication procedures are discussed in Section II-A3, which is intended for usage in situations that demand less memory and a lower level of computational complexity.

1. **Cryptographic Symmetric Security Protocols**

   Cryptographic methods are used often these days because of their capacity to guarantee availability, integrity, and secrecy. In particular, symmetric protocols are used in order to secure the protection of sensitive data, which may include text, photos, audio, or video. In symmetric security protocols, the information is encrypted using the same key that is used to decode it; this means that both the sender and the recipient of the information need to have the same key in order to access the original data. The employment of symmetric security protocols, such as the one time pad (OTP), is common practice when it comes to ensuring the safety of data transmissions. OTP mandates that the key size correspond exactly to the size of the data that has to be protected. In the context of pictures, for instance, if an image has M rows and N columns of pixels, the length of the key has to be equal to the length of the original image, which may be expressed as M times N. The OTP encryption is used to further bolster the safety of the wireless communication MAV connection described in reference [26].

A function that encrypts and decrypts the data is used in order to ensure the data's safety during transmission. The unmanned aerial vehicles (UAVs) may be controlled via a variety of instructions, such as "start UAV," "takeoff command," and "autopilot enable." These directives are all in the form of bits, which may be either 0 or 1, depending on how they are represented. When all of the bits are put together, a lengthy text is produced, which may then be encrypted using a specific method for more protection. OTP-based encryption systems each have their own set of advantages and disadvantages. For example, the size of the key has to be exactly the same as the length of the data. It is necessary for us to provide the key to the recipient if we are going to deliver data of a significant amount. As a result, the distribution of keys becomes problematic since it uses up a lot of bandwidth. In addition, the key may only be used once, which implies that for every safe transfer, a new key is required [26]. This necessitates the creation of new keys.

Applying several resilient transformation methods like discrete wavelet and discrete cosine transforms, for example, may make the system that is described in [26] more secure. These techniques can be used to enhance the scheme. Initially, the original message is changed into new frequency coefficients, which are entirely distinct from the original message. In addition, transformation carried out via the use of frequency coefficients is much quicker than transformation carried out directly on the original message [27, 28]. In the paper [10], a chaotic Lorenz system is utilized to encrypt and decode the original communications, as well as the messages that have been altered. Unpredictability over the long run is a feature of chaotic Lorenze systems, which also have the capacity to produce additional randomness by even minute adjustments to the seed values. The unmanned aerial vehicle (UAV) is responsible for gathering the data from the sensors and camera, after which it transmits the information to the Lorenz chaotic based encoder. It does not encrypt the raw message in an immediate manner. The information is first reduced to a form that can be understood in bits, and then it is encrypted. Up to the very end of the original data, the bits are constantly encrypted. Following the completion of the encrypting procedure, the UAV then delivers the information that has been encrypted to the receiver. The receiver then decrypts the information by following the opposite procedure of the chaotic Lorenze system. The suggested encryption method has a symmetrical structure, which means that the key that was used to encrypt the data in its original form by the sender is also used by the receiver to decrypt the data. Having said that, the procedure that was suggested [10] also has a few flaws. For instance, the suggested method does not include any kind of procedure for scrambling the data. In point of fact, the safety of any encryption method is contingent not only on the level of confusion (scrambling), but also on the level of diffusion [20].

2. **Cryptographic Asymmetric Security Protocols**

   When it comes to security, asymmetric protocols make use of two distinct keys. The first is known as the public key, while the second is known as the private key. The information is encrypted with the public key and decrypted using the user's private key. This process is performed by the user at both the transmitter and receiver ends. It is not required to keep the public key a secret due to the fact that once the information is encrypted using the public key, it cannot be decoded with the same public key that was used to encrypt it. Instead of the public key, retrieving the information requires the use of a secret key, also known as a private key. The authors of [1] propose a data authentication protocol that makes use of an asymmetric key algorithm technique in order to check whether the data received by the UAV was sent from the authentic ground station or the eavesdropper. This allows the authors to check whether the data was sent from the authentic ground station or the eavesdropper.

   For the purpose of ensuring that communications sent between the UAV and the GCS are not intercepted, asymmetric security protocols are used. On the other hand, symmetric key exchanges between the UAV and the GCS almost always make use of asymmetric protocols. This is because symmetric key exchanges involve a lot of extra transmission. Additionally, asymmetric security methods are used in order to guarantee the data integrity during transmission from one set of sensors or devices to another.

3. **Lightweight Authentication Protocols for UAV**

   Using encryption and authentication mechanisms that aren't too taxing on the system is another method for keeping sensitive information hidden from potential attackers. If these lightweight techniques are used, it's possible that the information may be encoded in a shorter amount of time. Additionally, it does not make extensive use of the program memory, which enables the UAV to carry out activities more quickly. In the paper [18], the authors provide a lightweight encryption protocol that is capable of functioning suitably despite the presence of frequent context switching in an environment that is substantially multi-tasked. The authors of article [13] present a lightweight blockchain-based stable routing algorithm for the networking of swarm unarmed aerial systems. This method is intended to prevent collisions among the systems (UAS). Wang et al. have employed a lightweight blockchain as a bargaining chip in order to improve the routing of swarm UAS networking that utilizes 5G cellular network technology. This was done in order to improve the routing of unmanned aerial system (UAS) swarms. The lightweight blockchain algorithm is distinct from traditional routing algorithms in that it is able to easily avoid the vindictive connections from the attackers, identify malicious UASs, and reduce the intensity of attacks from spiteful UASs. These are all things that traditional routing algorithms are unable to do. Additionally, the lightweight blockchain algorithm can identify malicious UASs.

The proposed algorithms for swarm UAVs are ones that aim to broaden the networking capabilities of deployment for swarm UAVs over a broad range. Through the use of the Internet of Things, low-cost devices may be integrated into UAVs in order to protect data from being stolen by intruders (IoT). Encrypting the data using session keys that are already known to the exact nodes that are going to be participating is a good way to lessen the damage that may be done by cyberattacks. On the other hand, due to performance limits, it is very difficult for low-cost IoT installations to embody the essential capabilities for both generations of secure session keys and encoding/decoding of the secret information. This is because it is very difficult for low-cost IoT installations to meet these requirements simultaneously. This is due to the nature of the constraints that have been placed. In their research, Demeri and colleagues made use of a low-cost aerial platform that included a number of cryptographic accelerators. This allowed them to implement a secure and public key data transmission system at the same time [21]. This may be found in their publication. An approach to design that combines software and hardware has led to the creation of drones that are free of charge thanks to the incorporation of the components via the use of application programming interference (API) that is moldable and expandable. UAVs are providing a significant amount of relief to the general population as a result of recent developments in wireless communication technology and the shrinking of all electronic gadgets. In addition, cybersecurity for unmanned aerial vehicles, also known as UAVs, is receiving an increasing amount of attention as a consequence of potential risks to national security, significant strategic and financial information, and the expanding significance of aerial applications. A lightweight authentication protocol was suggested in [29] to offer secure communication between UAVs and ground stations in order to provide security and authentication to the communication parties in addition to ensuring the privacy of the data. This was done in order to offer secure communication between UAVs and ground stations. This was done in order to ensure that the data is kept private.

A packet capture, also known as PCAP, was specified in the suggested plan in order to guarantee the confidentiality of the communications that took place between the two parties. The PCAP is based on the idea that both the UAV and the ground station use the seed values of the chaotic maps. These seed values then cause the chaotic maps to randomly shuffle the original message in accordance with the sequence that is produced by the chaotic maps [29]. UAVs are no longer considered reliable for device seizing and dabble attacks due to recent developments in remote areas and the easy availability of minimal resources. This is because of the developments. Because of this, there is a greater possibility that hostile actors would steal the data held in UAVs. Haque et al., in their paper [22], are solely concerned with the safe transmission of data that unmanned aerial vehicles (UAVs) provide to the base station. Data security and lightweightness were both topics of discussion, and a new framework was proposed as a solution to meet the necessary requirements. Specific encryption is carried out so that the system may remain as lightweight as possible. In addition to the use of cryptography, the suggested method also makes use of watermarking as a means of improving both the data's integrity and its level of secrecy. The stability between the UAVs in an environment with limited resources is something that may be achieved via the use of selective encryption. The use of selective encryption may also have some advantages, especially in real-time applications where it is required to undertake speedy processing. This is because selective encryption may reduce the amount of data that has to be processed.

4. **Physical Layer Security in UAVs**

The so-called secrecy rate [30] is a widely used performance parameter in the physical layer security architecture. This refers to the maximum speed at which sensitive information may be sent without being compromised. Traditional encryption systems have flaws in the way key distribution is handled and require a significant amount of processing time. It is possible for secure transmission to be supported by an investigation of the physical features of cellular channels. Physical layer security, often known as PLS, is a technique that is routinely used to provide the highest possible level of confidentiality for data that is being transported from one node to another. In point of fact, it is obligatory for any and all security controls as well as communication devices that are installed on the UAV. PLS takes use of the properties of cellular channels such as fading, interference, and noise in order to improve the signal reception at the authorized receiver while simultaneously lowering the quality of the signal that is received by the eavesdropper [23, 31]. This is in contrast to the traditional cryptographic security approaches, which rely on mathematical algorithms to decipher messages. Incorporating cryptographic protocols is one way to do PLS. There are various cryptographic security protocols that have been presented in the literature that provide a significant degree of security; nevertheless, there is no framework that offers a level of security that is ideal. As a result, PLS is receiving a growing amount of serious attention. Several works on PLS have been offered in order to improve and make the most of the level of secrecy that may be achieved via wireless communication in UAVs [13, 32, 33]. A number of decades ago, in order to enhance the performance of the preexisting PLS schemes, static relay-based communication systems were put into operation. UAV-enabled mobile relaying is a relatively new sort of reliance technique that has formed as a result of the remarkable advancements that have been achieved in self-driving vehicles such as UAVs. This method has developed into an essential piece of technology as a direct result of these advancements. In the paper [12], the authors suggest an enhanced version of a PLS system that makes use of mobile reliance that is provided by UAVs. To make the communication system more secure, a buffer-aided mobile relay has been implemented. This makes it possible for data to arrive independently and more rapidly, which is beneficial for applications that need real-time processing.

5. **Learning-Based Intrusion Detection**

The user may direct a digital machine to carry out a variety of activities, and the machine will respond accordingly. Machine learning (ML), deep learning, and neural networks are often utilized methods that are frequently employed in order to perform the automation of the operations. Training and testing are the two stages that machine learning algorithms go through. During the training phase, the model takes what it has learned from the data and uses it to make predictions about what will happen in the future. During the testing phase, the accuracy of the training model is assessed, and it is possible to enhance it by using a variety of different tactics. Pattern recognition may be used for intrusion detection in UAVs using learning-based approaches, which can be applied in such systems. After receiving training, the UAV will be able to detect the pattern of the incursion after it has occurred. Deep reinforcement learning and a weighted least squares method are used by the authors of paper [34] to estimate the strength of the jamming signal. This is done with the assistance of a convolution neural network (CNN) [35]. The suggested method begins with the initial step of selecting a relay power factor by taking into account the bit error rate (BER) as well as the channel gain. A convolutional neural network is used in the process of initializing the weights, which will ultimately be equivalent to the anti-jamming relays. These weights are kept up to date with the use of a method called stochastic gradient descent [64]. The BER value is then sent to the UAV from the base station after this step. In the event that the learning parameter is higher than the power factor associated with the relay power, the apparatus will choose a relay power at random. If it goes over zero, the unmanned aerial vehicle will use a technique called reinforcement learning to transmit a message along with a value for the power that was chosen at random. Take into consideration that the randomly selected relay power may contribute to a higher mistake rate. The algorithm may be able to avoid jamming of the UAVs and communications to some degree in the event that there is a large mistake rate; however, this may come at a very high cost (Fig. 4).

6. **Rules-Based Intrusion Detection**

It is necessary to provide a piece of hardware with certain instructions in order to endow it with intelligent behavior. When doing rule-based activities, it is necessary for the user to establish certain rules. The choice is made by the device based on those guidelines, and it then communicates its verdict to the base station. In the case of UAVs, various sets of rules are loaded onto the chip of the UAV for each individual job, and threshold values for the acceptance of each rule are calibrated. For instance, if the threshold is set at 80%, this indicates that the particular function will only be carried out by the UAV if it determines that the real state of the rules is either equal to or more than 80%, and vice versa. A novel intrusion detection system based on the particular behavior criteria was presented in reference to [66], with the goal of minimizing the number of false negative predictions. Within the framework of the suggested detection approach, seven distinct attacks,

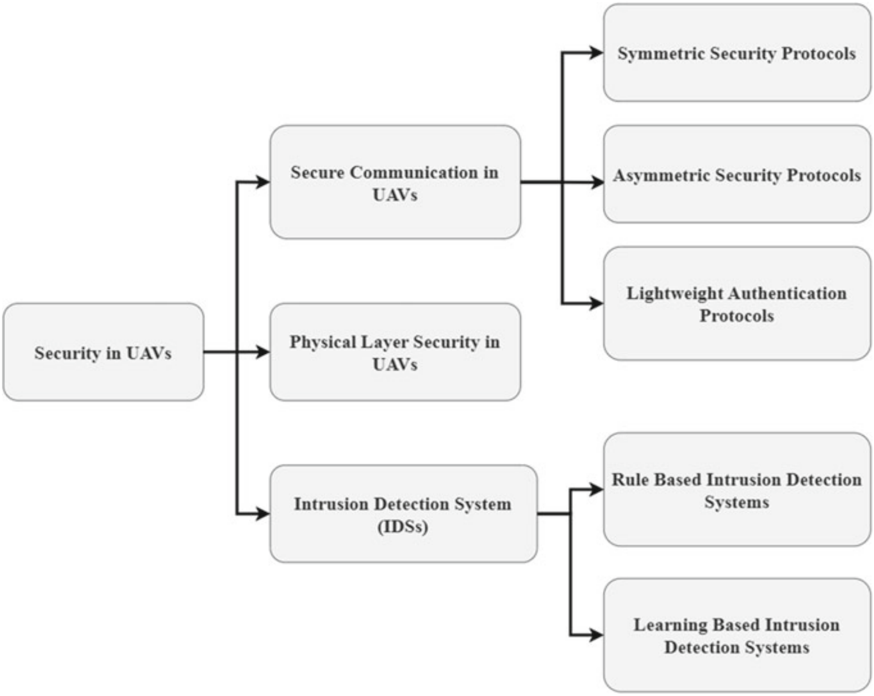

Security in UAVs
Secure Communication in UAVs
Physical Layer Security in UAVs
Intrusion Detection System (IDSs)
Symmetric Security Protocols
Asymmetric Security Protocols
Lightweight Authentication Protocols
Rule Based Intrusion Detection Systems
Learning Based Intrusion Detection Systems

Fig. 4 Security categories in UAVs

all of which are connected to availability, confidentiality, and integrity threats, were examined. The unmanned aerial vehicle (UAV) will initiate self-defense procedures if it is subjected to any of these seven types of attacks. When the unmanned aerial vehicle (UAV) first exits the secure zone, it immediately begins arming its weapons in preparation for an impending attack. Second, actions are carried out whenever the readings from the sensors do not match those from the trusted node. Third, the proper steps are conducted if negative suggestions are received about the trusted node and positive recommendations are made regarding the UAV that is acting inappropriately. The fourth indication is responsible for handling the circumstance in which the UAV deploys its landing gear in a location that is not acceptable. These four attacks are examples of attacks against the system's integrity. When the UAV begins providing data to individuals or organizations that are not authorized to receive it, the fifth indication becomes active. This exploit mirrors the secrecy attack that was described before. The seventh and final attack indication happens when the unmanned aerial vehicle (UAV) utilizes additional thrust to cross the limitation altitude that has been established by the authorized person. The sixth attack indicator takes place when the UAV deploys its countermeasures without first studying any attacks. The availability

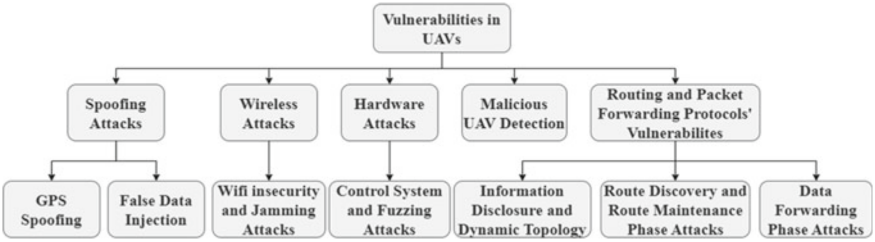

Vulnerabilities in UAVs
Spoofing Attacks
Wireless Attacks
Hardware Attacks
Malicious UAV Detection
Routing and Packet Forwarding Protocols' Vulnerabilites
GPS Spoofing
False Data Injection
Wifi insecurity and Jamming Attacks
Control System and Fuzzing Attacks
Information Disclosure and Dynamic Topology
Route Discovery and Route Maintenance Phase Attacks
Data Forwarding Phase Attacks

Fig. 5 Vulnerabilities in UAVs

attack is represented by the sixth and seventh attacks respectively. The aforementioned seven attacks are taken into consideration, and once an attack has been detected, the unmanned aerial vehicle (UAV) immediately begins a defensive phase to protect itself against the attacks described above. Additionally, intrusion detection systems, often known as IDS, are used in order to identify any abnormalities that may have occurred inside the network. In order to protect the systems from any dangers, the IDSs will now eliminate the negative effects of the attack. An intrusion detection system (IDS) is a crucial component of a network of unmanned aerial vehicles (UAVs) that helps identify potentially harmful nodes and defends genuine UAVs from attack (Fig. 5).

2 Conclusion

In this study, we offered a detailed overview and in-depth analysis of current attempts towards GPS spoofing. Specifically, we focused on how these efforts may be improved. Particularly, location spoofing of unmanned aerial vehicles (UAVs) was discussed in great depth. This was accomplished by associating GPS reliance with the operating modes of UAVs and assessing attack variants for static, limpet, and mobile (follower) spoofers. With the use of well created faked GPS signals, an adversary might misdirect, put in danger, destroy, or even hijack a spoofed unmanned aerial vehicle (UAV). We also offered a unique taxonomy to identify attack capabilities, location, stealthiness, and aims of multifarious spoofing strategies, while also categorizing and discussing the existing literature according to the definitions of our taxonomy. This was done when spoofing techniques are used. In addition to this, the report discussed some of the unresolved issues that might stimulate additional research in certain fields. In light of the many GPS spoofing attacks that have been carried out against aerial platforms, surface vehicles, and other statics services, it is imperative that security-aware and spoof-resistant GPS services be designed. On the other side, GPS spoofing has also showed promising possibilities for parametric defense to disable hostile drones. This is because of its ability to fool GPS receivers.

References

1. Yaacoub JPA, Noura M, Noura HN, Salman O, Yaacoub E, Couturier R, Chehab A (2019) Securing internet of medical things systems: limitations, issues and recommendations. Fut Gener Comput Syst 105:581–606
2. Park J, Kim S, Suh K (2018) A comparative analysis of the environmental benefits of drone-based delivery services in urban and rural areas. Sustainability 10(3):888
3. Humphreys T (2012) Statement on the vulnerability of civil unmanned aerial vehicles and other systems to civil GPS spoofing. University Texas Austin, Austin
4. Canis B (2015) Unmanned aircraft systems (UAS): commercial outlook for a new industry
5. Stocker C, Bennett R, Nex F, Gerke M, Zevenbergen J (2017) Review of the current state of UAV regulations. Remote Sens 9(5):459
6. Barfield F (2002) Autonomous collision avoidance: the technical requirements. In: Proceedings of the IEEE national aerospace and electronics conference, pp 808–813
7. Sharma R, Ghose D (2009) Collision avoidance between UAV clusters using swarm intelligence techniques. Int J Syst Sci 40(5):521–538
8. Johnson LK, Dorn AW, Webb S, Kreps S, Krieger W, Schwarz E, Shpiro S, Walsh PF, Wirtz JJ (2017) An INS special forum: intelligence and drones/eyes in the sky for peacekeeping: the emergence of UAVs in UN operations/the democratic deficit on drones/the German approach to drone warfare/pursuing peace: the strategic limits of drone warfare/seeing but unseen: intelligence drones in Israel/drone paramilitary operations against suspected global terrorists: us and Australian perspectives/the 'terminator conundrum' and the future of drone warfare. Int Natl Sec 32(4):411–440
9. Thiels CA, Aho JM, Zietlow SP, Jenkins DH (2015) Use of unmanned aerial vehicles for medical product transport. Air Med J 34(2):104–108
10. Rango A, Laliberte A, Steele C, Herrick JE, Bestelmeyer B, Schmugge T, Roanhorse A, Jenkins V (2006) Using unmanned aerial vehicles for rangelands: current applications and future potentials. Environ Pract 8(3):159–168
11. Sedjelmaci H, Senouci SM (2018) Cyber security methods for aerial vehicle networks: taxonomy, challenges and solution. J Supercomput 57:1–17
12. Mushtaq MF, Jamel S, Mohamad KM, Khalid SKA, Deris MM (2017) Key generation technique based on triangular coordinate extraction for hybrid cubes. J Telecommun Electron Comput Eng 9(3–4):195–200
13. Du H, Heldeweg MA (2017) Responsible design of drones and drone services: legal perspective synthetic report
14. Ueno S, Higuchi T (2011) Collision avoidance law using information amount. In: Numerical analysis-theory and application. InTech, Allithurai
15. Hamza A, Akram U, Samad A, Khosa SN, Fatima R, Mushtaq MF (2020) Unmaned aerial vehicles threats and defence solutions. In: IEEE 23rd international multi-topic conference (INMIC)
16. Israelsen J, Beall M, Bareiss D, Stuart D, Keeney E, Berg J (2014) Automatic collision avoidance for manually tele-operated unmanned aerial vehicles. In: IEEE international conference on robotics and automation (ICRA), pp 6638–6643
17. Boulos MNK, Geraghty EM (2020) Geographical tracking and mapping of coronavirus disease covid-19/severe acute respiratory syndrome coronavirus 2 (sars-cov-2) epidemic and associated events around the world: how 21st century GIS technologies are supporting the global fight against outbreaks and epidemics. Int J Health Geogr 19:1–12
18. Finn RL, Wright D (2012) Unmanned aircraft systems: surveillance, ethics and privacy in civil applications. Comput Law Sec 28(2):184–194
19. Cavoukian A (2012) Privacy and drones: unmanned aerial vehicles. Information and Privacy Commissioner of Ontario, Ontario
20. Jumaat N, Ahmad B, Dutsenwai HS (2018) Land cover change mapping using high resolution satellites and unmanned aerial vehicle. In: IOP conference series: earth and environmental science

21. Wackwitz K, Boedecker H (2015) Safety risk assessment for UAV operation. In: Drone industry insights, safe airspace integration project, part one, Hamburg
22. Finn RL, Wright D, Friedewald M (2013) Seven types of privacy. In: European data protection: coming of age. Springer, New York
23. Ramon Soria P, Bevec R, Arrue B, Ude A, Ollero A (2016) Extracting objects for aerial manipulation on UAVs using low cost stereo sensors. Sensors 16(5):700
24. Clarke R (2014) The regulation of civilian drones' impacts on behavioural privacy. Comput Law Sec Rev 30(3):286–305
25. Shepard DP, Bhatti JA, Humphreys TE, Fansler AA (2012) Evaluation of smart grid and civilian UAV vulnerability to GPS spoofing attacks. Proc ION GNSS Meet 3:3591–3605
26. Yanmaz E, Kuschnig R, Quaritsch M, Bettstetter C, Rinner B (2011) On path planning strategies for networked unmanned aerial vehicles. In: IEEE conference on computer communications workshops (INFOCOM WKSHPS), pp 212–216
27. Hernandez LH, Tsourdos A, Shin HS, Waldock A (2014) Multi-objective UAV routing. In: IEEE international conference on unmanned aircraft systems (ICUAS), pp 534–542
28. Vattapparamban E, Guvenc I, Yurekli AI, Akkaya K, Uluagac S (2016) Drones for smart cities: issues in cybersecurity, privacy, and public safety. In: IEEE international wireless communications and mobile computing conference (IWCMC), pp 216–221
29. Carr EB (2014) Unmanned aerial vehicles: examining the safety, security, privacy and regulatory issues of integration into us airspace. Natl Centre Policy Anal 23:2014
30. Lin X, Wiren R, Euler S, Sadam A, Maattanen HL, Muruganathan SD, Gao S, Wang YPE, Kauppi J, Zou Z (2018) Mobile networks connected drones: field trials, simulations, and design insights. arXiv Preprint arXiv:1801.10508
31. Abdallah A, Ali MZ, Misic J, Misi VB (2019) Efficient security scheme for disaster surveillance UAV communication networks. Information 10(2):43
32. Kim SJ, Lim GJ, Cho J (2018) Drone flight scheduling under uncertainty on battery duration and air temperature. Comput Ind Eng 117:291–302
33. Tseng CM, Chau CK, Elbassioni K, Khonji M (2017) Autonomous recharging and flight mission planning for battery-operated autonomous drones. arXiv preprint arXiv:1703.10049
34. Basan E, Basan A, Nekrasov A, Fidge C, Sushkin N, Peskova O (2022) GPS-spoofing attack detection technology for UAVs based on Kullback-Leibler divergence. Drones 6:8. https://doi.org/10.3390/drones6010008
35. Khan SZ, Mohsin M, Iqbal W (2021) On GPS spoofing of aerial platforms: a review of threats, challenges, methodologies, and future research directions. PeerJComput Sci 7:e507. https://doi.org/10.7717/peerj-cs.507
36. Chan K, Nirmal U, Cheaw W (2018) Progress on drone technology and their applications: a comprehensive review. In: AIP conference proceedings, 2030. AIP Publishing, College Park, p 020308
37. Liu Z, Li Z, Liu B, Fu X, Raptis I, Ren K (2015) Rise of mini-drones: applications and issues. In: Proceedings of the 2015 workshop on privacy-aware mobile computing. ACM, New York, pp 7–12
38. Altawy R, Youssef AM (2017) Security, privacy, and safety aspects of civilian drones: a survey. ACM Trans Cyber Phys Syst 1(2):7
39. He D, Chan S, Guizani M (2017) Drone-assisted public safety networks: the security aspect. IEEE Commun Mag 55(8):218–223
40. Yampolskiy M, Horvath P, Koutsoukos XD, Xue Y, Sztipanovits J (2013) Taxonomy for description of cross-domain attacks on CPS. In: Proceedings of the 2nd ACM international conference on high confidence networked systems. ACM, New York, pp 135–142
41. Guvenc I, Ozdemir O, Yapici Y, Mehrpouyan H, Matolak D (2017) Detection, localization, and tracking of unauthorized UAS and jammers. In: Proceedings of the 2017 IEEE/AIAA 36th digital avionics systems conference (DASC), IEEE, pp 1–10
42. Sturdivant RL, Chong EK (2017) Systems engineering baseline concept of a multispectral drone detection solution for airports. IEEE Access 5:7123–7138

43. Shi X, Yang C, Xie W, Liang C, Shi Z, Chen J (2018) Anti-drone system with multiple surveillance technologies: architecture, implementation, and challenges. IEEE Commun Mag 56(4):68–74
44. Nassi B, Shabtai A, Masuoka R, Elovici T (2019) Sok-security and privacy in the age of drones: threats, challenges, solution mechanisms, and scientific gaps. arXiv Preprint arXiv:1903.05155
45. Atherton KD (2016) The FAA says there will be 7 million drones flying over America by 2020. Popular Sci
46. Vattapparamban E, Guvenc I, Yurekli AI, Akkaya K, Uluagac S (2016) Drones for smart cities: issues in cybersecurity, privacy, and public safety. In: Wireless communications and mobile computing conference (IWCMC), 2016 international, IEEE, pp 216–221
47. Dalamagkidis K, Valavanis KP, Piegl LA (2012) Aviation history and unmanned flight. on integrating unmanned aircraft systems into the national airspace system. Springer, New York, pp 11–42
48. Juul M (2015) Civil drones in the European Union, Eur. Parliament. Res. Serv. (ed.). Eur. Union
49. Stopforth R (2017) Drone licenses-necessities and requirements. II. Ponte 73(1):149–156
50. Campos VS (2018) European union policies and civil drones. Ethics and civil drones. Springer, Cham, pp 35–41
51. Miah A (2020) Regulating drones. In: Drones: the brilliant, the bad and the beautiful. Emerald Publishing Limited, Bingley
52. Wright S (2020) Ethical and safety implications of the growing use of civilian drone. UK Parliament Website (Sci. Technol. Committee)
53. Lowbridge C (2015) Are drones dangerous or harmless fun? BBC News, London. https://www.bbc.com/news/uk-england-34269585. Accessed 07 Sept 2018
54. Cress JJ, Sloan JL, Hutt ME (2011) Implementation of unmanned aircraft systems by the US geological survey. Geocarto Int 26(2):133–140
55. Lipsitch M, Swerdlow DL, Finelli L (2020) Defining the epidemiology of covid-19—studies needed. N Engl J Med 382(13):1194–1196
56. Jiang F, Deng L, Zhang L, Cai Y, Cheung CW, Xia Z (2020) Review of the clinical characteristics of coronavirus disease 2019 (covid-19). J Gen Intern Med 35:1–5
57. Majeed R, Abdullah NA, Ashraf I, Zikria YB, Mushtaq MF, Umer M (2020) An intelligent, secure, and smart home automation system. Sci Program 57:1–14
58. Zeng Y, Zhang R, Lim TJ (2016) Wireless communications with unmanned aerial vehicles: opportunities and challenges. arXiv preprintarXiv:1602.03602
59. Rudinskas D, Goraj Z, Stankunas J (2009) Security analysis of UAV radio communication system. Aviation 13(4):116–121
60. Kerns AJ, Shepard DP, Bhatti JA, Humphreys TE (2014) Unmanned aircraft capture and control via GPS spoofing. J Field Rob 31(4):617–636
61. Seo SH, Lee BH, Im SH, Jee GI (2015) Effect of spoofing on unmanned aerial vehicle using counterfeited GPS signal. J Posit Navig Timing 4(2):57–65
62. Shafique A, Mehmood A, Elhadef M (2021) Survey of security protocols and vulnerabilities in unmanned aerial vehicles. IEEE Access 9:46927–46948. https://doi.org/10.1109/ACCESS.2021.3066778

Security Threats of Unmanned Aerial Vehicles

Ashok Vajravelu, N. Ashok Kumar, Swagata Sarkar, and Sheshang Degadwala

Abstract Civilian drones and military drones are the two primary classifications of unmanned aerial vehicles (UAVs), which are commonly known as drones. Drones are used for a wide range of tasks and are also referred to by their other name, unmanned aerial vehicles. The deployment of unmanned aerial vehicles for a broad range of tasks has shown phenomenal expansion over the course of the previous decade. Recently, a new generation of small unmanned aerial vehicles has been available for purchase, highlighting the growing danger that these devices present. This article discusses the potential threats to national security that unmanned aerial vehicles pose, including but not limited to the following: terrorist attacks; unauthorized surveillance and reconnaissance; smuggling; electronic eavesdropping; mid-air collisions; and electronic eavesdropping. It also analyzes the various forms of UAV incursions according to the objective for which they were carried out and the amount of expertise possessed by the operator. In the communication frameworks of the drones, several cryptographic approaches have been included. These techniques include key agreement, authentication, encryption and decryption, integrity, blockchain, and digital signatures. Civilian drones and military drones are the two types that may be differentiated based on the functions that they are designed to do.

Keywords Unmanned aerial vehicle · Security threats · Smart drones · Cybersecurity · Data privacy

A. Vajravelu
Department of Electronics, Faculty of Electrical Engineering, Universiti Tun Hussein Onn Malaysia, Batu Pahat, Johor, Malaysia

N. Ashok Kumar
Department of ECE, Mohan Babu University, Erstwhile of Sree Vidaynikethan Engineering College, Tirupati, Andhra Pradesh 517102, India

S. Sarkar (✉)
Artificial Intelligence and Data Science Department, Sri Sairam Engineering College, West Tambaram, Chennai, India
e-mail: swagata.b.sarkar@gmail.com

S. Degadwala
Department of Computer Engineering, Sigma Institute of Engineering, Vadodara, Gujarat, India

H. Jahankhani and A. El Hajjar (eds.), *Wireless Networks*, Advanced Sciences and Technologies for Security Applications,
https://doi.org/10.1007/978-3-031-33631-7_5

1 Introduction

In this post-atomic age, the majority of applications for drone technology may be found in the military and other defensive settings. The use of drone technology in military settings is seeing tremendous expansion. These little gadgets are now hovering around 200 feet above the earth in the air. This height range varies from one gadget to the next as well as depending on the intended use. This range may be measured in feet, meters, or kilometers, depending on your preference. The amount of time that these intelligent gadgets can remain airborne varies, too, depending on the device [1, 2]. Table 1 contains a discussion of the differences in frequency as well as their attributes.

2 Security, Protection, and Secrecy Apprehendions of Drones

Drone technology provides a variety of advantages and benefits to humans. It is utilized in everyday operations, the military, and weather monitoring, among other things. Nevertheless, despite their benefits, there are a number of privacy and safety risks linked with them. Breach of privacy and security should be dealt with in the appropriate manner. When using drones for recording or picture capture, care must be taken to protect the privacy and confidentiality of the subjects being filmed or photographed [15]. There are a number of studies that have been conducted, all of which evaluate and talk about the risks that are linked with using drones for sanctuary and risk assessment. Message-passing networks must meet the requirements for confidentiality, dependability, obtainability, verification, and non-denial

Table 1 Variations in frequency and their characteristics

Parameters	2 GHz	5 GHz
Frequency band	Low speed	High speed
Cost	Cheap	Costly
Range	Extended range	Undersized range
Effect of noise	Noisy	Less noisy
interference	Prone to interference	Less prone to interference
Physical barriers	Overcome physical barriers	Unable to overcome physical barriers
Performances	Disturb Wi-Fi speed	Don’t disturb Wi-Fi speed

of possessions. This is something that AAA's procedures and progressions can help with:

- Authorization can be obtained by granting access to the drone or UAV's control unit.
- Verification can be achieved through the use of multi-level authentication with a knowledge-specific key, identity verification, and biometric verification.

Drones provide a number of security risks, which may take the form of either physical or cyber assaults. It is mandatory to place restrictions on the usage of drones in public places and on private property. The inappropriate usage of drones is also becoming more common by the day. This use further complicates matters for the general populace and civilians. When flying their drones in restricted regions, owners of drones usually control them over Bluetooth or Wi-Fi channels. This might result in a loss of financial resources. Hacking Wi-Fi networks and Bluetooth signals may be accomplished with the use of drones. A compromise of this magnitude raises a great number of privacy and security concerns among individuals. The most significant dangers to drones are shown in Fig. 1, which may be seen below. There is also discussion of potential countermeasures to these dangers. The following is a rundown of some of the most pressing and impending security concerns.

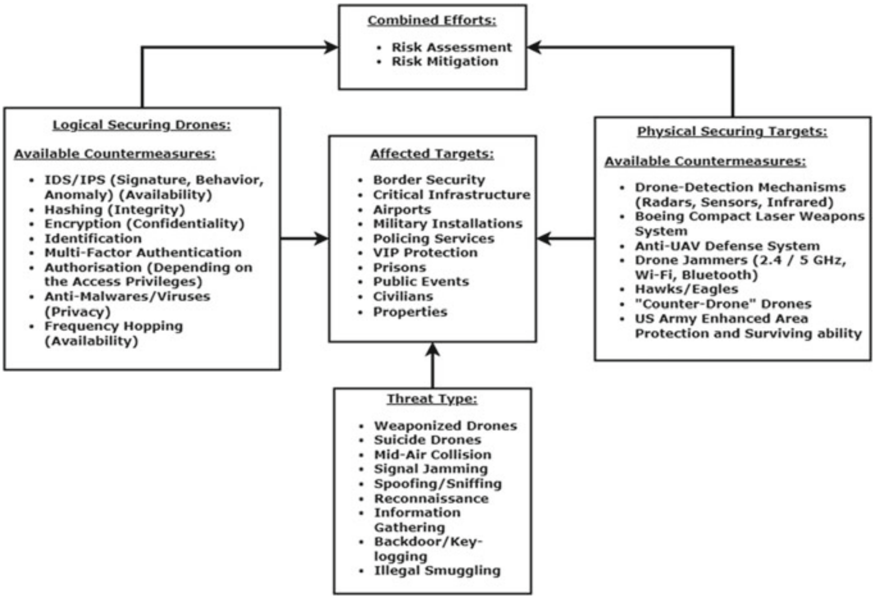

Combined Efforts:
• Risk Assessment
• Risk Mitigation
Logical Securing Drones:
Available Countermeasures:
• IDS/IPS (Signature, Behavior, Anomaly) (Availability)
• Hashing (Integrity)
• Encryption (Confidentiality)
• Identification
• Multi-Factor Authentication
• Authorisation (Depending on the Access Privileges)
• Anti-Malwares/Viruses (Privacy)
• Frequency Hopping (Availability)
Affected Targets:
• Border Security
• Critical Infrastructure
• Airports
• Military Installations
• Policing Services
• VIP Protection
• Prisons
• Public Events
• Civilians
• Properties
Physical Securing Targets:
Available Countermeasures:
• Drone-Detection Mechanisms (Radars, Sensors, Infrared)
• Boeing Compact Laser Weapons System
• Anti-UAV Defense System
• Drone Jammers (2.4 / 5 GHz, Wi-Fi, Bluetooth)
• Hawks/Eagles
• "Counter-Drone" Drones
• US Army Enhanced Area Protection and Surviving ability
Threat Type:
• Weaponized Drones
• Suicide Drones
• Mid-Air Collision
• Signal Jamming
• Spoofing/Sniffing
• Reconnaissance
• Information Gathering
• Backdoor/Key-logging
• Illegal Smuggling

Fig. 1 Drone threats taxonomy

3 Existing Approaches for Drone Cyber-Security Methods

The following are the many sorts of major security approaches that are used to ensure drone cybersecurity. This categorization takes into account the goals and intentions of the attacker. In the following paragraphs, we will cover the various methods now in use to address drone safety concerns.

A. ***Drone Network Security***

When drones are in the air and communicating with a base station, there are several opportunities for security breaches. In order to find a solution to these kinds of issues, researchers came up with a system of intrusion detection that can identify illicit activity. The techniques of intrusion detection monitor network traffic in order to identify suspicious activity. There are many different ways for detecting intrusions, and these approaches are used to investigate abnormalities. These approaches include methodologies such as rule-based detection, signature-based detection, and anomaly-based detection.

B. ***Drone Information Safety***

The data sent by drones has to be converted into packets in order to prevent the communication network from being overloaded. This kind of packing makes it possible to communicate in a reasonably risk-free manner. Nevertheless, such packaging is responsible for a wide variety of issues. One research article delves into the topic of cipher security, which safeguards data from prying eyes.

C. ***Scientific Resolutions***

The drone industry makes use of scientific methods, one of which involves analyzing the traffic on a network through the application of forensic monitoring techniques. This monitoring enables the identification as well as the detection of illegal access and capture.

4 Security Threats to Drones

The size of the drone, the purpose it serves, and the controlling system all factor into the complexity of its security. Wi-Fi, namely the IEEE 802.11 communication protocol, is used in many instances to operate the drone. Wi-Fi networks, along with their respective ground stations, form the foundation for the majority of communication systems built inside drones. These networks are susceptible to having their security compromised. Due to the lack of adequate encryption on their circuits, professional drones run the risk of being stolen. The man-in-the-middle attack is the second method of network hijacking that has been identified by the research community. These assaults are only feasible up to a distance of two kilometers. The obstacle that has shown itself so far is that there is no encryption, which makes it possible for humans to take control of drones. The Internet of Drones is a relatively new development in the field of drone safety (IoD). The idea is widely used in both the military and commercial sectors of drones. The Internet of Things has a broad variety of uses, including both civilian and military drones at the same time. The fundamental issue with drones is that they are designed without taking into account any kind of safety features. There were significant risks to users' personal information and privacy associated with the design of drone technology. The primary challenges confronting the field of Internet of Things (IoT) security have been identified as privacy leakage, data confidentiality, data protection, data flexibility, data accessibility, and data encryption and decryption procedures.

Researchers from a wide variety of fields have conducted a large number of studies over the last several years, during which time they have uncovered a wide variety of dangers to data privacy and data security. The discovered forms of cyberattacks may be broken down into four categories: compromised component attacks, jammers attacks, compromised protocol-based attacks, and jammers attacks. Table 2 provides an overview of the potential dangers that have been recognized as falling under each of these four categories of cyberattacks, as discovered by the literature research. As can be seen in Table 2, the bulk of the work that has been done on the cybersecurity and data privacy of industrial drones consists of little more than the identification of potential dangers. There is no known answer to the problems posed by these dangers. An attempt was made to encrypt data sent from a drone to a base station using a Key Encryption technique for secure packet delivery [18]. This was done in the hopes of preventing unauthorized access to the data. Over the last several years, the scientific community has been more interested in the use of miniature drones. These drones are extremely popular not only due to the fact that they have a shorter wingspan, but also due to the fact that they are lightweight. These tiny drones pose a danger not only to the safety and privacy of people but also to the security and privacy of governments. Other research, such as [16, 19–23], are also shedding light on the frequent problems and dangers associated with drone security.

Tian was able to ensure that the privacy of the drones Network by providing an efficient privacy-preserving authentication framework for edge-assisted internet of drones [24]. This framework was able to keep sensitive information private. In a similar manner, Hell described a drone system that might be used for the purpose of securing and monitoring a factory [25]. For reasons of safety, this system was able to keep an eye on a specific section of the plant where the action was taking place. Tosato presented a similar application in 2019, in which he offered an autonomous application of a swarm of drones for detecting industrial gas. The application was titled "Autonomous Application of a Swarm of Drones for Detecting Industrial Gas" [26]. This application was likewise comparable to the one shown by Tosato. These kinds of drones are becoming more popular in today's market for the purpose of monitoring and surveillance in an industrial area or an agricultural field for the purpose of risk management.

A. Gap Analysis of Drone Security Using Machine Learning

Learning on a machine may be split down into a few basic categories, including supervised learning, unsupervised learning, semisupervised learning, reinforcement learning, deep learning, and a few more. In the recent past, it was discovered that

Table 2 Threat to smart drones from typical cybersecurity and data privacy

	Common cybersecurity threats	Threats identified citations	Countermeasures citations
Protocol-based attacks	Security of communication link		
	Data confidentiality protection	[1]	
	Replay attack	[3, 4]	[5]
	Privacy leakage	[1, 6]	
	De-authentication attack	[7, 8],	
Sensors based attacked	GPS spoofing/jamming attack	[9–11]	[12, 13]
	Motion sensors spoofing	[14]	[15]
	UAV spoofing/jamming attack	[9]	
Compromised component	IoT security threats	[9], [S], [16]	
	Control/data interception	[9, 17]	
Jammers	Denial of service	[7–9]	
	Stop packet delivery	[18]	[18]

various attempts have been made to use machine learning solutions to handle cybersecurity attacks for mobile networks [27], wireless sensor networks [28], cloud computing [29], and Internet of Things (IoT) systems. This was discovered in the process of conducting a literature review. [27] Wireless sensor networks [28] Cloud computing [29] Internet of Things (IoT) systems [29–31], and other types of systems. Table 3 provides a summary of the different efforts made in the past to apply machine learning to the problem of ensuring the safety of various kinds of wireless networks. On the other hand, no evidence of any prior work has been uncovered that used machine learning-based cybersecurity solutions to address vulnerabilities posed by drones.

In addition, we recommend using a security solution that is based on machine learning in conjunction with Blockchain in order to improve the mechanisms that are used for authentication and access control in drone security. This can be accomplished by combining the two technologies. During the course of the in-depth survey of the literature that was carried out from 2010 to 2020 in the field of security, safety, and privacy concerns regarding drones and UAVs, more than thirty contributions were discovered in the form of research papers, the majority of which were published in journals issued by IEEE and ACM. The vast majority of these articles focus on the issues and problems that have arisen in the field of cybersecurity in recent years. These include GPS spoofing, IoT spoofing, drone hijacking, device interception, data privacy, and many other types of comparable cybersecurity concerns. However, the bulk of the published research only focuses on identifying the most significant dangers and problems to the safety of drones.

Table 3 Attacks and the security techniques

Sr. No.	Attacks	Security technique	Machine learning solution
1	Jamming	Secure offloading	Q-learning [27, 28] DQN [32]
2	Denial of service	Secure offloading	Neural Networks [29] Multivariate correlation analysis [33] Q-learning [34]
3	Malware	Access control	Q/Dyna-Q/PDS K-nearest neighbors Random Forest
4	Intrusion	Access control	Naive Bayes Support vector machine Neural network K-NN
5	Spoofing	Authentication	SVM DNN Dyna-Q Q-learning
6	Traffic blockage	Authentication	Q-learning

The vast majority of these studies do not provide any remedies or preventative steps to deal with the identified security risks. Only in [35] is the idea of utilizing blockchain for safe data transport using drones that are enabled with 5G and the internet of things. Nevertheless, a significant amount of human identification of threat types and levels is required by this system. A key-based authentication of devices that are not legitimate for the purpose of providing security is required for other initiatives as well, most notably in the field of Internet of Things-based drones. There is currently a significant research gap that needs to be filled in order to make drones secure and safe from major cybersecurity threats. Filling this gap is necessary in order to make drones usable for commercial and industrial reasons.

Drone/UAV security vulnerabilities and threats

There are many uses and applications for drones and unmanned aerial vehicles, and the list keeps growing as new technologies emerge. However, some of them have restricted operational resources, while others raise a variety of issues about safety, privacy, and security [3, 4]. It is recommended that licensing, regularization, and a variety of procedures (oversight) be implemented in order to place restrictions on the use of superfluous and/or nefarious UAV-based photography. Authorities in every region of the globe have to make it a top priority to enact laws and guidelines that regulate surveillance practices and procedures. The network coverage that is provided by a UAV cannot be compared to the network coverage that is provided by any Wireless Sensor Network (WSN) or Mobile Ad-hoc Network in terms of network security and risk assessment [5]. This is because of limitations on the available resources, since the UAV-based coverage is far larger and more extensive than that of WSN and MANETs. The following recommendations pertaining to AAA (Authorization Authentication Accounting) may be useful for unmanned aerial vehicles:

- ***Authorization***: Providing the controller of the UAV with administrative privileges in order to prevent any hostile takeovers with administrative rights.
- ***Authentication***: In order to prevent unauthorized access and control, unmanned aerial vehicles require a stringent authentication method.
- ***Accounting***: In the event that a UAV or drone is used to engage in illegal activity, the owner can be identified and brought to justice. Due to the ease of access, mischievous or criminal entities are able to use drones and unmanned aerial vehicles to conduct illegal surveillance, launch cyberattacks, and initiate privacy threats against individuals and organizations. Drones and other unmanned aerial vehicles are having their myriad mechanical and operational capabilities abused in order to carry out malicious acts [10]. The efforts that are made to make unmanned aerial vehicles and drones more secure and rigid also make them more effective for engaging in malicious activities. These kinds of events make the growth of UAVs and drones a double-edged sword.

4.1 Security Concerns

UAVs are an excellent option for illegal activity since they can be transported easily, are inexpensive, are readily available, do not need much maintenance, and are easy to handle. UAVs are often used by criminals and terrorists to carry out damaging actions and acts of sabotage, for instance. UAVs are efficient carriers for potentially hazardous chemicals or explosive materials because of their ability to attach a diverse selection of payloads. Further contributing to their usefulness is the fact that they can access areas that are inaccessible to people. They are able to transport anything, either undetected or in a stealthy manner [11].

4.2 Safety Concerns

Concerns around drones and other unmanned aerial vehicles go beyond only safety. Any drone that is flying over people or property runs the risk of experiencing a malfunction and crashing. These types of collisions have the potential to cause damage to structures as well as personal injury to persons [12]. There have been reports of events of this kind from all across the globe. Unfortunately, accidents to humans caused by unmanned aerial vehicles and drones are rather prevalent. A passenger plane was damaged by an unmanned aerial vehicle in April of 2016. (British AirwaysBA727). As a result of these incidents, the following recommendations about public safety might be made:

- ***Safety Feature***: Strong winds significantly increase the risk that an unmanned aerial vehicle or drone will be hacked or will become difficult to control. In these kinds of predicaments, there ought to be a choice between turning it off and regaining control of the situation.
- ***Weak Signal or jamming***: As part of a cyberattack, unmanned aerial vehicles and drones are more susceptible to being hacked and taken over when signal jamming is used.
- ***Design/Architecture safety***: The vast majority of the unmanned aerial vehicles and drones that are readily available to the general public are rotary-based kinds.

These drones have the capability of having extra safety measures. Although it is reasonable to assume that the addition of such safeguards would have an impact on the design and could cause performance issues, ensuring people's safety must come first. Regarding the precautionary precautions that should be taken with consumer drones and unmanned aerial vehicles, a standard has to be developed and implemented. These requirements should also contain elements that prevent accidents from occurring.

4.3 Privacy Concern

Privacy concerns have been brought to the forefront as a result of the ease with which unmanned aerial vehicles that are fitted with high-definition cameras and other electronic components can be acquired by anyone. Without the subjects' knowledge, it is simple to record or monitor someone while they are on their own private property. According to the Canadian Public Safety (CPS), unmanned aerial vehicles have given rise to a significant number of issues about safety, security, and privacy [13]. People have been subjected to extortion and other forms of illegal activity as a consequence of being photographed or recorded without their knowledge. In order to better govern how unmanned aerial vehicles are used, legal laws should be developed regulating the capturing of private photographs or recordings without the owner's agreement when utilizing UAVs, flying past premises, or hovering at window level.

Existing threats for drones/UAVs

Several unmanned aerial vehicles currently available on the market have significant design flaws because there is a lack of standardization. The absence of wireless security is one of the aspects of these problems that causes the most cause for concern.

Some researchers also carried out various forms of cyber-attacks on unmanned aerial vehicles in a simulated setting in order to test the impact and vulnerabilities [33]. Such experiments comprises of the following:

- ***DoS Attack***: Researchers controlled unmanned aerial vehicles via simultaneous requests. The excessive number of queries caused the response to become overloaded, which in turn caused the UAV system to fail.
- ***Buffer-Overflow***: After altering the packet request for controlling the drone or unmanned aerial vehicle, the researchers brought the system that was supposed to be in charge of operating the drone or UAV to a crashing halt.
- ***ARP Attack***: The researcher used the cache-poisoning strategy as part of the Address Resolution Protocol (ARP) assault, which ultimately led to the uncoupling of the UAV from its controller.

An assault on a UAV’s operating system (OS) or micro-controller unit is another facet of a cyber-attack on a UAV. This facet is distinct from attacks on communication connections or on ground control, which are two other aspects of cyber-attacks on UAVs. The operating systems used for UAVs are often fairly similar to those used for smartphones. Because of this commonality, numerous assaults that are successful against smartphone operating systems might also be advantageous when applied to unmanned aerial vehicle systems. Because of advances in technology and UAVs, the number of potential attack vectors against UAVs is growing. In the modern day, the availability of various forms of attacks is almost limitless thanks to advances in technology. The assaults that have been successfully carried out for instructional objectives are shown in Fig. 2, which may be found in references [33, 34]. GPS spoofing is one of the most popular forms of cyberattack against unmanned aerial vehicles and drones, and it is one of the threats described in this section. Signal jamming, de-authentication, and zero-day attacks are the most typical kinds of GPS assaults. Jamming the signal may also be used.

5 Existing UAV/Drone Security Systems and Countermeasures

The first step in mitigating security risks posed by drones and other unmanned aerial vehicles is to categorize the different kinds of assaults, as well as their targets and their goals. The following table details some of the most prominent cyberattacks that have been carried out against unmanned aerial vehicles and drones. Additionally, the type of the assault as well as certain preventative measures against the attacks are highlighted in the table. The verification procedure of a UAV or drone is the focus of the vast majority of the attacks detailed in Table 6. This demonstrates the need of making improvements to the authentication process used for UAVs and drones (Tables 4 and 5).

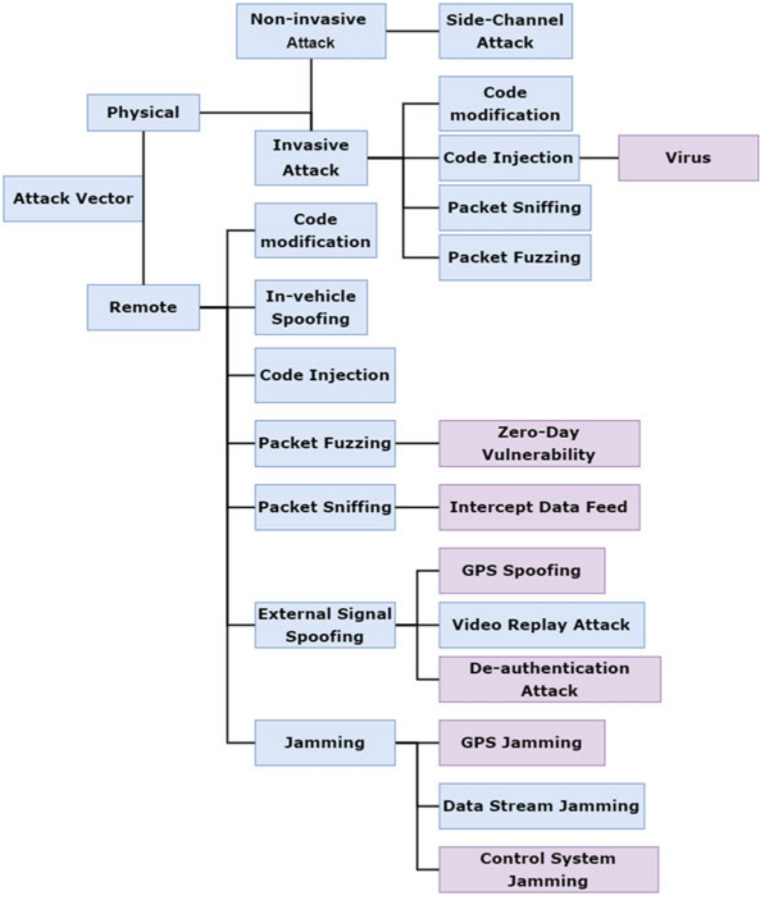


Fig. 2 Attack vector for drones/UAVs with known incidence or educational goal is shown in gray

5.1 Current Countermeasures

Wireless communication networks are beset by a slew of security weaknesses and threats. Recently, machine learning (ML)-based intrusion detection systems (IDS) have shown to be very successful against network threats. Several academics are focusing on resource management issues in machine learning-based intrusion detection systems. This is due to the fact that machine learning-based solutions need more resources than other kinds of solutions. Blockchain technology is also among the most effective methods for protecting the privacy and safety of unmanned aerial vehicles and drones [18].

Table 4 Logical counter measures for UAV/drone in an urban environment

Counter measure	Details
Wi-Fi jamming	Wi-Fi-based drone/UAV operates using a 2.4 GHz frequency. A conventional jammer can jam these frequencies within a limited range and can be used for privacy purposes
Wi-Fi air crack	Although it is an attacking method, it can be used to take control of any illegal or privacy-invading UAV/drone
Three-way handshake	Although it is also an attacking method, it can be used to deauthorize or even jam communication between the UAV/drone and the controller
DoS	Websploit Wi-Fi jammer can be an effective method to jam or de-authenticate UAV from its controller. However, to conduct DoS based attack, some knowledge about the communication channel is required
GPS spoofing	Encryption of civilian-based equipment is very costly and making it vulnerable to GPS spoofing attacks

Table 5 UAV/drone security limitations

Limitation	Details
Availability	UAV/drones are easily accessible for everyone to purchase. There is no owner registration or license registration for purchasing a UAV/drone
Design issue	Due to the absence of standardization, manufacturers are failing to comply with necessary requirements i.e., safe design, factory authentication, etc.
Policies	Standardization and policies are absent for UAV/drone operations and operators. In some countries, policies are defined for UAV/drones flying in proximity of sensitive areas. However, a general set of operating policies for a UAV/drone are still not available
Non-real-time countermeasures	Due to a lack of standardization for design and operational software, the current UAV/drones do not have real-time protection during flight. If a UAV/drone is compromised during flight it cannot be retained by the original owner
Limited testing	Due to limited testing, the available control and communication units are vulnerable to several types of attacks
Forensic limitations	In case of a harmful event, the limited availability of forensic tools and methods makes it difficult to identify the malicious operator of UAV/drones involved in the dangerous act
Unreliable security	Based on the hostile operational environment of UAV/drones, the default security measures are not suitable. Due to the harsh operating environment of UAV/drones, a robust security protocol is necessary. But due to design and resource limitations, improving security measures is very challenging
Authentication	Based on recent events as shown in Table 6, the currently employed authentication method for UAV/drone can easily be compromised. Except for the UAV/drones operated for defense purposes as they have trailered software to cope with the requirements
Limited frequency bands	The UAV/drones are being operated within a limited range of frequencies. Making them an easy target for jamming-based attacks

Table 6 Recommendations for improving UAV/drone security and privacy

Measure	Description
Licensing	Every UAV/drone should be registered and licensed. Such measures will make it easy for the authorities to identify the owner of any harmful drone/UAV
Flying permit	A flying permit similar to a driving license should be issued with a registered drone/UAV. Such regulation would limit. UAV/drone-based illegal or harmful activity
Education	The public should be educated on the harmful or illegal use of UAV/drones
Laws	Based on harmful and illegal events, laws should be introduced for the misuse of UAV/drones
Restricted zones	Areas that are classified or could pose a danger to drones/UAVs should be marked. Map-based public applications should also indicate areas that are no-fly zones for UAV/drones
Non-lethal measures	Non-lethal tools to counter drones/UAVs should be publically available. Such tools can play an important role in urban areas
Machine learning	Security tools such as ML-based IDS can vastly improve the security architecture of drones/UAVs
Multi-factor authentication	Rigid authentication methods can help in stopping several common security threats

5.1.1 Security for UAV/Drone Communication Networks

In the race to meet the most recent challenges in network security, ML-based intrusion detection systems have emerged as some of the most effective technologies. In most cases, IDS may be divided into the following three categories:

- ***Rule-Based***: The purpose of utilizing these kinds of IDS in the UAV domain is to identify false data-injection attacks, more specifically those that target signal strength between UAV and ground control.
- ***Signature-Based***: Signature-based intrusion detection systems (IDS) have also been used by some researchers on UAVs. The authors of the paper used a bio-inspired cyber-attack method that targets airborne networks in their research. Signature-based intrusion detection systems are just as ineffective against unknown and complex attacks as rule-based intrusion detection systems.
- ***Anomaly-Based***: In order to protect UAV networks from jamming assaults, these kinds of IDS are utilized. Jamming attacks include denial of service attacks, distributed denial of service attacks, triggering malfunctions, and attacks based on sensors. The high resource requirement is the only significant problem associated with anomaly-based ML IDS.

There has been an uptick in the amount of unmanned aerial vehicles and drones, which has resulted in an increase in the variety of potential solutions for the UNV communication network. In certain articles, the problems with the physical layer of the UAV communication network were discovered, and an iterative approach that was based on optimizing techniques was suggested. This algorithm demonstrated an improved detection rate of assaults. In a similar vein, additional publications have investigated concerns with ADS-B, line of sight, air-to-ground, and eavesdropping wireless communications, as well as air-to-air wireless communications. Researchers have come up with a number of potential solutions, some of which include making use of modulation, dual antennas, game theory-based algorithms, or Q-learning-based techniques. Encryption, in addition to these ways, is another essential component for ensuring the safety of communication between UAVs. Researchers have been looking at other types of encryption that do not need a lot of resources. Since conventional encryption techniques don't take resources or latency into account, none of those things is considered to be a relevant consideration. Not only does encryption guarantee the safety of communications, but it's also a great tool for verifying the legitimacy of unmanned aerial vehicles and drones.

5.1.2 Data Security

Data that is collected by a UAV or drone is first aggregated onboard the UAV before being sent in any direction. The reduction of network traffic is significantly helped by this aggregation in a significant way. On the other hand, the act of aggregating data and encrypting it results in additional problems. The symmetric cipher is not safe enough to defend against advanced attack techniques, and the asymmetric cipher demands a significant amount of computational power as well as a significant amount of resources. The use of an asymmetric encryption necessitates an increase in the storage overhead. Because of these limitations, researchers are exploring towards strong encryption techniques that are also lightweight for the purpose of protecting UAV and drone data.

5.1.3 Forensic Approaches

The field of digital forensics has the potential to play a pivotal role in determining the various forms of assaults carried out by UAVs and devising effective defenses against them. A general framework for NF was proposed by the authors of article, which may be found here (Network Forensics). The framework performs an analysis on the data that is sent via firewalls or IDS in order to discover any anomalies. In order to accomplish its mission, the framework's primary focus is not only on locating the unusual occurrence but also on tracing the origin of the activity. In another research, the authors propose an NF framework that makes use of DIP (Digital Investigation Process) and a number of other digital investigation approaches organized hierarchically. The methodology described in this study utilizes a two-tiered structure. Assessment, countermeasures, data collecting and analysis, writing up an incident report, and finally, event closure make up the first layer of this process.

The second tier is an object-oriented sub-phase that may be found. In addition, a forensic investigation of a UAV or drone may be divided down into three primary components. In a similar vein, a number of other researchers have suggested various approaches of using forensic methodologies to defend against sophisticated and complicated assaults. The reason why the forensic technique is being emphasized is because, as time passes, the nature of assaults and the goals they seek to achieve become more complicated and harder to determine. Both the culprit and the manner of assault may be determined with the assistance of forensic science. Once the sort of assault has been determined, the proper preventative measures may be put into place to forestall any such incidents.

6 Physical and Logical Attacks Countermeasures

According to the report, the number of incidents involving aircraft and drones increased from 6 to 93 between the years of 2014 and 2017. This highlights how vital it is for the authorities to address concerns over the privacy and safety of UAVs. Because of the rise in the number of cyberattacks on drones and other unmanned aerial vehicles, the government has to implement stringent laws and guidelines to reduce the impact of these worries. Because unmanned aerial vehicles are becoming more common among members of the general public, there is a heightened risk that they may become the target of unlawful activity. Physical and local countermeasures are the two categories into which civilian or domestic UAV defenses are separated.

Keeping in mind that the rational countermeasure for use against UAVs in urban areas does not include cutting-edge technology and is restricted in both its range and its functioning. The rational defenses against unmanned aerial vehicles (UAVs) and drones in an urban setting are outlined in Table 4.

6.1 Military and Government Counter-Measure Techniques

When it comes to countermeasures that are rooted on the military, the availability of resources is often not a concern. As was said previously, the employment of unmanned aerial vehicles and drones is not restricted to observation; rather, they may be used to conduct assaults or to designate sites for attacks, which makes them hazardous instruments on the battlefield. Figure 3 illustrates a few of the most common drone and unmanned aerial vehicle defenses. The armed forces of every nation on earth are very well prepared to counter threats posed by unmanned aerial vehicles and drones. Only a small portion of the information that is widely known and accessible to the public on anti-UAV and anti-drone weapon systems is included. Different strategies are used by government and military agencies in the process of drone detection. It is possible to identify them (UAVs or drones) by the use of audio, video, motion, thermal, radio, and RF-based detection technologies. All of these approaches come with their own set of benefits and drawbacks.

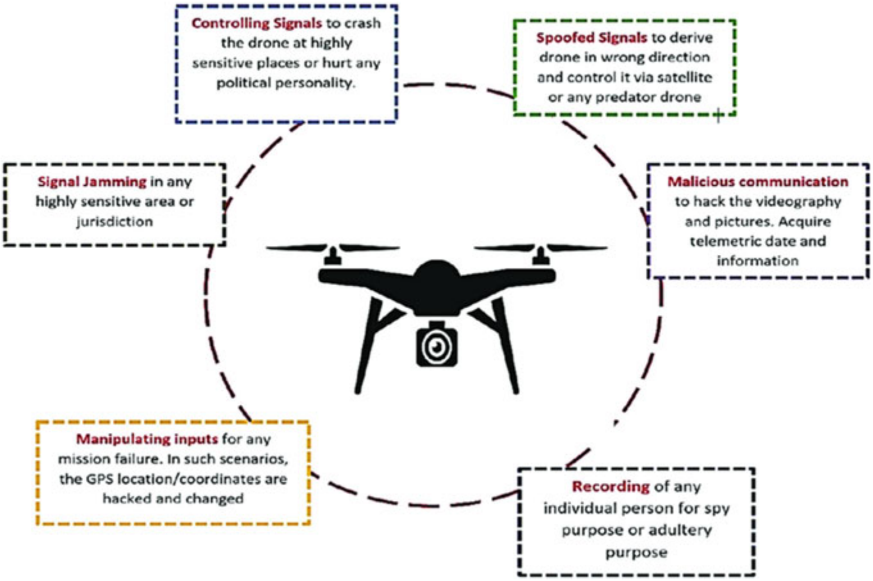

Controlling Signals to crash the drone at highly sensitive places or hurt any political personality.
Spoofed Signals to derive drone in wrong direction and control it via satellite or any predator drone
Signal Jamming in any highly sensitive area or jurisdiction
Malicious communication to hack the videography and pictures. Acquire telemetric date and information
Manipulating inputs for any mission failure. In such scenarios, the GPS location/coordinates are hacked and changed
Recording of any individual person for spy purpose or adultery purpose

Fig. 3 Security and Privacy threats of UAVs

Security implementation limitations

There are still many obstacles to overcome in order to successfully adopt and put into practice stringent security procedures for UAVs and drones. Table 5 outlines some of the most important concerns about the limits of UAVs and drones in terms of security. Standardizing the design of UAVs and drones, as well as communication protocols and basic factory default security measures, is one way to address the majority of the aforementioned restrictions.

Recommendations and summary

Tables 5 and 6 provide many suggestions that might enhance the level of privacy and protection afforded by UAVs and drones. There are some broad suggestions included in Table 5 that might be of assistance in enhancing the privacy and safety of UAVs. While Table 6 provides an inventory of the most current blockchain-based technologies for protecting the privacy and safety of UAVs, In addition, in order to address concerns relating to safety and privacy, regulatory bodies and the industry as a whole need to work together to regularize and standardize unmanned aerial vehicles and drones. Blockchain technology has the potential to provide UAVs and drones security that is both highly effective and significantly improved. The need for more processing resources is the sole issue that has to be addressed when considering blockchain-based solutions. On the other hand, the improvement that blockchain brings in terms of security and privacy is more than sufficient. This is due to the fact that blockchain may be decentralized. The blockchain-based solution has the potential to be a highly good choice for unmanned aerial vehicles that have been created with military and government applications in mind.

6.2 Criminal Attackers

These kinds of assaults may be either physical or intellectual in nature:

- **Physical Attacks**: The most significant risk is connected to the problem of private property monitoring, in which drones may easily be utilized to violate people's physical privacy. This is the most significant risk. The fact that drones are able to penetrate geoboundaries is a highly concerning problem. According to BBC News, people were able to smuggle narcotics, phones, and even blades inside high-security prisons while escaping ground monitoring. This was done in order to provide inmates with these items. This is often accomplished with the help of an octocopter that has the capacity to lift 20 pounds. Additionally, these kinds of assaults involve crashing drones into specific persons (accidentally or purposely) or crashing them into the properties of people, which may cause damages ranging from minor to severe. There is also a risk associated with the use of tiny quadcopters like the DJI Phantom 3, which has a range of 16,000 feet (480 m) and can fly at an altitude of 4000 feet (1220 m). This is a significant challenge, particularly with regards to accidents involving birds, which may result in significant difficulties for the engines of aircraft.
- **Logical Attacks**: Logical attacks include the use of a rogue Access Point (AP). Therefore, a potential attacker has the ability to get sensitive information, such as passwords and credit card data, from users. This also involves attaching a Raspberry Pi device to a drone and configuring it to intercept and take control of other nearby drones. This may be done in order to take over other people's drones. This transforms the malicious drone into a rogue access point (AP) for other drones and devices in the vicinity, and it is also capable of introducing malware into linked cellphones by intercepting and redirecting the data traffic of users, as well as via phishing (malicious links, fake advertisement, or false update). In point of fact, many other types of drone assaults, including as jamming and spoofing, were described and analyzed.

Finally, an adversary might target and exploit the sensor inputs of an unmanned aerial vehicle by manipulating the relevant settings in order to deceive the sensors.

6.3 Terrorist and Insurgent Attacks

Since these drones might be exploited by terrorists for nefarious objectives, the proliferation of drones has led to the emergence of major dangers and difficulties. When it comes to the use of drones, keeping them out of the wrong hands might have devastating effects. In fact, drones are being used by insurgents and terrorists alike. ISIS has also issued an instructive graphic describing their assaults in February 2017, utilizing a pro-ISIS channel known as "Ninawa Province," to display the video obtained before to a terrorist strike. This comes against the background of its increased usage of attack drones in Iraq and Syria. The terrible impact that drones have on the morale of both military and civilian people have caused the whole globe to become very frightened about the significant safety and security dangers posed by drones. In most cases, the following goals are related with terrorists making use of drones:

- **Drone Footage Interception**: Interception efforts of video streams and footage by military drones and unmanned aerial vehicles (UAVs) were common and often effective. One illustration of this would be the incident in 1997 in which Israeli drone video was captured before any further encryption was applied. An further instance of this took place during the Iraqi conflict, when rebels were able to intercept US predator drones by using initially a program with a value of $26 and subsequently the SkyGrabber software respectively.
- **Airstrike Disruption**: ISIS operators would fly and target the airstrike calling team in Raqqa, tricking their opponents into thinking it was a friendly drone hovering overhead. This strategy was adopted by ISIS in order to disrupt airstrikes that were being carried out against them in Raqqa. First, ISIS operators would wait for their adversaries to fly a drone. These drones were equipped with explosives the size of 40-mm grenades and had the ability to strike their target with a high degree of precision.
- **Burning/Incendiary Kites**: In a nutshell, the operation of drones and other unmanned aerial vehicles may be used in a variety of settings. As was just discussed, the danger posed by drones and other unmanned aerial vehicles is extremely concerning and appears to be growing at an alarming rate, particularly as the year 2020 draws closer. This is due to the growing number of instances in which criminals and terrorists use drones and other UAVs to carry out harmful activities. According to the information presented in this section, drones have been used in a variety of fields not just for beneficial goals, but also for harmful ones.

7 Drones Security, Safety and Privacy Concerns

The usage of drones presented benefits on a wide variety of fronts, ranging from the commercial to the personal. However, there are a variety of security, safety, and privacy concerns associated with drone systems. The most senior level of government should address the concerns raised by the many security and privacy risks posed by drones. In addition, there should be a very tight method in place to prevent the capability of drones to capture photographs and record videos of people and properties without the legal consent of the owners of such individuals and things. Traditional wireless networks, such as Wireless Sensor Networks (WSNs) and Mobile Ad-hoc

Networks (MANETs), are not the same as a drone-assisted public safety network from the point of view of security and threat analysis. This may be explained by the fact that it requires less power and carries less information in comparison to a public safety network that is helped by drones. In addition, the coverage area of the drone is larger and more extensive than that of WSNs and MANETs. As a result, the issues posed by security are mostly associated with the restrictions placed on UAVs about their resources as well as their latency. In addition, it is of the utmost importance to make certain that the qualities of secrecy, integrity, availability, authentication, and non-repudiation are satisfied through communication channels. This is carried out in accordance with the methodology and rules established by the AAA:

- **Authorisation**: by bestowing privileges on the personnel operating the UAV.
- **Authentication**: by using something only you have access to as part of a multi-factor authentication system, something you have (your username), and something you are (your biometric information) are considered to be your possessions.
- **Auditing/Accounting**: by conducting searches for and maybe arresting lawful drone and UAV owners in the event that illegal or harmful activity occurs.

The use of drones by malevolent organizations to carry out physical and cyber-attacks is a danger to society because it violates the privacy of the society's citizens and threatens the safety of the general public. These assaults may be carried out using drones. In point of fact, several technological and operational qualities of drones are being abused and misused for the purpose of planning and carrying out future attacks. This involves carrying out crucial activities based on offensive reconnaissance as well as conducting surveillance with the intention of following certain persons and certain places, which creates difficulties with both safety and privacy. In the event that a drone has a malfunction and crashes into a neighboring home, park, parked vehicle, or humans, this presents another potential threat to public safety.

The outcome of this would be the destruction of property as well as the injury or death of people. The present security procedures do not provide protection for such connections since they are based on the assumption that no one could approach them at a distance that would allow them to be compromised or that would allow them to access internal networks through wireless signals. These assumptions lead to poor single factor authentication and the use of common passwords that can be readily cracked, particularly when there is no encrypted connection present. Additionally, these assumptions lead to the usage of usual passwords. Because of this, it is just as simple to steal information from a private building as it is from a public coffee shop.

An adversary would take use of such weaknesses in order to compromise security, safety, and/or privacy. The most significant concerns to the safety of drones are outlined in Fig. 4, along with the countermeasures that may be taken to counteract each one. Following that, we will provide a brief summary of the present and upcoming security problems.

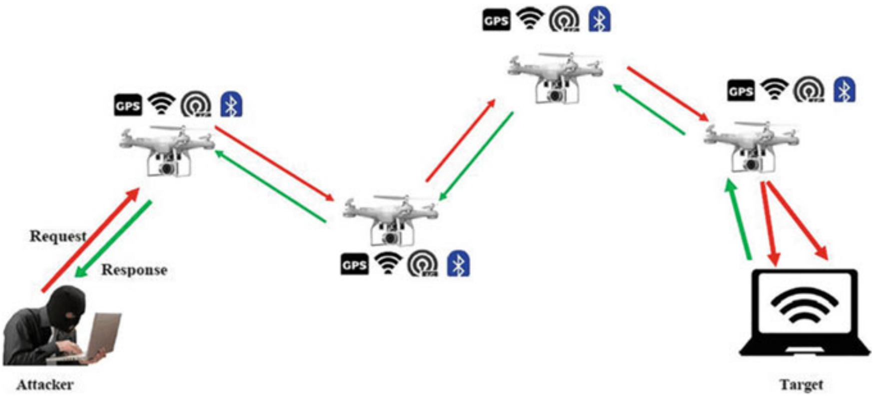


Fig. 4 Stepping stone attack using multiple UAVs

7.1 Security Concerns

The qualities of the drones, including their portability, affordability, and simplicity of operation and maintenance, make them an attractive option for criminals. Terrorists have also begun to focus more on the use of drones to carry out their attacks. This is mostly due to the fact that the nature of drones makes it less likely that they would be discovered. Drones may be armed and modified to deliver lethal poisons or bombs, and they can also be fitted with weapons to strike important infrastructure. In fact, this is already possible.

In addition, persons who are congregating in difficult-to-reach areas may be exposed to the detonation of explosives carried by drones. Because of this, it is much simpler for a terrorist to accomplish their goal, particularly considering the fact that drones combine the stealth of a suicide bomber with the range of an airplane. There is widespread fear among military experts about the possibility that drones may be employed for espionage against the United States. This is because ISIS is able to re-arm drones that are available for purchase in the commercial market and adapt them for use in combat operations over Iraq and Syria.

7.2 Safety Concerns

Both “safety” and “security” are not necessarily synonymous with one another. Outside of the realm of the military, civilian drones and unmanned aerial vehicles have the potential to malfunction and crash into a nearby house or a group of people in November of 2016, a youngster from Stourport-on-Severn, Worcester, United Kingdom, who was 18 months old at the time, had his eyeball slashed in two by the propeller of an uncontrollable drone. Before arriving at Heathrow Airport in April 2016, a passenger plane operated by British Airways and with the flight number

BA727 was struck by a drone. Nonetheless, there were no reports of casualties, and all 132 passengers and five members of the crew were unharmed. As a direct consequence of these occurrences, the following top issues about safety have been identified:

- **Signal Distortion-Jamming**: Because of this, a UAV is susceptible to being hacked, hijacked, and having its GPS or signal jammed as part of an act of cyberterrorism or cybercrime. This is primarily due to the fact that the UAV's command-and-control operation center is vulnerable to being exploited.
- **Lack of Governments Regulation and Awareness**: in particular with regard to the safety procedures and features that must be implemented to guarantee the safe incorporation of UAs into the national airspace domain.

7.3 Privacy Concerns

People's privacy is also at a high risk of being exposed by unwanted flying guests, which can record their movements and capture images of them. This is an indicator of how much our privacy is exposed to such a developing danger, and it should concern us. According to the Canadian Public Safety, unmanned aerial vehicle technology have produced a wide variety of concerns with regard to the gathering of photographs and videos. Blackmailing and other forms of fraud were related with this tactic, which consisted of threatening to reveal private photographs or films of the victim that were taken from above without their consent. The potential risks to one's privacy may, in general, be broken down into three distinct categories.

- **Physical Privacy**: entails flying unmanned aircraft systems (drones) over the property of another person or getting very close to their windows. As a result, the victims' right to personal freedom is put in jeopardy because their assailants have the ability to surreptitiously record videos and take pictures of themselves acting in potentially inappropriate ways.
- **Location Privacy**: is based on following and identifying individuals using a drone that is flying and buzzing over them without the persons being monitored being aware that they are being watched.
- **Behaviour Privacy**: is a situation in which the presence of a flying drone might influence how people behave and respond, particularly when they are aware that they are being watched. Because of this, not only would their freedom be restricted, but also their private would be violated and their privacy would be invaded. When it comes to the Internet of Things (IoT), particularly when it comes to drones and other unmanned aerial vehicles, security, safety, and privacy are essential needs that must be met. In this part, we will discuss the primary issues about privacy, safety, and security that may be imposed as a result of security breaches. These primary problems need to be addressed as soon as humanly feasible; if they aren't, the unlawful use of these substances will continue to steadily grow, which is particularly likely given the lack of stringent regulations, legal limits,

and consequences. Following this, we will discuss the primary security flaws and dangers that need to be taken into account in order to ensure that the safety of the drones is not jeopardized.

8 Drones Existing Threats and Vulnerabilities

The use of unmanned aerial vehicles and drones is increasingly seen as a significant risk to information security.

- **Prone to Spoofing**: The configuration and flight controllers of several types of unmanned aerial vehicles with many rotors were analyzed, and the results showed numerous flaws. Tests conducted shown that information may be readily obtained, manipulated, or injected by using GPS spoofing. These experiments revealed that this is possible. Because of this flaw in the data connection, hackers now have full control over the drone and may intercept and spoof transmissions.
- **Prone to Malware Infection**: Users are able to pilot drones using wireless remote controls such as mobile phones. This method, on the other hand, was proven to be vulnerable; it makes it possible for cybercriminals to generate a reverse-shell TCP payload, inject it into the memory of the drone, and use it to discreetly install malware on the computers that are responsible for operating the ground stations.
- **Prone to Data Interference and Interception**: telemetry feeds are utilized to monitor the vehicles and ease the sharing of information over open non-secure wireless communication, which leaves them subject to a variety of dangers. These include the stealing of data, the introduction of harmful material, and the modification of pre-determined flight trajectories.
- **Prone to Manipulation**: Due to the fact that drones follow pre-programmed and pre-defined flight paths, manipulation is possible, and this has the potential to have catastrophic repercussions.
- **Prone to Technical Issues**: A great number of drones have a variety of technical difficulties. This includes program issues such as a failed connection between a user's device and the drone, which might cause the drone to either crash or take off in the wrong direction. It is important to be aware that the batteries have a lower life lifetime in cold conditions, which results in a shorter flying duration as well as the possibility of malfunctioning.
- **Prone to Operational Issues**: The lack of flying abilities among drone owners is another big challenge, as is the variety of drones that are now in use. This has the potential to inflict significant damage and/or injuries to both workers and/or property. In point of fact, drones are delicately constructed, which means that even a little mishap might cause the drone to crash. If one of the rotaries fails to operate well or completely ceases operating, it might result in considerable turbulence, making it difficult to keep control of the drone. This would, in almost all circumstances, result in the drone plummeting to the ground. For instance, described an event in which an Israeli drone violated the airspace above Lebanon

and then crashed in the south of the country owing to a combination of technical and operational difficulties.

- **Prone To Natural Issues**: Due to the fact that they are so lightweight, drones are sometimes unable to endure the effects of wind. In addition, if the temperature is really high, the engine can overheat and stop working, causing the drone to crash. Additionally, the battery may burst into flames, resulting in significant property damage and even bodily danger. Drones do not come with any kind of protection against the rain, thus it is impossible for them to fly in it. This presents another problem for the industry. When drones fall into bodies of water like lakes, rivers, beaches, or even pools, they often cease functioning instantly. The reduced vision, which may drop from a few meters to less than a meter, can cause a breakdown in communications between the drone and the GPS, which in turn sends the drone outside of its control area until it crashes. Owners are recommended not to fly their drones during fog for this reason.

9 Drones Existing Cyber-Countermeasures

An attacker's primary reasons, aims, and goals may be used to categorize the primary countermeasures that can be implemented to secure drones from security threats. These countermeasures can be divided into the following groups. Following is a discussion on the many approaches that may be taken to ensure the safety of drones' networks, communications, and data.

9.1 Securing Drones/UAVs Networks

Drone networks are vulnerable to a number of attacks and problems related to security. Intrusion Detection Systems, often known as IDSes, have recently been implemented in order to identify harmful behaviors carried out by UAVs and drones as well as suspicious assaults that may be directed against them. In normal operation, an intrusion detection system (IDS) will monitor and analyze both incoming and outgoing network data in order to look for unusual behavior. Examining the data audits (trails) that were gathered at various points along the network is their plan for locating and determining the source of cyberattacks. In the following, we will discuss the many different IDS strategies that may be used to defend drone networks from unauthorized users.

- **Rule-Based Intrusion Detection** Strohmeier et al. devised a rule-based intrusion detection technique for the purpose of protecting the connection between an airplane and a ground station and published their findings. The purpose of this endeavor is to identify assaults of bogus data injection, particularly those that target the signal strength. They demonstrated that it is possible to identify attackers within a minute and a half. The authors made use of a UAV-IDS that was based on behavior rules. The guidelines for appropriate behavior were developed on the basis of predetermined attack models, which included careless, random, and opportunistic assaults. This enabled for the reduction of detection mistakes, including the rates of false positives and false negatives, while maintaining a crucial balance between the UAVs' level of safety and their overall performance. Mitchell et al. proposed BRUIDS, an adaptive behavior-rule specification-based intrusion detection system, in the article. This system is able to identify hostile UAVs in airborne systems. The findings of the simulation demonstrated that BRUIDS is capable of achieving a greater detection rate in comparison to the multi-trust anomaly-based IDS strategy, all while maintaining a reduced percentage of false positives. Rule-based intrusion detection systems, on the other hand, have a problem managing its complexity, which need human interaction for rules setting. In addition, this kind of intrusion detection system (IDS) is unable to identify unknown threats.

- **Signature-Based Intrusion Detection** An ADS-B intrusion detection framework was described by Kacem et al. in their paper, which was built to protect an aircraft against cyberattacks that target ADS-B communications. A system like this one is constructed using signature detection methods, which include analyzing the GPS location of an aircraft. A bio-inspired detection technique was developed by Casals et al. and published for the purpose of detecting cyber-attacks that target aerial networks. However, in the same way that a rule-based IDS is unable to identify unknown assaults, a signature-based IDS is also unable to detect attacks that use dynamic signatures.
- **Anomaly-Based Detection** In the UAV industry, the primary function of an anomaly-based detection intrusion detection system (IDS) is to protect against jamming attempts. An anomaly-based learning system was proposed by Rani et al. in their paper to defend UAV nodes against DoS and DDoS assaults. This system prevents the motors of drones from operating at temperatures that are outside of their normal range. This method provides the possibility to avert motor failure by landing the drone in the event that it has overheated, although it does not completely prevent the problem. The results of the experiments show that it is possible to securely operate the drone by using the information provided by the sensors. A method was designed to defend against distributed denial of service attacks, and its performance was evaluated using real-time traffic. The findings demonstrated an accurate identification of many distinct kinds of anomalies. However, further testing is necessary before determining whether or not it is effective.

An Intrusion Detection and Response Framework (IDRF) was introduced by Sedjelmaci et al. with the purpose of protecting a UAV network from assaults on data integrity and network availability, as well as protecting a UAV-aided VANET from hostile threats. These kinds of attacks can be particularly damaging. This strategy works to identify malicious network abnormalities by operating at the level of the

UAV as well as the base station. Mitchell et al. developed a specification-based intrusion detection system (IDS) in their paper for the purpose of securing sensors and actuators that are integrated in a UAS. The IDS was tested on UAVs to study the impact that an attacker's behavior might have on the system in order to determine how successful their solution is. According to the findings, the approach makes an effective trade-off between a high detection probability and a high false positive rate in order to provide improved safety for applications that use UAS. In view of the fact that gateways for drone networks could be operating under certain restrictions (fog nodes), there is a need for a lightweight host-based anomaly detection approach that calls for just a minuscule amount of processing resources. Either a straightforward method of machine learning or a statistical strategy using the fewest available characteristics may be used to accomplish this goal. This structure should be built on top of a hybrid approach. A system like this one would rely on both machine learning and the expertise of human security professionals.

9.2 Securing Drones/UAV Communications

There has been a growth in the number of drone and unmanned aerial vehicle (UAV) film interceptions, which led to the presentation of several ways to secure UAV communication. The results of the simulation demonstrated a substantial increase in the level of discretion provided by UAV communication systems, which was one of the objectives of the project. The findings of the simulation indicated an increase in the secrecy rates of communications between ground stations and unmanned aerial vehicles (UAVs and G2Us). An iterative sub-optimal approach was proposed by the authors by utilizing the block coordinate descent method, the S-procedure, and the successive convex optimization method. The findings of the simulation demonstrated a discernible rise in their worst-case average secrecy rate.

The results of the simulation demonstrated a successful reduction in the UAV assault rate as well as an improvement in the system's capability for maintaining secret. Encryption of drone and unmanned aerial vehicle communications is an absolute need, and should be used in addition to modulation methods. Various cryptographic techniques, including the encryption and authentication of messages, were recently suggested in this context as potential solutions. In addition, this may be done in such a manner that the source authentication, together with the integrity and confidentiality of the data that is being transferred, is maintained. Elliptic Curve Cryptography, often known as ECC, digital signatures, hashing, and other cryptographic processes are all included into UAV applications under TPPA. The use of battery-powered devices across long distances necessitates the use of lightweight cryptographic methods and protocols in order to ensure the confidentiality of drone communications. Recent research provided novel cryptographic methods that only need one round of functions or a small number of iterations. In addition, authentication mechanisms that already exist to protect users' privacy may make use of these lightweight cryptographic algorithms with just a little amount of additional latency. Additionally, the settings of the physical layer may be used for multi-factor authentication.

9.3 Securing Drones Data

It is necessary to combine all of the data that is obtained by drones in order to reduce the amount of traffic that is regularly delivered to the base station. Unfortunately, present HE solutions have problems with either their performance or their level of security. Both symmetric and asymmetric ciphers have security flaws, although symmetric ciphers are more susceptible to attacks that combine plaintext and ciphertext, while asymmetric ciphers have a higher computational and resource cost, in addition to the storage overhead that is associated with them.

9.4 Forensic Solutions

Within the realm of unmanned aerial vehicles and drones, digital forensics methods are seeing considerable use. Through the use of a chain-of-custody that is composed of six stages, the purpose of such a model is to pinpoint the origin of the assault. Another framework was described, and it promotes a complete multi-tier hierarchical digital investigation paradigm by using a Digital Investigation Process (DIP). The following are the two levels that make up this structure:

1. **First-Tier**: consists of three phases: the period of assessment and incident response, the phase of data collecting and analysis, and the phase of presenting results and closing the event.
2. **Second-Tier**: consists of a phase that is focused on objects. Bouafif et al. published the findings of their digital forensic investigation carried out on a Parrot AR drone 2.0 in the article. This may be accomplished by the examination of flight records, the recognition of artifacts, and the recording of digital information from the drones. Clark et al. introduced an open source forensics tool called DRone Open source Parser (DROP). This program parses proprietary data files taken from the DJI Phantom III's nonvolatile internal storage as well as text files found on the mobile device that is used to operate the drone. According to the findings, it is feasible to determine GPS positions, battery life, and total flying duration, in addition to having the capacity to connect a specific drone to the mobile device that controls it based on the serial number of the drone. Further investigation indicated that it is possible to retrieve data for forensic purposes by physically removing the Secure Digital (SD) card from the drone.

This framework was the product of an investigative procedure that was based on a physical crime scene. In addition, a procedure for conducting a forensic examination of a UAV was described in. This procedure, which followed a step-by-step method based on three primary initial stages, was offered.

- **Preparation Phase**: This is done so that the chain of command may be identified after the UAV has fallen and been taken as the first piece of equipment to be confiscated. It makes it possible to conduct a traditional forensic investigation in order to identify any DNA or fingerprints that could be on the drone or UAV. Therefore, a conventional piece of evidence, such as witness statements, together with a digital piece of evidence might be integrated.
- **Examination Phase**: Identifying the data storage locations is just one step in the process. This necessitates the use of non-destructive extraction methods, utilizing either commercial or non-commercial forensic tools, in order to safeguard the original data. Alternatively, destructive extraction methods may be utilized.
- **Reporting and Analysis Phase**:

  It is based on an initial analysis of the extracted data. As a result, it is essential to have a solid understanding of how the recording function works in order to successfully intercept the data and convert it into a format that can be read by humans. In addition, a well-fitting forensic model that was given the name "waterfall model" was proposed as a reaction to the large disparities that existed between several commercial models.

  It has become necessary to build effective countermeasures in order to retrieve genuine evidence. It is important for these anti-anti-forensics solutions to be created in a manner that allows them to withstand anti-forensics approaches while still preserving the primary functionality of drone systems. This section provided an overview of the various security solutions that are currently available for safeguarding drone systems. These solutions included both cryptographic and non-cryptographic approaches. In essence, the goal of the cryptographic solutions is to secure the communication between the drones as well as the data that is conveyed, while the goal of the non-cryptographic solutions (IDS) is to identify and recover from any potential security threats. The following subsections detail the typical assaults carried out by UAVs, also known as unmanned aerial vehicles, on various healthcare equipment.

Deauthentication attack

One kind of distributed denial of service attack is known as a deauthentication assault. This assault may be carried out in any of two ways:

(1) **Against the authenticated Clients**: An assortment of deauthentication frames are sent to the clients by the attacker, with the request that they severe their connection to the access point (AP).

(2) **Against the AP**: The attacker starts the process of re-authenticating all of the connected clients by sending a series of deauthentication packets to the access point. Through the process of re-authentication, valid clients and AP engage in

this handshake with one another. This assault is initiated with the intention of disconnecting every single client that is currently connected [36].

Stepping stone attack

The stepping stone assault is a kind of attack in which numerous hosts, or unmanned aerial vehicles (UAVs) in this example, are used to launch an attack on the target. The stepping stone assault, which makes use of several UAVs, is seen in Fig. 4. The attacker sets up the UAV network such that all of the drones are linked to each other through a mobile hotspot.

Drone-in-the-middle (DitM) attack

The UAVor drone-in-the-middle (DitM) attack is used to take control of the communication path between two devices, then intercept and reroute all of the communications that are being sent and received. The DitM attack is depicted in Fig. 5, which can be found here. When it comes to BAN and IMD, the actual device itself serves as the target, and the data receiver of the device takes the place of the Wi-Fi router in this scenario.

Cloud assisted UAV attack

The majority of unmanned aerial vehicles (UAVs) on the market today are developed with advanced features such as internet of things, sensor cloud, and cloud. The attacker will utilize the UAVs that are equipped with cloud capabilities to remotely store the data that has been compromised. This will allow the attacker to retrieve the data at a time and place of his choice. In most cases, the data packets that are created by a wireless network are enormous, which necessitates the use of advanced processing in order to extract important information. UAVs that just have little storage space and a small amount of backup battery power are unable to complete these sophisticated

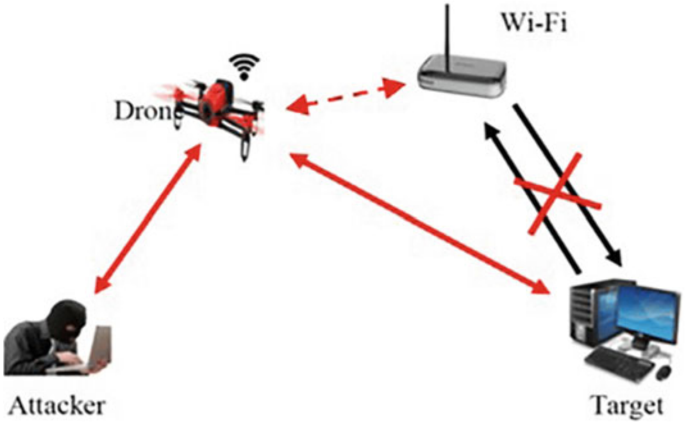


Fig. 5 UAV in the middle attack

calculations. UAVs that are helped by the cloud may be used so that data can be readily sent to the cloud with low drain on the battery. This helps reduce the load of storage while also extending the life of the battery (as shown in Fig. 3).

Evil twin attack

The evil twin assault, which is shown in Fig. 4, is similar to a DitM attack; however, rather than the UAV inserting itself in the midst of a data stream, the evil twin attack involves the UAV taking over as the receiver for the BAN or IMD. The assault that comes from the evil twin is carried out in two distinct stages. At first, the attacker will produce deauthentication probes with the intention of deauthenticating clients that are connected to a genuine access point. Next, the adversary will start a bogus access point, spoofing the MAC address, reallocating the channels used by the original AP, and broadcasting the SSID [36]. This will allow the adversary to assume the identity of the legitimate AP. Last but not least, the clients are compelled to go through another round of authentication with the UAV playing the role of the AP.

Wifiphishing

Wifiphishing is a form of masquerading attack that is carried out on a Wi-Fi network in order to steal sensitive information such as login passwords, information regarding medical accounts, and other similar data. There are two stages to the process of wifiphishing. The first phase of the attack is an evil twin attack, and the second phase involves a fake login page that is forcefully displayed on the client side. This page prompts the clients to enter the valid credentials in order to re-connect with the access point (AP). In a similar vein, the adversary can make use of any phishing pages in order to acquire vital information such as passwords for patient portals.

UAV cyber attack experiment

The HackerUAV that is seen in Fig. 5 is used to transport a Raspberry Pi3 that is powered by batteries. The Hacker unmanned aerial vehicle has an average flying duration of 35 min. A Wi-Fi hotspot may also be enabled by configuring and attaching an external Wi-Fi adapter to the Raspberry Pi3 module [3]. All of the traffic that is collected is kept not just on the local hard disk but also in Dropbox, which is a cloud storage service that is accessible online.

UAV cyber attack scenarios

Two separate tests are carried out as part of this study to illustrate the cyberattack capabilities of UAVs. The first reveals how to get into healthcare automation systems, while the second shows how to take over and manipulate BAN healthcare equipment.

The term “smart hospital automation” refers to an automated hospital control system that gives consumers the ability to operate a variety of hospital appliances by means of Wi-Fi sensor devices [5]. Applications such as this include the automated identification of patients and healthcare professionals, the monitoring of hospital resources using RFID technology, and the management of lighting, TVs, and other environmental systems like as HVAC [10]. If an attacker is able to get into any one of the gateway devices remotely at a wireless smart hospital, then it provides a channel for the attacker to break into additional smart devices that are linked with the compromised gateway device. A denial of service assault is used as an example in this scenario to investigate how a UAV may hack into smart hospital Wi-Fi routers and other wireless systems. The unmanned aerial vehicles (UAVs) are built with the capability of disrupting the wireless signal that runs between the device controllers and the gateway device. After the signals are disrupted, the link between the UAVs and the hospital control system will be severed, and the UAVs will assume control of the whole hospital control system.

10 Conclusions

An age of autonomous aerial vehicles is about to begin as a direct result of the current trend and exponential rise in the usage of unmanned aerial vehicles and drones. The use of unmanned aerial vehicles and drones brings a number of benefits to both the military and the civilian sectors. Despite this, substantial issues over privacy and safety have arisen as a direct result of the widespread usage and accessibility of the internet. These gadgets have become particularly valuable instruments for deceitful actions as a result of their adaptability, cheap cost, simplicity of deployment, and mobility. These vehicles (UAV/drone) are still quite effective for carrying out damaging acts, despite the availability of various defenses against the malicious use of these vehicles. There are also extremely serious concerns about privacy when it comes to UAVs and drones. In today's technology era, protecting one's privacy is one of the most important concerns for both people and businesses.

Because they are autonomous, flexible, and easy to use, as well as having a low cost and energy consumption, drones and unmanned aerial vehicles have ushered in a new era of aviation that features autonomous aerial vehicles in both the civilian and military spheres. This has resulted in a multitude of benefits, including economic, commercial, and industrial, and it has led to a new era of aviation overall. However, the widespread usage of these technologies has resulted in a multitude of safety, security, and privacy concerns. These concerns have surfaced in the form of a variety of cyber assaults, threats, and problems, all of which are described in this article. This report included a complete analysis of these (security and privacy) issues, which included an outline of the reasons that are driving these concerns along with potential countermeasures. The study also included a variety of suggestions, one of which was the use of already available blockchain-based solutions. These technologies may offer increased data integrity, authenticity, and accessibility to unmanned aerial vehicles and drones. According to the findings of the UAV tests, there are four potential security risk mitigation strategies that should be used to protect medical BAN and IMD devices in addition to other Wi-Fi enabled equipment in hospitals from being compromised by an external agent. These four strategies for risk reduction are examples of the latter kind of security approach and entail the addition of additional security features to the device in question via the use of programming.

References

1. Bombe MK (2020) Unmanned aerial vehicle (UAV) market worth $21.8 billion by 2027- pre and post COVID-19 market analysis report by Meticulous Research. Retrieved from https://www.meticulousresearch.com/download-samplereport/cp_id=5086. Accessed on 18 Aug 2022
2. Kumar R, Kumar P, Tripathi R, Gupta GP, Gadekallu TR, Srivastava G (2021) SP2F: a secured privacy-preserving framework for smart agricultural unmanned aerial vehicles. Comput Netw 187:107819
3. CyanogenMod (2017) CyanogenMod android operating system. Retrieved from https://github.com/CyanogenMod
4. Dinan S (2017) Mexican drug cartels using drones to smuggle heroin, meth, cocaine into U.S.—Washington Times. Retrieved from https://www.washingtontimes.com/news/2017/aug/20/mexican-drug-cartels-usingdrones-to-smuggle-heroi/
5. DJI (2018) Phantom 3 Professional—specs, FAQ, tutorials, downloads and DJI GO—DJI. Retrieved from https://www.dji.com/phantom-3-pro/info#specs
6. Irizarry MJ, Gheisari B (2012) Walker, usability assessment of drone technology as safety inspection tools. Electron J Inf Technol Constr 17:194–212
7. Bowden M (2013) How the predator drone changed the character of war. Smithson Mag. Retrieved from https://www.smithsonianmag.com/history/how-the-predatordrone-changed-the-character-of-war-3794671/. Accessed on Nov 2022
8. O'Donnell S (2017) Consortiq. Retrieved from https://consortiq.com/short-history-unmanned-aerialvehicles-uavs/. Accessed on Nov 2022
9. Chen R, Yang B, Zhang W (2020) Distributed and collaborative localization for swarming UAVs. IEEE Internet Things J 8:5062–5074
10. Gartner (2018) Gartner says worldwide sales of smartphones recorded first ever decline during the fourth quarter of 2017. Retrieved from https://www.gartner.com/newsroom/id/3859963gnuplot.(2017).gnuplottool. Retrieved from http://www.gnuplot.info/download.html
11. Rambling D (2017) Islamic state now using off-the-shelf drones I. Defense content from Aviation Week. Retrieved from http://aviationweek.com/defense/islamicstate-s-new-weapon-choice-shelf-drones
12. Horsman G (2016) Unmanned aerial vehicles: a preliminary analysis of forensic challenges. Digit Invest 16:1–11. https://doi.org/10.1016/J.DIIN.2015.11.002
13. Jain U, Rogers M, Matson ET (2017) Drone forensic framework: sensor and data identification and verification. In: 2017 IEEE sensors applications symposium (SAS). IEEE, pp 1–6. https://doi.org/10.1109/SAS.2017.7894059
14. Karlsson K-J, Glisson WB (2014) Android anti-forensics: modifying CyanogenMod. In: 2014 47th Hawaii international conference on system sciences. IEEE, pp 4828–4837. https://doi.org/10.1109/HICSS.2014.593
15. Kernel (2009) Linux_2_6_32—Linux Kernel Newbies. Retrieved from https://kernelnewbies.org/Linux2_6_32
16. de Croon GCHE, Groen MA, De Wagter C, Remes B, Ruijsink R, van Oudheusden BW (2012) Design, aerodynamics and autonomy of the DelFly. Bioinspir Biomim 7:025003
17. Chan KW, Nirmal U, Cheaw WG (2018) Progress on drone technology and their applications: a comprehensive review. AIP Conf Proc 2030:020308
18. Berg TR (2020) Air Space Mag. Retrieved from https://www.airspacemag.com/daily-planet/first-map-compiledaerial-photographs-180973929/. Accessed on Nov 2022
19. Ali BS, Saji S, Su MT (2022) An assessment of frameworks for heterogeneous aircraft operations in low-altitude airspace. Int J Crit Infrastruct Prot 37:100528
20. Wright S (2019) Ethical and safety implications of the growing use of civilian drone. UK Parliament website (science and technology committee)
21. Coach U (2020) Master list of drone laws (organized by state and country). Retrieved from https://uavcoach.com/drone-laws/. Accesses on Nov 2022
22. Aljehani M, Inoue M, Watanbe A, Yokemura T, Ogyu F, Iida H (2020) UAV communication system integrated into network traversal with mobility. SN Appl Sci 2:2749

23. Cheaw BH, Ho HW, Abu Bakar E (2019) Wing design, fabrication, and analysis for an X-wing flapping-wing micro air vehicle. Drones 3:65
24. Teoh ZE, Fuller SB, Chirarattananon P, Prez-Arancibia NO, Greenberg JD, Wood RJ (2012) A hovering flapping-wing microrobot with altitude control and passive upright stability. In: Proceedings of the 2012 IEEE/RSJ international conference on intelligent robots and systems, Vilamoura-Algarve, Portugal, pp 3209–3216
25. Professionals, drones and remotely piloted aircraft (UAS/RPAS)-frequencies and radio licenses, Traficom (2021). Retrieved from https://www.traficom.fi/en/transport/aviation/drones-and-remotely-piloted-aircraft-uasrpasfrequenciesand-radio-licences. Accessed on Nov 2022
26. Carnahan C (2014) ISO/TC 20/SC 16 unmanned aircraft systems. Retrieved from https://www.iso.org/committee/5336224.html. Accessed on Nov 2022
27. Luo A (2016) Drones hijacking. Dejean. Maarse M, Sangers L, Ginkel JV, Pouw M (2016) Digital forensics on a DJI Phantom 2 Vision + UAV
28. Majendie A, Chia K (2018) The future of flying is all about drones—Bloomberg. Retrieved from https://www.bloomberg.com/news/articles/2018-02-08/in-the-global-game-of-hideand-seek-the-drones-are-winning
29. Parrot (2017) Quad copter AR drone 2.0 power edition I. Parrot Store Official. Retrieved from https://www.parrot.com/uk/drones/parrot-ardrone-20-power-edition#parrot-ardrone-20-power-edition-details
30. Hartmann KSC (2013) The vulnerability of UAVs to cyber, in cyber conflict (CyCon). In: Proceedings of the 2013 5th international conference, Tallinn, Estonia
31. Abdullah, Q.A. Introduction to the Unmanned Aircraft Systems. Available online: https://www.eeducation.psu.edu/geog892/node/643 (accessed on November2022).
32. Mikelionis L (2018) Drug cartels using drones to smuggle drugs at border. Fox News. Moskwa W (2016) World drone market seen nearing $127 billion in 2020. PwC Says—Bloomberg. Retrieved from https://www.bloomberg.com/news/articles/2016-05-09/world-drone-market-seennearing-127-billion-in-2020-pwc-says
33. Pleban J-S, Band R, Creutzburg R (2014) Hacking and securing the AR drone 2.0 quadcopter: investigations for improving the security of a toy
34. Creutzburg R, Akopian D (eds) International society for optics and photonics, vol. 9030, p 90300L. 10.1117 / 12.2044868
35. Pilot (2022) What's the difference between drones, UAV, and UAS? Definitions and terms. Pilot Institute. Retrieved from https://pilotinstitute.com/drones-vs-uav-vs-uas/. Accessed on Nov 2022
36. Carrier B (2002) Open source digital forensics tools: the legal argument

A Machine Learning Based Approach to Detect Cyber-Attacks on Connected and Autonomous Vehicles (CAVs)

Safwan Abdul Nazaruddin and Umair B. Chaudhry

Abstract Connected and Autonomous Vehicles (CAVs) are gaining more interest and are growing steadily in recent years. They will surely become the backbone of next generation intelligent vehicles offering safe travels, comfort, reduced pollution, with many other beneficial features. However, with CAVs being equipped with high levels of automation and connectivity also opens several attack points or vulnerable points for adversaries to conduct attacks. Such security issues need to be addressed before commercialising CAVs. In this research paper, the focus is to develop a few machine learning models using different machine learning algorithms and evaluate them using defined evaluation criterions to identify and recommend the best suitable model for detecting attacks in CAVs. In addition, this paper also defines different terms related to CAVs such as CAV, CAV cyber security, CAV architecture and different vulnerabilities and risks present in the CAN bus. The paper then describes the different attacks possible on CAVs and the corresponding mitigation methods and detection techniques.

Keywords Anomaly detection · Connected autonomous vehicle · Controller area network bus · Cyber-attacks · Machine learning

1 Introduction

Connected and Autonomous Vehicles (CAVs) use both the Connected Vehicle (CV) and Autonomous Vehicles (AV) technologies for navigation, driving, communication, and to react to nearby environments in real-time without any human intervention. CAVs help in reducing pollution, traffic congestions, and road accidents by providing traffic management functions and driving assistance which reduces human

S. A. Nazaruddin
Northumbria University London, London, UK

U. B. Chaudhry (✉)
Queen Mary University of London, London, UK
e-mail: u.b.chaudhry@qmul.ac.uk

H. Jahankhani and A. El Hajjar (eds.), *Wireless Networks*, Advanced Sciences and Technologies for Security Applications,
https://doi.org/10.1007/978-3-031-33631-7_6

driving mistakes. Moreover, the elderly and physically challenged people are greatly benefitted from CAVs or completely self-driving vehicles [1].

Although CAVs provide many benefits, there exists several security and privacy challenges. The security risks in CAVs are increasing rapidly as these vehicles are connected and have access to the internet [2]. If an adversary compromises a CAV, then they will be able to control the vehicle remotely which will not only disrupt vehicle systems but also might cause accidents and injuries to people inside or nearby the vehicle. For example, two security engineers in 2015 were able to demonstrate that autonomous vehicles such as Jeep Cherokee are vulnerable to many attacks and successfully conducted attacks by exploiting a vulnerability found in the vehicle's radio system [3]. By entering the vehicles system through the entertainment unit, they were able to control wind shield wipers, air-conditioning, accelerator, brakes, and the steering wheel from a remote place which creates a real danger to everyone in and around the vehicle, if the attacks were conducted by a real attacker. Consequently, the vehicle manufacturer recalled all their autonomous vehicles for manually installing patches for this vulnerability. Before this incident, most of the automobile manufacturers believed that it was not possible to perform distant attacks on vehicles and this event has been a watershed for all of them [2].

Therefore, before deploying CAVs worldwide into the transportation system, the potential cyber-security vulnerabilities and risks should be addressed. Hence, there is a need to research how to define, evaluate, and detect different types of cyber-attacks on CAVs.

2 Literature Review

In this era of fast paced development of technology, main interest of automotive engineers has been on developing autonomous vehicles. The development in this sector can be seen by the increasing number of Electronic Control Units (ECU), applications, and sensors used in vehicles which in turn helps in building a more reliable and efficient driving experience [4]. Modern vehicles now are reported to contain hundred million lines of code to provide drivers an easier and safer experience [5].

Even though CAVs are not yet commercialised, many of the CAV software and applications are being installed and used in commercialised modern vehicles [4]. To illustrate, most of the modern vehicles uses Advanced Driving Assistant System (ADAS) which helps in the reduction of accidents caused by human mistakes [6]. With massive development and usage of wireless technologies in vehicles, such as Radio Frequency Identification (RFID), it is now possible to automatically charge vehicles passing through toll stations and parking lot exits without stopping and thereby improves traffic efficiency [7].

CAVs have also received great interest from the public. Based on a 2015 survey carried out by Cetelem, 81% of the surveyed drivers claimed that they wanted to own a fully autonomous vehicle by 2025 [8].

The autonomous vehicles market is booming and is expected to reach around 34 billion pounds by 2025 [8]. Waymo exclusively for developing autonomous vehicles and have completed around 4 million kilometres of trial run [9]. Apollo, a free open-source platform for autonomous driving which was designed to tackle all the concerns associated with precise sensing and decision making [10]. Uber, have also created CAVs and completed successful trial runs on public roads in Arizona [11]. Similar projects and road tests are also conducted by different automotive companies such as, Benz and Audi.

In USA, all the CAV relevant rules and regulations are carried out at state level and 20 states had released guidelines related to autonomous vehicle in 2016 [4]. The Chinese government have launched several CAV projects and chosen Shanghai as the main test zone for CAVs [12]. In Japan, a 10 mile field have been set up and used for CAV testing since 2017 [13]. However, most of these research, not much focus has been given to CAV cyber security until last few years which is a significant part in its development.

It is crucial that along with the development of modern connected and autonomous vehicles, engineers should also focus on securing such vehicles from outside threats and attack.

2.1 Connected and Autonomous Vehicle (CAV)

Connected Vehicles (CVs) are vehicles that have their own internet connection and can connect and share data with surrounding devices and other nearby CVs through wireless networks [14]. Such important information transfers such as location and speed between CVs, toll booths, and other roadside infrastructures during traffic and intersections provides many benefits, some of which are:

- Automatic braking to avoid collisions
- Adaptive cruise control
- Traffic redirections to avoid congestion
- Sending useful messages to drivers related to nearby traffic

Autonomous Vehicles (AVs) are also often called as self-driving or driverless as they drive themselves to pre-determined locations by scanning their surroundings through cameras, radar, sensors, and Artificial Intelligence (AI). Sensory information from sensors and radars can be interpreted by the vehicle to detect bumps, barriers, and obstacles on the road and choose the most suitable path for the vehicle (2018). The US Society of Automotive Engineers (SAE) have classified autonomous driving system into six different levels ranging from level zero to level five. Level zero corresponds to zero automation where all the responsibility falls onto the driver and level five corresponds to vehicle's being completely automated and no human intervention is required.

CAVs can understand their surroundings, drive, and perform reliably without any human involvement along with having connectivity features that permits them to be coordinated, cooperative, up-to-date, and pro-active [15]. People with special mobility needs, including the elderly and the disabled greatly benefit from CAVs or completely autonomous vehicles [1].

CAVs consist of large number of onboard sensors and Controller Area Network (CAN) bus that allows the sensors to communicate among each other and neighbouring vehicles and infrastructures as shown in Fig. 1 [16]. These communications are of three types: Vehicle-to-Vehicle (V2V), Vehicle-to-Infrastructure (V2I), and Infrastructure-to-Infrastructure (I2I).

The onboard sensors used in CAVs work in different ranges varying from proximity (5 m), long range (250 m), medium (80–160 m), and short range (30 m) sensors. All these sensors of different ranges collectively help CAVs to detect obstacles and objects over a widespread range. Long range sensors along with information from other internal sensors and neighbouring vehicles are used to enable Adaptive Cruise Control (ACC) [17]. Various sensors and their range are illustrated in Fig. 2.

CAVs also contain more than hundred embedded Electronic Control Units (ECUs) that can control several parts of the vehicle such as powertrain, lighting, brakes, etc. and executes 100 million lines of code to provide various functions including acceleration, braking, and steering [19]. Most of the attacks on CAVs happen through vulnerabilities in ECUs and ECU communications (CAN bus). These attacks can also be conducted remotely to gain access to the vehicle [20]. As the number of ECUs are increasing in a vehicle along with rising levels of automation and connectivity, attack points and security risks are also rapidly increasing.

The ECUs communicate and send messages among each other through the CAN bus as shown in Fig. 3.

ECUs transmit messages using CAN frames. CAN frames are of 2 types: CAN 2.0A with standard 11-bit identifier and an extended CAN 2.0B with 29-bit identifier [22] (Fig. 4).

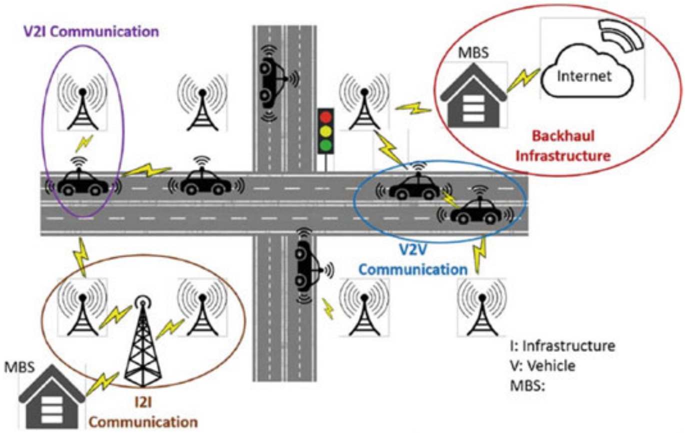


Fig. 1 CAV basic system architecture [16]

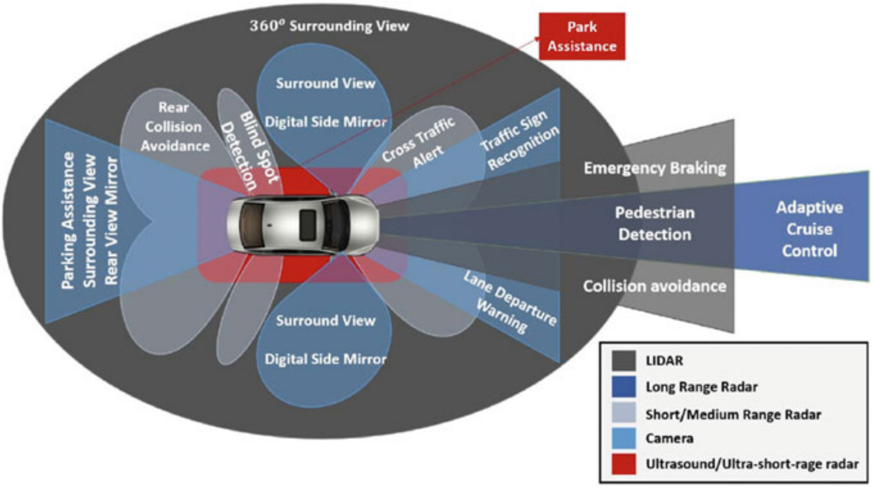


Fig. 2 CAV major sensor types and range [18]

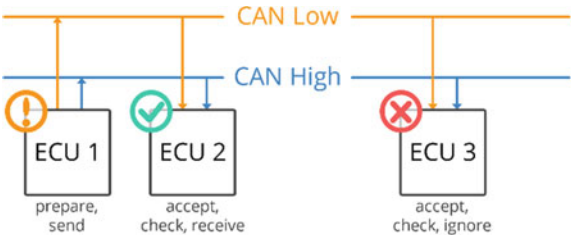


Fig. 3 ECU communication through CAN bus [21]

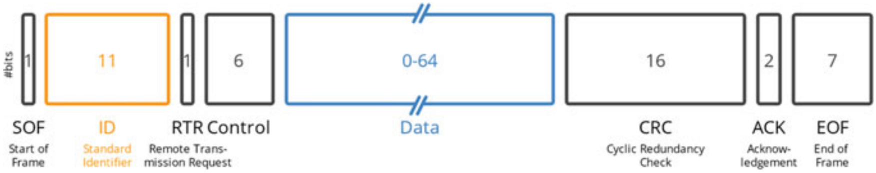


Fig. 4 CAN 2.0A frame [21]

SOF: It is the starting bit of the frame and a ‘0’ is to inform other ECUs that a CAN node plans to talk.

Identifier (ID): It is the next 11 bits and acts as the frame identifier. The priority of a message increases from higher IDs to lower.

Remote Transmission Request (RTR): It is a 1-bit indicator which indicates whether the ECU is sending or requesting data.

Control: It consists of 6 bits. The first 2 specifies whether the ID is CAN 2.0A (11-bits) or CAN 2.0B (29 bits). The next 4-bits indicates the length of transmitting data.

Data: the next 0–64 bit is the actual message to be transmitted.

Cyclic Redundancy Check (CRC): 16-bit code to ensure integrity.

Acknowledgment (ACK): 2-bit code to indicate whether the ECU have received and acknowledged the data.

End of Frame (EOF): It consists of seven bits and denotes the end of frame.

Their exists many vulnerabilities in CAN. There is no sender or receiver address mentioned in CAN packets and all the ECUs that receive a packet accepts or rejects it only based on the CAN ID [23]. Therefore, an ECU cannot decide whether a packet they receive is designed for them, nor know who send the packet and thus, ECUs in the CAN bus cannot verify the legitimacy of the packets they receive. This is a very crucial vulnerability as attackers can send messages from a compromised ECU and other ECUs receiving the packets have no means to authenticate the packet origin and will accept the packet without any issues [23].

Secondly, to send messages in the CAN bus, an attacker has to first compromise and gain access to an ECU. ECUs in CAVs are connected to the respective automobile manufacturer so that they can upload latest patches and updates remotely. This connection is usually accomplished using cellular base stations (BTS) which provide connectivity features in mobile networks. An attacker can conduct man-in-the-middle attack by setting up a rogue BTS and making the ECU transmit messages through it [24]. Another weakness in ECUs is that most of them use Short Message Service (SMS) for communications which are poorly encrypted and can easily be cracked by the hackers and gain access to the message [24].

If an attacker is able to access and control a vehicle remotely, then this might put the passengers and nearby people's life at risk. Hence, vulnerabilities and cyber security risks related to CAVs should be properly addressed before deploying them for public use.

2.2 Cyber Security in CAVs

The UK administration in 2017 issued key principles regarding cyber security in CAVs making it the first country to release guidance at a national level [25]. The EU has also released guidelines and practices to be followed for security of smart vehicles in 2017 through ENISA, a European Union agency for cyber security. This document included a list of all identified vulnerabilities and threats to smart vehicles and was later updated in 2019 and 2021 to include CAVs [26].

The US traffic administration agency, NHTSA released a guidance in 2016 which described the best practices for cyber security in modern vehicles and was later updated in 2017 and 2020 [27]. MIIT (Ministry of Industry and Information Technology) in China have released guidance for manufacturing of IOV (Internet of Vehicles) cyber security systems [28].

Although there are many CAV cyber security laws and regulations set by different governments, many have not yet made the laws compulsory for the manufacturers to follow as the CAV technology is still growing and not yet mature [4].

Protecting CAVs from cyber-attacks is a very important step for vehicle manufactures before releasing them to the public. To discuss further about CAV cyber security, first the different cyber-attacks have to be described and their mitigation techniques. It is also crucial to detect cyber-attacks instantly if they occur in CAVs to control and reduce the impact of the attack which will be discussed later.

2.3 Cyber-Attacks in CAVs

There are several attack points in CAVs that an attacker can target to conduct attacks. These attack points are shown in Fig. 5. According to Sun, Yu, and Zhang, the different attacks can be divided into two: the attacks occurring due to vulnerabilities in the in-vehicle network and the one's due to V2X (Vehicle-to-Everything) network.

CAVs exchange information and communicate with other vehicles and roadside infrastructures of CAVs. This communication is enabled through vehicle to everything network and an attacker can exploit the vulnerabilities in such networks and conduct different attacks, some of which are discussed below.

Eavesdropping attack: In this kind of attacks, the adversary listens to the network traffic and tries to retrieve messages in the network. This would give the attacker all the required information regarding the victim's vehicle such as current location and behaviours. Conducting this attack does not directly impact the network and thus, it is difficult to detect such attacks.

DoS (Denial of Service) attack: An attacker could insert random messages into the communication channel or create issues between different nodes in the network to block the entire channel or network so that genuine users are deprived from using

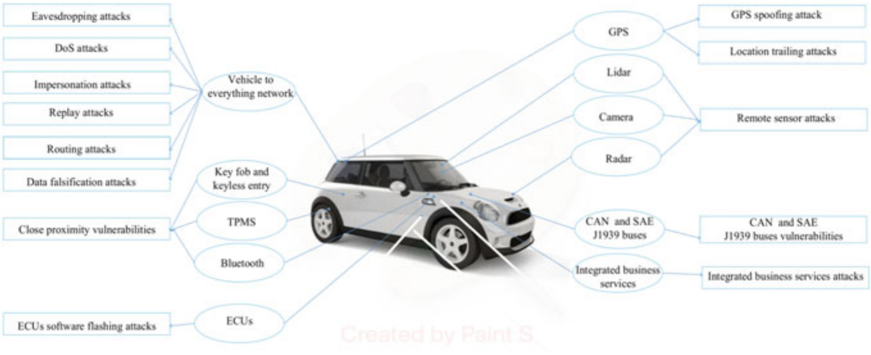

Eavesdropping attacks
DoS attacks
Impersonation attacks
Replay attacks
Routing attacks
Data falsification attacks
Close proximity vulnerabilities
ECUs software flashing attacks
Vehicle to everything network
Key fob and keyless entry
TPMS
Bluetooth
ECUs
GPS
Lidar
Camera
Radar
CAN and SAE J1939 buses
Integrated business services
GPS spoofing attack
Location trailing attacks
Remote sensor attacks
CAN and SAE J1939 buses vulnerabilities
Integrated business services attacks

Fig. 5 Potential attack points in CAVs [2]

network services. Such attacks in CAVs cause the messages from authentic nodes to be delayed which thereby effects the security of the vehicle [29].

Impersonation attack: All the vehicles have their own distinctive identification that allows others to identify the vehicle and messages. This attack happens when an attacker uses a fake or someone else's identity and are of two types, sybil attacks where many of the identities are spoofed simultaneously and node impersonation attack where only one identity is spoofed. Sybil attacks can also perform various malicious activities at a time, for example, drop critical messages, modify and spread received messages, and sending fake messages [30].

Replay attack: it happens when an attacker records every message and packets in a channel and retransmits them at a later time. This will lead to confusion in the authorities and can affect vehicular safety. This attack often happens along with impersonation attack as the attacker replays the messages as a legitimate node or vehicle [31].

Routing attack: There are many vulnerabilities in routing protocol which an attacker can exploit and drop messages in a channel or disrupt the regular routing process. There are three types of routing attacks namely, wormhole, black hole, and grey hole attacks. There will be a minimum of 2 supportive nodes in wormhole attacks that helps in forming a high-speed tunnel and lets the attacker capture packets from one location and tunnel to another [32]. Attacks started using one compromised node are known as black hole attacks [33]. In grey hole attacks, attacker removes messages or packets in a timely method. It is hard to detect grey hole attacks, as it can occasionally switch to correct behaviour [34].

Data falsification attack: This attack happens when an attacker broadcasts or sends false or fake messages in the network. This fake message can be created by tampering, altering, suppressing, or fabricating an original message. Such fake messages can affect vehicles safety and may disrupt navigation system, rise in travel time, and increase in traffic congestion [35].

Following attacks fall under in-vehicle network attacks:

GPS spoofing attack: GPS signals are used by vehicles to select the shortest route between two locations enabling them to be autonomous and operate without human help. However, there are many vulnerabilities in GPS navigation system that an attacker can exploit and conduct attacks such as spoofing or jamming. To launch any GPS attack, initially, the attackers disruptive signal should be in synchronize with satellite signal after which the attacker can make the target GPS to connect with their disruptive signal by increasing its signal strength and thereby manipulate the target GPS location [36].

Location trailing attack: Here, the attacker tries to gain drivers personal data by tracking and locating their vehicles. By tracking the location, an adversary will be able to understand the actions and behaviours of the vehicle and consequently, be able to disrupt the transportation system such as, rising number of traffic in roads.

Sensor attacks: There are several sensor nodes in CAVs that work at different ranges and collectively they combine computation, sensing, and communication to perform automated driving. All these sensors are susceptible to malicious interference attacks which can be performed from remote as well as physical. Remote interference attacks can be conducted from roadside where the attacker fixes one or more attack equipment along the road or the attacking tool is placed in the attacker's vehicle and they follow the victims vehicle. The attacking tools are used to disrupt the working of sensors. To conduct physical interference attacks, an adversary needs physical access to the victim's vehicle in order to mount attacking tools that tampers the sensors such as magnetic encoders or sound absorbing foams or they can directly damage the sensors [37].

Attacks on SAE J1939 and CAN buses: SAE J1939 is a high-level communication protocol used in vehicles on CAN bus for diagnostics and communications between internal components [38]. As discussed earlier in Sect. 2.2, due to the CAN bus not having proper authentication methods, an adversary could join, send, and listen to all the messages in the network and thereby access drivers' sensitive information's. An adversary could also exploit the CAN bus feature where it selects a message for transmission based on its priority bit to conduct Denial of Service (DOS) attacks. Therefore, if a malicious ECU is always sending messages with high priority (0 × 000), then rest of the ECUs wouldn't be able to communicate [2].

Integrated business services attack: Most of the CAVs will usually have their integrated system connected to the back-end manufacturer's network so that the vehicle manufacturers could update latest patches and software remotely. But there are many vulnerabilities present in integrated systems that an adversary could exploit and gain client access to back-end software of the vehicle which will then allow the attacker to obtain access to systems in other vehicle.

Close proximity vulnerability: There are 3 main attack methods that exploit the vulnerabilities in short range communication technique in CAVs. The attack methods are through the keyless or key fob entry system, TPMS (Tyre Pressure Monitoring System), and Bluetooth.

There are mainly 2 ways to enter a vehicle namely, keyless and key fob entry. An attacker can install devices such as house light controllers or gate openers nearby vehicles. These devices help in blocking the key fob signals and thereby does not allow the driver to lock their vehicle. Whereas signals cannot be blocked in a keyless entry, but an adversary can capture the fixed signal and replicate it to obtain entry to vehicle.

TPMS communication mostly works on simple protocols and standard regulatory schemes. An adversary can perform reverse engineering on TPMS messages as these protocols are not cryptographically secured. These messages can be correctly retrieved using an antenna within ten metres and within forty metres using an amplifier and consequently, allowing the attacker to eavesdrop the communication from nearby vehicles.

A potential memory exploit vulnerability has been found in Bluetooth control code that permits an attacker to execute code through any Bluetooth device that is paired. If a vehicle is paired with a compromised device, then it can attack the vehicles ECU without letting the driver detect the attack.

Attacks on ECU software flashing: As described in Sect. 2.2, ECUs are electronic control units and can control most of the vehicle parts such as steering wheel, gear shift, windows, ignition system, etc. However, there exist many vulnerabilities in

ECU which an attacker could exploit and conduct attacks mainly phlashing, reverse engineering, fuzzing attacks, and code modification [39]. In phlashing attacks, the attacker exploits the unpatched vulnerabilities in ECUs to deceive a remote system into permitting the attacker to flash its firmware causing the system to be removed and replaced as it cannot be rebooted after flashing [40]. Reverse engineering can cause disclosure of information. Fuzzing attacks help in detecting and finding vulnerabilities in the system and code modifications cause existing data to be corrupt and deteriorate hardware performance [41].

2.4 Mitigation Techniques

The corresponding mitigation techniques for all the CAV threats and vulnerabilities discussed in the preceding section are provided in Table 1.

2.5 Attack Detection

Although the mitigation techniques help in preventing most of the attacks, attackers will always search for new vulnerabilities and new methods to exploit existing vulnerabilities. Therefore, it is crucial to have a good detection method that is able to detect an attack before it leads to any danger.

As millions of data are processed in CAVs each second, manual attack detection is not possible, and given the dynamic environment, any delay in detection can lead to serious accidents. From the research's conducted by Hartzell and Stubel, they have reported that ECUs and CAN bus are the most vulnerable and easiest part to attack in CAVs with a lot of entry points for the attackers which they can exploit remotely and gain physical access to the vehicle. Therefore, this paper will be focusing on detecting attacks that occur on ECUs and CAN bus namely, spoofing, fuzzy and DoS attacks.

Intrusion Detection System (IDS) is the most popular technique for detecting attacks. IDS can be a device or software that observes unusual activities in a network or system and notify the administrator of any potential attacks. IDS can be classified based on the method of detection used which are: anomaly based, signature based, and specification based.

Signature based IDS is mainly used to detect known attacks. They are trained with a list of already known attacks and generate an IOC (Indicators of Compromise) list. The IOC list will contain information about how the network will behave before an attack happens and the IDS uses this information to detect and notify attacks while traversing through the network packets in real-time.

Whereas anomaly-based IDS can also detect zero-day attacks. It utilises machine learning algorithms to train and recognize a normal network behaviour. The IDS then compares the real time network traffic with the normal behaviour and reports an

Table 1 Mitigation techniques

Attack types		Mitigation strategy
Vehicle to everything network	Eavesdropping attack	Message anonymization using fog server [42], scheduling mechanism, trust-based recommendation [43], and resource management are some of the methods used to defend from eavesdropping [44]
	DoS attack	It is easy to detect than mitigate DoS attacks. Kumar and Mann [29] created a method for detecting and preventing DoS attack based on entropy and bandwidth of messages in the channel. Luo et al. [45] created a mechanism centred on port-hopping technique that could identify and filter out malicious packets
	Impersonation attack	Securing transmissions using geo-data for vehicular networks [46], verifying message integrity using hash-based function [47], and authentication of messages using elliptic curve cryptography are few methods to defend impersonation attack [48]
	Replay attack	Merco et al. [49] made use of a cross correlator and noisy signal control method to design a diagnosis algorithm that helps in detecting replay attacks in connected vehicle systems. Similarly, for pilotless aircraft, Sanchez et al. [50] utilized a detection method based on frequency where a time-varying sine wave was used for authentication
	Routing attack	An ant colony optimization technique based routing protocol was developed by Panda and Kumar [51] which will help find the best path between transmitter and recipient. Hassan et al. [52] developed a new detection scheme to prevent routing attacks in CAVs
	Data falsification attack	Boeira et al. [77] proposed a mechanism that learns from location detection techniques to identify location falsification attacks before leading to an accident amongst line of CAVs. Shukla and Sengupta [35] developed an attack detection mechanism by observing the dynamic time window usage
In-vehicle network attacks	GPS spoofing attack	A GPS spoofing attack can be detected by observing the average signal strength. The strength magnitude will be significantly larger during attacks than normal strength of signals from satellites

(continued)

Table 1 (continued)

Attack types		Mitigation strategy
	Location trailing attack	K-anonymity method can be used to blur the driver's current location, which also increases driver's location privacy while enjoying a more precise location services [53]. A mix-zone framework was proposed by [54] for securing the physical location of CAVs
	Sensor attack	Petit et al. [55] recommends utilizing signals of varying wavelengths for LiDAR's which would make the adversary struggle to target different wavelengths simultaneously. In addition, LiDAR's can also randomise probing so that the duration between laser pulses are different which helps in preventing adversaries from predicting when to insert dummy pulses [56]
	Attacks on CAN bus	Authentication, network segmentation, and encryption are few methods to prevent CAN bus attacks. In segmentation, the most attack prone important ECUs are kept separate from other ECUs to prevent adversary's from accessing such critical ECUs. For encryption and authentication, several software-based and cypher-based mechanisms have been developed respectively
	Integrated business service attack	Different encryption mechanism can be used here along with virtualization of hardware or software, data separation, and content filtering
	Close proximity vulnerability	Bluetooth systems can be secured by making use of the different security protocols developed specifically for Bluetooth using cryptographic techniques. TPMS packets can be protected by encrypting using a cryptographic algorithm and an additional cryptographic checksum [57]. To prevent key fob attacks, simply ensure that the doors are locked after activating the key fob
	Attacks on ECU software flashing	Encrypting ECU data will help in preventing reverse engineering attacks [58]. Integrity check will prevent modification of software by unauthorized users and authentication will help in identifying the software origin accurately [59]

attack if it finds any suspicious behaviour. Even though, Anomaly based IDS helps in detecting zero-day attacks, they are more prone to false positives than signature-based IDS as it raises alert for everything that does not match the normal recorded behaviour, for example, someone trying to access the system after business hours. Both the IDS techniques have their own advantages and disadvantages and are often used in conjunction.

Shenfield et al. [60] used artificial neural network for anomaly detection on network traffic. The method was successful with accuracy rate 98% and false positive rates below 2%. Despite not being done in real time, this proved that using machine learning models for detecting anomalies is feasible.

Levi et al. [61] developed a regression-based anomaly detection method to detect attacks in connected vehicles using simulated dataset. The simulated dataset was generated by simulating around 4000 drivers through a city and recording each drivers' activities. The model was found to be efficient and very accurate. However, the performance of these models with real-world datasets cannot be studied as they were developed using simulated dataset.

Salman and Bresch [62] proposed an IDS which relies on features extracted from CAN messages. They evaluated their IDS using simulated as well as real world environment which they conducted in a remote space. They have discussed about the different challenges and constraints that might occur during IDS development such as hardware constrains, challenges in data selection, placement of the IDS, etc. The developed IDS was only a prototype and not a final product.

Song et al. [63] explained the importance of ECUs and CAN bus in CAVs and the vulnerabilities present in them. They captured CAN messages and developed an IDS based on the time-interval between the captured messages. Based on their method, Bi et al. [64] integrated an additional message transfer feature along with time interval feature to develop an IDS. The proposed model was efficient in detecting DoS with 100% accuracy but lacked accuracy in detecting fuzzy and replay attacks.

He [4] developed an anomaly detection framework using machine learning algorithms for detecting attacks in CAVs. She developed models using different set of simulated and real-world datasets. Although she tried to enhance the models using a feature selection method, only two machine learning algorithms were used to develop the models, decision tree and naïve. Hence, the performance of other machine learning algorithms could not be computed.

Rajbahadur et al. [65] conducted an in-depth study of 65 anomaly detection papers on autonomous vehicles. The authors discovered that all the papers mostly used simulated data for detecting attacks and conducting studies. Models developed using simulated data may not predict correctly while testing real-world data as real-world data may contain incomplete, illegible, and missing values. Moreover, most of the models only classifies data as an attack or normal and could not specify the type of the attack. These simulated data sets were also not published which creates additional challenge.

Based on the limitations found on other research papers, in this paper, machine learning models are developed using 5 different machine learning algorithms. The models are trained using a real-world dataset so that models are easily adaptable to a real-world environment. The models are trained such that they will be able to classify different attack types, which will greatly help automotive engineers to easily respond and mitigate the attack.

3 CAVs and AI

This section presents classification models trained for identifying spoofing, fuzzy, and DoS attacks. Different models used are then evaluated and compared based on accuracy, prediction time, model development time, false negative, and false positive rates. Results are generated through MATLAB on a dataset used for developing and testing the model was generated using a real vehicle and made publicly available for future research projects [66].

3.1 Machine Learning Process

The Basic machine learning processes is illustrated in Fig. 6.

The initial stage in machine learning is to collect good reliable data. The next step is to clean the data as most real-world data will contain missing, unorganized, or noisy values. After processing the dataset, it needs to be split to training and testing set.

The machine learning model is then developed and trained using the training set. Moving further, five different classification models (kNN, classification tree, naïve bayes, discriminant analysis, and neural network) were trained to find the best possible model for the available dataset. The trained model is then validated using the test set. The predictions made from the test set are then compared with the actual output to compute false positive rates and accuracy. If the accuracy is below a particular threshold value, then the model is improved by modifying model specific parameters until a satisfactory accuracy rate is obtained.

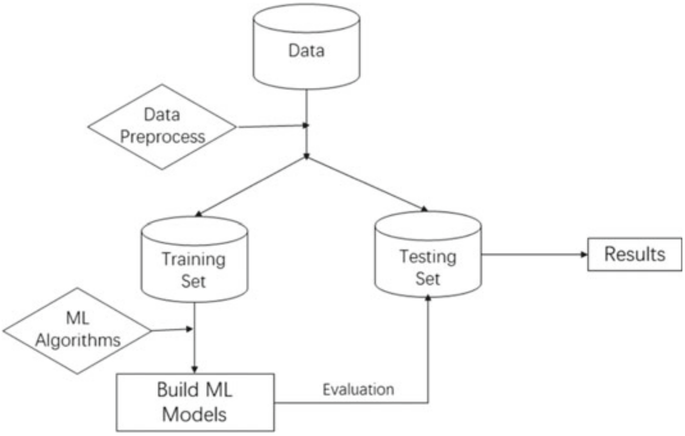


Fig. 6 Machine learning steps [4]

3.2 Car Hacking Dataset

Eunbi et al. generated the data set by recording CAN traffic through the On-Board Diagnostics 2 (OBD-2) port while conducting different attacks including DoS, fuzzy, spoofing the RPM gauge and drive gear on a real vehicle. Each attack was conducted for three to five seconds with all four datasets containing around thirty to forty minutes of CAN traffic. The attacks were conducted as follows:

DoS Attack: Every 0.3 ms, message packets with CAN ID ‘0000’ were injected into the CAN bus. CAN ID ‘0000’ is given the most priority in CAN bus protocol and hence, the injected messages will be given access to the bus before other normal messages.

Fuzzy Attack: Every 0.5 ms, messages with randomly generated data values and CAN IDs were injected into the CAN bus.

Spoofing the gear/RPM Attack: Every 1 ms, messages with CAN ID’s associated with gear and RPM ECUs were injected.

The amount of data generated for each of the attacks is shown in Table 2.

In order to train the model, all the datasets were concatenated together to create one single dataset containing all the attack types, which was further partitioned as presented in Table 3, a 30% testing set and 70% training set.

The dataset provided by [66] consisted of CAN messages and an identifier column indicating whether a specific row of data is an attack or not. A sample from the dataset is shown in Fig. 7.

The different attributes in the dataset are:

Timestamp: It is the time of recording the particular row of data in seconds.

CAN ID: This column consist of CAN message identifier in hexadecimal values.

Length: This column mentions the number of data bytes sent in the corresponding message (0–8 bytes).

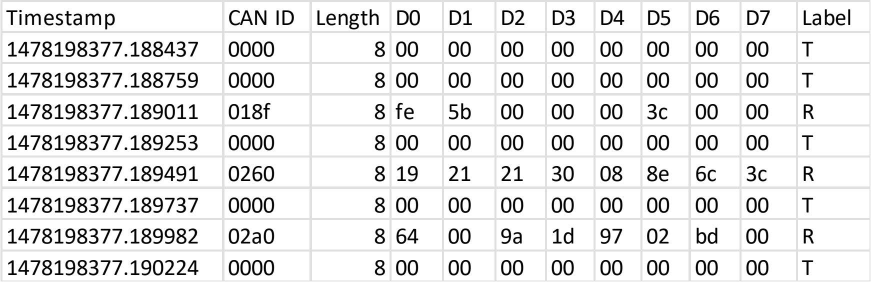
D [0–7]: The message being send as data values in hexadecimal.

Table 2 Overview of datasets

Attack types	Injected messages	Normal/attack free messages	Total number of messages
Fuzzy attack	491,847	3,347,013	3,838,860
DoS attack	587,521	3,078,250	3,665,771
RPM gauze spoofing	654,897	3,966,805	4,621,702
Drive gear spoofing	597,252	3,845,890	4,443,142

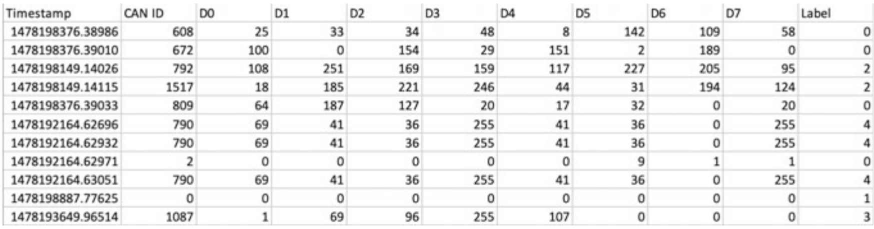
Table 3 Training and testing data

Dataset	Attack data	Normal data
Training set	1,632,090	9,966,544
Testing set	699,427	4,271,414



Timestamp	CAN ID	Length	D0	D1	D2	D3	D4	D5	D6	D7	Label
1478198377.188437	0000	8	00	00	00	00	00	00	00	00	T
1478198377.188759	0000	8	00	00	00	00	00	00	00	00	T
1478198377.189011	018f	8	fe	5b	00	00	00	3c	00	00	R
1478198377.189253	0000	8	00	00	00	00	00	00	00	00	T
1478198377.189491	0260	8	19	21	21	30	08	8e	6c	3c	R
1478198377.189737	0000	8	00	00	00	00	00	00	00	00	T
1478198377.189982	02a0	8	64	00	9a	1d	97	02	bd	00	R
1478198377.190224	0000	8	00	00	00	00	00	00	00	00	T

Fig. 7 Sample dataset



Timestamp	CAN ID	D0	D1	D2	D3	D4	D5	D6	D7	Label
1478198376.38986	608	25	33	34	48	8	142	109	58	0
1478198376.39010	672	100	0	154	29	151	2	189	0	0
1478198149.14026	792	108	251	169	159	117	227	205	95	2
1478198149.14115	1517	18	185	221	246	44	31	194	124	2
1478198376.39033	809	64	187	127	20	17	32	0	20	0
1478192164.62696	790	69	41	36	255	41	36	0	255	4
1478192164.62932	790	69	41	36	255	41	36	0	255	4
1478192164.62971	2	0	0	0	0	0	9	1	1	0
1478192164.63051	790	69	41	36	255	41	36	0	255	4
1478198887.77625	0	0	0	0	0	0	0	0	0	1
1478193649.96514	1087	1	69	96	255	107	0	0	0	3

Fig. 8 Processed dataset

Label: This column is used to identify the message as normal (R) or an attack (T).

The above dataset was processed and converted to a new simpler dataset in order to develop machine learning models. Firstly, the irrelevant features which does not affect in identifying whether the data is normal or an attack data are identified and removed such as the length of the message. This will help in reducing the complexity of the model. Secondly, the hexadecimal values present in the dataset are converted to decimals as machine learning models have difficulty in processing hexadecimal values. Finally, label values are converted to integers with values as: 0 for normal data, 1 for DoS attack, 2 for fuzzy attack, 3 for spoofing the gear attack, and 4 for spoofing the RPM gauge. The attacks were given different values in order for the models to classify and identify different attacks. The processed dataset is shown in Fig. 8.

3.3 Machine Learning Models

Here, supervised classification models will be used as labelled inputs are available and the different models developed are k-Nearest Neighbor (kNN), classification trees, naïve bayes, discriminant analysis and neural networks.

The function provided by MATLAB for developing classification models is 'fitc' along with the name of the model being developed. For example, for building kNN model, the function name will be 'fitcknn', for classification tree, it will be 'fitctree' and so on. The function can be called as shown in Eq. 1.

$$\begin{aligned}\text{model} =&\text{fitc} + \text{model type(Training dataset, Output Variable Name,}\\ &\text{'Hyperparameters', Hyperparameter value)}\end{aligned} \tag{1}$$

The input to 'fitc' function are the training dataset, output variable which is the label column in this project that indicates whether the data is an attack or not, hyperparameters and their values.

Hyperparameters can be optimized either manually or using automated functions. MATLAB provides an automated optimize hyperparameter option that automatically by default tries out 30 different combinations of hyperparameter values and selects the one with the least model classification error. The equation is shown in (2). Although the automated model tries 30 different combinations, it wouldn't be covering all the possible combinations and models developed after automated optimizations are often overfitted models. Hence, in this project, both manual and automated optimization approach will be taken to develop models which will be evaluated and compared to find the best fit with maximum accuracy.

$$\begin{aligned}\text{Optimised Model} =&\text{fitc} + \text{model type(Training dataset, Output variable name,}\\ &\text{'OptimizeHyperparameter', Options)}\end{aligned} \tag{2}$$

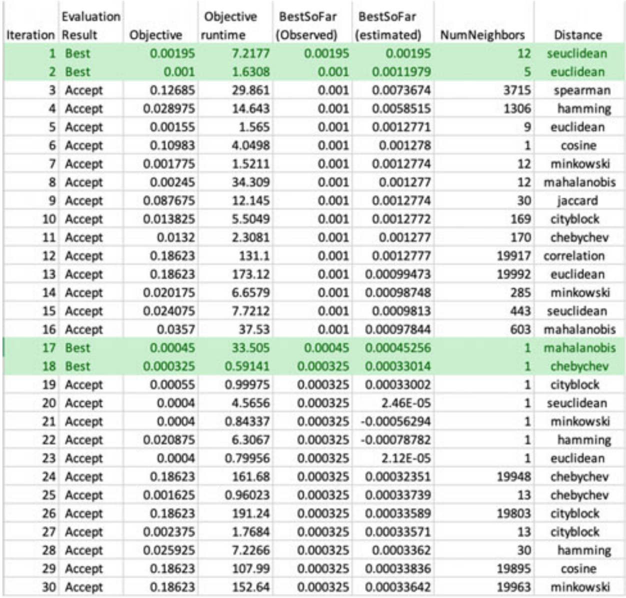
All the models below are developed using the training set created and validated using the test set.

3.4 K-Nearest Neighbor Algorithm (kNN)

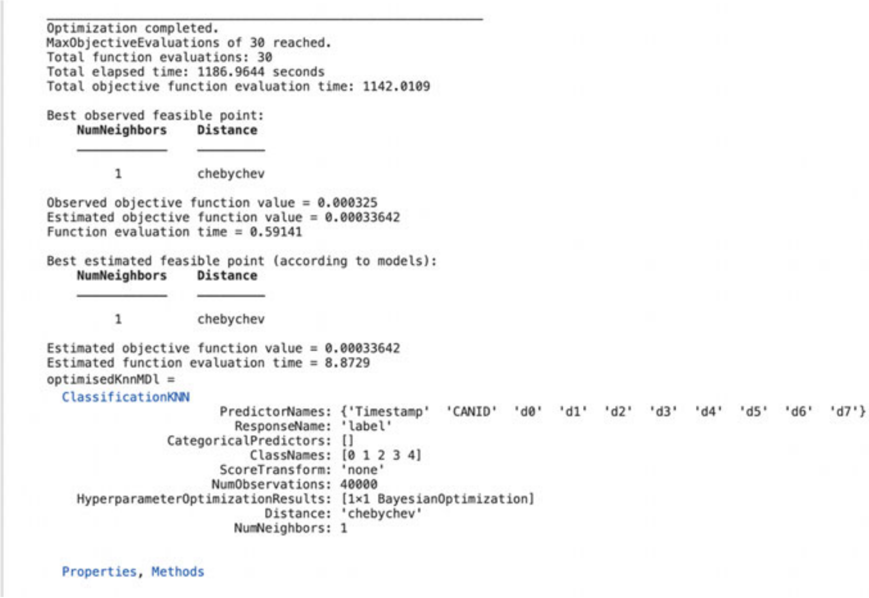
kNN algorithm generates an input dataset to output variable mapping function by assuming that things that are related exist close to each other. The mapping function mainly depends on the distance between two data points and the number of nearest neighbors used for predicting a new data. This distance can be calculated using different methods namely, city block, correlation, cosine, Euclidean, hamming, and Jaccard. Different combinations of distance calculation methods and number of nearest neighbors are used to find the best model with the least false positive and highest accuracy rate.

In MATLAB, the command 'fitcknn' is used to build kNN classification models. The output after optimizing distance calculation method and number of nearest neighbors using the 'OptimizeHyperparameter' option is shown in Fig. 9.

Thirty different combinations have been tried and 4 of them are found to be the best fit. Out of which the model with Chebyshev distance method and number of neighbors as 1 was reported as the best estimated feasible point.



Iteration	Evaluation Result	Objective	Objective runtime	BestSoFar (Observed)	BestSoFar (estimated)	NumNeighbors	Distance
1	Best	0.00195	7.2177	0.00195	0.00195	12	seuclidean
2	Best	0.001	1.6308	0.001	0.0011979	5	euclidean
3	Accept	0.12685	29.861	0.001	0.0073674	3715	spearman
4	Accept	0.028975	14.643	0.001	0.0058515	1306	hamming
5	Accept	0.00155	1.565	0.001	0.0012771	9	euclidean
6	Accept	0.10983	4.0498	0.001	0.001278	1	cosine
7	Accept	0.001775	1.5211	0.001	0.0012774	12	minkowski
8	Accept	0.00245	34.309	0.001	0.001277	12	mahalanobis
9	Accept	0.087675	12.145	0.001	0.0012774	30	jaccard
10	Accept	0.013825	5.5049	0.001	0.0012772	169	cityblock
11	Accept	0.0132	2.3081	0.001	0.001277	170	chebychev
12	Accept	0.18623	131.1	0.001	0.0012777	19917	correlation
13	Accept	0.18623	173.12	0.001	0.00099473	19992	euclidean
14	Accept	0.020175	6.6579	0.001	0.00098748	285	minkowski
15	Accept	0.024075	7.7212	0.001	0.0009813	443	seuclidean
16	Accept	0.0357	37.53	0.001	0.00097844	603	mahalanobis
17	Best	0.00045	33.505	0.00045	0.00045256	1	mahalanobis
18	Best	0.000325	0.59141	0.000325	0.00033014	1	chebychev
19	Accept	0.00055	0.99975	0.000325	0.00033002	1	cityblock
20	Accept	0.0004	4.5656	0.000325	2.46E-05	1	seuclidean
21	Accept	0.0004	0.84337	0.000325	-0.00056294	1	minkowski
22	Accept	0.020875	6.3067	0.000325	-0.00078782	1	hamming
23	Accept	0.0004	0.79956	0.000325	2.12E-05	1	euclidean
24	Accept	0.18623	161.68	0.000325	0.00032351	19948	chebychev
25	Accept	0.001625	0.96023	0.000325	0.00033739	13	chebychev
26	Accept	0.18623	191.24	0.000325	0.00033589	19803	cityblock
27	Accept	0.002375	1.7684	0.000325	0.00033571	13	cityblock
28	Accept	0.025925	7.2266	0.000325	0.0003362	30	hamming
29	Accept	0.18623	107.99	0.000325	0.00033836	19895	cosine
30	Accept	0.18623	152.64	0.000325	0.00033642	19963	minkowski



```
__________________________________________________________
Optimization completed.
MaxObjectiveEvaluations of 30 reached.
Total function evaluations: 30
Total elapsed time: 1186.9644 seconds
Total objective function evaluation time: 1142.0109

Best observed feasible point:
    NumNeighbors    Distance
    ____________    _________

         1          chebychev

Observed objective function value = 0.000325
Estimated objective function value = 0.00033642
Function evaluation time = 0.59141

Best estimated feasible point (according to models):
    NumNeighbors    Distance
    ____________    _________

         1          chebychev

Estimated objective function value = 0.00033642
Estimated function evaluation time = 8.8729
optimisedKnnMDl =
  ClassificationKNN
                     PredictorNames: {'Timestamp'  'CANID'  'd0'  'd1'  'd2'  'd3'  'd4'  'd5'  'd6'  'd7'}
                       ResponseName: 'label'
              CategoricalPredictors: []
                         ClassNames: [0 1 2 3 4]
                     ScoreTransform: 'none'
                    NumObservations: 40000
    HyperparameterOptimizationResults: [1×1 BayesianOptimization]
                           Distance: 'chebychev'
                       NumNeighbors: 1


  Properties, Methods
```

Fig. 9 kNN optimization summary

The Chebyshev distance between two points or vectors a and b, with coordinates ai and bi, is:

$$D\text{a,b} = \max_{i}(|a\text{i} - b\text{i}|) \tag{3}$$

Based on this model, a new data point, P is predicted to be under the class in which its nearest neighbor falls. The nearest neighbor is found using the Chebyshev distance between P and nearby neighbors and selecting the neighbor with shortest distance.

Two models were developed manually with distance as Euclidean and number of nearest neighbors as 1 and 5 respectively. Euclidean distance between two points *a* and *b* is the length of the line segment between those points and is computed as:

$$D_{ab} = \sqrt{\sum_{i=1}^{n} (a_i - b_i)^2} \tag{4}$$

where,

n is the dimension space, which is 1 for one dimension, 2 for two dimension and so on.

a_i and b_i corresponds to the coordinates of the points *a* and *b* respectively.

The Euclidean distance between those points is given by *Dab*.

Here, a new data point, *P* will be predicted depending on the class of one of its shortest neighbors for the model with number of neighbors as 1 and for the model with number of neighbors as 5, prediction for *P* will depend on the classes of 5 of its shortest neighbors.

All the developed models are then used to predict the outcomes of the test set. The command for prediction is:

$$\text{Predictions} = \text{predict(model name, test dataset)} \tag{5}$$

The predicted outcomes are then compared with the actual known outcomes to evaluate the model performance.

3.5 Classification Trees

Classification Tree models are developed by identifying and learning the features that help in classifying a data point into different classes. Contrary to kNN algorithm, classification trees does not make any assumptions about the data. They predict new data by passing it through a tree like structure and are mainly made up of decision nodes and leaves. The decision nodes divide the data according to its values, while the leaves specify the outcome. Decision nodes mostly consist of yes or no questions.

For example, to predict whether a person got COVID based on information's such as fever, breathing problem, and age, the classification tree might look like this (Fig. 10).

The above shown example is a binary classification problem as the tree only contains yes or no questions. Below is shown the output summary after optimizing classification tree for finding the minimum number of leaves needed using 'OptimizeHyperparameter' option (Fig. 11).

Out of 30 different minimum leaf sizes tried, two values were found to provide the best performance and the classification tree with minimum leaf size as 1 was recommended as the best feasible point. Two models were developed manually with minimum leaf sizes as 50 and 100.

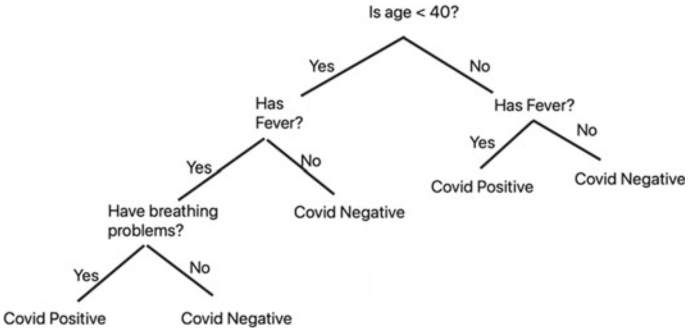
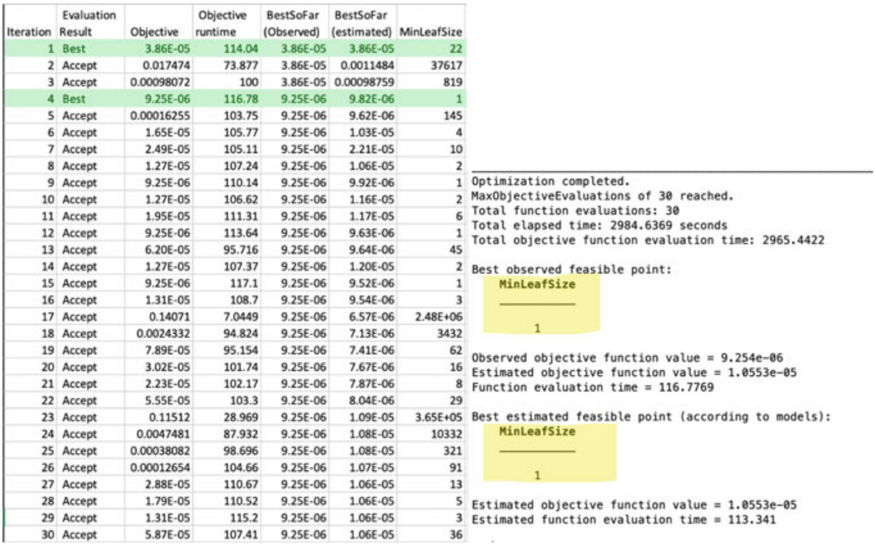


Fig. 10 Classification tree



Iteration	Evaluation Result	Objective	Objective runtime	BestSoFar (Observed)	BestSoFar (estimated)	MinLeafSize
1	Best	3.86E-05	114.04	3.86E-05	3.86E-05	22
2	Accept	0.017474	73.877	3.86E-05	0.0011484	37617
3	Accept	0.00098072	100	3.86E-05	0.00098759	819
4	Best	9.25E-06	116.78	9.25E-06	9.82E-06	1
5	Accept	0.00016255	103.75	9.25E-06	9.62E-06	145
6	Accept	1.65E-05	105.77	9.25E-06	1.03E-05	4
7	Accept	2.49E-05	105.11	9.25E-06	2.21E-05	10
8	Accept	1.27E-05	107.24	9.25E-06	1.06E-05	2
9	Accept	9.25E-06	110.14	9.25E-06	9.92E-06	1
10	Accept	1.27E-05	106.62	9.25E-06	1.16E-05	2
11	Accept	1.95E-05	111.31	9.25E-06	1.17E-05	6
12	Accept	9.25E-06	113.64	9.25E-06	9.63E-06	1
13	Accept	6.20E-05	95.716	9.25E-06	9.64E-06	45
14	Accept	1.27E-05	107.37	9.25E-06	1.20E-05	2
15	Accept	9.25E-06	117.1	9.25E-06	9.52E-06	1
16	Accept	1.31E-05	108.7	9.25E-06	9.54E-06	3
17	Accept	0.14071	7.0449	9.25E-06	6.57E-06	2.48E+06
18	Accept	0.0024332	94.824	9.25E-06	7.13E-06	3432
19	Accept	7.89E-05	95.154	9.25E-06	7.41E-06	62
20	Accept	3.02E-05	101.74	9.25E-06	7.67E-06	16
21	Accept	2.23E-05	102.17	9.25E-06	7.87E-06	8
22	Accept	5.55E-05	103.3	9.25E-06	8.04E-06	29
23	Accept	0.11512	28.969	9.25E-06	1.09E-05	3.65E+05
24	Accept	0.0047481	87.932	9.25E-06	1.08E-05	10332
25	Accept	0.00038082	98.696	9.25E-06	1.08E-05	321
26	Accept	0.00012654	104.66	9.25E-06	1.07E-05	91
27	Accept	2.88E-05	110.67	9.25E-06	1.06E-05	13
28	Accept	1.79E-05	110.52	9.25E-06	1.06E-05	5
29	Accept	1.31E-05	115.2	9.25E-06	1.06E-05	3
30	Accept	5.87E-05	107.41	9.25E-06	1.06E-05	36

```
__________________________________________________________
Optimization completed.
MaxObjectiveEvaluations of 30 reached.
Total function evaluations: 30
Total elapsed time: 2984.6369 seconds
Total objective function evaluation time: 2965.4422

Best observed feasible point:
    MinLeafSize
    ___________

         1

Observed objective function value = 9.254e-06
Estimated objective function value = 1.0553e-05
Function evaluation time = 116.7769

Best estimated feasible point (according to models):
    MinLeafSize
    ___________

         1

Estimated objective function value = 1.0553e-05
Estimated function evaluation time = 113.341
```

Fig. 11 Classification tree optimization summary

Table 4 Training loss of pruned classification trees

Classification tree (prune level)	Training loss
1	0.0000042209 (4.2209e − 06)
2	0.0000042209 (4.2209e − 06)
3	0.0000038181 (3.8181e − 06)
4	0.0000038181 (3.8181e − 06)
5	0.0000040191 (4.0191e − 06)

Classification Trees are more prone to overfitting. MATLAB provides a pruning function which allows to compress a developed classification tree model through the command given below:

$$\text{Pruned Model} = \text{prune}\big(\text{Optimized tree model},\ '\text{Level}',\ \text{value}\big) \tag{6}$$

How a model fits a training data can be assessed using the training loss metric. The different tree levels and their corresponding training loss for the optimized tree are shown in Table 4.

For the model with minimum leaf size 50, every pruning level gave the same training loss of 0.00002392 (2.3920e − 05) and for the model with minimum leaf size 100, least training loss was found on prune level 5 with value 0.00002392 (2.3920e − 05).

3.6 Naïve Bayes Classification

Naïve Bayes works by assuming that each class has different predictor probability distributions and that every predictor in a class independently contribute in identifying the class of a data. For example, a student is considered passed if he scores above 50 in Mathematics, above 45 in Science, and above 40 in English. Even though these features are inter-dependent or exist upon other features, they independently contribute in identifying the result of the student and thus, called naive.

Naïve Bayes algorithm is build on Bayes probability theorem which calculates the posterior probability ($P_{(c|x)}$) as:

$$P_{(c|x)} := \frac{P_{(x|c)} P_{(C)}}{P_{(x)}} \tag{7}$$

where,

The posterior probability of the target class C is given by $P_{(c|x)}$, given predictor attributes, X.

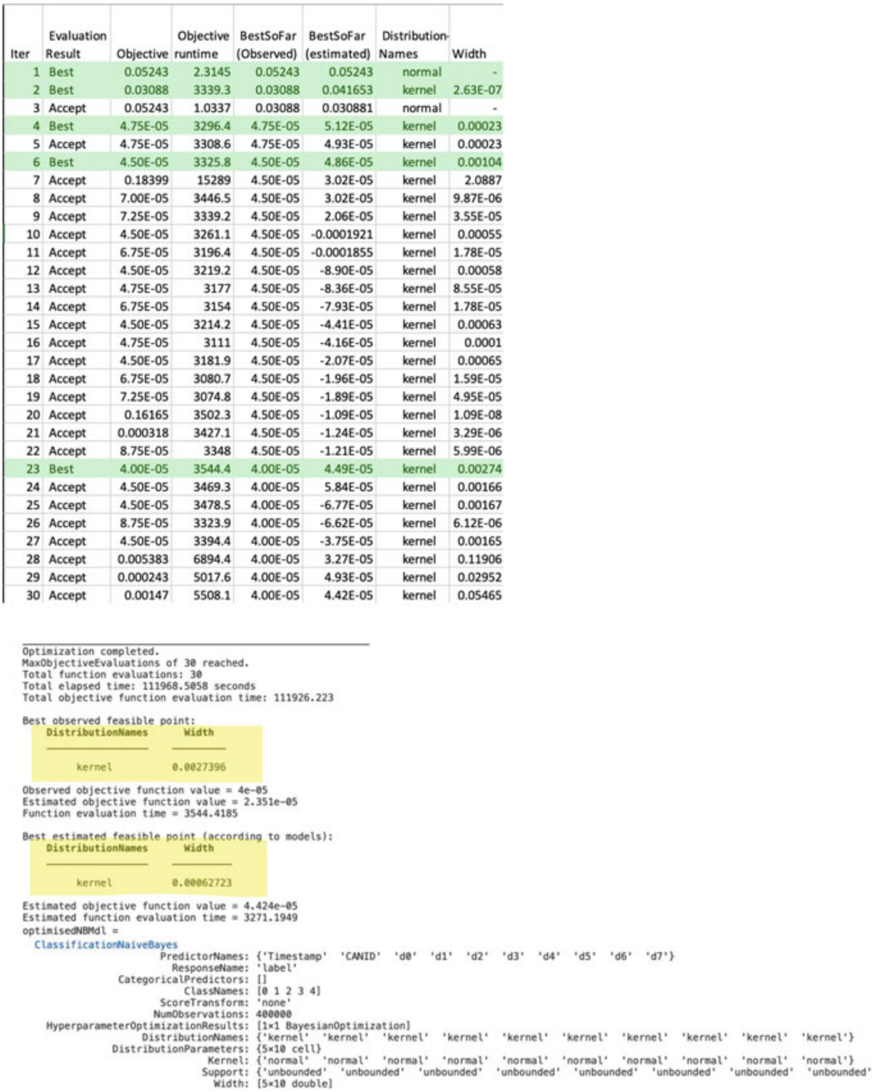
The probability of predictor given class is $P_{(X|C)}$.

$P(c)$ is the class probability before new data class is predicted.

The prior predictor probability is $P(x)$.

In MATLAB, ‘fitcnb’ command is used to create naïve bayes models and the optimum property settings can be found by using the hyperparameter option. Kernel smooth density width is used with the kernel distribution and defines the shape of the distribution. The output after optimizing naïve bayes model (Fig. 12).

The model with kernel as distribution and its width as 0.00062723 was found to best estimated model after optimization. Another model was created using the Gaussian distribution.



Iter	Evaluation Result	Objective	Objective runtime	BestSoFar (Observed)	BestSoFar (estimated)	Distribution-Names	Width
1	Best	0.05243	2.3145	0.05243	0.05243	normal	-
2	Best	0.03088	3339.3	0.03088	0.041653	kernel	2.63E-07
3	Accept	0.05243	1.0337	0.03088	0.030881	normal	-
4	Best	4.75E-05	3296.4	4.75E-05	5.12E-05	kernel	0.00023
5	Accept	4.75E-05	3308.6	4.75E-05	4.93E-05	kernel	0.00023
6	Best	4.50E-05	3325.8	4.50E-05	4.86E-05	kernel	0.00104
7	Accept	0.18399	15289	4.50E-05	3.02E-05	kernel	2.0887
8	Accept	7.00E-05	3446.5	4.50E-05	3.02E-05	kernel	9.87E-06
9	Accept	7.25E-05	3339.2	4.50E-05	2.06E-05	kernel	3.55E-05
10	Accept	4.50E-05	3261.1	4.50E-05	-0.0001921	kernel	0.00055
11	Accept	6.75E-05	3196.4	4.50E-05	-0.0001855	kernel	1.78E-05
12	Accept	4.50E-05	3219.2	4.50E-05	-8.90E-05	kernel	0.00058
13	Accept	4.75E-05	3177	4.50E-05	-8.36E-05	kernel	8.55E-05
14	Accept	6.75E-05	3154	4.50E-05	-7.93E-05	kernel	1.78E-05
15	Accept	4.50E-05	3214.2	4.50E-05	-4.41E-05	kernel	0.00063
16	Accept	4.75E-05	3111	4.50E-05	-4.16E-05	kernel	0.0001
17	Accept	4.50E-05	3181.9	4.50E-05	-2.07E-05	kernel	0.00065
18	Accept	6.75E-05	3080.7	4.50E-05	-1.96E-05	kernel	1.59E-05
19	Accept	7.25E-05	3074.8	4.50E-05	-1.89E-05	kernel	4.95E-05
20	Accept	0.16165	3502.3	4.50E-05	-1.09E-05	kernel	1.09E-08
21	Accept	0.000318	3427.1	4.50E-05	-1.24E-05	kernel	3.29E-06
22	Accept	8.75E-05	3348	4.50E-05	-1.21E-05	kernel	5.99E-06
23	Best	4.00E-05	3544.4	4.00E-05	4.49E-05	kernel	0.00274
24	Accept	4.50E-05	3469.3	4.00E-05	5.84E-05	kernel	0.00166
25	Accept	4.50E-05	3478.5	4.00E-05	-6.77E-05	kernel	0.00167
26	Accept	8.75E-05	3323.9	4.00E-05	-6.62E-05	kernel	6.12E-06
27	Accept	4.50E-05	3394.4	4.00E-05	-3.75E-05	kernel	0.00165
28	Accept	0.005383	6894.4	4.00E-05	3.27E-05	kernel	0.11906
29	Accept	0.000243	5017.6	4.00E-05	4.93E-05	kernel	0.02952
30	Accept	0.00147	5508.1	4.00E-05	4.42E-05	kernel	0.05465

```
Optimization completed.
MaxObjectiveEvaluations of 30 reached.
Total function evaluations: 30
Total elapsed time: 111968.5058 seconds
Total objective function evaluation time: 111926.223

Best observed feasible point:
    DistributionNames      Width
    _________________    _________

         kernel          0.0027396

Observed objective function value = 4e-05
Estimated objective function value = 2.351e-05
Function evaluation time = 3544.4185

Best estimated feasible point (according to models):
    DistributionNames      Width
    _________________    __________

         kernel          0.00062723

Estimated objective function value = 4.424e-05
Estimated function evaluation time = 3271.1949
optimisedNBMdl =
  ClassificationNaiveBayes
                          PredictorNames: {'Timestamp'  'CANID'  'd0'  'd1'  'd2'  'd3'  'd4'  'd5'  'd6'  'd7'}
                            ResponseName: 'label'
                   CategoricalPredictors: []
                              ClassNames: [0 1 2 3 4]
                          ScoreTransform: 'none'
                         NumObservations: 400000
       HyperparameterOptimizationResults: [1×1 BayesianOptimization]
                       DistributionNames: {'kernel'  'kernel'  'kernel'  'kernel'  'kernel'  'kernel'  'kernel'  'kernel'  'kernel'  'kernel'}
                  DistributionParameters: {5×10 cell}
                                  Kernel: {'normal'  'normal'  'normal'  'normal'  'normal'  'normal'  'normal'  'normal'  'normal'  'normal'}
                                 Support: {'unbounded'  'unbounded'  'unbounded'  'unbounded'  'unbounded'  'unbounded'  'unbounded'  'unbounded'
                                   Width: [5×10 double]
```

Fig. 12 Naive Bayes optimization summary

3.7 Discriminant Analysis

Discriminant analysis is almost similar to naïve bayes as it assumes that each class has different predictor probability distributions. However, it does not that assume that predictor variables independently contribute in identifying a class and hence, use multivariate normal distribution. It is mainly used for dimensionality reduction where the dataset contains many features related to each other that needs to be plotted in two or three dimensions. Here, linear discriminant analysis is used to develop the model as quadratic models require predictor variables to have zero variance for each class. The equation for prediction is given below:

$$\hat{y} := \underset{y = 1, .., n}{\text{argmin}} \sum_{n=1}^{N} \widehat{P}(n|x)C(y|n) \tag{8}$$

where,

$\hat{y}$ is the class predicted for the new data.

The total number of classes in the dataset is N.

$\widehat{P}(n|x)$ is the posterior probability of a class n for a given observation x.

$C(y|n)$ is classification cost for classifying a data as y when n is its true class.

The command for building discriminant analysis model in MATLAB is ‘fitdiscr’ and can be optimized similar to other models using the optimize hyperparameters option. By default, optimize hyperparameter will optimize gamma and delta values for linear models. The output after optimization is shown in Fig. 13.

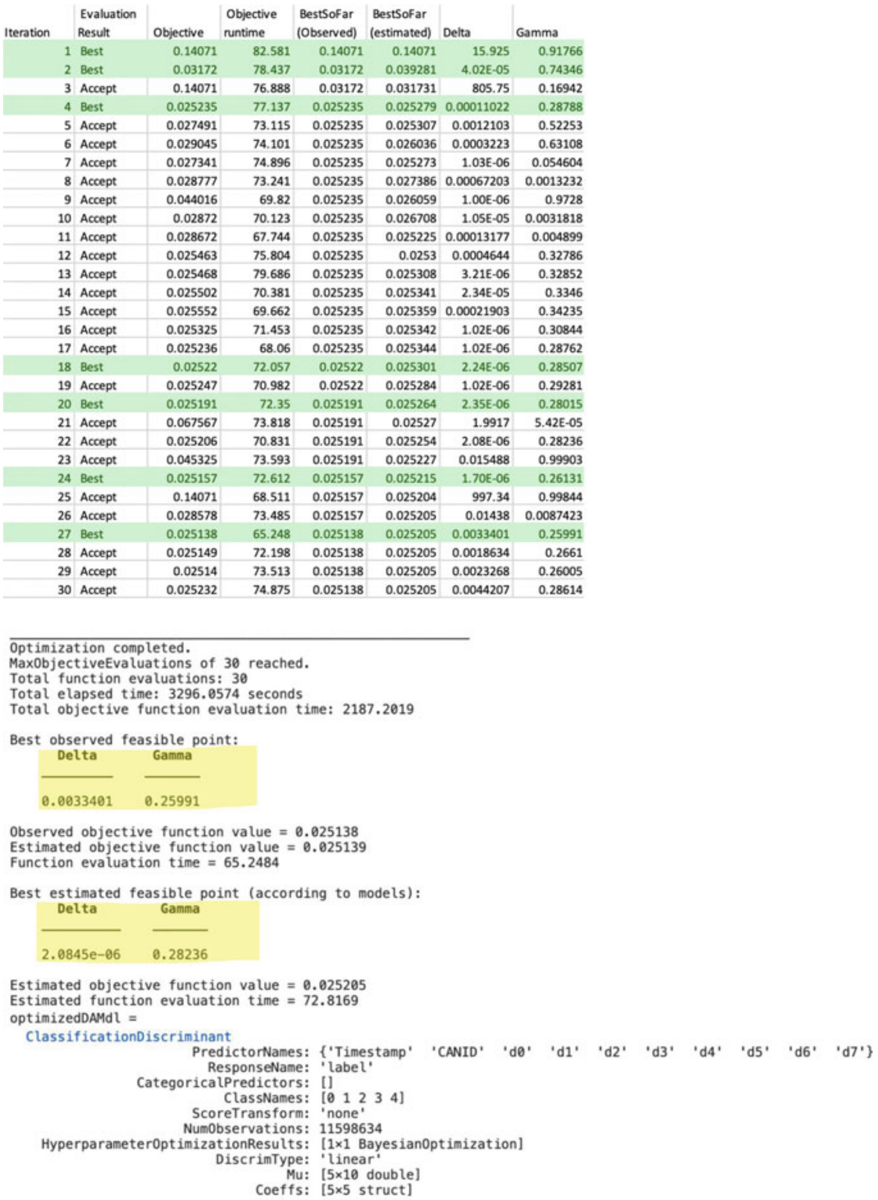
Out of 30 different value combinations for gamma and delta for linear models, 7 combinations were producing best results and the model with values 2.0845e − 06 for delta and 0.28236 for gamma was found to be the best estimated feasible point.

Four linear discriminant analysis models were developed manually with gamma and delta values as shown in Table 5.

3.8 Neural Networks Classification

Neural networks try to behave like a human brain and consist of interconnected neurons. They learn to identify data patterns by modifying the neural connections through a trial-and-error method. Each neuron acts as a function and receives one or more inputs to which the function is applied to generate an output which then acts as the input to the neurons in the next level. The final result is generated by the neurons at the last or terminal level. A sample neural network with two inner neuron levels is shown in Fig. 14 where x is the initial input which is passed to the functions in first level h1, h2, and h3 whose output is then passed to second level of functions g1, and g2 and the final output is received from function f.

In MATLAB, neural network is modelled using the command ‘fitcnet’ and the hyperparameters that can be altered include layer sizes, activations, lambda, and



Iteration	Evaluation Result	Objective	Objective runtime	BestSoFar (Observed)	BestSoFar (estimated)	Delta	Gamma
1	Best	0.14071	82.581	0.14071	0.14071	15.925	0.91766
2	Best	0.03172	78.437	0.03172	0.039281	4.02E-05	0.74346
3	Accept	0.14071	76.888	0.03172	0.031731	805.75	0.16942
4	Best	0.025235	77.137	0.025235	0.025279	0.00011022	0.28788
5	Accept	0.027491	73.115	0.025235	0.025307	0.0012103	0.52253
6	Accept	0.029045	74.101	0.025235	0.026036	0.0003223	0.63108
7	Accept	0.027341	74.896	0.025235	0.025273	1.03E-06	0.054604
8	Accept	0.028777	73.241	0.025235	0.027386	0.00067203	0.0013232
9	Accept	0.044016	69.82	0.025235	0.026059	1.00E-06	0.9728
10	Accept	0.02872	70.123	0.025235	0.026708	1.05E-05	0.0031818
11	Accept	0.028672	67.744	0.025235	0.025225	0.00013177	0.004899
12	Accept	0.025463	75.804	0.025235	0.0253	0.0004644	0.32786
13	Accept	0.025468	79.686	0.025235	0.025308	3.21E-06	0.32852
14	Accept	0.025502	70.381	0.025235	0.025341	2.34E-05	0.3346
15	Accept	0.025552	69.662	0.025235	0.025359	0.00021903	0.34235
16	Accept	0.025325	71.453	0.025235	0.025342	1.02E-06	0.30844
17	Accept	0.025236	68.06	0.025235	0.025344	1.02E-06	0.28762
18	Best	0.02522	72.057	0.02522	0.025301	2.24E-06	0.28507
19	Accept	0.025247	70.982	0.02522	0.025284	1.02E-06	0.29281
20	Best	0.025191	72.35	0.025191	0.025264	2.35E-06	0.28015
21	Accept	0.067567	73.818	0.025191	0.02527	1.9917	5.42E-05
22	Accept	0.025206	70.831	0.025191	0.025254	2.08E-06	0.28236
23	Accept	0.045325	73.593	0.025191	0.025227	0.015488	0.99903
24	Best	0.025157	72.612	0.025157	0.025215	1.70E-06	0.26131
25	Accept	0.14071	68.511	0.025157	0.025204	997.34	0.99844
26	Accept	0.028578	73.485	0.025157	0.025205	0.01438	0.0087423
27	Best	0.025138	65.248	0.025138	0.025205	0.0033401	0.25991
28	Accept	0.025149	72.198	0.025138	0.025205	0.0018634	0.2661
29	Accept	0.02514	73.513	0.025138	0.025205	0.0023268	0.26005
30	Accept	0.025232	74.875	0.025138	0.025205	0.0044207	0.28614

```
__________________________________________________________
Optimization completed.
MaxObjectiveEvaluations of 30 reached.
Total function evaluations: 30
Total elapsed time: 3296.0574 seconds
Total objective function evaluation time: 2187.2019

Best observed feasible point:
      Delta        Gamma
    _________    _______

    0.0033401    0.25991

Observed objective function value = 0.025138
Estimated objective function value = 0.025139
Function evaluation time = 65.2484

Best estimated feasible point (according to models):
      Delta         Gamma
    __________    _______

    2.0845e-06    0.28236

Estimated objective function value = 0.025205
Estimated function evaluation time = 72.8169
optimizedDAMdl =
  ClassificationDiscriminant
                         PredictorNames: {'Timestamp'  'CANID'  'd0'  'd1'  'd2'  'd3'  'd4'  'd5'  'd6'  'd7'}
                           ResponseName: 'label'
                  CategoricalPredictors: []
                             ClassNames: [0 1 2 3 4]
                         ScoreTransform: 'none'
                        NumObservations: 11598634
    HyperparameterOptimizationResults: [1×1 BayesianOptimization]
                            DiscrimType: 'linear'
                                     Mu: [5×10 double]
                                 Coeffs: [5×5 struct]
```

Fig. 13 Discriminant analysis optimization summary

Table 5 Linear discriminant analysis hyperparameter values

Gamma	Delta
0	0
0	0.5
0.5	0
1	0.5

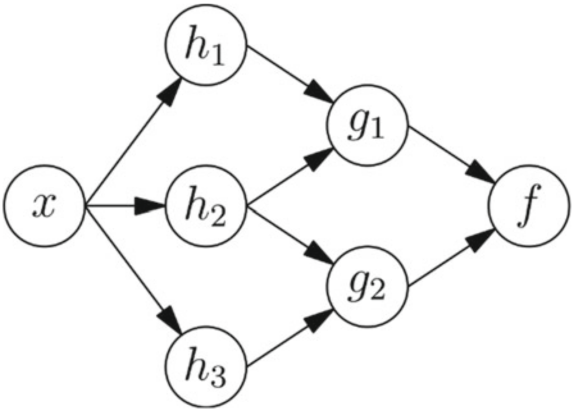


Fig. 14 Simple neural network [67]

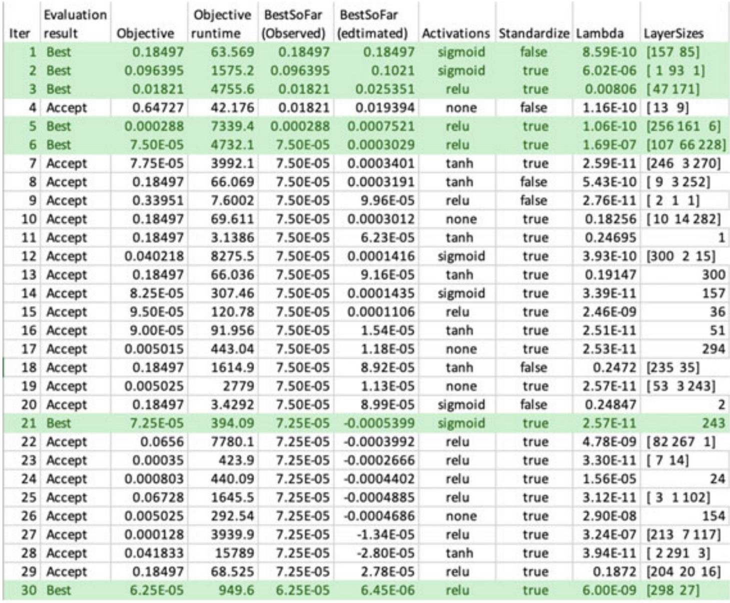
standardize. The number of neurons required in a layer can be specified using the layer sizes parameter, for example, 5 neurons in first layer and 20 neurons in second layer can be specified as [5 20]. The function to be applied on the inputs of a neuron at each fully connected layers can be specified in the activation parameters. The functions available in Table 6.

Similar to other models, optimum values for neural model hyperparameters can be found using the optimize hyperparameter function and the parameters optimized by default will be layer sizes, activations, and lambda. The output after optimization (Fig. 15).

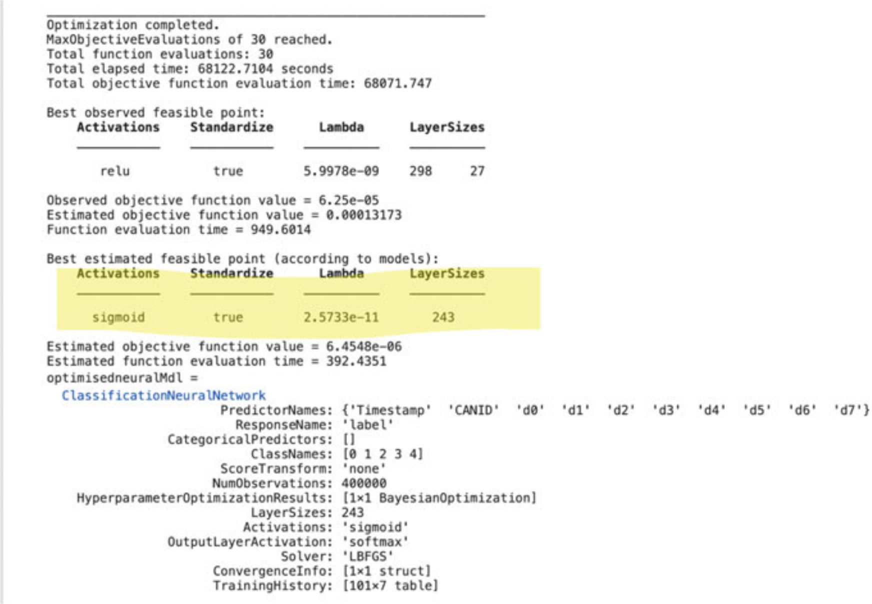
The feasible model found after optimization is the standardized model with a single layer that contains 243 neurons and uses sigmoid function on its inputs. Another two model were developed manually, one containing single layer of neurons

Table 6 Activation functions

Function	Description (all the functions mentioned below are applied on every input element in a layer)
'relu'	$f(x) := \{^{x, x \geq 0}_{0, x < 0}$ (9)
'sigmoid'	$f(x) := \frac{1}{1+e^{-x}}$ (10)
'none'	$f(x) := x$ (11)
'tanh'	The tanh function is applied on each input element



Iter	Evaluation result	Objective	Objective runtime	BestSoFar (Observed)	BestSoFar (edtimated)	Activations	Standardize	Lambda	LayerSizes
1	Best	0.18497	63.569	0.18497	0.18497	sigmoid	false	8.59E-10	[157 85]
2	Best	0.096395	1575.2	0.096395	0.1021	sigmoid	true	6.02E-06	[1 93 1]
3	Best	0.01821	4755.6	0.01821	0.025351	relu	true	0.00806	[47 171]
4	Accept	0.64727	42.176	0.01821	0.019394	none	false	1.16E-10	[13 9]
5	Best	0.000288	7339.4	0.000288	0.0007521	relu	true	1.06E-10	[256 161 6]
6	Best	7.50E-05	4732.1	7.50E-05	0.0003029	relu	true	1.69E-07	[107 66 228]
7	Accept	7.75E-05	3992.1	7.50E-05	0.0003401	tanh	true	2.59E-11	[246 3 270]
8	Accept	0.18497	66.069	7.50E-05	0.0003191	tanh	false	5.43E-10	[9 3 252]
9	Accept	0.33951	7.6002	7.50E-05	9.96E-05	relu	false	2.76E-11	[2 1 1]
10	Accept	0.18497	69.611	7.50E-05	0.0003012	none	true	0.18256	[10 14 282]
11	Accept	0.18497	3.1386	7.50E-05	6.23E-05	tanh	true	0.24695	1
12	Accept	0.040218	8275.5	7.50E-05	0.0001416	sigmoid	true	3.93E-10	[300 2 15]
13	Accept	0.18497	66.036	7.50E-05	9.16E-05	tanh	true	0.19147	300
14	Accept	8.25E-05	307.46	7.50E-05	0.0001435	sigmoid	true	3.39E-11	157
15	Accept	9.50E-05	120.78	7.50E-05	0.0001106	relu	true	2.46E-09	36
16	Accept	9.00E-05	91.956	7.50E-05	1.54E-05	tanh	true	2.51E-11	51
17	Accept	0.005015	443.04	7.50E-05	1.18E-05	none	true	2.53E-11	294
18	Accept	0.18497	1614.9	7.50E-05	8.92E-05	tanh	false	0.2472	[235 35]
19	Accept	0.005025	2779	7.50E-05	1.13E-05	none	true	2.57E-11	[53 3 243]
20	Accept	0.18497	3.4292	7.50E-05	8.99E-05	sigmoid	false	0.24847	2
21	Best	7.25E-05	394.09	7.25E-05	-0.0005399	sigmoid	true	2.57E-11	243
22	Accept	0.0656	7780.1	7.25E-05	-0.0003992	relu	true	4.78E-09	[82 267 1]
23	Accept	0.00035	423.9	7.25E-05	-0.0002666	relu	true	3.30E-11	[7 14]
24	Accept	0.000803	440.09	7.25E-05	-0.0004402	relu	true	1.56E-05	24
25	Accept	0.06728	1645.5	7.25E-05	-0.0004885	relu	true	3.12E-11	[3 1 102]
26	Accept	0.005025	292.54	7.25E-05	-0.0004686	none	true	2.90E-08	154
27	Accept	0.000128	3939.9	7.25E-05	-1.34E-05	relu	true	3.24E-07	[213 7 117]
28	Accept	0.041833	15789	7.25E-05	-2.80E-05	tanh	true	3.94E-11	[2 291 3]
29	Accept	0.18497	68.525	7.25E-05	2.78E-05	relu	true	0.1872	[204 20 16]
30	Best	6.25E-05	949.6	6.25E-05	6.45E-06	relu	true	6.00E-09	[298 27]



```
__________________________________________________________
Optimization completed.
MaxObjectiveEvaluations of 30 reached.
Total function evaluations: 30
Total elapsed time: 68122.7104 seconds
Total objective function evaluation time: 68071.747

Best observed feasible point:
    Activations    Standardize      Lambda       LayerSizes
    ___________    ___________    __________    __________

       relu           true        5.9978e-09    298     27

Observed objective function value = 6.25e-05
Estimated objective function value = 0.00013173
Function evaluation time = 949.6014

Best estimated feasible point (according to models):
    Activations    Standardize      Lambda       LayerSizes
    ___________    ___________    __________    __________

      sigmoid         true        2.5733e-11       243

Estimated objective function value = 6.4548e-06
Estimated function evaluation time = 392.4351
optimisedneuralMdl = 
  ClassificationNeuralNetwork
                           PredictorNames: {'Timestamp'  'CANID'  'd0'  'd1'  'd2'  'd3'  'd4'  'd5'  'd6'  'd7'}
                             ResponseName: 'label'
                    CategoricalPredictors: []
                               ClassNames: [0 1 2 3 4]
                           ScoreTransform: 'none'
                          NumObservations: 400000
    HyperparameterOptimizationResults: [1×1 BayesianOptimization]
                               LayerSizes: 243
                              Activations: 'sigmoid'
                    OutputLayerActivation: 'softmax'
                                   Solver: 'LBFGS'
                          ConvergenceInfo: [1×1 struct]
                          TrainingHistory: [101×7 table]
```

Fig. 15 Neural optimization summary

and other with two layers. Both of the models contained 10 neurons in all the layers with relu functions being used on inputs.

4 Data Analysis and Critical Discussion

The different models developed in chapter two are first validated using the test set followed by evaluation using the criteria's selected for evaluation. The models are then compared to find the best model that predicts with the most accuracy rate in the least time. In CAVs, attack detection time is very crucial as even a few seconds delay in detecting attacks may lead to casualties. Hence, the developed models should be able to correctly detect attacks in the least time possible.

Presently, there are no general standards for evaluating the performance of CAV cyber security, which causes difficulty in evaluating and comparing models developed by different individuals. However, a few evaluation criteria needs to be set to compare and evaluate the models developed in this project and the criteria's used will be false positive rate, accuracy, and attack detection time or runtime.

False Positives (FP) occur when a model classifies a data as an attack when the data is actually a normal data and not an attack. The equation is as follows:

$$\text{FP rate} = \frac{\text{FP}}{\text{FP} + \text{TN}} \tag{12}$$

where,

TN stands for true negatives, i.e., the data rightly predicted as normal data.

4.1 FP Means False Positives

Accuracy is the percentage of correctly predicted data against all the data in the dataset. The equation for accuracy is given below:

$$\text{Accuracy} = \frac{(\text{TP} + \text{TN})}{(\text{TN} + \text{TP} + \text{FN} + \text{FP})} \tag{13}$$

where,

True Negatives (TN) is the number of data that are rightly predicted as normal data.

True Positive (TP) is the number of data rightly predicted as an attack.

False Negative (FN) is the number of data predicted as ordinary attack-free data when it is actually an attack data.

FP stands for false positives as mentioned in the Eq. 14.

Attack detection time or model runtime is very crucial in the evaluation of different models due to the dynamic and real-world environment of CAVs. The models should be able to correctly detect attacks in the least time. The time taken to test the testing dataset is considered for this purpose.

4.2 Model Evaluation

All the selected evaluation criterions in Sect. 4.2 are now used to evaluate the models developed in the previous chapter. All the models developed are first made to detect attacks in the test dataset using the 'predict' MATLAB function. The predict function is used as follows:

$$\text{Predictions} = \text{predict}(\text{modelname}, \text{testdataset}) \tag{14}$$

A confusion chart is a matrix which provides prediction results summary. The formula for generating the confusion chart function in MATLAB is:

$$\text{confusionchart}(\text{actualoutput}, \text{predictedoutput}) \tag{15}$$

A sample confusion chart generated after predicting a small test set using neural model is shown in Fig. 16.

In Fig. 16, the values shown in blue are correctly predicted numbers and the values in orange are incorrectly predicted. The false positives for each attack can be easily found from the chart, for example number 37 in the above chart highlighted in orange is the only false positive number where 37 normal data were predicted as attack type

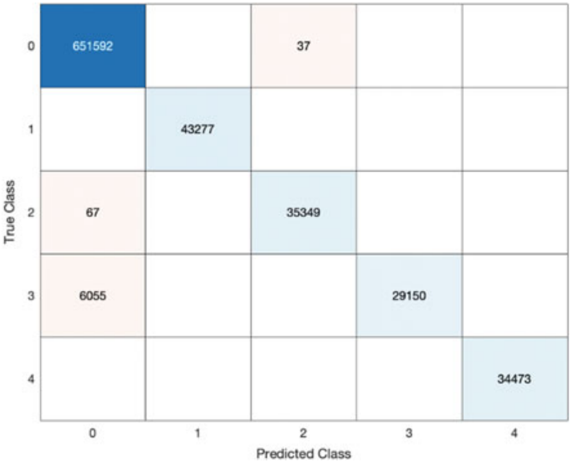
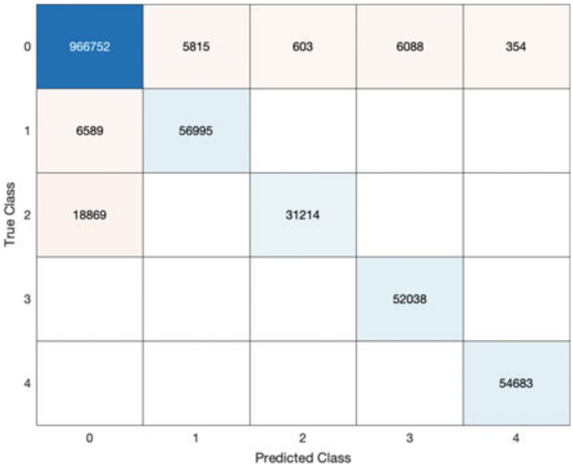


Fig. 16 Sample confusion chart



	0	1	2	3	4
0	966752	5815	603	6088	354
1	6589	56995			
2	18869		31214		
3				52038	
4					54683

Fig. 17 Confusion chart for kNN model with Chebyshev distance and nearest neighbours as 1

2 which is fuzzy attack. The rest number in orange boxes are false negatives where 67 fuzzy and 6055 gear spoofing attacks were predicted as normal attacks.

The runtime of a model can be found using the 'tic' and 'tac' functions provided by MATLAB which acts as a stopwatch timer. The testing set used in this project contains 4,970,841 CAN frames.

4.3 K-Nearest Neighbor Algorithm (kNN)

Three different kNN models were developed which included optimized model with Chebyshev distance and two manually developed models with Euclidean distance and nearest neighbors as 1 and 5. The models using Euclidean distance took more than 60 s for predicting the outputs for test set, which is a very long time in real-world environment, whereas the optimized model with Chebyshev distance took 20 s for prediction. Hence, the Euclidean models will not be considered further. The confusion chart for the optimized model is shown in Fig. 17.

4.4 Classification Trees

Four different pruned classification trees were developed in Chap. 3 with minimum leaf sizes 1, 50, and 100. All of the models were tested using the testing set and the corresponding confusion charts are shown below.

It can be observed from the above charts that tree with minimum leaf size 1 (*a* and *b* in Fig. 18) have the least incorrect predictions compared to rest of the models and that the training error is the least for model with prune level 3. Training error is

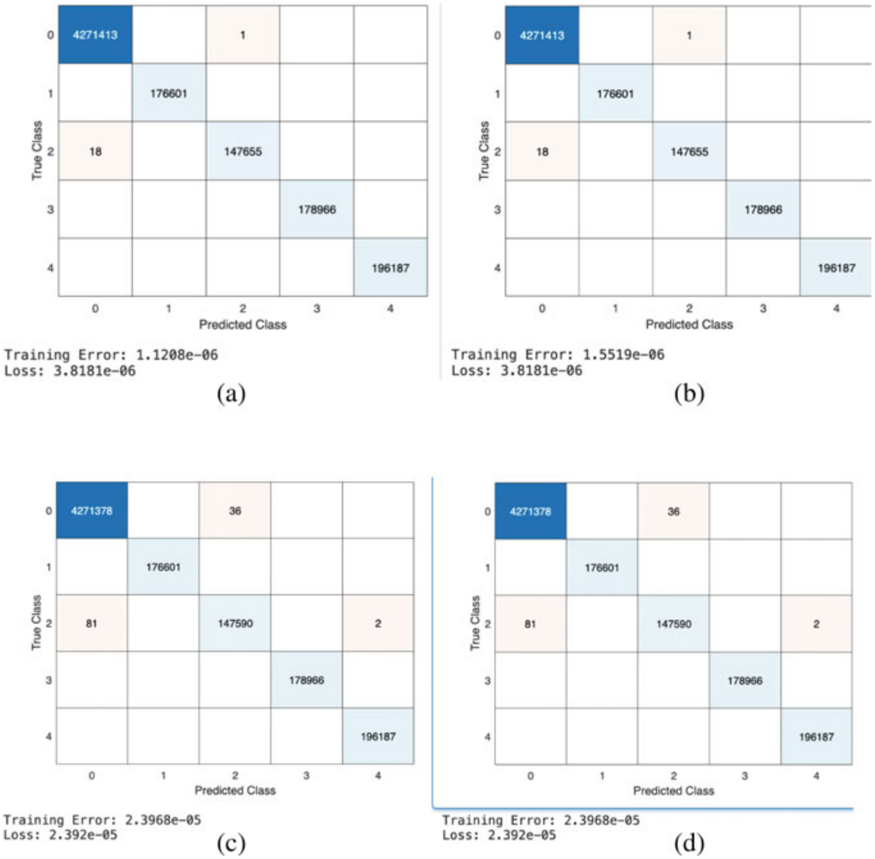


Fig. 18 Confusion charts for classification tree with **a** leaf size 1 and prune level 3. **b** leaf size 1 and prune level 4. **c** leaf size 50. **d** leaf size 100 and prune level 5

defined as the prediction error when the model is applied to predict for the training dataset. The runtime for the model with minimum leaf size 1 and prune level 3 was 2.048 s and for the same model with prune level 4 was 2.239 s. Hence, the model with minimum leaf size 1 and prune level 3 is selected as the best classification tree.

4.5 Naïve Bayes Classification

Two naïve Bayes model were developed:

- Optimized model with kernel distribution and
- Width as 0.00062723 and manually developed model with Gaussian distribution.

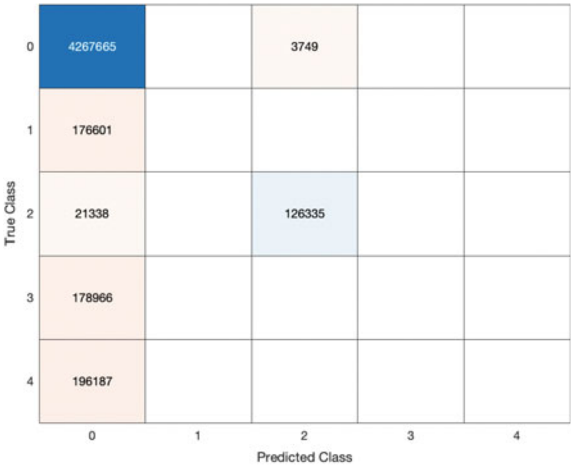


Fig. 19 Confusion charts for Naïve Bayes with Gaussian distribution

The optimized model took more than 60 s for predicting the testing set and thus, will not be considered further. The confusion chart for Gaussian model is shown in Fig. 19.

As seen from Fig. 19, most of the data were predicted as false negatives and cannot be considered as the best model for real world environments.

4.6 Discriminant Analysis

Five models were developed using discriminant analysis, one using optimization method and other four were developed manually. All the five were tested and their confusion charts (Fig. 20).

The false positive rate and accuracy can be calculated by taking the values from the above charts. The FP rate, accuracy, and runtime of different DA models are given in Table 7.

It can be seen that the three models highlighted in Table 7 have the highest accuracy with 97.3, 97.39, and 97.51% and the least FP rates. While model 5 have a slightly higher accuracy and lower FP rate compared to the other two models, it is 0.2 s slower and model 4 is 0.3 s slower in testing than model 2. To get a clearer distinction between the two models in 2 and 5, they are compared by the FP rate and accuracy in detecting different attacks as shown in Table 8. M1 in Table 8 represents the model with gamma 0.5 and delta 0, and M2 in table represents gamma 0.2824 and delta $2.048e-06$.

From Table 8, it can be observed that the model with gamma 0.2824 and delta $2.048e-06$ only have a slightly higher accuracy rate for all the attack types except fuzzy attacks. Even though this model have slightly higher accuracy, the model with gamma 0.5 and delta 0 will be considered as the best DA model since the runtime

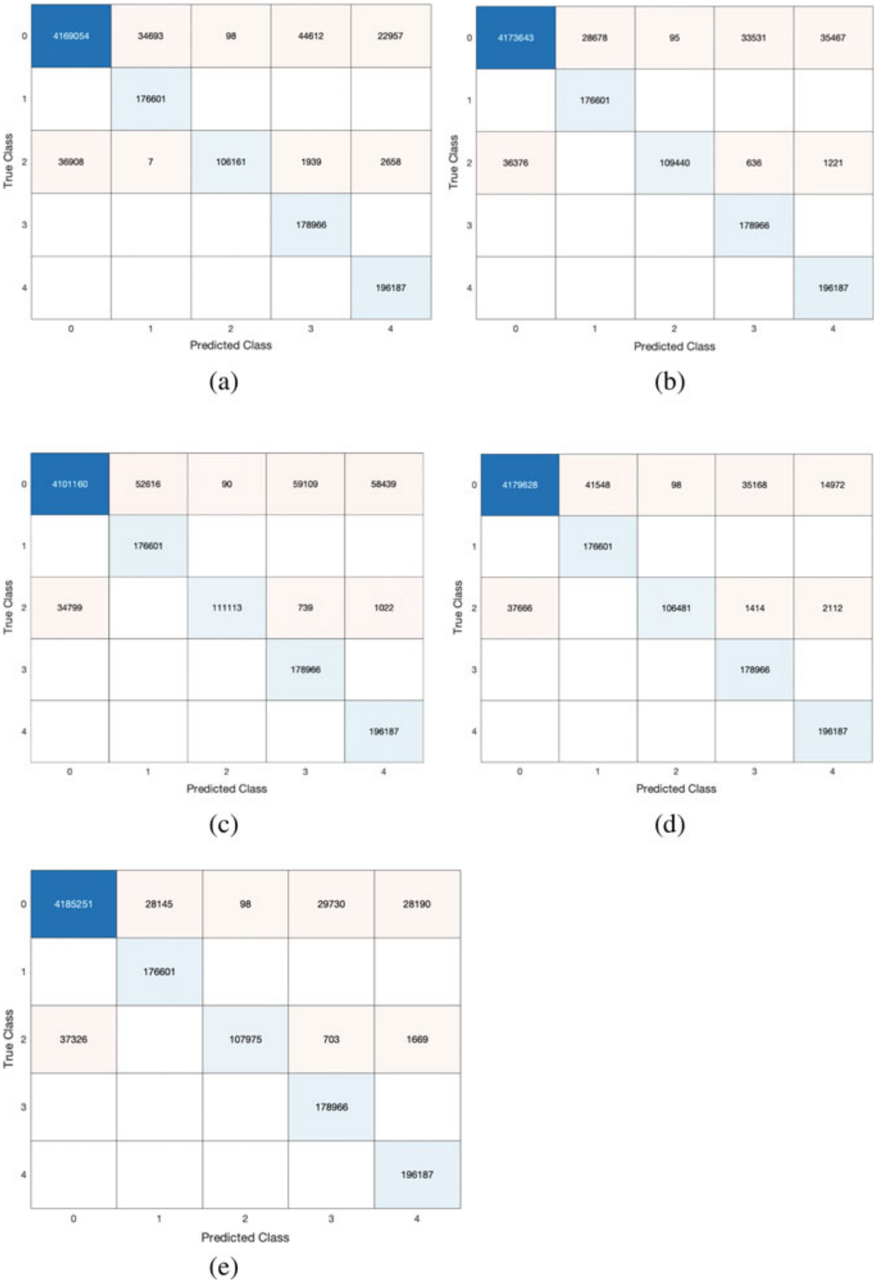


Fig. 20 Confusion Charts for DA models with **a** gamma and delta 0. **b** gamma 0.5 and delta 0. **c** gamma 1 and delta 0.5. **d** gamma 0 and delta 0.5. **e** gamma 0.2824 and delta 0.000002084

Table 7 FP rate, accuracy, and runtime of DA models

SI. no	Model characteristics	FP rate (%)	Accuracy (%)	Runtime (s)
1	Gamma and delta 0	0.0239	97.1	4.402221
2	Gamma 0.5 and delta 0	0.0228	97.3	2.651
3	Gamma 1 and delta 0.5	0.039	95.8	2.8386
4	Gamma 0 and delta 0.5	0.0214	97.39	2.917
5	Gamma 0.2824 and delta 2.084e − 06	0.020	97.51	2.829

Table 8 Model comparison based on different attacks

Attack types	M1 FP rate (%)	M1 accuracy (%)	M2 FP rate (%)	M2 accuracy (%)
Normal	0.052	97.3	0.053	97.5
DoS	6.11e − 04	99.3	5.992e − 04	99.4
Fuzzy	2.01e − 06	99.2	2.068e − 06	99.1
Gear spoofing	7.150e − 4	99.31	6.33e − 04	99.39
RPM spoofing	7.587e − 4	99.27	6.02e − 4	99.4

is 0.2 s faster and have lower FP rates which are given more importance than an accuracy difference of 0.1%.

4.7 Neural Networks Classification

Three neural models were developed of which the optimized model took more than 60 s for testing and hence will not be considered. The other two models with single layer and two layers finished predicting the test set within 1.948 and 2.167 s respectively and the corresponding confusion charts (Fig. 21).

It is clear from Fig. 21 that the model with single layer have better prediction accuracy and less false positives than the other model. It also runs 0.2 s faster than the second model and hence is considered as the best fit neural model.

4.8 Model Comparison and Results

The different models discussed above are now compared to find the best model that works with CAV CAN frames. The FP rate, accuracy rate, and runtime in seconds for each model are shown in Table 9.

Classification tree and neural network model has the same accuracy of 99.99% but the tree model has lower FP rate with only 0.07 s slower than neural network.

Fig. 21 Confusion charts for neural model with **a** single layer with 10 neurons. **b** 2 layers with 10 neurons each

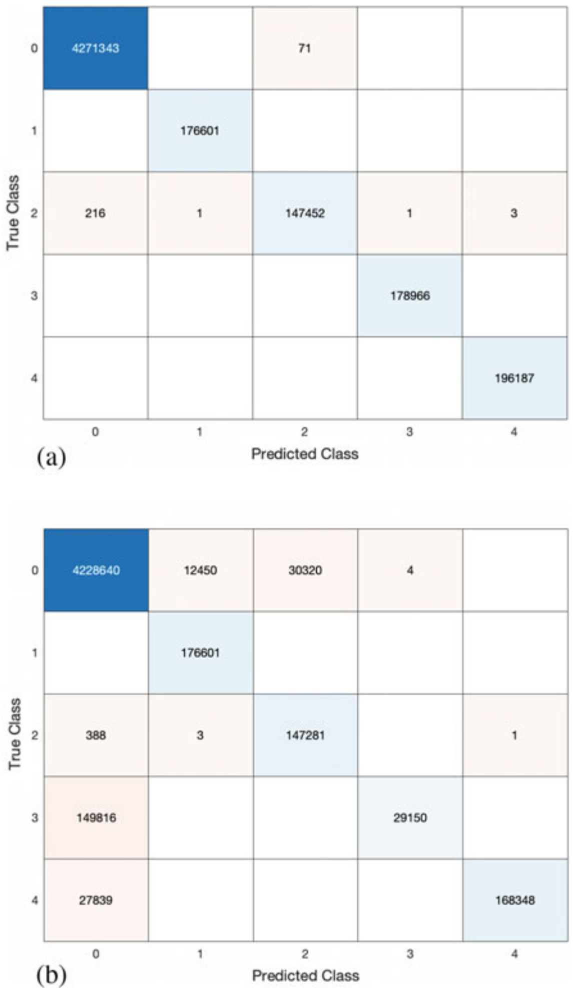


Table 9 Model comparison

Model	FP rate (%)	Accuracy (%)	Runtime (s)
kNN	0.0131	96.8	20.01
Classification tree	2.341e − 08	99.99	2.01
Naïve Bayes	8.776e − 05	88.39	2.36
Discriminant analysis	0.0228	97.3	2.651
Neural network	1.662e − 06	99.99	1.94

Table 10 Classification tree and neural network model performance comparison

Attack types	Tree FP rate (%)	Tree accuracy (%)	Neural FP rate (%)	Neural accuracy (%)
Normal	4.214e − 07	99.99	3.088e − 05	99.98
DoS	0	100	2.085e − 08	99.99
Fuzzy	2.07e − 08	99.99	1.472e − 06	99.99
Gear spoofing	0	100	0	100
RPM spoofing		100	0	100

The results after comparing those two models for their performance in detecting the different attacks are shown in Table 10.

It can be observed that except for DoS, both the models have similar FP rates and accuracy in detecting all the other attacks. Tree model achieved 100% accuracy and 0% FP rate for detecting DoS attacks while neural model achieved 99.99% accuracy and 2.085e − 08% FP rate.

Based on the comparisons in Tables 9 and 10, it can be said that classification tree model and the neural model performed better than all the other models. The tree model and neural model were able to detect a total of 699,419 and 699,206 attacks respectively from a dataset that contained 4,970,841 data in a very short time. Selecting one model over the other depends on what evaluation metric is considered more critical. In this experimentation, accuracy and FP rate are given a marginally higher weightage than a small difference in time because falsely alarming a vehicle may cause more issues than providing correct predictions with 0.07 s delay and hence, the classification tree model is recommended. However, it is still unclear how this model would perform on unknown attacks and requires further research.

5 Conclusion and Future Works

CAVs combine the technologies in Connected Vehicles (CV) and autonomous vehicles (AV) to help in driving tasks and replace humans. Even though CAVs are gaining more interest, lot of research gaps still exist. The main aim of this project is to use machine learning algorithm to develop anomaly detection models for attack detection in CAVs.

The different terms related to CAVs such as CAV, CAV cyber security, CV, and AV were first defined. Then, the CAV architecture is discussed, especially the CAN bus and ECUs in CAVs followed by listing all the vulnerabilities and potential attacks in CAVs. Several mitigation techniques were then recommended based on the attack types after which the different types of attack detection methods were explained, and the anomaly-based intrusion detection was found to be the most effective in detecting attacks.

Different machine learning models were developed and evaluated using MATLAB, of which neural model and classification tree model achieved the best results. The models were evaluated and compared using three different metrics, accuracy, FP rate, and runtime. While tree model has smaller FP rate compared to neural model, it takes 0.07 s more than neural model for testing the test set. In this project, tree model is recommended as the best performance model for detecting attacks in CAVs as lower FP rate is given more weightage than small difference in runtime.

There were many limitations found in this research. One of the main problems is the limited availability of CAV attacks dataset. As CAVs are not yet commercialised, there are only limited number of real-world datasets that were generated by conducting attacks on CAVs in controlled environments. Moreover, these datasets consist of only few of the attack types. Hence, this will affect the capability of machine learning models in detecting different attack types.

In the future, researchers could try to get more comprehensive datasets. CAV cyber security experts can help by defining different possible attacks on CAVs and CAV manufacturers could help in this area by conducting different type of attacks on CAVs in controlled environments and publishing such datasets for research purposes. Furthermore, this research mainly focused on developing supervised machine learning models for detecting attacks. These models usually perform poorly in detecting unknown attacks. Hence, different models, such as unsupervised models could be developed to detect unseen attacks, but these models have lower accuracy. Additionally, all the datasets used in this research were pre-processed and well-formatted before training and testing the models. Real-time detection of attacks in a real-world environment is still unknown and requires further study.

References

1. Brake (2021) Connected and autonomous vehicles. https://www.brake.org.uk/get-involved/take-action/mybrake/knowledge-centre/vehicles/connected-and-autonomous-vehicles. Accessed 02 May 2022
2. Sun X, Yu FR, Zhang P (2022) A survey on cyber-security of connected and autonomous vehicles (CAVs). IEEE Trans Intell Transp Syst 23(7):6240–6259
3. Greenberg A (2015) Wireless communication between cars could be a security risk. Available at: https://slate.com/technology/2015/10/wireless-communication-between-cars-could-be-asecurity-risk.html (Accessed: 14 June 2023)
4. He Q (2021) A machine learning-based anomaly detection framework for connected and autonomous vehicles cyber security. Mathematics 8:1311
5. Chakraborty S et al (2016) Automotive cyber-physical systems: a tutorial introduction. IEEE Des Test 33(4):92–108
6. Lyu N, Duan Z, Xie L, Wu C (2017) Driving experience on the effectiveness of advanced driving assistant systems. In: Proceedings of the 4th international conference on transportation information and safety, pp 987–992
7. Tsiropoulou EE, Baras JS, Papavassiliou S, Sinha S (2017) Rfid-based smart parking management system. Cyber Phys Syst 3(4):22–41

8. Anon (2014) Consommation en Europe: 2009–2014 Les Annees Qui Ont Tout Change. http://observatoirecetelem.com
9. Jones L (2017) Driverless cars: when and where? Automotive autonomous vehicles. Eng Technol 12(2):36–40
10. Fan H et al (2018) Baidu apollo em motion planner. http://arxiv.org/abs/1807.08048
11. Cottam BJ (2018) Transportation planning for connected autonomous vehicles: how it all fits together. Transp Res Rec 2672:12–19
12. Kuang X, Zhao F, Hao H, Liu Z (2018) Intelligent connected vehicles: the industrial practices and impacts on automotive value-chains in china. Asia Pacif Bus Rev 24(1):1–21
13. Anon (2017) Japan plans test site for self-driving cars. http://asia.nikkei.com/Tech-Science/Tech/Japan-plans-test-site-for-self-driving-cars. Accessed 21 June 2022
14. Locke J (2020) What is connected vehicle technology and what are the use cases? https://www.digi.com/blog/post/what-is-connected-vehicle-technology-and-use-cases. Accessed 18 June 2022
15. Nikitas A, Michakopoulou K, Njoya ET, Karampatzakis D (2020) Artificial intelligence, transport and the smart city: definitions and dimensions of a new mobility era. Sustainability 12(7):2789
16. Qayyum A, Usama M, Qadir J, Al Fuqaha A (2020) Securing connected and autonomous vehicles: challenges posed by adversarial machine learning and the way forward. IEEE Commun Surv Tutor 22(2):998–1026
17. Shladover SE, Nawakowski C, Lu XY, Ferlis R (2015) Cooperative adaptive cruise control: definitions and operating concepts. Transp Res Rec 2489(1):145–152
18. Stazswezki R, Estl H (2013) Making cars safer through technology innovation, Dallas. Accessed 17 June 2022
19. Jonsson E, Kleberger P, Olovsson T (2011) Security aspects of the in-vehicle network in the connected car. In: IEEE intelligent vehicle symposium (IV), pp 528–533
20. Koscher K, Czeskis A, et al. (2010) Experimental security analysis of a modern automobile. In: IEEE symposium on security and privacy (SP), pp 447–462
21. Martin (2022) CAN bus explained: a simple intro. https://www.csselectronics.com/pages/can-bus-simple-intro-tutorial. Accessed 15 July 2022
22. Bouzima S, Braham R (2019) An anomaly detector for CAN bus networks in autonomous cars based on neural networks. In: Proceedings of the 2019 international conference on wireless and mobile computing, networking and communications (WiMob), pp 1–6
23. Carsten P, Andel TR, Yampolskiy M, McDonald JT (2015) In-vehicle networks: attacks, vulnerabilities, and proposed solutions. In: CISR '15: proceedings of the 10th annual cyber and information security research conference, vol 1, pp 1–8
24. Knight A (2016) Understanding electronic control units (ECUs) in connected automobiles and how they can be hacked. https://cybersecurity.att.com/blogs/security-essentials/understanding-electronic-control-units-ecus-in-connected-automobiles-and-how-they-can-be-hacked. Accessed 13 July 2022
25. GOV.UK (2017) The key principles of vehicle cyber security for connected and automated vehicles. https://www.gov.uk/government/publications/principles-of-cyber-security-for-connected-and-automated-vehicles. Accessed 13 July 2022
26. ENISA (2019) Cyber security and resilience of smart cars. http://www.enisa.europa.eu/publications/cyber-security-and-resilience-of-smart-cars. Accessed 17 July 2022
27. NHTSA (2020) Cyber security best practices for the safety of modern vehicles. https://www.nhtsa.gov/sites/nhtsa.gov/files/documents/vehicle_cybersecurity_best_practices_01072021.pdf. Accessed 14 July 2022
28. Huld A (2022) China internet of vehicles—new guidelines set framework for industry standards. https://www.china-briefing.com/news/china-internet-of-vehicles-new-guidelines-set-framework-for-industry-standards/. Accessed 13 July 2022
29. Kumar S, Mann KS (2019) Prevention of DoS attacks by detection of multiple malicious nodes in VANETs. In: Proceedings of the 2019 international conference on automation, computational and technology management, pp 89–94

30. Appathurai A, Mangoran G, Chilamkurti N (2018) Trusted FPGA-based transport traffic inject, impersonate (I2) attacks beaconing in the internet of vehicles. IET Netw 8(2):106–115
31. Mondal A, Jana M (2019) Detection of fabrication, replay and suppression attack in VANET-a database approach. Proceed Conf Adv Comput Commun Elect Paradigm 1(18):38–42
32. Verma A, Saha R, Kumar G, Kim TH (2021) The security perspectives of vehicular networks: A taxonomical analysis of attacks and solutions, applied Sciences, 11(10):4682. https://doi.org/10.3390/app11104682
33. Albouq SS, Fredericks EM (2017) Lightweight detection and isolation of black hole attacks in connected vehicles. In: Proceedings of the 2017 IEEE 37th international conference on distributed computing systems workshops (ICDCSW), pp 97–104
34. Purohit K, Dimri S, Jasola S (2017) Mitigation and performance analysis of routing protocols under black-hole attack in vehicular ad-hoc network (VANET). Wireless Pers Commun 97:5099–5114
35. Shukla RM, Sengupta S (2018) Analysis and detection of outliers due to data falsification attacks in vehicular traffic prediction application. In: Proceedings of the 2018 9th IEEE annual ubiquitous computing, electronics and mobile communication conference (UEMCON), pp 688–694
36. Kamal M et al (2021) GPS location spoofing attack detection for enhancing the security of autonomous vehicles. In: Proceedings of the 2021 IEEE 94th vehicular technology conference (VTC2021-Fall), pp 1–7
37. El-Rewini Z et al (2020) Cybersecurity attacks in vehicular sensors. IEEE Sens J 20(22):13752–13767
38. Hill C (2022) A brief introduction to the SAE J1939 protocol. https://copperhilltech.com/a-brief-introduction-to-the-sa-j1939-protocol/. Accessed 19 July 2022
39. Brooks RR, Sander S, Deng J, Taiber J (2009) Automobile security concerns. IEEE Vehicul Technol Mag 4(2):52–64
40. Higgins KJ (2009) Permanent denial-of-service attack sabotages hardware. https://www.darkreading.com/permanent-denial-of-service-attack-sabotages-hardware/d/d-id/1129499. Accessed 20 July 2022
41. Jeong DR et al (2019) Razzer: finding kernel race bugs through fuzzing. In: Proceedings of the 2019 IEEE symposium on security and privacy (SP), pp 754–768
42. Arif M, Wang G, Balas VE (2018) Secure VANETs: trusted communication scheme between vehicles and infrastructure based on fog computing. Stud Inform Control 27(2):235–246
43. Liang W et al (2019) TBRS: a trust based recommendation scheme for vehicular CPS network. Fut Gen Comput Syst 92:383–398
44. Wu Y et al (2018) Secrecy-driven resource management for vehicular computation offloading networks. IEEE Netw 32(3):84–91
45. Luo YB, Wang BS, Cai GL (2014) Effectiveness of port hopping as a moving target defense, In: 2014 7th International Conference on Security Technology, Hainan, China, 7–10. https://doi.org/10.1109/SecTech.2014.9
46. Limbasiya T, Das D (2018) Secure and effective geo-data transmission scheme for vehicle-to-vehicle communication. In: Proceedings of the 2018 IEEE SmartWorld, ubiquitous intelligence and computing, advanced and trusted computing, scalable computing and communications, cloud and big data computing, internet of people and smart city innovation, pp 389–396
47. Hegde N, Manvi SS (2019) Hash based integrity verification for vehicular cloud environment. In: Proceedings of the 2019 IEEE international conference on cloud computing in emerging markets (CCEM), pp 75–79
48. Sutrala AK et al (2020) On the design of conditional privacy preserving batch verification-based authentication scheme for internet of vehicles deployment. IEEE Trans Vehicul Technol 69(5):5535–5548
49. Biron A, Merco R, Pisu P (2018) Replay attack detection in a platoon of connected vehicles with cooperative adaptive cruise control. In: 2018 Annual American Control Conference (ACC), pp. 5582–5587

50. Sánchez HS, Rotondo D, Vidal ML, Quevedo J (2019) Frequency-based detection of replay attacks: application to a quadrotor UAV. In: Proceedings of the 2019 8th international conference on systems and control (ICSC), pp 289–294
51. Panda N, Pattanayak K (2018) Energy aware detection and prevention of black hole attack in MANET. Int J Eng Technol 7(26):135–140
52. Hassan Z, Mehmood A, Maple C, Khan MA, Aldegheishem A (2020) Intelligent detection of black hole attacks for secure communication in autonomous and connected vehicles. IEEE Access 8:199618–199628
53. Qiu Y, Liu Y, Li X, Chen J (2020) A novel location privacy-preserving approach based on blockchain. Sensors 20(12):3519
54. Zhou Y, Zhang D (2019) Double mix-zone for location privacy in VANET. In: ICIT 2019: proceedings of the 2019 7th international conference on information technology: IoT and Smart City, pp 322–327
55. Petit J, Stottelaar B, Feiri M (2015) Remote attacks on automated vehicles sensors: experiments on camera and LiDAR. Black Hat Europe
56. Parkinson S, Ward P, Wilson K, Miller J (2017) Cyber threats facing autonomous and connected vehicles: future challenges. IEEE Trans Intell Transp Syst 18(11):2898–2915
57. Shao F, Wu Y (2018) The TPMS module in the vehicle positioning and safety warning system. Int Conf Appl Techn Cyber Sec Intell 842:1307–1314
58. Alam MSU, Iqbal S, Zulkernine M, Liem C (2019) Securing vehicle ECU communications and stored data. In: Proceedings of the ICC 2019—2019 IEEE international conference on communications (ICC), pp 1–6
59. Lenard T, Bolboacă R, Genge B, Haller P (2020) MixCAN: mixed and backward-compatible data authentication scheme for controller area networks. In: IFIP networking conference, pp 395–403
60. Shenfield A, Day D, Ayesh A (2018) Intelligent intrusion detection systems using artificial neural networks. ICT Express 4(2):95–99
61. Levi M, Allouche Y, Kontorovich A (2018) Advanced analytics for connected car cybersecurity. In: Proceedings of the 2018 IEEE 87th vehicular technology conference (VTC Spring), pp 1–7
62. Salman N, Bresch M (2017) Design and implementation of an intrusion detection system (IDS) for in-vehicle networks. https://publications.lib.chalmers.se/records/fulltext/251871/251871.pdf. Accessed 4 Oct 2022
63. Song HM, Kim HR, Kim HK (2016) Intrusion detection system based on the analysis of time intervals of CAN messages for in-vehicle network. In: Proceedings of the 2016 international conference on information networking (ICOIN), pp 63–68
64. Bi Z, Xu G, Xu G, Tian M, Jiang R, Zhang S (2022) Intrusion detection method for In-vehicle CAN bus based on message and time transfer matrix, security and communication networks, Article ID 2554280, 19. https://doi.org/10.1155/2022/2554280
65. Rajbahadur GK, Malton AJ, Walenstein A, Hassan AE (2018) A survey of anomaly detection for connected vehicle cybersecurity and safety. In: IEEE intelligent vehicles symposium (IV), pp 421–426
66. Eunbi S, Song HM, Kim HK (2018) GIDS: GAN based intrusion detection system for in-vehicle network. In: Proceedings of the 2018 16th annual conference on privacy, security and trust (PST)
67. Anon (2013) Ann dependency (graph). https://commons.wikimedia.org/wiki/File:Ann_dependency_(graph).svg. Accessed 12 Aug 2022
68. Boeira F, Asplund M, Barcellos M (2019) Decentralized proof of location in vehicular Ad Hoc networks, Comput Commun 147:98–110. Available at: https://doi.org/10.1016/J.COMCOM.2019.07.024

Security and Privacy Concerns in Next-Generation Networks Using Artificial Intelligence-Based Solutions: A Potential Use Case

Murat Kuzlu, Ferhat Ozgur Catak, Yanxiao Zhao, Salih Sarp, and Evren Catak

Abstract Next-generation communication networks (NextG or 5G and beyond) have become more essential to be able to realize cutting-edge applications, such as autonomous cars, mobile healthcare and education, metaverse, digital twins, virtual reality, and many more. All those applications need high-speed, low latency, and secure data transmission. Artificial intelligence (AI) technologies are the main drivers and play a critical role because of their significant contribution to all layers in NextG, i.e., from the physical to the application layer. On the other hand, the security and privacy concerns for applications using AI-based methods in next-generation networks have not been fully investigated in terms of cyber vulnerabilities. This book chapter focuses on the AI-enabled applications on the physical layer of NextG networks, including multiple input multiple output (MIMO) beamforming, channel estimation, spectrum sensing, and intelligent reflecting surfaces (IRS), as well as provides a comprehensive analysis of the potential use case, i.e., channel estimation, along with its vulnerability under adversarial machine learning attacks with and without the defensive distillation mitigation method. According to simulations outcomes, AI-enabled Next-G applications are vulnerable to adversarial attacks, and the proposed mitigation methods are able to improve the robustness and performance of AI-enabled models under adversarial attacks.

M. Kuzlu
Batten College of Engineering & Technology, Old Dominion University, Norfolk, VA, USA
e-mail: mkuzlu@odu.edu

F. O. Catak (✉)
Department of Electrical Engineering and Computer Science, University of Stavanger, Rogaland, Norway
e-mail: f.ozgur.catak@uis.no

Y. Zhao · S. Sarp
Department of Electrical and Computer Engineering, Virginia Commonwealth University, Richmond, USA

E. Catak
Independent Researcher, Stavanger, Norway
e-mail: evren.catak@ieee.org

H. Jahankhani and A. El Hajjar (eds.), *Wireless Networks*, Advanced Sciences and Technologies for Security Applications,
https://doi.org/10.1007/978-3-031-33631-7_7

Keywords Next-generation networks · 5G and beyond · Cybersecurity · Adversarial machine learning

1 Introduction

The next-generation networks, i.e., 5G and beyond, have been penetrated into all sectors, including infrastructure, computing, security, and privacy. The main goal of NextG networks is to realize cutting-edge applications, including metaverse, mobile healthcare, and education, autonomous cars, augmented reality (AR), virtual reality (VR), and others. It is expected that NextG networks will support very high data transmission (more than 100 Gbps), ultra-low latency (milliseconds), and a high cellular traffic capacity (10 million devices per square kilometer) [1–3]. Advanced communication technologies are key drivers to achieve these goals, which include millimeter wave (mmWave), massive multiple-input multiple-output (massive MIMO), and artificial intelligence (AI). In the literature, advanced communication technologies have been studied in [4–8]. In frequency bands above 24 GHz, mmWave provides many advantages in terms of throughput, capacity, and latency. The advanced version of MIMO, i.e., massive MIMO, can also significantly increase the quality throughput and capacity of the radio link by using a group of antennas at both the transmitter and receiver sides.

AI also plays an essential role in achieving these requirements to improve network applications' efficiency, latency, and reliability [9]. AI has been applied to especially several NextG applications at the physical layer, including beamforming, channel estimation, spectrum sensing, intelligent reflecting surfaces (IRS), and others. The authors in [4] investigate the role of AI-based solutions in deploying and optimizing 5G and beyond network operations. They stressed that NextG networks are different from current networks in terms of architecture, communication and computing technologies, and applications. The study [10] emphasized the contribution of AI-based solutions to NextG networks in terms of improving network performance and provided an extensive review of NextG networks using AI-based solutions, which focus on physical layer applications, including reconfigurable intelligent surface (RIS), massive MIMO, and multi-carrier (MC) waveform. These AI-based algorithms significantly improve the overall system performance for NextG networks.

On the other hand, AI-based algorithms brings security and privacy concerns. In the literature, there are several studies regarding this concern, e.g., model poisoning in the wireless research community is studied [11–16]. The authors in [17] proposed a robust framework to detect adversarial attacks for industrial artificial intelligence systems (IAISs). According to the results, the framework can detect several adversarial attacks, including DeepFool and fast gradient signed method (FGSM), with high accuracy and low delay. Since AI-enabled models could be vulnerable to adversarial attacks, AI-enabled models should be evaluated in terms of risk assessment, vulnerabilities, security and privacy concerns before deploying in the next-generation wireless communication networks.

This book chapter provides a comprehensive review of security and privacy concerns in the NextG network using AI-based solutions along with a potential use case. It also provides a brief description of widely used adversarial attacks and mitigation methods. The attacks include Fast Carlini & Wagner (C&W), Basic Iterative Method (BIM), Momentum Iterative Method (MIM), Projected Gradient Descent (PGD), and, Gradient Sign Method (FGSM), while mitigation methods include adversarial machine learning and defensive distillation. It also implements a potential use case, i.e., channel estimation, along with its vulnerability under adversarial attacks with and without the mitigation method.

2 Next Generation Networks Architecture

The next-generation networks (NextG or 5G and beyond) have been paying more attention from academia and industry to meet the demands of future applications, such as metaverse, mobile healthcare, autonomous cars, AR, VR, and many more. Significant improvements need to be performed in next-generation network architecture to meet requirements along with the driving force behind the evolution of wireless networks. Future applications have more rigid requirements in terms of data transmission and latency, which will force the limits of 5G networks. NextG networks are expected to enhance information transmission performance, i.e., up to 1 Tbps data rate and ultra-low latency (microseconds). One goal of NextG is to provide global coverage through satellite communication networks and underwater communications [18]. It is also expected NextG will offer energy-efficient and seamless wireless connections in a global scope as well as guarantee future application requirements, such as ultra-high throughput and ultra-low latency. The NextG architecture is also different from the traditional one, i.e., combined terrestrial and non-terrestrial networks, integration of fully AI-based models for all layers, and enhanced network protocol stack framework. Big data and AI will play a crucial role in NextG networks to meet the requirements in terms of efficient network management, distributed computing, resource sharing, and security and privacy concerns. The authors in [19] proposed an architecture to tackle these challenges. Figure 1 derived from [19] represents the NextG network architecture. The architecture consists of three layers, i.e., (1) Resource level, (2) Network function level, and (3) Service and application level. The first layer (resource level) provides the main resource for the upper layers, including communication, distributed cloud data, and computing resources. The second level (network function level) manages the resources and conducts the network functions for the service and application levels. The third level (service and application level) can generally be classified into two categories: (1) vertical services focusing on specific applications, e.g., vehicles or drones, and (2) horizontal services crossing different applications, e.g., reporting and tracking the location of users and their devices. This architecture also consists of four planes: (1) Sharing and cooperation plane, (2) Data collection plan, (3) AI plane, and (4) Security plane. The sharing and cooperation plane is the most important plane to address the decentral-

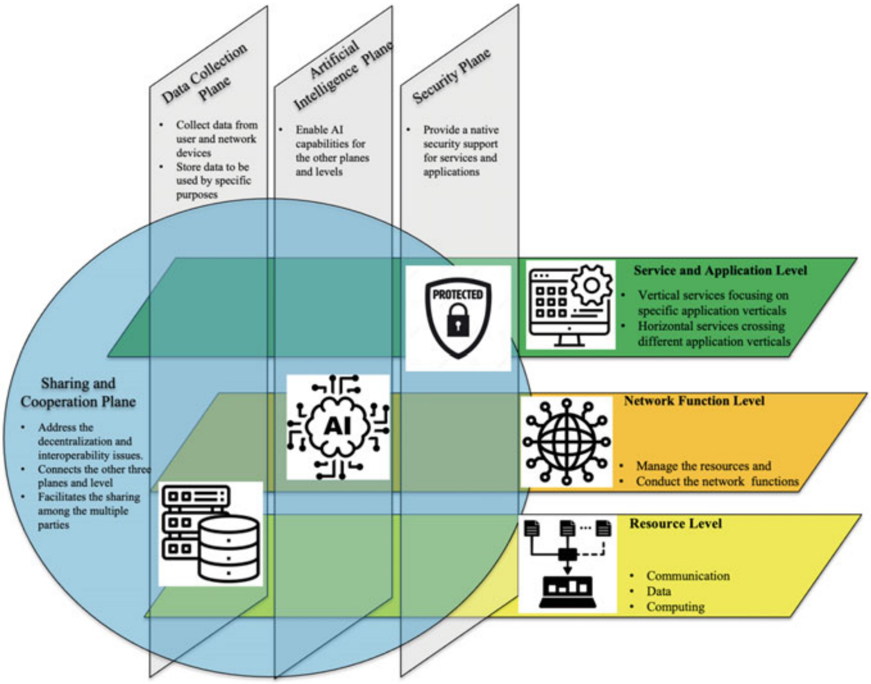

Data Collection Plane
Collect data from user and network devices
Store data to be used by specific purposes
Artificial Intelligence Plane
Enable AI capabilities for the other planes and levels
Security Plane
Provide a native security support for services and applications
Service and Application Level
Vertical services focusing on specific application verticals
Horizontal services crossing different application verticals
PROTECTED
AI
Sharing and Cooperation Plane
Address the decentralization and interoperability issues.
Connects the other three planes and level
Facilitates the sharing among the multiple parties
Network Function Level
Manage the resources and
Conduct the network functions
Resource Level
Communication
Data
Computing

Fig. 1 Conceptual NextG network architecture [19]

ization and interoperability issues. It connects the other three planes and facilitates the sharing among multiple parties. The data collection plane is responsible for data collecting from the user and network devices as well as storing them to be used for specific purposes, such as network operation and optimization. The AI plane is the other important plane in this architecture. It provides AI-enabled capabilities for the security plane, resource level, network function level, and service and application level on demand. The last plane is the security plane, which provides native security support for networks, services, and applications.

3 CyberSecurity Framework for Next Generation Networks

Below is a proposed framework alongside some of widely used cybersecurity frameworks available. These frameworks help enterprises manage potential cyber risks efficiently and allow them to plan for future detection of cyber threats or investigation of security incidents during application and system development.

3.1 Available Cybersecurity Frameworks

3.1.1 ML Cyber Kill Chain

Lockheed Martin created the Cyber Kill Chain methodology to support organizations understand and assess the risks they face from a potential cyber-attack. There are seven phases in a typical cyber-attack. These phases are *reconnaissance*, *weaponization*, *delivery*, *exploitation*, *installation*, *command and control/actuation*, and *actions on objectives*. Organizations can assess the potential effect of an effective cyber-attack on their operations by understanding the activities that occur during each cyber-attack phase.

3.1.2 MITRE ATT&CK

MITRE ATT&CK is designed to catalog the tradecraft and behaviors of adversaries to identify their activities better and generate an effective response strategy. By providing a common language and framework, organizations can more easily communicate their security processes and make attackers' techniques and tactics more identifiable.

3.1.3 MITRE Atlas

MITRE Atlas is a framework that includes information on how attackers might try to harm AI systems so that people can be better prepared to defend against those attacks. It is similar to MITRE Att&ck, which is a general framework for regular systems, not just AI systems. MITRE Atlas is a resource that includes information from security groups and academic research.

3.2 Proposed Framework

Our study aims to address security threats and possible solutions by matching the Cyber Kill Chain and MITRE Atlas frameworks to catch and mitigate the vulnerabilities of AI models. These models will be a new part of potential AI-based 5G and beyond networks. Figure 2 illustrates 3 stages of the cyber kill chain for AI-based applications.

The first stage of creating an adversarial AI model is to gather information about the AI model we want to exploit. This can be done by finding datasets from publicly available sources like the weights and hyperparameters used in the training process. After this, the adversary can make their own replica of the AI model to make malicious inputs. The second stage is to build the replicated model, find its vulnerabilities, and generate malicious pilot signals that will be used as inputs to the target AI model. The third stage is to execute the target AI model with the malicious input signals.

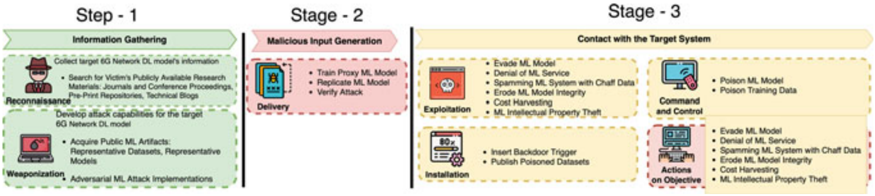

Step - 1
Information Gathering
Collect target 6G Network DL model's information
• Search for Victim's Publicly Available Research Materials: Journals and Conference Proceedings, Pre-Print Repositories, Technical Blogs
Reconnaissance
Develop attack capabilities for the target 6G Network DL model
• Acquire Public ML Artifacts: Representative Datasets, Representative Models
• Adversarial ML Attack Implementations
Weaponization
Stage - 2
Malicious Input Generation
• Train Proxy ML Model
• Replicate ML Model
• Verify Attack
Delivery
Stage - 3
Contact with the Target System
• Evade ML Model
• Denial of ML Service
• Spamming ML System with Chaff Data
• Erode ML Model Integrity
• Cost Harvesting
• ML Intellectual Property Theft
Exploitation
Command and Control
• Poison ML Model
• Poison Training Data
80x
• Insert Backdoor Trigger
• Publish Poisoned Datasets
Installation
Actions on Objective
• Evade ML Model
• Denial of ML Service
• Spamming ML System with Chaff Data
• Erode ML Model Integrity
• Cost Harvesting
• ML Intellectual Property Theft

Fig. 2 Cyber kill chain for AI-based applications of 6G wireless communication networks

This will make the AI model fabricate incorrect outcomes, which the attacker can use to exploit the AI model and install a backdoor. With the backdoor, the adversary will take control of the AI model and the target system.

The tactics and methodologies described in the adversarial tactics and methodologies section of MITRE Atlas will take place in the Cyber kill chain stages.

(i) The reconnaissance phase is when the adversary gathers information about the organization and its networks, systems, and employees. This information can create a profile of the organization, employees, network, and procedures. Social engineering attacks can be made with this information by the attackers.

(ii) The weaponization phase occurs when the attacker utilizes the information collected during the reconnaissance phase to develop the tools they need to successfully make an attack against the organization. The adversary will use the information collected during the previous stage to choose the best delivery instrument to get the information it wants to deliver to the organization's IT infrastructure. The adversary can then concentrate on the delivery phase, using the same tools to provide information or files to the organization's IT infrastructure.

(iii) The attacker must make use of a vulnerability in the organization's network once the information has been provided. The information gathered during the reconnaissance phase can be used to identify the software operated by the organization, operating systems, and applications running on the organization's systems.

(iv) After the adversary has gathered information about the target organization during the reconnaissance phase, they will use this information to exploit the organization's network during the exploitation phase. The adversary will identify the best software, operating systems, and applications to exploit to install malicious software on the organization's systems. This malicious software will allow the adversary to manipulate or listen in the organization's network.

(v) The command and control phase refers to when the attacker uses the malicious program installed during the exploitation phase to place further malicious software on the organization's systems. This allows them to control the organization's systems.

(vi) The attacker may utilize the malicious program placed in the course of the exploitation phase to reach the organization's systems and loot information during the actions on objectives phase. They may also interfere with the organization's network.

The cyber kill chain is a process that details the steps an adversary takes to launch a successful cyberattack. Once the adversary has completed all the process steps, the organization's ability to employ its network can be affected.

3.3 Adversarial Machine Learning Attacks

There are two main types of adversarial machine learning models: the attacker's and the user's models. The attacker's goal is to manipulate the output of the user's model so that the attacker can benefit from the user's perspective [20]. Adversarial machine learning attacks are effective if the attacker accesses the training data. However, the proposed scheme is robust to the perturbations of the adversarial samples of the training data, which in turn makes the proposed scheme robust to adversarial machine learning attacks.

For example, to attack a deep learning model that predicts beamforming vectors, the attacker first needs to find a noise vector $\sigma \in \mathbb{C}^k$ that will maximize the loss function ℓ output. The attacker then uses the lowest possible budget to corrupt the inputs, which increases the distance (i.e., mean squared error (MSE)) between the model's prediction and the real beam vector. Therefore, σ is calculated as

$$\sigma^* = |\sigma|_p \leq \epsilon \text{arg max } \ell(\omega, \mathbf{x} + \sigma, \mathbf{y}) \tag{1}$$

where $\mathbf{y} \in \mathbb{R}^m$ is the label (i.e., beamforming vectors), and p is the norm value, and it can be $0, 1, 2, \infty$.

There are two primary methods of constructing adversarial examples: content-based and gradient-based [21]. Gradient-based attacks were chosen due to their simplicity and variety. Gradient-based attacks use the gradient of the loss function to generate adversarial examples, which are then incorrectly labeled.

(i) Fast Gradient Sign Method (FGSM): FGSM tries to fool a neural network by changing the data given a little bit. The idea is to add noise to the data in the same direction as the loss function. The noise is controlled by a small number, epsilon. This makes the data look slightly different to the neural network, but enough to fool it.

$$\mathbf{x}^{adv} = \mathbf{x} + \epsilon \cdot sign(\nabla_x \ell(\omega, \mathbf{x}, y)) \tag{2}$$

(ii) Basic Iterative Method (BIM): The BIM attack is a variation of the FGSM single-step attack. It works by iteratively updating adversarial examples multiple times, with each value calculated in the neighborhood of the original input. The selected input with a smaller step size is manipulated by BIM iteratively.

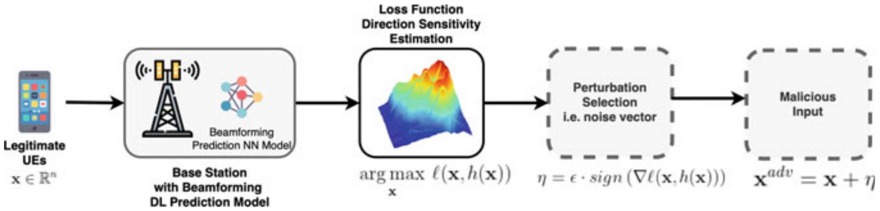


Fig. 3 Typical adversarial machine learning-based malicious input generation

FGSM is applied multiple times to a small step size alpha instead of taking one significant step, i.e., epsilon/alpha. By doing this, BIM creates less distortion while still fooling the neural network. However, this increases the computing cost and complexity. The BIM can be explained using the following equation.

$$\mathbf{x}_0^{adv} = \mathbf{x}, \mathbf{x}_{N+1}^{adv} = Clip_{\mathbf{x},\epsilon}\{\mathbf{x}_N^{adv} + \epsilon \cdot sign(\nabla_x \ell(\omega, \mathbf{x}_N^{adv}, y))\} \tag{3}$$

(iii) Projected Gradient Descent (PGD): PGD creates adversarial examples by starting the search at random points in a specified region and running several iterations to find an example that maximizes loss, which will be similar to a real input but different enough to trip up the ML model. PGD can generate more powerful attacks than BIM and FGSM. However, the size of the perturbation is kept smaller than a specified value, referred to as epsilon, so that the adversarial example is still realistic and isn't just a random input.

(iv) Momentum Iterative Method (MIM): MIM is another derivation of the BIM adversarial attack that improves the convergence of BIM by introducing a momentum term and integrating it into iterative attacks [22]. The step size of the ϵ also determines the attack level of MIM as an attack parameter. MIM is better at finding the minimum amount of change needed to fool a model than BIM and can do so more quickly.

A characteristic adversarial ML-based malicious input generation process is indicated in Fig. 3.

3.4 Mitigation Methods for Wireless Networks

The 5G and future generations of networks relying on DL are vulnerable to adversarial machine learning attacks. Adversarial training and defensive distillation are two possible methods of mitigating these attacks and protecting wireless networks.

3.4.1 Adversarial Training

The goal of iterative adversarial training is to reduce the adversarial inputs' impact on the training process. The DL model is first trained with the normal training data in iterative adversarial training. Then, the DL model is trained with the adversarial examples using the correct labels. The DL model is trained multiple times with normal and adversarial examples. However, iterative adversarial training is not practical. To increase the robustness of the victim model, it must train against all the different attack types and parameters which will take a quite long time.

The pseudo-code of adversarial training is shown in the algorithm 1.

Algorithm 1 Iterative adversarial training-based mitigation

```
Input $h$: vulnerable model, $\Omega$: attacks, $\Pi$: epsilon values, $\mathbf{x}_{train}$: training data, $\mathbf{y}_{train}$ training data output , $x_{test}$: test data, $y_{test}$: test data output
Output $\hat{h}$: robust model
for $\epsilon \in \Pi$ do {For each epsilon budget}
    for $attack \in \Omega$ do {For each epsilon budget}
        $\mathbf{x}^{adv} \leftarrow attack(\mathbf{x}_{train}, \epsilon)$ {Generate malicious inputs with $attack$ and $\epsilon$ budget.}
        $\mathbf{x}^{adv\_train} \leftarrow \mathbf{x} \bigcup \mathbf{x}^{adv}$ {Merge newly created malicious inputs $\mathbf{x}^{adv}$ and $\mathbf{x}_{train}$ }
        $h.fit(\mathbf{x}^{adv\_train}, \mathbf{y}_{train})$ {Re-train the model $h$ with new training data}
    end for
end for
```

3.4.2 Defensive Distillation

Papernot et al. [23] proposed defensive distillation technique as an adversarial ML defense method against attacks. In knowledge distillation, a larger model (the teacher) is used to train a smaller model (the student). The teacher model is first trained with a high-temperature parameter to soften the softmax probability outputs of the DNN model. The student model is then trained using the outputs of the teacher model. The goal is for the student model to learn the knowledge of the teacher model but be smaller and faster. Equation 4 shows the modified softmax activation function as follows:

$$p_i = \frac{\exp(\frac{z_i}{T})}{\sum_j \exp(\frac{z_i}{T})} \tag{4}$$

where p_i is the probability of i-th class and z_i are the logits. The teacher model is used to predict each sample to acquire the training data's soft labels which are used to train the student model. Figure 4 shows the overall steps for this technique.

The beamforming prediction model (i.e., student model) is drawn in Fig. 4 which is trained and used in base stations to protect against adversarial machine learning attacks. The student model inherits the training parameters after the teacher model's

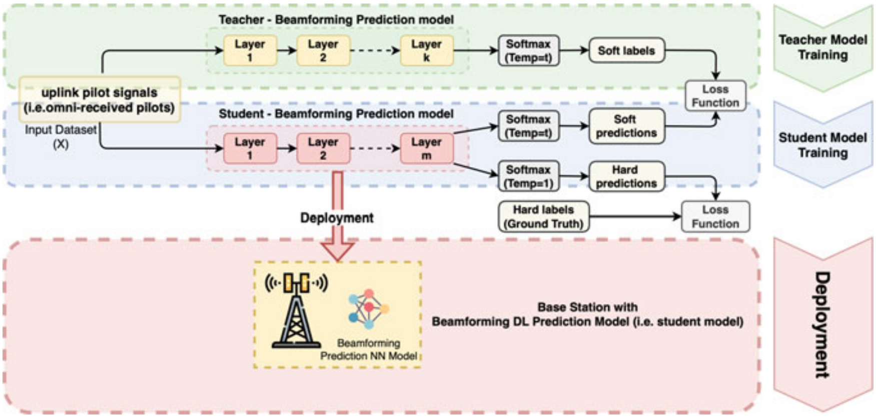

Teacher - Beamforming Prediction model
Layer 1
Layer 2
Layer k
Softmax (Temp=t)
Soft labels
Teacher Model Training
uplink pilot signals (i.e.omni-received pilots)
Input Dataset (X)
Loss Function
Student - Beamforming Prediction model
Layer 1
Layer 2
Layer m
Softmax (Temp=t)
Soft predictions
Student Model Training
Softmax (Temp=1)
Hard predictions
Hard labels (Ground Truth)
Loss Function
Deployment
Beamforming Prediction NN Model
Base Station with Beamforming DL Prediction Model (i.e. student model)
Deployment

Fig. 4 Defensive distillation

training as a first step. In the second step, the student model is trained using the teacher models parameters, and the loss function is created with the actual labels and predictions of the student model. This technique allows preserving the teacher model's knowledge to be compressed and transferred to the student model. And as a last step, student model is deployed to the base stations.

A technique called defense distillation can be used to reduce the effects of gradient-based untargeted attacks. This technique lowers the gradients to zero, making the standard objective function impractical.

4 Potential Use Cases

In this section, we will introduce several potential use cases including MIMO beamforming, spectrum sensing, channel estimation and IRS.

4.1 MIMO Beamforming

Signal to noise ratio is one of the key metrics for a channel that is affected by signal fading. Having diverse sources for a signal considerably reduces the error rate as each of the signal paths is not affected similarly. There are three ways to increase the diversity of the signals, i.e., Time diversity, Frequency, and space diversity. First, two uses use various times and frequencies, such as channel coding and OFDM. Space diversity benefits from the distribution of multiple antennas to capture different radio paths.

MIMO is one of the widely used RF technology that provides increased link capacity and spectral efficiency. MIMO systems utilize multiple antennas for both the receiver and transceiver ends to handle more data simultaneously.

Wireless signals can take various paths during the transmission between transmitter and receiver. Also, the change in the location of any antennas will create additional paths. This multipath propagation nature of the signal is caused by the objects along the transmission path. Previously, multipath propagation is seen as interference that causes signal degradation.

However, MIMO systems benefit from multipath propagation, where each additional signal path is considered as an additional channel to transmit additional data to the receiver. This is one of the main reasons that MIMO systems provide a robust link between the two ends. That is why the reliability of the MIMO systems depends on multipath propagation.

4.2 Spectrum Sensing

The electromagnetic spectrum that ranges 1 Hz to 3 THz is called the radio spectrum. It is one of the keys and limited resources that is not fully utilized due to region-based regulations and technical hardships. The majority of the existing radio spectrum is allocated to high-demand service providers, such as cellular communication, TV, and radio broadcasting. However, According to the report released by the Federal Communications Commission (FCC), there is still an underutilized spectrum, such as the licensed 0–6 GHz band having the 90% of underage [24, 25]. To increase the utilization of the limited spectrum, FCC recommends the use of free bands by a secondary user(s) until the primary user needs it. That’s why “spectrum sensing” processes are developed to check specific bands to detect non-occupied frequency bands.

Spectrum sensing is also one of the notable research fields in cognitive radio (CR). CR is an intelligent software-based wireless communication concept that is introduced by Mitola in 1999 [26]. CR has a dynamic structure that senses and learns the wireless channels in its vicinity. It will then adopt the operating parameters to steer clear of user interference and congestion.

There has been a constant interest in spectrum sensing and related fields in the literature. For example, the study [27], provides a comprehensive survey of spectrum sensing for CR. Enabling algorithms, challenges, sensing standards, approaches, and cooperative and multi-dimensional spectrum sensing is presented. Also, the study [28], provides detailed spectrum sensing techniques such as the optimal likelihood ratio test, energy detection, matched filtering detection, cyclostationary detection, eigenvalue-based sensing, joint space-time sensing, and robust sensing methods.

Even though there are many studies and proposed methods for spectrum sensing, spectrum sensing is still subject to research because of the changeable nature of wireless communication channels, complexity, interferences, and noise in communication. AI methods would be a good alternative solution for spectrum sensing to deal with communication’s complexity and changeable nature.

4.3 Channel Estimation

Transmitters and receivers utilize various mediums or channels to exchange information. In the case of wireless communication, a channel is simply the band of Radio Frequency that is used for the transmission of the signals. The characteristic and state of the channel is called channel state information (CSI). The transmitted signal $(x(t))$ is exposed to three main distortions to some degree, i.e., attenuation by a factor of h_0, delay by a certain time τ_0 and noise, depending on the properties of the channel. The delay of τ_0 based on the electromagnetic wave's speed and attenuation h_0 is determined by the transmitter/receiver gains, frequency, and propagation medium. To transmit a signal from one point to another point meaningfully, the received signal $(y(t))$ needs to be decoded correctly. The first step to decode a signal is to understand the CSI such that the added noise and distortion can be rectified at the receiver. This process is called channel estimation. The signal at the receiver can be shown as:

$$y(t) = h_0 * x(t - \tau_0) \tag{5}$$

Scattered and reflected signals also reach the receiver with various delays and attenuation. These are also summed on the receiver side. Moreover, the mobility of the communication sides affects the attenuation h_l^t and delay τ_l^t of the CSI by introducing a doppler frequency shift.

$$y(t) = \sum_{l=0}^{l} h_l^t * x(t - \tau_l^t) \tag{6}$$

where l is the specific path/tap at a time.

To fully utilize the capacity of the channel and increase the overall performance of the information transmission, channel estimation is one of the critical topics in wireless communication.

4.4 Intelligent Reflecting Surfaces (IRS)

IRS has been recognized as valuable ingenious technology [29]. This newly emerged technology could be perceived as the extension of massive MIMO [30]. It will enable increased data rate and channel capacity that NextG wireless communication requires without the vast amount of energy consumption and complexity of massive MIMO applications.

An IRS composes of a large number of predominantly passive elements, i.e., micro-strip type small antennas. Each of these elements' properties, such as load impedance, could be tunable by PIN diodes or varactors. PIN diodes are turned on or off to alter the phase-shift difference of IRS elements with different load impedances. Varactors' bias voltage is another parameter that can be utilized to tune phase shift by altering the load impedance of each element. The reflected signals amplitude is also changed with the variable resistor's resistivity. By controlling the load impedance and resistivity of each element, different reflection coefficients are achieved individually.

If the phase shifts of individual elements are controlled in a way that the reflected signals are added constructively or constructively, the signals could be directed at certain guidance. An IRS controller is responsible for receiving the reconfiguration request communication. A field-programmable gate array (FPGA) could be employed to implement the IRS controller. Besides the passive elements, a few active IRS elements are also included in some of the IRS architectures. These active elements gather two orthogonal uplink communication links from both transmitter and receiver to predict the channel vectors and environment descriptors. AI-based techniques are adopted to utilize active elements as well.

5 A Potential Use Case: AI-Enabled Channel Estimation Model

In this section, we will take AI-based channel estimation modelling as a specific use case via presenting the dataset and experimental results. Experimental results cover the vulnerability analysis of the AI-enabled models to adversarial machine learning attacks with and without the selected mitigation method, i.e., defensive distillation. The model vulnerability will be evaluated through the MSE performance metric. MSE measures the average squared difference between the actual and predicted values. A high MSE score represents a high prediction error.

5.1 Dataset Preparation

In recent years, several network simulation tools have provided a wide range of examples for next-generation network communications systems, including NS3, OMNET++, NetSim, RemCom, MATLAB, and many more [31]. These tools are usually used for evaluating the performance of communication networks or dataset generation. In this study, a reference example in MATLAB 5G Toolbox [32], i.e., "Deep Learning Data Synthesis for 5G Channel Estimation," is selected to obtain datasets for DL-based models. It also allows to customize and generate communication components, such as waveforms, antennas, and channel models.

Channel estimation model is created with a single-input single-output (SISO) antenna by using demodulation reference signal (DM-RS) and the physical downlink shared channel (PDSCH) to generate 256 training datasets. Each dataset presents 8568 data points, i.e., 612X14X1 or 612 subcarriers, 14 OFDM symbols, and 1 antenna. Then, each data point is converted to a real-valued 612-14-2 matrix, i.e., from a complex (real and imaginary) 612-14 matrix. It is required to provide real

Table 1 The channel estimation parameters with values

Channel parameter	Value	Channel parameter	Value
Delay profile	TDL-A/B/C/D/E	Modulation	16QAM
Delay spread	1–300 ns	Transmit antenna	1
Doppler shift	5–400 Hz	Receive antenna	1
NFFT	1024	Transmission direction	Downlink
Sample rate	30,720,000	Polarization	Co-Polar
Symbols per slot	14	Windowing	36
Slots per subframe	2	Slots per frame	20

inputs instead of complex ones into the convolutional neural network (CNN) model used in the reference model during the training process. This is because the resource grids include complex data points, i.e., real and imaginary, in the channel estimation scenario. However, the CNN model handles the resource grids as 2-D images with real numbers. Finally, 4-D arrays (612-14-1-2N) are created from the training dataset with N as the number of training examples (256). In this study, 80% of the dataset is used for training, while 20% is used for testing.

For each dataset, a new channel characteristic is generated based on selected channel parameters and tuned through MATLAB 5G toolbox. Table 1 below provides the channel estimation scenario parameters with values.

5.2 Experimental Results

This section investigates the experimental results of an AI-powered channel estimation model against adversarial machine learning attacks. These results are represented in two ways: (1) line plots showing the impact of each adversarial machine learning attack (FGSM, MIM, BIM, and PGD) on the undefended and defended model performance, i.e., MSE, and (2) the table showing the performance (i.e., MSE) of the defended and undefended models for each adversarial attack. Figures 5 and 6 show the line plots, while Table 2 shows the prediction performance results of the defended and undefended AI-powered channel estimation models against adversarial attacks.

Figure 5 shows MSE values for the FGSM, MIM, BIM, and PGD attack methods for undefended models under attack powers from $\epsilon = 0.01$ to $\epsilon = 3.0$. MSE values are close to each other for attack methods with a low power attack, i.e., $\epsilon < 0.5$. However, these values dramatically increase along with higher power attacks ($\epsilon > 0.5$). For example, MSE values can reach from 1.51, 153 to 10.69, 9.32 for BIM and PGD. The case is different for FGSM and MIM attacks, i.e., MSE values are low compared to BIM and PGD. The reason is that FGSM and MIM attacks are simple types of attacks, and then MSE values do not dramatically increase with high attack power. According to the results, the AI-powered models are exposed to

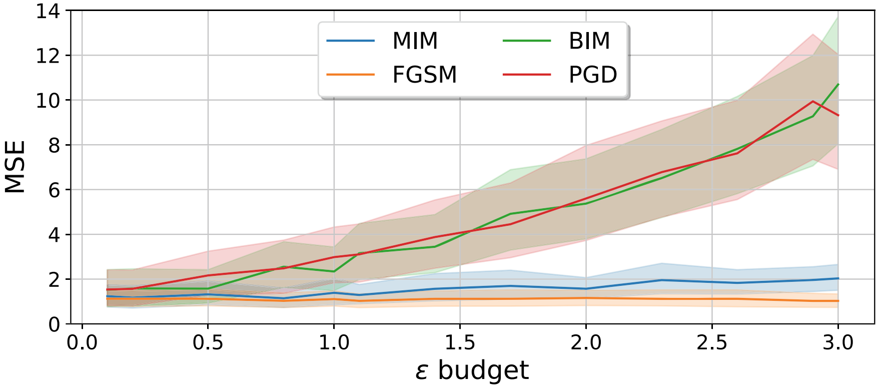


Fig. 5 MSE comparison for undefended channel estimation model under adversarial attacks

adversarial attacks, especially PGD and BIM, and MSE can be very high under a heavy adversarial attack. Fortunately, the mitigation methods (such as adversarial training and defensive distillation) can significantly contribute to improving the AI-powered model's robustness against adversarial attacks. In this study, the defensive distillation method is used as a mitigation method. The model performance is shown in Fig. 6 after applying the mitigation method for the selected adversarial attacks and attack powers in terms of MSE. According to Fig. 6, defended AI-powered models are still vulnerable to adversarial attacks. However, the models' robustness is better under adversarial attacks. Models can resist high attack power. For example, MSE values can go from 1.51, 1.12, 1.22, and 1.51 to 2.1, 1.03, 1.79, and 2.26 with the lowest attack power ($\epsilon = 0.1$) and the highest attack power ($\epsilon = 3.0$) for BIM, FGSM, MIM, and PGD, respectively. The impact of the mitigation method on the model performance is different for some attack types. It has a high impact on the BIM and PDG attacks. This is because they are more complex attacks, and the MSE values can go very high under these attacks. As expected, the change in MSE is more compared to simple type attacks. For FGSM and MMI, the mitigation method has almost no impact on the models' performance under adversarial attacks.

Table 2 shows the impact of attack power (ϵ) on undefended and defended models' performance, i.e., MSE, for each adversarial attack in detail. The value of ϵ ranges from 0.1 to 3.0. The higher value of ϵ means a powerful attack. The lowest MSE value is 1.12 (under FGSM attack), and the highest MSE value is 10.69 (under BIM attack) for defended models. On the other hand, the lowest MSE value is 1.12 (under FGSM attack), and the highest MSE value is 2.26 (under PGD attack). MSE values dramatically go down from 10.69/9.32 to 2.10/2.26 for BIM/PGD after the mitigation method is applied. It is clear that the mitigation method significantly improves the model's robustness, especially BIM and PGD. However, it cannot be said for FGSM and MIM attacks. According to Table 2, MSE values do not change as expected; they look closely to undefended and defended models, e.g., MSE values are 1.02 and 1.03 for undefended and defended models under an FGSM attack.

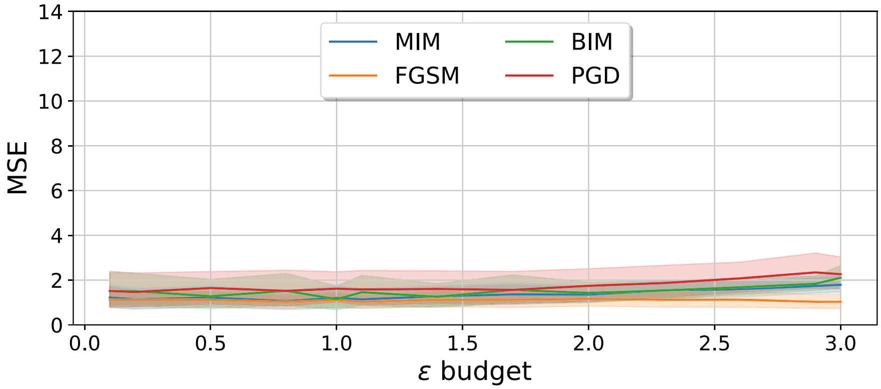


Fig. 6 MSE comparison for defended channel estimation model under adversarial attacks

Table 2 MSE results

	Defended				Undefended			
ϵ	BIM	FGSM	MIM	PGD	BIM	FGSM	MIM	PGD
0.1	1.510613	1.121487	1.223872	1.513761	1.517611	1.123785	1.236382	1.534755
0.2	1.508010	1.121527	1.140600	1.468598	1.582042	1.123365	1.171341	1.566335
0.5	1.277997	1.121636	1.221769	1.646010	1.575610	1.122185	1.319650	2.164850
0.8	1.520606	1.031109	1.062509	1.520017	2.553312	1.029960	1.143569	2.482308
1.0	1.146857	1.109705	1.206056	1.617474	2.340146	1.108166	1.388278	2.982269
1.1	1.458215	1.031218	1.139865	1.580210	3.158410	1.029011	1.291160	3.105877
1.4	1.254450	1.121870	1.279377	1.603026	3.444848	1.119346	1.567613	3.878579
1.7	1.562587	1.124703	1.360767	1.563201	4.917432	1.121440	1.695858	4.451830
2.0	1.424730	1.160261	1.351300	1.744564	5.372514	1.156977	1.569844	5.602715
2.3	1.538028	1.122384	1.544590	1.869615	6.512692	1.117764	1.955341	6.778334
2.6	1.679046	1.125183	1.597183	2.076902	7.816463	1.120118	1.830526	7.618081
2.9	1.834858	1.032794	1.741633	2.342456	9.272282	1.026461	1.961652	9.940795
3.0	2.105044	1.032966	1.791616	2.264387	10.693936	1.026504	2.031071	9.321798

5.3 *Observations*

This study investigates undefended and defended AI-powered channel estimation models in NextG networks in terms of their vulnerabilities against adversarial attacks, i.e., FGSM, MIM, BIM, and PGD. Defensive distillation, as the migration method, is applied to the defended models. The overall results show that AI-powered models are vulnerable to adversarial attacks, and models' vulnerabilities can be significantly reduced for some types of attacks, i.e., to be improved the models' robustness. Observations can be given as follows:

1: AI-powered channel estimation models are vulnerable to adversarial attacks, espe-

cially, under a high attack power ($\epsilon > 0.5$) for BIM and PDG.
2: The attack power (ϵ) has no impact on some adversarial attacks, i.e., FGSM and MIM.
3: The selected mitigation method can significantly increase the model robustness, especially for BIM and PGD.
4: The strongest attack is BIM, while the weakest is FGSM for undefended models.
5: The strongest attack is PDG, while the weakest is FGSM for defended models.

6 Security and Privacy Concerns

6.1 Homomorphic Encryption

Homomorphic encryption is a cryptosystem that enables computation on ciphertexts, producing an encrypted result that, when decrypted, matches the result of the operations as if they had been performed on the plaintext. The definition of homomorphic encryption (HE) scheme is given in [33] as follows:

Definition 6.1 A homomorphic encryption scheme consists of a randomized polynomial-time algorithm, $\mathcal{E}$, which takes as input a security parameter λ and a message $m \in M$ and outputs a ciphertext $c = \mathcal{E}(1^{\lambda}, m)$. The ciphertext space C is a polynomial-time deterministic function of λ. There is a randomized polynomial-time algorithm $\mathcal{D}$, which takes as input a security parameter λ and a ciphertext $c \in C$, and outputs a message $m \in M$, such that $m = \mathcal{D}(1^{\lambda}, c)$, with probability at least $1 - \epsilon(\lambda)$.

There are several homomorphic encryption schemes proposed in the literature, such as Paillier cryptosystem [34], ElGamal encryption scheme [35], Goldwasser-Micali (GM) scheme [36], Boneh-Goh-Nissim (BGN) scheme [37], and Paillier-HOM scheme [33]. Among these schemes, Paillier, ElGamal, and GM schemes are additive homomorphic and can support only simple operations on ciphertexts. On the other hand, BGN and Paillier-HOM are multiplicative homomorphic and can support more complex computations on ciphertexts.

A homomorphic encryption scheme is a pair of algorithms, Enc and Dec, with the following properties:

(i) A polynomial-time randomized algorithm Enc which takes as input a security parameter $\lambda \in \mathbb{N}$ and a message $m \in M$ and outputs a ciphertext $c = \mathsf{Enc}(\lambda, m)$ such that $c \in C$.
(ii) A polynomial-time randomized algorithm Dec which takes as input a security parameter $\lambda \in \mathbb{N}$ and a ciphertext $c \in C$ and outputs a message $m \in M$ such that $m = \mathsf{Dec}(\lambda, c)$ with probability at least $1 - \epsilon(\lambda)$.

Additively homomorphic and multiplicatively homomorphic are the most common encryption types.

Table 3 Computational cost and security of various HE schemes

Additively homomorphic schemes				
Scheme	Security	Runtime	Key	Ciphertext
Paillier [34]	IND-CPA	$O(n^6)$	$O(n^2)$	$O(n^2)$
ElGamal [35]	IND-CPA	$O(n^3)$	$O(n^2)$	$O(n^2)$
GM [36]	SEM-IND-CPA	$O(n^3)$	$O(n^2)$	$O(n^2)$
Multiplicatively homomorphic schemes				
Scheme	Security	Runtime	Key	Ciphertext
BGN [37]	IND-CPA	$O(n^4)$	$O(n^3)$	$O(n^3)$
Paillier-HOM [33]	IND-CPA	$O(n^6)$	$O(n^2)$	$O(n^2)$

Definition 6.2 Homomorphic encryption $\mathcal{E}$ is additively homomorphic if

(i) $\mathcal{E}(1^\lambda, m_1 + m_2) = \mathcal{E}(1^\lambda, m_1) + \mathcal{E}(1^\lambda, m_2)$
(ii) $\mathcal{E}(1^\lambda, m) = \mathcal{E}(1^\lambda, -m)$

Definition 6.3 Homomorphic encryption $\mathcal{E}$ is multiplicatively homomorphic if

(i) $\mathcal{E}(1^\lambda, m_1 m_2) = \mathcal{E}(1^\lambda, m_1) \times \mathcal{E}(1^\lambda, m_2)$
(ii) $\mathcal{E}(1^\lambda, m) = \mathcal{E}(1^\lambda, 1/m)$

Homomorphic encryption has several applications in distributed systems, cloud computing, data mining, and database security. In these applications, the data is stored in the cloud, and the data owner wants to keep its data private. The data owner can encrypt the data and store it in the cloud. The cloud user can perform computations on the encrypted data, and the result will also be encrypted. The data owner can decrypt the result and get the required information (Table 3).

6.2 *Security of Homomorphic Encryption*

Many HE schemes have been proposed in the literature in the past decade. The security of these schemes is analyzed under different security models. The security of HE schemes can be categorized under three different security models:

(i) **Partial homomorphic encryption**
With partial homomorphic encryption, the user can perform only limited operations on the ciphertext. In [38], Rivest et al. proposed a scheme that can support only a limited number of multiplications in the ciphertext. In this scheme, a ciphertext can be decrypted only if all the multiplications in the ciphertext are performed.

(ii) **Limited homomorphic encryption**
With limited homomorphic encryption, a ciphertext can be decrypted after any

number of operations are performed on the ciphertext. However, the number of operations that can be performed on the ciphertext is limited.

(iii) **Fully homomorphic encryption**
With fully homomorphic encryption, a ciphertext can be decrypted after any number of operations are performed on the ciphertext. In [33], Gentry, Sahai, and Waters proposed a scheme that supports both multiplications and addition in the ciphertext. In this scheme, a ciphertext can be decrypted after any number of multiplications and divisions are performed in the ciphertext. In [39], Brakerski and Vaikuntanathan proposed a scheme that supports only a limited number of multiplications in the ciphertext. In this scheme, a ciphertext can be decrypted after any number of multiplications are performed in the ciphertext.

The global model w_t can be trained on the aggregated dataset $\cup_{i=1}^{m} D_i$ using any machine learning algorithm.

6.3 Federated Learning

In this section, we briefly describe the federated learning (FL) framework. We refer to [40, 41] for more details.

Definition 6.4 (FL model) A federated learning (FL) model is a tuple $M = (\{M_i\}_{i=1}^{N}, \{w_i\}_{i=1}^{N}, \{D_i\}_{i=1}^{N}, w, \{R_i\}_{i=1}^{N})$, where

1. M_i is the model trained on the local dataset D_i at client i,
2. w_i is the weight of client i,
3. D_i and D are the local and global datasets, respectively,
4. w is the global model trained on the global dataset D,
5. R_i is the loss of client i on the global dataset D.

In the FL framework, the global model w is trained by optimizing the following objective:

$$\min_{w} \frac{1}{N} \sum_{i=1}^{N} w_i R_i(w, D_i). \tag{7}$$

The objective function (7) is minimized by training individual models M_i on local datasets and aggregating the models by averaging the weights. FL is an iterative approach to finding the best global model w. In each iteration, the client trains the individual model M_i on the local dataset D_i and sends the weights w_i to the central server. The server aggregates the weights and updates the global model w. The process is repeated until the global model converges. The FL framework has several advantages compared to traditional learning approaches, including improved privacy and security and lower communication and computational costs.

7 Summary

The NextG projects have been initiated to support a wide range of diverse applications, from AR/VR, metaverse, mobile healthcare, autonomous cars to digital twins and many more, by both the academia and the industry integrated with advanced cloud communication and data, computing, AI technologies in recent years. It has no doubt that AI is the most important tool in terms of significant contribution to all layers in NextG, i.e., from the physical to the application layer. On the other hand, the security and privacy concerns for NextG applications using AI-enabled solutions have not been fully addressed due to its complexity and multidisciplinary. This book chapter focuses on the AI-enabled applications on the physical layer of NextG networks, including beamforming, channel estimation, spectrum sensing, and IRS, and intends to investigate the vulnerability of AI-enabled channel estimation models under the selected adversarial attacks, such as FGSM, MIM, BIM, and PGD, with and without the selected mitigation (defensive distillation). According to the results, the AI-enabled channel estimation model is vulnerable to adversarial attacks. On the other hand, mitigation methods can significantly improve the performance and robustness of AI-enabled models under adversarial attacks.

References

1. Agiwal M, Roy A, Saxena N (2016) Next generation 5G wireless networks: a comprehensive survey. IEEE Commun Surv Tutorials 18(3):1617–1655. https://doi.org/10.1109/COMST.2016.2532458
2. Ziegler V, Yrjola S (2020) 6G indicators of value and performance. In: 2020 2nd 6G wireless summit (6G SUMMIT), pp 1–5. https://doi.org/10.1109/6GSUMMIT49458.2020.9083885
3. Johansson NA, Wang Y-PE, Eriksson E, Hessler M (2015) Radio access for ultra-reliable and low-latency 5G communications. In: IEEE international conference on communication workshop (ICCW), pp 1184–1189. https://doi.org/10.1109/ICCW.2015.7247338
4. Letaief KB, Chen W, Shi Y, Zhang J, Zhang Y-JA (2019) The roadmap to 6G: AI empowered wireless networks. IEEE Commun Mag 57(8):84–90. https://doi.org/10.1109/MCOM.2019.1900271
5. Kaur J, Khan MA, Iftikhar M, Imran M, Haq QEU (2021) Machine learning techniques for 5G and beyond. IEEE Access 9:23472–23488
6. Wilhelmi F, Carrascosa M, Cano C, Jonsson A, Ram V, Bellalta B (2021) Usage of network simulators in machine-learning-assisted 5G/6G networks. IEEE Wireless Commun 28(1):160–166
7. Khan S, Hussain A, Nazir S, Khan F, Oad A, Alshehri MD (2022) Efficient and reliable hybrid deep learning-enabled model for congestion control in 5G/6G networks. Comput Commun 182:31–40
8. Piran MJ, Suh DY (2019) Learning-driven wireless communications, towards 6G. In: 2019 international conference on computing, electronics & communications engineering (ICCECE). IEEE, pp 219–224
9. Morocho Cayamcela ME, Lim W (2018) Artificial intelligence in 5G technology: a survey. In: 2018 international conference on information and communication technology convergence (ICTC), pp 860–865. https://doi.org/10.1109/ICTC.2018.8539642

10. Ozpoyraz B, Dogukan AT, Gevez Y, Altun U, Basar E (2022) Deep learning-aided 6G wireless networks: a comprehensive survey of revolutionary PHY architectures. arXiv:2201.03866
11. Dang S, Amin O, Shihada B, Alouini M-S (2020) What should 6G be? Nat Electron 3(1):20–29
12. Kuzlu M, Fair C, Guler O (2021) Role of artificial intelligence in the internet of things (IoT) cybersecurity. Discov Internet Things 1(1):1–14
13. Porambage P, Gür G, Osorio DPM, Liyanage M, Ylianttila M (2021) 6G security challenges and potential solutions. In: Proceedings of IEEE joint European conference on networks and communications (EuCNC) 6G Summit, pp 1–6
14. Siriwardhana Y, Porambage P, Liyanage M, Ylianttila M (2021) AI and 6G security: opportunities and challenges. In: Proceedings of IEEE joint European conference on networks and communications (EuCNC) 6G Summit, pp 1–6
15. Catak FO, Kuzlu M, Catak E, Cali U, Unal D (2022) Security concerns on machine learning solutions for 6G networks in mmwave beam prediction. Phys Commun 52:101626. https://doi.org/10.1016/j.phycom.2022.101626
16. Catak E, Catak FO, Moldsvor A (2021) Adversarial machine learning security problems for 6G: mmwave beam prediction use-case. In: IEEE international Black Sea conference on communications and networking (BlackSeaCom), pp 1–6. https://doi.org/10.1109/BlackSeaCom52164.2021.9527756
17. Li G, Ota K, Dong M, Wu J, Li J (2020) Desvig: decentralized swift vigilance against adversarial attacks in industrial artificial intelligence systems. IEEE Trans Ind Inf 16(5):3267–3277. https://doi.org/10.1109/TII.2019.2951766
18. Yastrebova A, Kirichek R, Koucheryavy Y, Borodin A, Koucheryavy A (2018) Future networks 2030: architecture & requirements. In: 10th international congress on ultra modern telecommunications and control systems and workshops (ICUMT). IEEE, pp 1–8
19. Liu G, Huang Y, Li N, Dong J, Jin J, Wang Q, Li N (2020) Vision, requirements and network architecture of 6G mobile network beyond 2030. China Commun 17(9):92–104. https://doi.org/10.23919/JCC.2020.09.008
20. Faruk Tuna O, Ozgur Catak F, Taner Eskil M (2021) Exploiting epistemic uncertainty of the deep learning models to generate adversarial samples, arXiv e-prints arXiv:2102.04150
21. Vardhan R (2021) An ensemble approach for explanation-based adversarial detection, Ph.D. thesis
22. Fostiropoulos I, Shbita B, Marmarelis M. Robust defense against L p-norm-based attacks by learning robust representations
23. Papernot N, McDaniel P, Wu X, Jha S, Swami A (2016) Distillation as a defense to adversarial perturbations against deep neural networks. arXiv:1511.04508
24. Ma J, Li GY, Juang BH (2009) Signal processing in cognitive radio. Proc IEEE 97(5):805–823
25. Develi I et al (2020) Spectrum sensing in cognitive radio networks: threshold optimization and analysis. EURASIP J Wireless Commun Netw 2020(1):1–19
26. Mitola J, Maguire GQ (1999) Cognitive radio: making software radios more personal. IEEE Personal Commun 6(4):13–18
27. Yucek T, Arslan H (2009) A survey of spectrum sensing algorithms for cognitive radio applications. IEEE Commun Surv Tutorials 11(1):116–130
28. Zeng Y, Liang Y-C, Hoang AT, Zhang R (2010) A review on spectrum sensing for cognitive radio: challenges and solutions. EURASIP J Adv Signal Process 1–15
29. Sarp S, Tang H, Zhao Y (2021) Use of intelligent reflecting surfaces for and against wireless communication security. In: IEEE 4th 5G World Forum (5GWF). IEEE, pp 374–377
30. Rusek F, Persson D, Lau BK, Larsson EG, Marzetta TL, Edfors O, Tufvesson F (2012) Scaling up mimo: opportunities and challenges with very large arrays. IEEE Signal Process Mag 30(1):40–60
31. 5G Simularion Software, Network Simulation Tools. https://se.mathworks.com/products/5g.html
32. Matlab 5G Toolbox. https://www.mathworks.com/products/5g.html. Accessed 30 Sept 2021

33. Gentry C (2009) Fully homomorphic encryption using ideal lattices. In: Proceedings of the forty-first annual ACM symposium on theory of computing, STOC ’09, Association for Computing Machinery, New York, NY, USA, 2009, pp 169–178. https://doi.org/10.1145/1536414.1536440
34. Paillier P (1999) Public-key cryptosystems based on composite degree residuosity classes. In: Stern J (ed) Advances in cryptology—EUROCRYPT ’99. Springer, Heidelberg, pp 223–238
35. Elgamal T (1985) A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE Trans Inf Theor 31(4):469–472. https://doi.org/10.1109/TIT.1985.1057074
36. Goldwasser S, Micali S (1982) Probabilistic encryption amp; how to play mental poker keeping secret all partial information. In: Proceedings of the fourteenth annual ACM symposium on theory of computing, STOC ’82, Association for Computing Machinery, New York, NY, USA, 1982, pp 365–377. https://doi.org/10.1145/800070.802212
37. Boneh D, DeMillo RA, Lipton RJ (1997) On the importance of checking cryptographic protocols for faults. In: Fumy W (ed) Advances in cryptology—EUROCRYPT ’97. Springer, Heidelberg, pp 37–51
38. Rivest RL, Dertouzos ML (1978) On data banks and privacy homomorphisms
39. Brakerski Z, Vaikuntanathan V (2011) Fully homomorphic encryption from ring-LWE and security for key dependent messages. In: Rogaway P (ed) Advances in cryptology—CRYPTO 2011. Springer, Heidelberg, pp 505–524
40. McMahan HB, Moore E, Ramage D, Hampson S, Arcas BA (2047) Communication-efficient learning of deep networks from decentralized data. In: International conference on artificial intelligence and statistics
41. Konečný J, McMahan HB, Yu FX, Richtarik P, Suresh AT, Bacon D (2016) Federated learning: strategies for improving communication efficiency. In: NIPS workshop on private multi-party machine learning. arXiv:1610.05492

A Blockchain-Enabled Approach for Secure Data Sharing in 6G-based Internet of Things Networks

Hussein El Ghor and Bilal Nakhal

Abstract The 6th generation of wireless networks (6G) promises to provide ultra-reliable, high-speed, and low-latency communication for Internet of Things (IoT) devices. However, securing data transmission and storage in these networks is a critical challenge due to potential security threats. Blockchain technology provides a solution to enhance security in IoT networks by enabling secure, decentralized, and tamper-proof data sharing. In this paper, we proposed a novel solution for securing data sharing and storage in 6G-based IoT networks using blockchain technology, hybrid encryption, and IPFS. The proposed approach consists of four algorithms that enhance the security of the system: a user authentication algorithm, a data access algorithm, a data storage algorithm, and a secure data sharing algorithm. The secure data sharing algorithm enables secure, tamper-proof data sharing among authorized devices using a permissioned blockchain. These algorithms are implemented using hybrid encryption, which ensures data confidentiality, and have been evaluated for their effectiveness in enhancing security in 6G-based IoT networks. Our work contributes to the growing body of research on blockchain-enabled solutions for securing data in IoT networks and provides insights into the potential of blockchain technology, hybrid encryption, and IPFS to enhance security in 6G-based IoT networks. The proposed approach using these algorithms provides secure and tamper-proof data sharing, making the system more secure and reliable. We presented the technical details of our approach and evaluate its effectiveness in terms of security, with a particular focus on the role of hybrid encryption and IPFS in enhancing the security and reliability of the system. Our results demonstrate that the proposed approach enhances data security in 6G-based IoT networks by providing secure and tamper-proof data sharing. The use of hybrid encryption and IPFS makes the system more secure and reliable, with hybrid encryption ensuring data confidentiality and IPFS providing decentralized and fault-tolerant storage.

H. El Ghor (✉) · B. Nakhal
CyberVision Lab, Department of Mathematics and Computer Science,
Beirut Arab University, Beirut, Lebanon
e-mail: h.elghor@bau.edu.lb

B. Nakhal
e-mail: b.nakhal@bau.edu.lb

H. Jahankhani and A. El Hajjar (eds.), *Wireless Networks*, Advanced Sciences
and Technologies for Security Applications,
https://doi.org/10.1007/978-3-031-33631-7_8

1 Introduction

The emergence of the Internet of Things (IoT) has led to the proliferation of connected devices and generated massive amounts of data [1]. IoT has become a key component of our daily lives, with billions of interconnected devices generating and transmitting data across the network. With the advent of the 6th generation of wireless networks (6G), IoT devices are expected to transmit and process data with ultra-reliable, high-speed, and low-latency communication. The 6th Generation (6G) of mobile communication technology is currently under development and is expected to provide a new level of connectivity to the Internet of Things (IoT) devices. 6G-based IoT networks are characterized by ultra-low latency, high bandwidth, and massive device connectivity, which will enable new applications and services that are not possible with the current 5G networks.

The architecture of 6G-based IoT networks is expected to be based on a distributed and decentralized architecture, which will enable devices to communicate with each other directly, without the need for central servers. This architecture will enable new use cases such as peer-to-peer communication, real-time collaboration, and edge computing.

Currently, data sharing in IoT networks is done using centralized approaches, where data is collected and processed by central servers. This approach has several limitations, including high latency, lack of scalability, and vulnerability to cyber-attacks. Additionally, centralized approaches are not suitable for applications that require real-time data processing, such as autonomous driving and remote surgery.

However, the distributed and decentralized architecture of 6G-based IoT networks also poses several challenges related to security and privacy. One of the key challenges is how to enable secure data sharing among the devices in the network. Data sharing is essential in IoT networks for enabling applications such as smart homes, smart cities, and smart transportation.

To overcome these limitations, new approaches for data sharing in 6G-based IoT networks are needed. One promising approach is the use of blockchain technology, which provides a decentralized and secure way of storing and sharing data. Blockchain technology enables data to be shared directly between devices, without the need for central servers, while ensuring the integrity and confidentiality of the data.

In summary, 6G-based IoT networks offer new opportunities for connectivity and innovation, but also pose several challenges related to security and privacy. Centralized approaches to data sharing are not suitable for these networks, and new approaches such as blockchain technology are needed to enable secure and efficient data sharing.

Additionally, the rapid growth of IoT networks has also created significant security challenges, particularly when it comes to data sharing between devices [2]. Hence, securing data transmission and storage in these networks is a critical challenge due to potential security threats, such as unauthorized access, data breaches, and data tampering [3, 4]. One possible solution to this problem is the use of blockchain technology, which has the potential to enable secure and trusted data sharing in IoT networks [5].

Blockchain technology has gained significant attention in recent years as a potential solution to enhance security in IoT networks. By enabling secure, decentralized, and tamper-proof data sharing, blockchain technology offers a promising approach to address the security challenges associated with IoT networks [6]. It provides a tamper-proof record of all transactions, making it an ideal platform for secure data sharing in IoT networks [7]. Additionally, blockchain can help to address some of the key challenges facing IoT networks, such as data privacy, security, and authenticity [8].

One of the promising tools that can be used with blockchain for secure data sharing is the InterPlanetary File System (IPFS). IPFS is a peer-to-peer network that allows users to store and share files in a decentralized manner [9]. By using IPFS with blockchain, users can store and access data in a secure and distributed manner, without relying on centralized servers. In this paper, we propose a blockchain-enabled approach for secure data sharing in 6G-based IoT networks, leveraging hybrid encryption and IPFS as decentralized storage.

Secure data sharing is crucial in IoT networks because it allows authorized devices to access and share data securely and efficiently [10]. The proposed solution aims to enhance data security in 6G-based IoT networks by providing secure and tamper-proof data sharing through the use of blockchain technology, hybrid encryption, and IPFS. The permissioned blockchain ensures that only authorized devices can participate in the network and access data [11]. Hybrid encryption ensures data confidentiality, while IPFS provides decentralized and fault-tolerant storage [12].

This paper aims to propose a novel solution for securing data sharing and storage in 6G-based IoT networks using blockchain technology, hybrid encryption, and IPFS. The paper's contributions include the proposal of four algorithms that enhance the security of the system: a user authentication algorithm, a data access algorithm, a data storage algorithm, and a secure data sharing algorithm.

The user authentication algorithm ensures that only authorized devices can participate in the network and share data securely. The data access algorithm ensures that authorized devices can access only the data they are authorized to access. The data storage algorithm provides a decentralized and fault-tolerant storage solution using IPFS. The secure data sharing algorithm enables secure, tamper-proof data sharing among authorized devices using a permissioned blockchain.

The paper highlights the use of hybrid encryption to ensure data confidentiality and IPFS to provide decentralized and fault-tolerant storage. The effectiveness of the proposed approach in terms of security has been evaluated, and the results demonstrate that the proposed approach enhances data security in 6G-based IoT networks by providing secure and tamper-proof data sharing.

Overall, the paper's contributions are in the area of enhancing security in 6G-based IoT networks using blockchain technology, hybrid encryption, and IPFS. The proposed algorithms aim to address the critical challenge of securing data transmission and storage in these networks and provide a more secure and reliable solution.

The remainder of this paper is organized as follows. In Sect. 2, we provide a literature review of blockchain-based approaches for securing data sharing in IoT networks. In Sect. 3, we present the design methodology of our proposed solution. In Sect. 4, we evaluate the effectiveness of our proposed approach in terms of security. Finally, we conclude the paper in Sect. 5 and highlight potential future work.

2 Related Work

Blockchain technology has been widely explored for secure data sharing in 6G-based IoT networks. In recent years, there has been growing interest in the use of blockchain technology for secure data sharing in IoT networks. Researchers have proposed various approaches to leverage the benefits of blockchain technology, such as decentralization, immutability, and transparency, for secure data sharing in IoT networks. In this section, we provide an overview of some recent papers that are related to our proposed approach for secure data sharing in 6G-based IoT networks using blockchain and IPFS and highlight the advantages and limitations of each approach.

Lu et al. [13] proposed a secure data sharing platform using blockchain and IPFS for Industry 4.0. Their approach uses blockchain to maintain an immutable and transparent record of transactions, and IPFS to store and share data in a decentralized manner. The authors evaluated their approach in a case study involving a smart factory, and demonstrated its effectiveness in terms of security, privacy, and efficiency.

Zhang et al. [14] proposed a blockchain-enabled efficient distributed attribute-based access control (ABAC) for healthcare IoT. Their approach uses blockchain to maintain a trusted and decentralized access control policy, and enables secure and efficient data sharing among different healthcare organizations. The authors evaluated their approach using a real-world dataset, and demonstrated its effectiveness in terms of security, efficiency, and scalability.

Feng et al. [15] proposed an efficient and secure data sharing approach for 5G flying drones using blockchain. Their approach uses blockchain to maintain a secure and decentralized record of transactions, and enables efficient data sharing among different drones. The authors evaluated their approach using a real-world dataset, and demonstrated its effectiveness in terms of security, efficiency, and scalability.

Eltayeb et al. [16] proposed a blockchain platform for user data sharing, ensuring user control and ownership. Their approach uses blockchain to maintain a decentralized and transparent record of transactions, and enables users to control and own their data. The authors evaluated their approach using a real-world dataset, and demonstrated its effectiveness in terms of security, privacy, and transparency.

Al-Fuqaha et al. [17] proposed a blockchain-enabled K-harmonic framework for industrial IoT data sharing. Their approach uses blockchain to maintain a secure and decentralized record of transactions, and enables secure and efficient data sharing among different industrial IoT devices. The authors evaluated their approach using a

Table 1 Comparison of the previous work

References	Paper title	Main topic	Key contributions	Advantages	Disadvantages
[13]	A Secure and Efficient Data Sharing Platform for Industry 4.0 Using Blockchain and IPFS	Secure data sharing in Industry 4.0	Blockchain and IPFS for secure and efficient data sharing	High security and efficiency	No evaluation of scalability
[14]	Blockchain-Enabled Efficient Distributed Attribute-Based Access Control for Healthcare IoT	Secure data sharing in healthcare IoT	Blockchain for trusted and decentralized access control policy	High security, efficiency, and scalability	No real-world deployment
[15]	Efficient and Secure Data Sharing for 5G Flying Drones: A Blockchain-Enabled Approach	Secure data sharing among flying drones	Blockchain for secure and decentralized record of transactions	High security, efficiency, and scalability	Limited to flying drones
[16]	A Blockchain Platform for User Data Sharing, Ensuring User Control and Ownership	Secure and decentralized user data sharing	Blockchain for decentralized and transparent record of transactions	High security, privacy, and transparency	Limited to user data sharing
[17]	Blockchain-Enabled K-Harmonic Framework for Industrial IoT Data Sharing	Secure data sharing in industrial IoT	Blockchain for secure and decentralized data sharing	High security, efficiency, and scalability	No evaluation of real-world dataset

real-world dataset, and demonstrated its effectiveness in terms of security, efficiency, and scalability.

Table 1 compares the previous works mentioned earlier, outlining details such as the title of the paper, authors, main subject matter, notable contributions, as well as the strengths and weaknesses of each.

All the above references propose blockchain-enabled approaches for secure data sharing in IoT networks. They all use blockchain to maintain an immutable and transparent record of transactions and enable secure and efficient data sharing among different IoT devices. However, each approach focuses on a different IoT context and proposes unique key contributions.

Advantages of these approaches include high security, efficiency, and scalability. However, some of these approaches have limitations, such as being limited to a specific IoT context or lacking evaluation of certain criteria

In summary, these papers provide valuable insights into the potential of blockchain technology for secure data sharing in various IoT contexts, and demonstrate the effectiveness of blockchain-enabled approaches in addressing key security and privacy challenges in IoT networks.

3 Design Methodology

3.1 Data Requester (User) Authentication

The User Authentication Model Design Framework is a set of principles and guidelines for creating secure and reliable user authentication systems. The model is intended to be used by designers, developers, and security professionals to create effective authentication solutions for their applications.

The User Authentication Model is designed to be flexible and adaptable, allowing 6G based iot devices to implement user authentication solutions that meet their specific needs and requirements. The framework includes several key components, including user authentication methods, security controls, and risk management processes.

The authentication model involves five main components: data requester (user), IoT devices, blockchain network, IPFS network, and smart contract.

- Users: The user is the data requester or entity who is trying to access the system and needs to be authenticated. They provide their login credentials, which are encrypted and sent to the IoT device for further processing.
- IoT Device: The IoT device is responsible for encrypting the user's login credentials using AES and then encrypting the symmetrical key K using the user's public key (K_p). It also stores this hybrid encrypted credentials on the IPFS network and creates a user authentication request containing the IPFS address, hybrid encrypted credentials, and metadata. Finally, it sends the authentication request to the blockchain network.
- Blockchain: The blockchain network is used to store and share the user authentication request with other nodes on the network. It also deploys a smart contract to handle user authentication and receives the user's authentication request, which is then sent to the smart contract.

- Smart Contract: The smart contract is deployed on the blockchain network and receives the user's authentication request. It retrieves the hybrid encrypted credentials from the IPFS network and decrypts them using the user's private key (K_r). The smart contract then verifies the user's credentials and generates a signed authentication token if the credentials are valid. If the credentials are not valid, the smart contract rejects the authentication request.
- IPFS: IPFS is used to store the encrypted encrypted credentials generated by the IoT device. The IPFS network stores the encrypted credentials at a specific IPFS address, which is included in the user authentication request sent to the blockchain network.

In summary, this algorithm uses a combination of encryption, blockchain, IPFS, and smart contracts to securely authenticate users and grant them access to the system.

The proposed authentication model is as follows (Fig. 1):

① The user enters their login credentials ($login\_credentials = enter\_login\_credentials()$). The user's credentials are now encrypted using AES by the function $encrypted\_credentials = encrypt\_with\_aes(login\_credentials)$. The encrypted credentials are then sent to the IoT device ($send\_to\_iot\_device(encrypted\_credentials)$)

② The IoT device encrypts the encrypted credentials using the user's public key (K_p) by the function $hybrid\_encrypted\_credentials = encrypt\_with\_rsa(K_p, encrypted\_credentials)$. The hybrid encrypted credentials are stored on the IPFS network ($ipfs\_address = store\_on\_ipfs(hybrid\_encrypted\_credentials)$)

③ The $ipfs\_address$ is returned to the IOT device.

④ The IoT device creates a user authentication request containing the IPFS address, the hybrid encrypted credentials, and metadata by using the function $user\_auth\_request = create\_user\_auth\_request(ipfs\_address, hybrid\_encrypted\_credentials, metadata)$. The user authentication request is now shared with the blockchain network thanks to the function $share\_with\_blockchain(user\_auth\_request)$.

⑤ A smart contract is deployed on the blockchain network to handle user authentication $deploy\_smart\_contract()$ and the user's authentication request is sent to the smart contract $send\_to\_smart\_contract(user\_auth\_request)$.

⑥ The smart contract retrieves the hybrid encrypted credentials from the IPFS network using the provided address $retrieved\_encrypted\_credentials = retrieve\_from\_ipfs(ipfs\_address)$.

⑦ The smart contract decrypts the encrypted credentials using the user's private key (K_r) $decrypted\_credentials = decrypt\_with\_rsa(K_r, retrieved\_encrypted\_credentials)$ to verify the user's credentials. if $verify\_credentials(decrypted\_credentials)$.

If the user's credentials are valid, the smart contract generates a signed authentication token (T) granting access to the user $auth\_token = generate\_auth\_token(decrypted\_credentials)$. The signed authentication token (T) is broadcasted to the blockchain network $broadcast\_auth\_token(auth\_token)$.

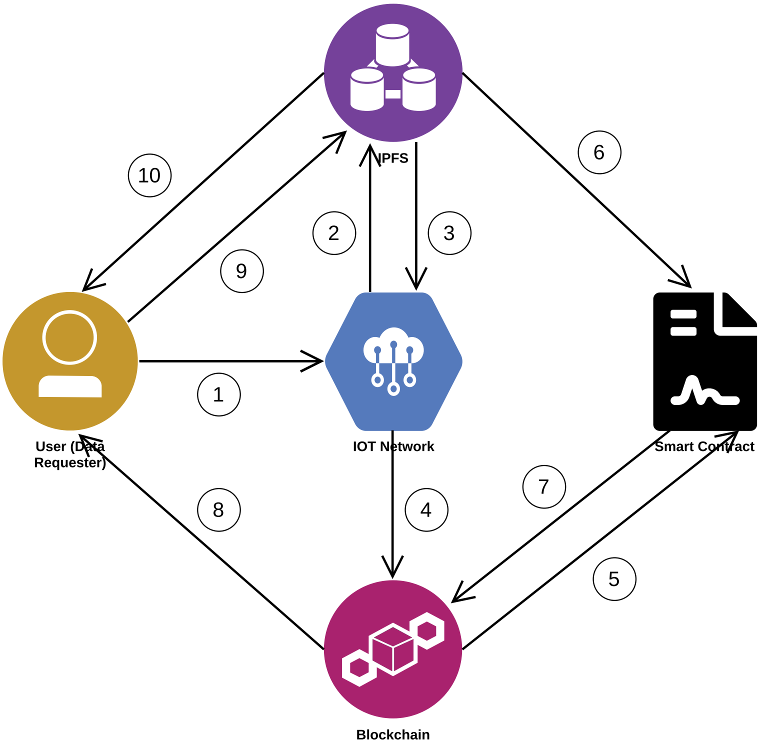


Fig. 1 Authentication model design framework

⑧ The user receives a notification that his authentication was successful and can now access the system $notify\_user\_success()$.
⑨ User accesses the IPFS to verify the token T.
⑩ IPFS returns the requested data.
⑪ If the user's credentials are not valid, the smart contract rejects the authentication request $reject\_auth\_request()$. The user receives a notification that their authentication was unsuccessful and cannot access the system $notify\_user\_failure()$

The overall process for user authentication is stated in Algorithm 1.

3.2 *Data Access Model*

In the proposed blockchain-enabled approach for secure data sharing in 6G-based IoT networks, users can access data based on their permissions defined in the smart contracts on the blockchain (refer to Algorithm 1). Each smart contract defines the access control policy for a specific set of data, where the policy can specify the

Algorithm 1 User authentication

```
$login\_credentials = enter\_login\_credentials()$ {The user enters their login credentials}
$encrypted\_credentials = encrypt\_with\_aes(login\_credentials)$ {The user's credentials are encrypted using AES}
$send\_to\_iot\_device(encrypted\_credentials)$ {The encrypted credentials are sent to the IoT device}
$hybrid\_encrypted\_credentials = encrypt\_with\_rsa(K_p, encrypted\_credentials)$ {The IoT device encrypts the encrypted credentials using the user's public key ($K_p$)}
$ipfs\_address = store\_on\_ipfs(hybrid\_encrypted\_credentials)$ {The hybrid encrypted credentials are stored on the IPFS network}
$user\_auth\_request = create\_user\_auth\_request(ipfs\_address, hybrid\_encrypted\_credentials, metadata)$ {The IoT device creates a user authentication request containing the IPFS address, the hybrid encrypted credentials, and metadata}
$share\_with\_blockchain(user\_auth\_request)$ {The user authentication request is shared with the blockchain network}
$deploy\_smart\_contract()$ {A smart contract is deployed on the blockchain network to handle user authentication}
$send\_to\_smart\_contract(user\_auth\_request)$ {The user's authentication request is sent to the smart contract}
$send\_to\_smart\_contract(user\_auth\_request)$ {The user's authentication request is sent to the smart contract}
$retrieved\_encrypted\_credentials = retrieve\_from\_ipfs(ipfs\_address)$ {The smart contract retrieves the hybrid encrypted credentials from the IPFS network using the provided address}
$decrypted\_credentials = decrypt\_with\_rsa(K_r, retrieved\_encrypted\_credentials)$ {The smart contract decrypts the hybrid encrypted credentials using the user's private key ($K_r$)}
$verify\_credentials(decrypted\_credentials)$ {The smart contract verifies the user's credentials}
if $valid\_credentials()$ then
    $auth\_token = generate\_auth\_token(decrypted\_credentials)$ {the smart contract generates a signed authentication token ($T$) granting access to the user}
    $broadcast\_auth\_token(auth\_token)$ {The signed authentication token ($T$) is broadcasted to the blockchain network}
    $notify\_user\_success()$ {The user receives a notification that their authentication was successful and can now access the system}
else
    $reject\_auth\_request()$ {If the user's credentials are not valid, the smart contract rejects the authentication request}
    $notify\_user\_failure()$ {The user receives a notification that their authentication was unsuccessful and cannot access the system}
end if
```

authorized users, their roles, and the level of access they have. The smart contract verifies the user's identity and permissions and grants or denies access accordingly.

In our design, the IoT devices generate and collect data (D) and generate a symmetric key (K) for hybrid encryption. The symmetric key is then encrypted using the recipient's public key (K_p) and stored in IPFS network. The data is encrypted and stored in IPFS network along with its corresponding metadata. The hash of the data is computed using a hash function (H) and added to the blockchain network as a transaction (T), along with the encrypted symmetric key (C_2) and the encrypted data (C_1). The transactions are grouped into blocks (B) and added to the blockchain (Fig. 2).

Below are the the detailed steps of the Data Access algorithm:
Step 1: Initialize 6G network, IPFS network, and Blockchain network. IoT devices will generate and collect data (D).
Step 2: IoT devices encrypt data (D) using hybrid encryption. This is done by the following steps:

- Generate a symmetric key (K) for AES encryption.
- Encrypt the data using AES encryption with the symmetric key (C_1=*AES_Encrypt* (D, K)).
- Generate public and private keys (K_p, K_r) for RSA encryption.
- Encrypt the AES symmetric key using RSA encryption with the public key K_p ($C_2 = RSA\_Encrypt(K, K_p)$).
- Store the ciphertext (C_1) and the encrypted symmetric key (C_2) in IPFS network along with their corresponding metadata.

Step 3: IoT devices compute the hash (H) of the data (D) using a hash function ($H = hash(D)$).
Step 4: IoT devices create a transaction (T) containing the encrypted data (C_1, C_2), its metadata, and the computed hash (H).
Step 5: IoT devices sign the transaction (T) with their private key (K_r) to ensure authenticity and integrity.
Step 6: IoT devices broadcast the signed transaction (T) to the blockchain network.
Step 7: Blockchain network verifies the authenticity and integrity of the transaction (T) using the corresponding public key (K_p).
Step 8: Blockchain network adds the transaction (T) to the next available block (B) in the blockchain.
Step 9: Repeat steps 1–8 as new data is generated and collected.
Step 10: User requests access to specific data in the IPFS network. Authorized users can access the data by performing the following steps:

- Retrieve the transaction T from the blockchain.
- Retrieve the corresponding ciphertext C_1 and encrypted symmetric key C_2 from IPFS network using the IPFS hash in the transaction metadata.
- Decrypt the symmetric key using RSA decryption with the private key ($K = RSA\_Decrypt(C_2, K_r)$).
- Decrypt the data using AES decryption with the symmetric key ($D = AES\_Decrypt(C_1, K)$).

Decrypted data (D) is now accessible to the user.

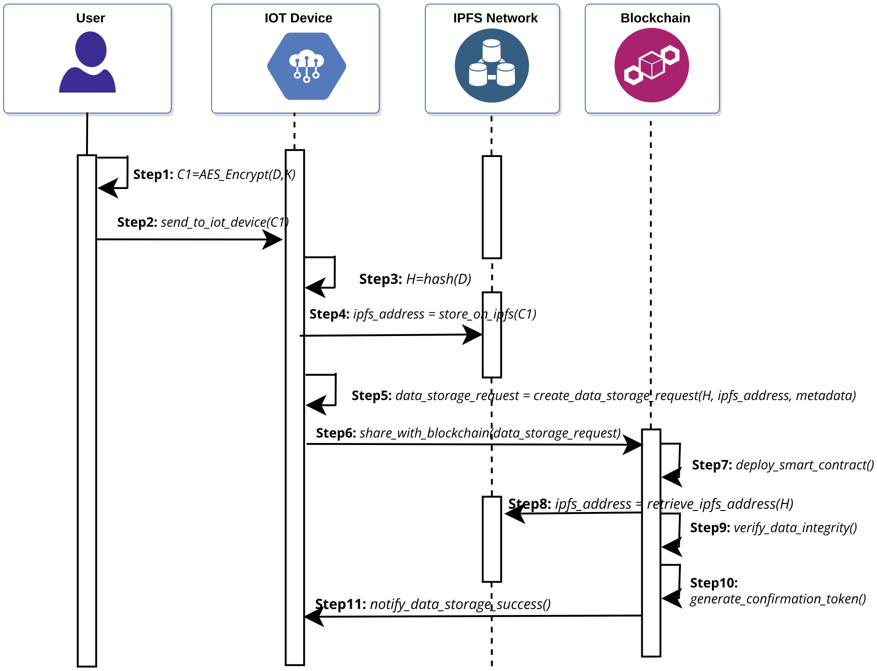

User
IOT Device
IPFS Network
Blockchain
Step1: *C1=AES_Encrypt(D,K)*
Step2: *send_to_iot_device(C1)*
Step3: *H=hash(D)*
Step4: *ipfs_address = store_on_ipfs(C1)*
Step5: *data_storage_request = create_data_storage_request(H, ipfs_address, metadata)*
Step6: *share_with_blockchain(data_storage_request)*
Step7: *deploy_smart_contract()*
Step8: *ipfs_address = retrieve_ipfs_address(H)*
Step9: *verify_data_integrity()*
Step10: *generate_confirmation_token()*
Step11: *notify_data_storage_success()*

Fig. 2 Data storage model

3.3 *Data Storage Model*

Once the user is authenticated, he/she can request data from the data storage. The data is stored in IPFS and the IPFS hash is stored on the blockchain network. When the user requests data, the data is retrieved from IPFS using the stored hash and sent back to the user. If the user wants to store new data, it is first stored in IPFS and then the IPFS hash is stored on the blockchain network.

Algorithm 2 outlines the steps involved in storing data in the data storage component. It includes hybrid encryption of data, generating a hash value, storing the encrypted data on the IPFS network, creating a data storage request, sharing the request with the blockchain network, deploying a smart contract to handle the request, verifying the integrity of the data, and generating a signed confirmation token if the data is valid. It also includes error handling steps to notify the IoT device in case of a failure in the data storage process.

Algorithm 2 Data Storage Algorithm

```
$C_1 = AES\_Encrypt(D, K)$ {The user encrypts the data using AES}
$send\_to\_iot\_device(C_1)$ {The encrypted data is sent to the IoT device}
$H = hash(D)$ {The IoT device generates a hash value of the data}
$ipfs\_address = store\_on\_ipfs(C_1)$ {The IoT device stores the encrypted data on the IPFS network and obtains an IPFS address}
$data\_storage\_request = create\_data\_storage\_request(H, ipfs\_address, metadata)$ {The IoT device creates a data storage request containing the hash value, IPFS address, and metadata}
$share\_with\_blockchain(data\_storage\_request)$ {The data storage request is shared with the blockchain network}
$deploy\_smart\_contract()$ {A smart contract is deployed on the blockchain network to handle data storage}
$send\_to\_smart\_contract(data\_storage\_request)$ {The data storage request is sent to the smart contract}
$ipfs\_address = retrieve\_ipfs\_address(H)$ {The smart contract retrieves the IPFS address from the data storage request using the provided hash value}
$verify\_data\_integrity(ipfs\_address, H)$ {The smart contract verifies the integrity of the data by comparing the hash value of the retrieved data with the provided hash value}
if $valid\_data\_integrity()$ then
    $confirmation\_token = generate\_confirmation\_token()$ {the smart contract generates a signed confirmation token $(T)$}
    $store\_confirmation\_token(confirmation\_token)$ {store $T$ on the blockchain}
    $notify\_data\_storage\_success()$ {The IoT device receives a notification that the data was successfully stored and can now delete the original encrypted data}
else
    $store\_error\_message()$ {the smart contract rejects the data storage request and stores an error message on the blockchain}
    $notify\_data\_storage\_failure()$ {The IoT device receives a notification that the data storage failed and should try again later}
end if
```

3.4 Secure Data Sharing

In this section, we provide a secure data sharing model which ensures that only authorized users can access sensitive data. It uses encryption and decryption techniques to protect the data, and access tokens are used to control access to the data. The access tokens have an expiration date, and access logs are maintained to monitor who accessed the data and when. Additionally, an access control mechanism is implemented to restrict access to specific data only to authorized users or groups. Finally, encryption and decryption keys are regularly updated and managed securely to avoid any unauthorized access to sensitive data. The use of IPFS and blockchain technologies provides an additional layer of security and immutability to the data storage and sharing process.

In the secure data sharing model, sensitive data is shared among authorized parties through a secure and controlled process. The model consists of the following components:

- Data Owners: are the individuals or entities that own the sensitive data and have the ability to grant or revoke access to it. Data consumers, on the other hand, are the individuals or entities that require access to the sensitive data and must be authorized by the data owners to gain access. Access tokens are generated by the data owners and given to the data consumers to access the sensitive data. These tokens can have an expiration date to limit the time frame in which the data can be accessed, and access logs can be maintained to monitor who accessed the data and when.
- Data Consumers: These are the individuals or entities that require access to the sensitive data. They need to be authorized by the data owners to gain access.
- Access Tokens: These are tokens that are generated by the data owners and given to the data consumers to access the sensitive data. The access tokens can have an expiration date to limit the time frame in which the data can be accessed. Access logs can also be maintained to monitor who accessed the data and when.
- Access Control Mechanism: An access control mechanism is implemented to restrict access to specific data only to authorized users or groups. This mechanism can be implemented using various techniques such as role-based access control, attribute-based access control, and mandatory access control. Encryption and decryption keys are used to encrypt and decrypt the sensitive data to protect it from unauthorized access. These keys can be regularly updated and managed securely to avoid any unauthorized access to sensitive data.
- Hybrid Encryption and Decryption Keys: These are keys that are used to encrypt and decrypt the sensitive data to protect it from unauthorized access. The encryption and decryption keys can be regularly updated and managed securely to avoid any unauthorized access to sensitive data.

This algorithm outlines the steps for secure data sharing between data owners and data consumers. It includes the use of hybrid encryption, digital signatures, access tokens, and timers to ensure the confidentiality, integrity, and availability of sensitive data. The algorithm also emphasizes the importance of best practices for information security and user awareness.

Step 1: Data owner generates a AES symmetric encryption key and an RSA public-private key pair for digital signature and encryption.

```
function generate_keys() {
  K = secure_random_number_generator();
  <K_p,K_r> = generate_keypair();
  return {K, K_p,K_r};
}
```

Step 2: Data owner encrypts the sensitive data D using the symmetric key K and uploads it to IPFS platform:

- Encrypt the data using AES encryption with the symmetric key ($C_1 = AES\_Encrypt(D, K)$).

- Generate public and private keys (K_p, K_r) for RSA encryption $(C_2 = RSA\_Encrypt(K, K_p))$.
- Encrypt the AES symmetric key using RSA encryption with the public key K_p

```
function encrypt_and_upload(K, D) {
  C_1 = AES_Encrypt(D, K);
  C_2 = RSA_Encrypt(K, K_p)
  ipfs_address=storage_platform.upload(C_1,C_2);
  return true;
}
```

Step 3: Data owner creates a smart contract on the blockchain with the $ipfs_address$ and access control rules.

```
function create_smart_contract(ipfs_address, access_control_rules) {
  smart_contract_address = blockchain.create_contract(ipfs_address, access_control_rules);
  return smart_contract_address;
}
```

Step 4: Data owner signs the smart contract with his/her private key P_r to verify ownership.

```
function sign_contract(smart_contract_address, K_r) {
  signature = digital_signature(smart_contract_address, K_r);
  return signature;
}
```

Step 5: Data requester sends an access request to the smart contract with an access token T.

```
function send_access_request(smart_contract_address, T) {
  transaction = smart_contract.send_access_request(T);
  return transaction;
}
```

Step 6: Smart contract verifies the access request and grants access to the requester.

```
function verify_access_request(smart_contract_address, T) {
  access_granted = smart_contract.verify_access_request(T);
  return access_granted;
}
```

Step 7: Data requester receives the $ipfs\_address$ and $smart\_contract\_address$ from the data owner.

```
function receive_data(K, ipfs_address, encrypted_contract_address, K_p,K_r) {
```

```
contract_address = hybrid_decrypt(K_r,encrypted_contract_address);
is_verified = verify_signature(contract_address, K_p,signature);
if (is_verified) {
return {ipfs_address, contract_address};
} else {
throw new Error('Invalid signature');
}
}
```

Step 8: Data requester sends the access token to the smart contract to gain access to the data on the IPFS platform.

```
function request_access(smart_contract_address, access_token) {
transaction = smart_contract.request_access(access_token);
return transaction;
}
```

Step 9: Smart contract verifies the access token and grants access to the data on the IPFS platform.

```
function verify_access_token(smart_contract_address, access_token) {
access_granted = smart_contract.verify_access_token(access_token);
return access_granted;
}
```

Step 10: Data requester downloads the encrypted data from the secure storage platform and decrypts it using the symmetric key.

```
function download_and_decrypt(K, ipfs_address) {
  encrypted_data = storage_platform.download(ipfs_address);
  decrypted_data = hybrid_decrypt(K, C_1);
  return decrypted_data;
}
```

Step 11: Data requester performs operations on the decrypted data and then uploads any changes to the secure storage platform.

```
function encrypt_and_upload_changes(K, changes) {
  encrypted_changes = hybrid_encrypt(K, changes);
  storage_platform.upload(encrypted_changes);
  return true;
}
```

Step 12: Data requester sends the encrypted symmetric key to the device owner with their public key so the device owner can decrypt the changes.

```
function send_encrypted_key(K, K_p) {
  encrypted_key = hybrid_encrypt(K, K_p);
  send_secure_message(C_2 K_p);
}
```

Step 13: Device owner decrypts the symmetric key with their private key and then decrypts the changes made by the data requester.

```
function receive_encrypted_key(C_2,K_p,K_r) {
  symmetric_key = hybrid_decrypt(K_r, C_2);
  return symmetric_key;
}


function decrypt_changes(K,C_2) {
  changes = hybrid_decrypt(K, encrypted_changes);
  return changes;
}
```

Step 14: Device owner can revoke access to the data by removing the data from the secure storage platform and destroying the smart contract.

```
function revoke_access(ipfs_address, smart_contract_address) {
  storage_platform.remove(ipfs_address);
  blockchain.destroy_contract(smart_contract_address);
}
```

The secure data sharing algorithm has the ability to prevent and detect different types of cyber attacks, such as hacking, phishing, and social engineering, due to several security measures that are implemented within the algorithm.

Firstly, the algorithm can prevent hacking attacks by implementing strong encryption techniques that protect the data from unauthorized access. This makes it difficult for hackers to gain access to the data even if they manage to breach the system.

Secondly, the algorithm can detect phishing attacks by implementing access control mechanisms that verify the identity of the user before granting access to the data. This prevents unauthorized users from accessing the data and reduces the risk of phishing attacks.

Thirdly, the algorithm can detect and prevent social engineering attacks by implementing user awareness training programs that educate users on how to recognize and respond to social engineering attacks. This reduces the chances of users falling for social engineering attacks and providing access to the data.

In addition to these measures, the algorithm can also implement other security mechanisms such as firewalls, intrusion detection systems, and antivirus software that can detect and prevent different types of cyber attacks.

Overall, the secure data sharing algorithm has the ability to prevent and detect different types of cyber attacks due to the multiple layers of security measures that are implemented within the algorithm. By implementing these measures, the algorithm ensures that the data is protected from unauthorized access and that the users can securely share the data without any security risks.

4 Performance Evaluation

In order to evaluate the effectiveness of our proposed approach for securing data sharing and storage in 6G-based IoT networks using blockchain technology, hybrid encryption, and IPFS, we conducted a simulation study. The simulation study allowed us to assess the performance and security of our proposed approach under a variety of conditions and scenarios. In this section, we describe the simulation methodology and parameters used in our study.

4.1 Simulation Methodology

We conducted a discrete-event simulation using the NS-3 network simulator, which is a widely used open-source network simulation tool. Our simulation model was based on a realistic 6G-based IoT network architecture. We used a variety of parameters and scenarios to test the performance and security of our proposed approach.

Specifically, we simulated the sharing and storage of data in the network, as well as the use of blockchain technology, hybrid encryption, and IPFS for securing the data. We varied parameters such as the number of nodes in the network, the size of the data being transmitted, the network topology, and the type of attacks being launched against the network.

4.2 Network Topology

In this part, we studied the impact of different network topologies on the performance and security of our proposed approach.

Based on the simulation study (Fig. 2), we found that the ring topology is the best option for our approach, as it offers the lowest latency and highest throughput, as well as high security. The star topology is a reasonable alternative, with slightly higher latency and lower throughput, but still providing moderate security. The mesh

Table 2 Network topology simulation results

Network topology	Latency (ms)	Throughput (Gbps)	Security
Ring	5	10	High
Star	10	5	Medium
Mesh	20	2	Low

Table 3 Data size simulation results

Data size	Latency (ms)	Throughput (Gbps)	Security
Small (10 kB)	3	12	High
Medium (1 MB)	8	8	Medium
Large (100 MB)	15	3	Low

topology should be avoided, as it has the highest latency and lowest throughput, as well as low security.

It is worth noting that these results are specific to the simulation conditions and parameters used in our study, and may not apply to all scenarios. However, they provide a useful starting point for evaluating the impact of different network topologies on the performance and security of our proposed approach.

We also measured various performance metrics such as throughput, packet loss, and delay, as well as security metrics such as the number of successful attacks on the network. By analyzing the results of our simulations, we were able to assess the effectiveness of our proposed approach for securing data transmission and storage in 6G-based IoT networks.

4.3 Data Size

Table 3 summarizes the results about the impact of different data sizes on the performance and security of your proposed approach.

These results found that smaller data sizes offer the best overall performance and security for your proposed approach, while larger data sizes have a negative impact on performance and security. Specifically, the small data size had the lowest latency and highest throughput, while the large data size had the highest latency and lowest throughput. The medium data size had intermediate performance and security characteristics.

5 Conclusion

this paper proposed a novel solution for enhancing security in 6G-based IoT networks using blockchain technology, hybrid encryption, and IPFS. The proposed approach consists of four algorithms that enhance the security of the system: a user authentication algorithm, a data access algorithm, a data storage algorithm, and a secure data sharing algorithm. The paper's contributions include the use of hybrid encryption to ensure data confidentiality and IPFS to provide decentralized and fault-tolerant storage.

Through evaluation, the proposed approach was found effective in enhancing data security in 6G-based IoT networks by providing secure and tamper-proof data sharing. The results demonstrate the potential of blockchain technology, hybrid encryption, and IPFS to enhance security in 6G-based IoT networks.

Future work could focus on the scalability of the proposed approach to larger networks and the use of other technologies to further enhance security in 6G-based IoT networks. Additionally, the proposed approach could be extended to address other security challenges in these networks, such as protecting against denial of service attacks or ensuring privacy.

References

1. Srivastava A, Das DK (2022) A comprehensive review on the application of Internet of Thing (IoT) in smart agriculture. Wireless Pers Commun 122:1807–1837
2. Xu H, Klaine PV, Onireti O, Cao B, Imran M, Zhang L (2020) Blockchain-enabled resource management and sharing for 6G communications. Digital Commun Netw 6(3):261–269
3. Bodkhe U, Tanwar S (2021) Secure data dissemination techniques for IoT applications: research challenges and opportunities. Softw Pract Exper 51:2469–2491
4. Dahiya P, Kumar V (2023) IOT security: recent trends and challenges, emerging technologies in data mining and information security, pp 3–10
5. Deshmukh A, Sreenath N, Tyagi AK, Eswara Abhichandan UV (2022) Blockchain enabled cyber security: a comprehensive survey. In: 2022 international conference on computer communication and informatics (ICCCI), Coimbatore, India, pp 1–6
6. Rathod T, Jadav NK, Tanwar S, Sharma R, Tolba A, Raboaca MS, Marina V, Said W (2023) Blockchain-driven intelligent scheme for IoT-based public safety system beyond 5G networks. Sensors 23(2):969
7. Wang J, Ling X, Le Y, Huang Y, You X (2021) Blockchain-enabled wireless communications: a new paradigm towards 6G. Natl Sci Rev 8(9) (2021)
8. Li W, Su Z, Li R, Zhang K, Wang Y (2020) Blockchain-based data security for artificial intelligence applications in 6G networks. IEEE Netw 34(6):31–37
9. Dwivedi SK, Amin R, Vollala S (2022) Smart contract and IPFS-based trustworthy secure data storage and device authentication scheme in fog computing environment. In: Peer-to-peer network and applications
10. Deep S, Zheng X, Jolfaei A, Yu D, Ostovari P, Kashif Bashir A (2022) A survey of security and privacy issues in the Internet of Things from the layered context. Trans Emerging Tel Tech 33
11. Yeasmin A, Baig A (2020) Permissioned blockchain-based security for IIoT. In: 2020 IEEE international IOT, electronics and mechatronics conference (IEMTRONICS), pp 1–7

12. Moraes Rossetto AG, Sega C, Leithardt VRQ (2022) An architecture for managing data privacy in healthcare with blockchain. Sensors 22
13. Naz M, Al-zahrani FA, Khalid R, Javaid N, Qamar AM, Afzal MK, Shafiq M (2019) A secure data sharing platform using blockchain and interplanetary file system. Sustainability 11(24)
14. Ye Z, Leyou Z, Wu Q, Mu Y (2022) Blockchain-enabled efficient distributed attribute-based access control framework with privacy-preserving in IoV. J King Saud Univ—Comput Inf Sci 34(10):9216–9227
15. Feng C, Yu K, Bashir A, AI-Otaibi Y, Lu Y, Chen S, Zhang Di (2020) Efficient and secure data sharing for 5G flying drones: a blockchain-enabled approach. IEEE Netw 35
16. Shrestha AK, Vassileva J, Deters R (2020) A blockchain platform for user data sharing ensuring user control and incentives. Front Blockchain 3
17. Baalamurugan KM, Bacanin N et al (2023) Blockchain-enabled K-harmonic framework for industrial IoT-based systems. Sci Rep 13:1004

Combining NFC Authenticated Tags with NFTs to Spot Counterfeit Luxury Products Using Solana Blockchain

Matteo Zocca and Hamid Jahankhani

Abstract The phenomenon of counterfeiting continues to grow steadily. According to Global Brand Counterfeiting (GBC in The Global Brand Counterfeiting Report, 2018), the volume of international trade in counterfeit goods reached 1.097 trillion euros in 2017 and will exceed 1.65 trillion euros in 2020. To minimize this growing trend, the following project undertook an in-depth analysis of the problem, delving into and implementing a system that can effectively address the phenomenon of counterfeit luxury goods. The approach involves the combined use of NFC and NFT tags to protect these products. Its use has proven effective in several respects. Although it has already been tested by several start-ups and consortia, the approach has never been thoroughly studied and its behaviour has never been analysed. This project implemented its mechanism simulation environment with off the shelf technologies, thus analyzing behaviours and criticalities. Based on the experiments conducted, guidelines were drafted to support future implementations based on this mechanism. Possible future studies will focus on the implementation of the mechanism in the context of high-value products, monitoring the system's response to counterfeiting and the degree to which the entire ecosystem is able to provide security for the company.

Keywords NFC · NFT · Counterfeit · Solana blockchain · Ixkio

1 Introduction

Counterfeit phenomenon has been growing gradually over the years. According to the Global Brand Counterfeiting [11], the volume of international trade in counterfeit goods reached €1.097 trillion in 2017 and has passed the €1.65 trilion in 2020. More evidence are reported by the Organization for Economic Cooperation and Development (OECD), which estimates in the Trends in Trade in Counterfeit and

M. Zocca · H. Jahankhani (✉)
Northumbria University London, London, UK
e-mail: Hamid.jahanhani@northumbria.ac.uk

H. Jahankhani and A. El Hajjar (eds.), *Wireless Networks*, Advanced Sciences and Technologies for Security Applications,
https://doi.org/10.1007/978-3-031-33631-7_9

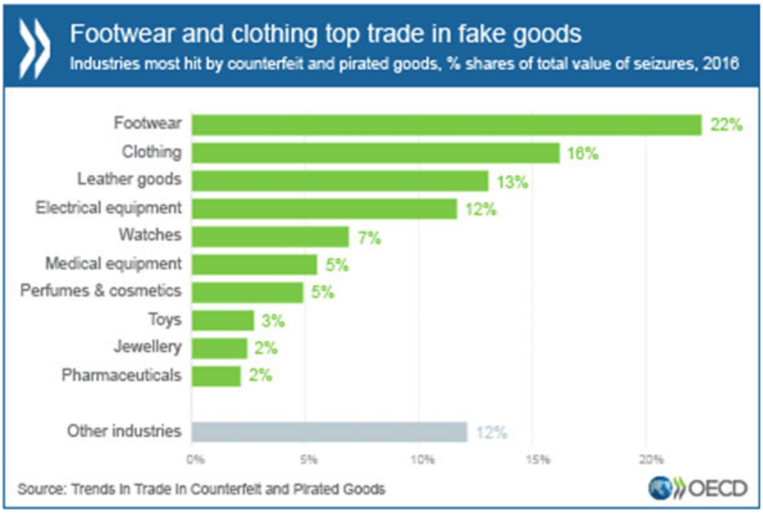


Fig. 1 Industry categories most hit by counterfeit and pirated goods according to the Global Brand Counterfeiting [24]

Pirated Goods research [24] that the value of counterfeits goods imported worldwide reaches the $509 billion according to the custom seizure data. For the European Union, counterfeit trade represented 6.8% of imports from non-EU countries.

Furthermore, it can also cause problems on the ethical level. According to counterfeit investigator [13], the purchase of fake items can contribute to the financing of terrorism and organised crime.

The counterfeit damages reported by the companies are therefore evident, both in terms of economic and reputational level. Some sectors are badly affected, especially for the luxury clothing and footwear (see Fig. 1).

A solution is needed to protect the original product from imitations. The blockchain implementation, when paired with NFC and IoT technologies, offers consumers the ability to access the entire history of a product, whether it is new or second-hand.

The objective of this research is to develop a blockchain system capable of protecting original luxury products from counterfeiting, by analysing the functioning of the entire model (highlighting its features and shortcomings) and providing a general framework to be fulfilled for future new implementations.

This will be carried out through the creation of a test environment via the Solana blockchain. Each sample product used in the test environment will be associated with a Near-Field-Communication (NFC) tag inside. Once scanned, a user will be able to verify the originality of the product by checking the Non-Fungible-Tokens (NFT) correlated to the tag and ascertain its authenticity.

Thus, the product is registered on the blockchain via the NFT, which certifies that the item's information has not been altered from the original information entered into the system by the parent company.

The objective is to prevent and guarantee:

- Ownership
- Authenticity and
- Product traceability

In other words, the NFT represents the digital counterpart of the product in the blockchain environment. By consulting this latter, consumers can learn about the authenticity, the origin of the product and the brand's history.

2 Literature Review

A blockchain is a shared immutable ledger capable of process transactions and tracking assets in a commercial network. The treated asset can be associate to something tangible (such as money, a car, or an item) or intangible (ownership and intellectual property) depending on the type of business related to the company [14]. The idea of blockchain was originally introduced in the publication 'Bitcoin: A peer-to-peer electronic cash system' [23], where the author describes this new system as:

"A purely peer-to-peer version of electronic cash that allows online payments to be sent directly from one party to an- other without going through a financial institution" [23].

The correlation between blockchain and Bitcoin is as close as it is crucial. Released in 2009, Bitcoin was the first cryptocurrency to use this new type of distributed ledger. Among the innovations introduced by this new coin was the fact that every transaction was legitimised by a decentralised network and not by central authorities. The history of this cryptocurrency in a short time has marked and stimulated the evolution of Blockchain technologies, amidst experimentation, perplexity, and an unprecedented media hype.

A transaction is defined as a chain of digital signatures. Each owner transfers the asset or currency to the next by digitally signing the hash of the previous transaction and the public key of the next owner and adding them to the end of the transaction. A beneficiary can check the signatures to verify the authenticity of the chain (Fig. 2).

Problems arise when the transferee cannot guarantee that one of the owners has not spent twice and therefore has not signed past transactions. The technology must meet the same quality standards as centralised systems in order to compete with them and guarantee a reliable ecosystem. A common solution is to introduce a trusted central authority, or mint, which checks every transaction to ensure that there is no double spending. However, this implies that with this solution the control of the entire monetary system is centralised and therefore depends solely on a third party.

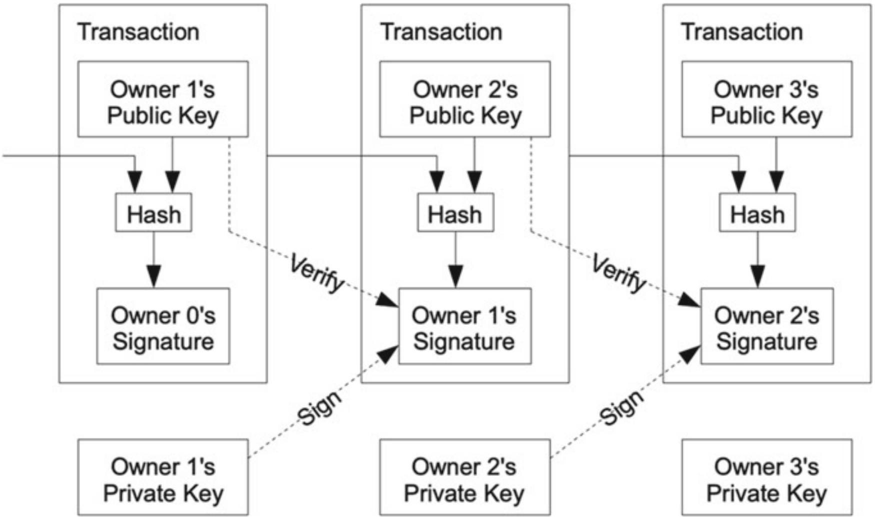


Fig. 2 Example of a transaction chain [23]

The first implementation of blockchain technology, according to the paper written by [23], stipulates that only the first transaction recorded in the system will be counted, as subsequent double-spending attempts will not be considered. The idea is therefore to publicly announce all transactions made within the blockchain and allow participants to agree on a single history of the order in which they were received, a sort of public ledger. In this way, the beneficiary can have a proof that at the time of each transaction a majority of the nodes agreed that it was the first to be received.

More in detail, the proposed solution involves the use of a timestamp server. A timestamp server works by taking the hash of the blocks that have already been processed and widely publishing their hash, in the same way in a Usenet post [31]. The timestamp thus proves that the data existed at that time, of course, in order to have been included in the next element. Each timestamp includes the previous timestamp in its hash, forming a chain, with each additional timestamp reinforcing the previous ones (Fig. 3).

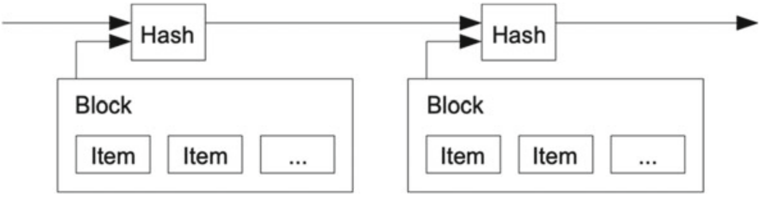


Fig. 3 Hashes includes hashes of the previous blocks [23]

2.1 *How is Consent Reached (Proof-of-Work)?*

To implement a distributed timestamp server on a peer-to-peer basis, a method called proof-of-work is used, which involves the work of a computer to solve a cryptographic puzzle. In a nutshell, each computer has to find that number, which once appended to the block and given as input to the hash function (as in the case of SHA-256), the digest starts with a certain amount of zero bits. The average work required is exponential to the number of zero bits required and can be verified by running a single hash. Every 2016 blocks, the network calculates the average time required to extract them. They then multiply the difficulty by this time divided by two weeks so that with this new difficulty it would take two weeks to extract the 2016 blocks (corresponding to one every 10 min). This translates into setting the right amount of zeros to validate a block.

As in the lottery, computers increment this value, called a nonce, in the block until they find a value that gives the hash of the block the required zero bits. Once CPU effort has been expended to satisfy the proof-of-work, the block cannot be modified without redoing the work. Since subsequent blocks are concatenated after it, the work to change the block would include redoing all subsequent blocks (Fig. 4).

Proof-of-work is used to solve the problem of determining the valid ledger approved by the majority. If the majority relied on IP addresses for a vote, it could be subverted by anyone able to obtain a large amount of them. Proof-of-work allows a vote to be correlated for each CPU. The majority decision is represented by the longest chain, which is considered by the other nodes to be the one with the most effort invested on it. This method allows in a scenario where most of the CPU power is controlled by honest nodes, the honest chain will grow faster and surpass any fraudulent or competing chains. To modify a past block, an attacker would have to redo the proof-of-work of the fraudulent block and all subsequent blocks, and then catch up and overtake the work of the honest nodes. It will be shown in the next section that the probability of an attacker being able to recover the other chain decreases exponentially with the addition of successive blocks. To compensate for the increase in hardware speed and the different interest of nodes running over time, the difficulty of proof-of-work is determined as mentioned above by a moving average. If they are generated too fast, the difficulty increases.

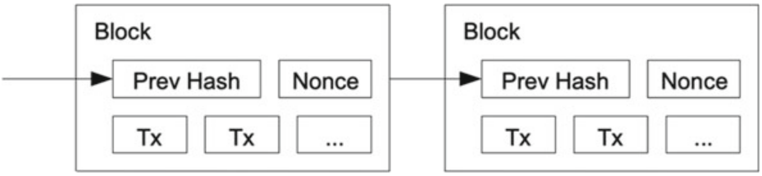


Fig. 4 Example of a chain [23]

2.2 Why Blockchain is Considered Secure?

Consider the scenario of an attacker attempting to generate an untruthful alternative chain that is faster than the honest chain, so that the attacker can insert arbitrary data into the blockchain. From the precise block where the attacker inserts the false data, the system effectively responds to attempted changes, such as attempting to create new assets or appropriating it.

Because of asymmetric cryptography systems, nodes will not accept an invalid transaction as payment and honest nodes will never accept a block that contains them. An attacker can only try to modify one of his transactions to recover money he has recently spent. The challenge between the honest chain and the attacker's chain can be expressed through the binomial random walk problem, where the success event is the addition of the block to the honest chain which is denoted by $+ 1$, while the failure event is expressed by the addition of a block to the attacker's chain, which reduces the gap by $- 1$.

As reported in Nakamoto's paper [23], the probability of an attacker recovering a given gap between his blockchain and the honest one is analogous to the problem of Gambler Ruin. Suppose that a gambler with a certain deficit has to catch up the other competitor with unlimited credit starts and can potentially play an infinite number of trials. The probability calculation for reaching the draw, i.e. that an attacker reaches the honest chain, can be expressed as follows [8]:

p = probability that an honest node solves the puzzle and process the next block
q = probability that the attacker node solves the puzzle and process the next block
$\mathrm{p_q}$ = probability the attacker will reach the n-blocks that were left behind

$$\mathrm{p_q} = \left\{ \begin{matrix} 1 & \text{if } p \leq q \\ (p/q)^n & \text{if } p > q \end{matrix} \right\}$$

Considering the hypothesis that p > q, i.e. in a scenario where the blockchain has already been up and running for some time, note how the probability decreases exponentially as the number of blocks the attacker has to recover increases (which is indicated in the formula with n). In fact, with the probability against him, if the attacker is unable to actively participate in the beginning of the blockchain's development, his chances become smaller and smaller as he falls behind.

At this point, the waiting time of the recipient of the transaction is analyzed in order to consider it legitimate and unchangeable in the future.

Suppose the sender wants to set up a fraudulent scam in order to make the recipient believe that he has paid him, and then credit the transaction to himself later. In other words, the sender hopes that by the time the recipient realises it is too late.

Whenever the receiver has to sign a transaction, he generates a new key pair and delivers the public key to the other party just before signing. This prevents an attacker from storing the key for a long period of time, thus avoiding him from working on a blockchain in advance, until he can get far enough ahead and execute the transaction at that time. Once the transaction has been executed, the attacker to carry out his fraud starts to secretly works on a parallel blockchain containing the transaction for re-crediting the money spent, building an alternative version of the blockchain.

The recipient, as is the practice, waits until the transaction has been added to a blockchain and waits until n blocks have been connected after it in order to consider it safe. Furthermore, the victim have no clue about the exact amount of progress made by the attacker, and assuming that the honest blocks took the expected average time per block, the potential progress of the attacker is expressed as a Poisson distribution with expected value:

$$\lambda = z\frac{q}{p}$$

To calculate the attacker's relative probability of catching up with the legitimate blockchain, the Poisson density for each of its possible advances is multiplied by the probability he had at that specific instant.

$$\sum_{k=0}^{\infty}\frac{\lambda^k e^{-\lambda}}{k!}\cdot\left\{\begin{array}{c}\left(\frac{q}{p}\right)^{(z-k)}\text{if}\quad k\le z\\ 1\quad\text{if}\quad k>z\end{array}\right\}$$

Rewriting the formula to avoid adding up the infinite tail of the distribution gives:

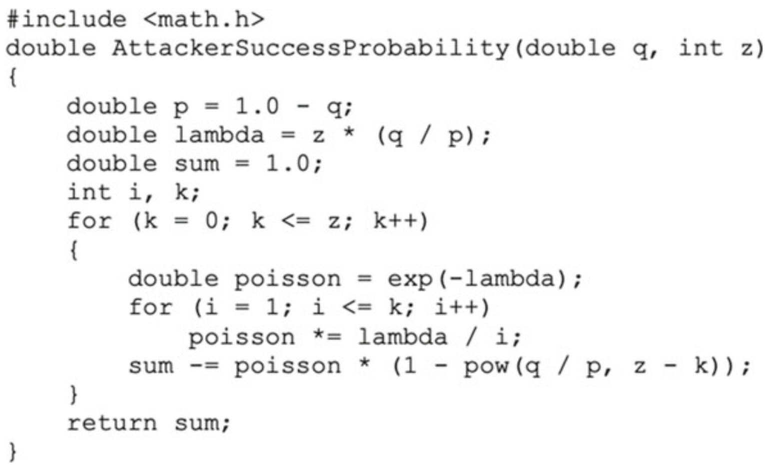
$$1-\sum_{k=0}^{z}\frac{\lambda^k e^{-\lambda}}{k!}\left(1-\left(q/p\right)^{(z-k)}\right)$$

As reported in Nakamoto's study [23], this can be written in c language to calculate the probability as the number of blocks queued after the block in question increases (Fig. 5).

By running simulations, it can be seen that the probability drops exponentially as z increases (Fig. 6).

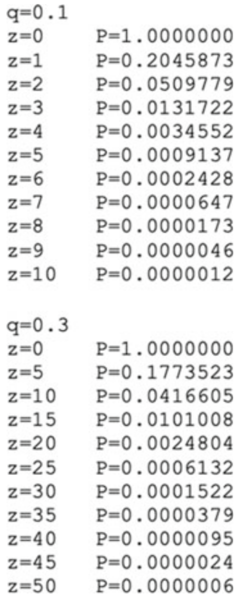
2.3 Blockchain Contexts of Use

The exclusion of a trusted third party has made it possible, through the use of blockchain technologies, to fully decentralise systems and gain the advantages of peer-to-peer approaches. The growing interest of people has also attracted large amounts of capital to invest in this trust-based model. As reported in the Kharpal article [4], the market value of cryptocurrencies exceeded USD 2 trillion for the first time in April 2021. Further evidence of the continued adoption of blockchain can be found in the implementations that several companies, spurred by the benefits of this technology especially in the aspects of end-to-end traceability and tracking, are using to improve user experience and help companies combat counterfeiting to a large extent. Some notable examples are Walmart's blockchain [32], called DL



```
#include <math.h>
double AttackerSuccessProbability(double q, int z)
{
    double p = 1.0 - q;
    double lambda = z * (q / p);
    double sum = 1.0;
    int i, k;
    for (k = 0; k <= z; k++)
    {
        double poisson = exp(-lambda);
        for (i = 1; i <= k; i++)
            poisson *= lambda / i;
        sum -= poisson * (1 - pow(q / p, z - k));
    }
    return sum;
}
```

Fig. 5 Function to calculate the probability in C language [23]



```
q=0.1
z=0     P=1.0000000
z=1     P=0.2045873
z=2     P=0.0509779
z=3     P=0.0131722
z=4     P=0.0034552
z=5     P=0.0009137
z=6     P=0.0002428
z=7     P=0.0000647
z=8     P=0.0000173
z=9     P=0.0000046
z=10    P=0.0000012

q=0.3
z=0     P=1.0000000
z=5     P=0.1773523
z=10    P=0.0416605
z=15    P=0.0101008
z=20    P=0.0024804
z=25    P=0.0006132
z=30    P=0.0001522
z=35    P=0.0000379
z=40    P=0.0000095
z=45    P=0.0000024
z=50    P=0.0000006
```

Fig. 6 Probability value drops as z increases [23]

Freight, which is used to add transparency to the ecosystem by monitoring the food supply chain and procurement process in real time. Ford, on the other hand, uses this technology in collaboration with IBM to track cobalt supplies [9]. The company FedEx relies on blockchain to protect its chain of custody [25].

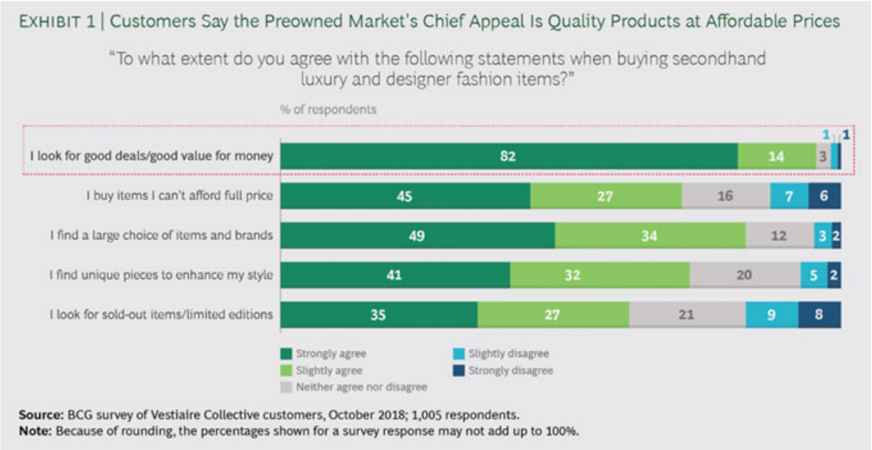
An example even closer to the intentions of this project is the one proposed by Alfa Romeo, who has introduced on its first car the presence of blockchain technology [5] in combination with NFT (non-fungible token). A special cryptographic token that represents the deed and certificate of authenticity written on blockchain of a unique asset, which in this case represents a physical asset. Non-fungible tokens are used to create a 'unique' digital property. This technology will allow the user to track the entire 'life cycle' of the car, with information such as acceleration or braking history, routine and extraordinary maintenance and kilometres travelled.

2.4 The Use of Blockchain as a Method to Combat Counterfeiting

The dream of owning a luxury item is coveted by many but not everyone can afford it, often people are forced to turn to the second-hand market as it is more accessible for their wallets. According to the latest research, the second-hand market is estimated to be worth US$32.61 billion, and is likely to reach US$51.77 billion by 2026 [12].

In the second-hand market, buyers are incentivised to buy and sell products mainly because of the good value for money that can be found. In fact, according to the survey conducted by the Boston Consulting Group [2], about 96% of the buyers surveyed say they buy second-hand items partly because they are looking for good deals (See Fig. 7).

It is therefore evident that the buying and selling of used luxury goods at affordable prices, especially online, is a growing phenomenon. Products such as Gucci are easy to find on Instagram, but also used Prada bags on eBay, and online shops selling used Nike Adidas and Hermès clothing, and so on. Resale has become the hottest new trend in online retail. According to some estimates [20], the second-hand market is growing four times faster compared to the primary market.

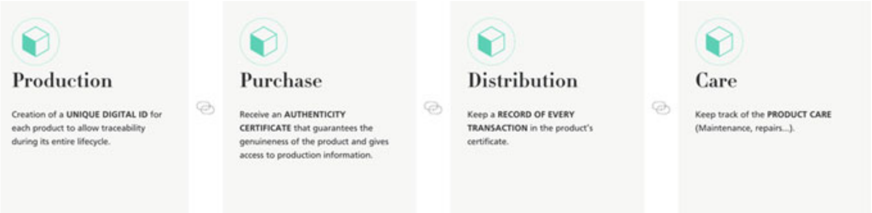


Source: BCG survey of Vestiaire Collective customers, October 2018; 1,005 respondents.
Note: Because of rounding, the percentages shown for a survey response may not add up to 100%.

Fig. 7 Results of surveys conducted by the Boston Consulting Group

However, purchasers who deal in and consult this type of market primarily may stumble upon non-authentic products. This results in damage to the brand image of the counterfeit garment and the financing of organised crime, which often runs these kind of activities [13]. Despite new technologies, the problem of counterfeiting still persists and is highly unlikely to be solved any time soon. For a large customer base, recognising an authentic luxury item from a fake one is still considered a priority, as a fake product could generate negative peer reviews. Furthermore, according to research conducted by a group of researchers at Yale, it is assumed that there is also a psychological factor behind owning an original product. In fact, it is reported in the study that the feeling one gets after purchasing an authentic luxury good plays an important role as it represents a sense of belonging to the brand [15].

It is precisely because of the value of this market that several companies and accelerators have started to invest in possible ways to combat counterfeiting. The continued use of blockchain has made it increasingly interesting for companies, especially to be able to recognize original products and discern them from non-authentic ones. The advantages are several: cost reduction, speed, security and above all autonomy. The adoption of a blockchain approach can revolutionise and drastically change the system of traceability of luxury products, simplifying the bureaucracy behind it. There are several projects aimed at defending authentic products and combating counterfeiting, the Aura Blockchain Consortium is one of them: a conglomerate of companies created in April 2021 by Moët Hennessy Louis Vuitton SE (LVHM), and with the participation of the Prada Group and Cartier, the OTB Group, and later Mercedes-Benz in May 2022. The aim is to give consumers unmediated access to the product history of luxury brands and their guarantee of authenticity [1]. The intention is to make the entire product life cycle, from creation to distribution, transparent by providing reliable data throughout the process. An initiative that will, in the intentions of its creators, strengthen people's relationship with their brands and increase customer confidence in the sustainable practices and responsible sourcing conducted by individual brands. The technological system, a release explains, consists of a private multi-nodal blockchain and is protected by ConsenSys and Microsoft technology. Thanks to this system, it will be possible to record information in a secure and non-reproducible manner and generate a unique certificate for each owner, 'increasing the desirability of valuable items that are the result of unique know-how and made from high-quality sustainable materials' [1] (Fig. 8).



Creation of a **UNIQUE DIGITAL ID** for each product to allow traceability during its entire lifecycle.

Receive an **AUTHENTICITY CERTIFICATE** that guarantees the genuineness of the product and gives access to production information.

Keep a **RECORD OF EVERY TRANSACTION** in the product's certificate.

Keep track of the **PRODUCT CARE** (Maintenance, repairs...).

Fig. 8 Product process monitored by the Aura blockchain [1]

Benefits for customers:

- Prove the authenticity and ownership of goods;
- Access to product history information;
- Strengthen customer relationships through transparency;
- Access to services provided by brands;

Benefits for brands:

- Ensure that products are manufactured and managed according to the standards set by brands;
- Building a relationship of trust with customers, without intermediaries;
- Protect markets from counterfeiting and at the same time control the second-hand market.

The practical part of the Aura project has been released through the "Software as a Service" (Saas) implementation on 13 January 2022, the first blockchain-based platform designed exclusively for the luxury brands sector, with the aim of accompanying the entire industry to embrace the Blockchain and Web 3.0 revolution within different business functions, including: supply chain, customer service, marketing, manufacturing, sustainability, procurement, logistics and legal.

Aura SaaS enables Aura member brands to start using the platform quickly and easily, maximising customer value and digital innovation, and enabling traceability both upstream and downstream in the supply chain—making it one of the best direct-to-consumer offerings on the market.

The platform involves the use of the Ethereum-based ConsenSys Quorum blockchain technology, allowing the common ledger to be maintained and updated through the consent provided by the remaining members of the blockchain block by block. Each Brand is required to manage at least two Quorum nodes and ensure their viability.

Furthermore, to complete this system, a centralised part is added relating to the needs required by the company and consisting of:

Blockchain services: which enable the connection between the blockchain and other applications.

Off-chain services: including APIs used to connect business services to the platform.

Front-end applications: for interactions with consumers.

The architecture of the platform is shown below (Fig. 9):

The ambitions of the Aura project are in line with those of the following project, albeit on a smaller scale. The intention to succeed in linking the two physical and digital worlds through the use of nfc tags and non-fungible tokens respectively represents a challenge that has not yet been widely documented.

There is therefore no study of the validity of this mechanism, nor any information on its implementation and guidelines to help refine the entire infrastructure. This project aims to analyse in detail the process of implementing this approach by using solana's blockchain technology to create the non-fungible tokens that, after proper configuration, will be linked to the NFC tags incorporated in the asset.

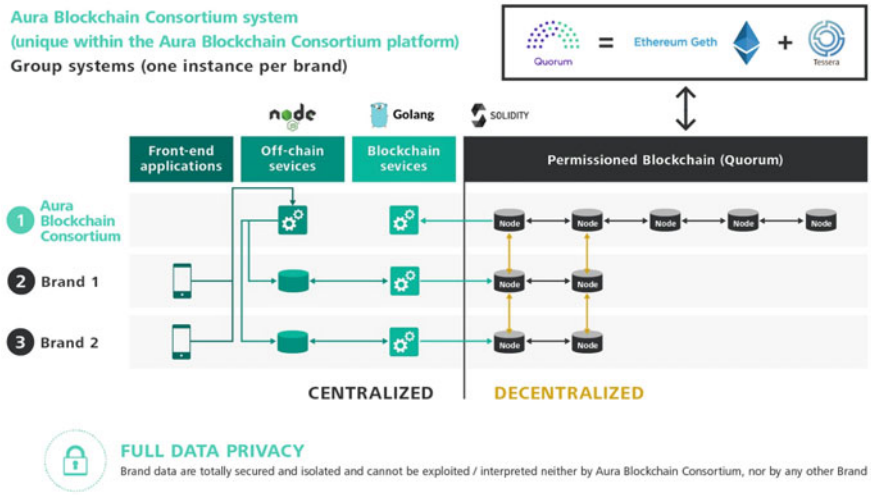

Aura Blockchain Consortium system
(unique within the Aura Blockchain Consortium platform)
Group systems (one instance per brand)
Quorum
=
Ethereum Geth
+
Tessera
node
Golang
SOLIDITY
Front-end applications
Off-chain sevices
Blockchain sevices
Permissioned Blockchain (Quorum)
1 Aura Blockchain Consortium
2 Brand 1
3 Brand 2
Node
CENTRALIZED
DECENTRALIZED
FULL DATA PRIVACY
Brand data are totally secured and isolated and cannot be exploited / interpreted neither by Aura Blockchain Consortium, nor by any other Brand

Fig. 9 Saas architecture [1]

The company will then have to find a way to connect these two worlds, associating the unique value of the NFC with the NFC tag, which must also be protected against replication attacks. This information must then be recorded in a secure location, away from external threats and tampering by unauthorised personnel. It is precisely this last stage of registration that is considered the most critical, since although blockchain technology can guarantee that the information within the ledger has not been tampered with, external users could write non-integral and authentic data during entry. In other words, if false information has been entered into the blockchain, it will remain there forever. This means that if entry permissions are not meticulously granted to third parties such as wholesalers, they could bypass the system by simply creating an entry for a counterfeit garment and go unnoticed. Therefore, quoting Mansour's article, for the project to be functional, it is crucial to remember that:

> Trust in the integrity of each party involved is somewhat necessary for a Blockchain ledger to have the desired effect in the luxury market. [21]

This research aims to develop a simulation environment using Solana Blockchain in order to evaluate its effectiveness and develop a framework to reduce this type of risk. This is a set of good rules that minimise the danger of incorrect information being entered into the Blockchain. A conceptual system that can ensure full transparency from third parties and prevent the involvement of wrongdoers.

Some previous work has been mentioned highlighting the potential in the use of blockchain as a method of counterfeiting, doing an in-depth analysis related to luxury goods, but it is still at an early stage. The low uptake of blockchain is due to the lack of regulation for information sharing between brands and the limited possibility of collaboration [3]. Despite several years having passed since its first introduction [23], blockchain continues to be poorly implemented in mainstream sectors.

This research aims to address the aforementioned problems by defining a common framework for blockchain adoption in the luxury goods sector.

3 Configuration of the Simulation Environment

In the previous section, the basic idea of the research was introduced, explaining in general terms how blockchain works and its distinguishing features. Its implementation has been extensively tested in various fields, with large consortia or companies beginning to invest large amounts of capital in this new technology. In spite of this, its use is still underrepresented in today's world. The presentation of blockchain therefore appears to be relegated exclusively to projects that are still in the development phase and are not currently marketable [16].

The implementation of this technology as a method of combating the counterfeiting of luxury goods such as clothes and handbags was then discussed in more detail, with some of the leading companies in this sector believing in the adoption of this mechanism in order to protect their profits and disincentivise the counterfeiting market. The AURA system [1] is therefore promising in many respects, but it is still unclear what the procedures behind it are and how companies can actually be protected in adopting this mechanism. There is a lack of in-depth study on this issue, especially with regard to a framework capable of designating general guidelines for the implementation and adoption of this mechanism as an anti-counterfeiting method. More precisely, it is not yet clear whether the association of an NFC tag with its NFT counterpart in the blockchain can actually add an additional layer of security to the whole system.

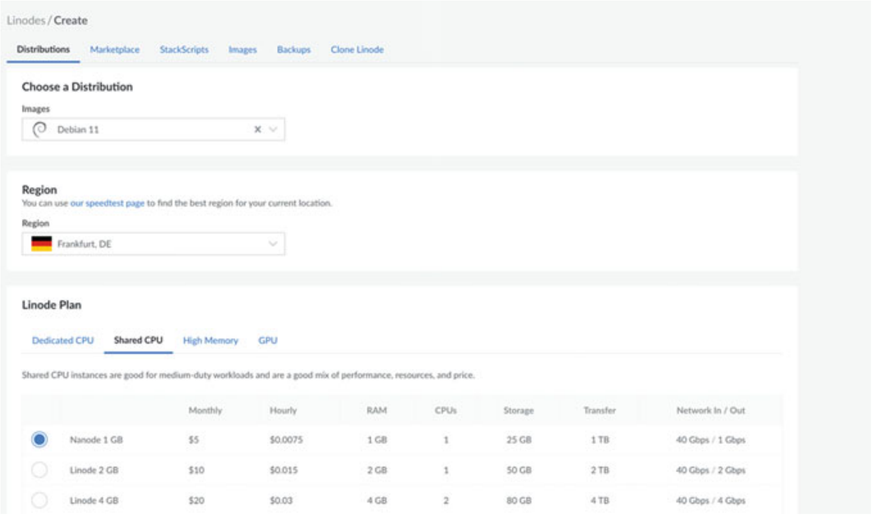
From this chapter onwards, a development environment will be set up capable to simulate the blockchain approach and, in combination with NFC tags and NFTs, to assess the entire system in order to evaluate its main characteristics and possible problems.

3.1 Configuration of a New Debian Machine

The environment involves the use of the Solana blockchain. The machine in charge of creating the token and NFT was configured on Linode, a Cloud Hosting Provider specialising in provisioning Linux machines in the cloud, with SSD disks and top network performance.

During the configuration phase, a basic configuration was chosen as the workload does not require excessive use of resources. As shown in Fig. 10, the machine running Debian version 11 has a single CPU with 1 GB RAM (Fig. 11).

Since the machine has been configured without a graphic interface, access is only done via SSH by the root user from a computer on the Internet, which means that it is outside the LAN (Fig. 12).



Choose a Distribution

Images: Debian 11

Region

You can use our speedtest page to find the best region for your current location.

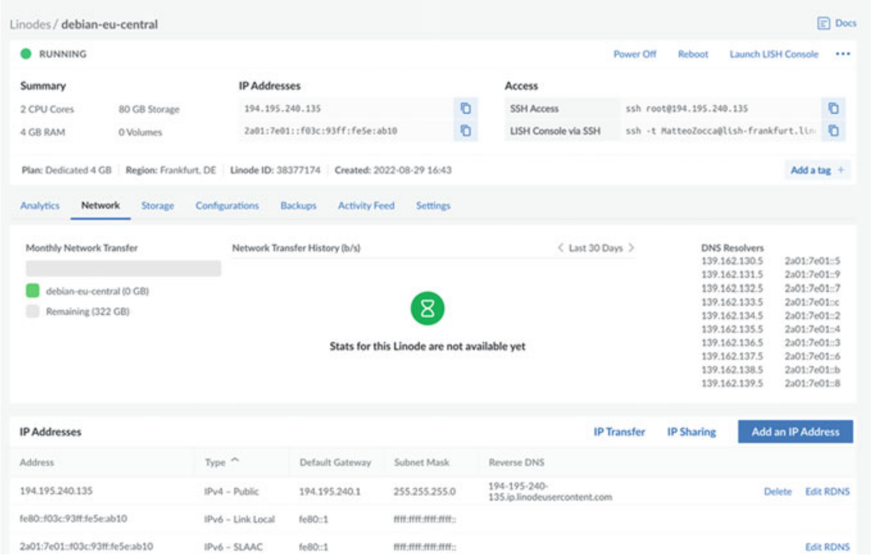
Region: Frankfurt, DE

Linode Plan

Shared CPU instances are good for medium-duty workloads and are a good mix of performance, resources, and price.

		Monthly	Hourly	RAM	CPUs	Storage	Transfer	Network In / Out
●	Nanode 1 GB	$5	$0.0075	1 GB	1	25 GB	1 TB	40 Gbps / 1 Gbps
○	Linode 2 GB	$10	$0.015	2 GB	1	50 GB	2 TB	40 Gbps / 2 Gbps
○	Linode 4 GB	$20	$0.03	4 GB	2	80 GB	4 TB	40 Gbps / 4 Gbps

Fig. 10 Configuration details of the Debian 11 machine



RUNNING

Summary

2 CPU Cores 80 GB Storage
4 GB RAM 0 Volumes

IP Addresses

194.195.240.135
2a01:7e01::f03c:93ff:fe5e:ab10

Access

SSH Access	ssh root@194.195.240.135
LISH Console via SSH	ssh -t MatteoZocca@lish-frankfurt.lin

Plan: Dedicated 4 GB | Region: Frankfurt, DE | Linode ID: 38377174 | Created: 2022-08-29 16:43

Monthly Network Transfer

🟩 debian-eu-central (0 GB)
▢ Remaining (322 GB)

Network Transfer History (b/s)

Stats for this Linode are not available yet

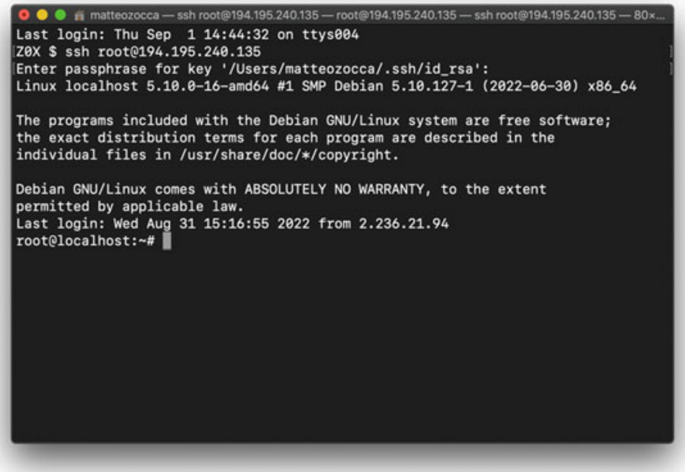
DNS Resolvers

139.162.130.5	2a01:7e01::5
139.162.131.5	2a01:7e01::9
139.162.132.5	2a01:7e01::7
139.162.133.5	2a01:7e01::c
139.162.134.5	2a01:7e01::2
139.162.135.5	2a01:7e01::4
139.162.136.5	2a01:7e01::3
139.162.137.5	2a01:7e01::6
139.162.138.5	2a01:7e01::b
139.162.139.5	2a01:7e01::8

IP Addresses

Address	Type	Default Gateway	Subnet Mask	Reverse DNS	
194.195.240.135	IPv4 – Public	194.195.240.1	255.255.255.0	194-195-240-135.ip.linodeusercontent.com	Delete Edit RDNS
fe80::f03c:93ff:fe5e:ab10	IPv6 – Link Local	fe80::1	ffff:ffff:ffff:ffff::		
2a01:7e01::f03c:93ff:fe5e:ab10	IPv6 – SLAAC	fe80::1	ffff:ffff:ffff:ffff::		Edit RDNS

Fig. 11 Network information of the Debian 11 machine



matteozocca — ssh root@194.195.240.135 — root@194.195.240.135 — ssh root@194.195.240.135 — 80×...

```
Last login: Thu Sep  1 14:44:32 on ttys004
Z0X $ ssh root@194.195.240.135
Enter passphrase for key '/Users/matteozocca/.ssh/id_rsa':
Linux localhost 5.10.0-16-amd64 #1 SMP Debian 5.10.127-1 (2022-06-30) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed Aug 31 15:16:55 2022 from 2.236.21.94
root@localhost:~#
```

Fig. 12 Access to the machine via ssh from a machine terminal outside the LAN

3.2 Installation of Solana Tools

This section shows the installation of the commands needed to create wallets, coins, NFTs, which will be discussed in the pages to come. The chosen version of solana is v1.8.6. The installation process only requires entering a command, more precisely the curl command, which calls up the wizard from the official Solana site.

The command in question is as follows:

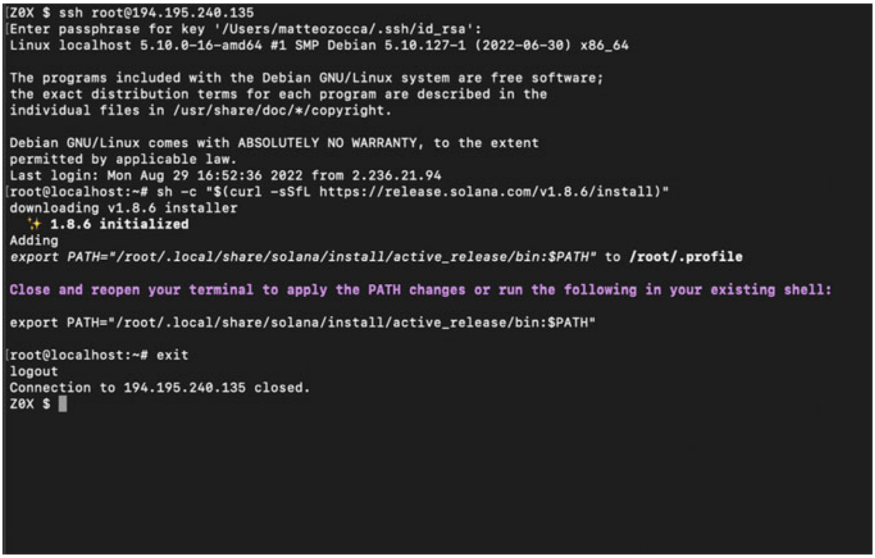
sh -c "$(curl -sSfL https://release.solana.com/v1.8.6/install)"

After issuing the command, it starts downloading the selected version by installing the environment variables and the path in the root user's .profile (Fig. 13).

The second step involves the installation of Rust. Rust is a multi-paradigm programming language that supports functional, imperative and object-oriented programming. Starting out as Graydon Hoare's personal project within Mozilla for the development of the Firefox browser, it has developed into an open source project with a large, active and productive community [26].

Rust is also a language for writing client and server applications that communicate over the Internet. As such, it focuses on security, control over memory layout and concurrency, guaranteeing excellent performance levels. Rust's syntax is derived from C and C++, but its semantics are similar to those of the Haskell programming language, and allow for ad hoc polymorphism.

Solana does not only require the installation of Rust, but also the installation of an add-on relating to this programming language, which is useful for managing dependencies and compiling the project. The application in question is Cargo, capable of managing Rust packages during the compilation of the project. Cargo therefore



```
[Z0X $ ssh root@194.195.240.135
[Enter passphrase for key '/Users/matteozocca/.ssh/id_rsa':
Linux localhost 5.10.0-16-amd64 #1 SMP Debian 5.10.127-1 (2022-06-30) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Mon Aug 29 16:52:36 2022 from 2.236.21.94
[root@localhost:~# sh -c "$(curl -sSfL https://release.solana.com/v1.8.6/install)"
downloading v1.8.6 installer
  ✨ 1.8.6 initialized
Adding
export PATH="/root/.local/share/solana/install/active_release/bin:$PATH" to /root/.profile

Close and reopen your terminal to apply the PATH changes or run the following in your existing shell:

export PATH="/root/.local/share/solana/install/active_release/bin:$PATH"

[root@localhost:~# exit
logout
Connection to 194.195.240.135 closed.
Z0X $ █
```

Fig. 13 Solana tool installation wizard

facilitates various activities that would otherwise have to be controlled by the user, such as downloading the libraries on which the code depends, building these libraries and constructing the code. In other words, a basic programme such as “Hello, world!” that is handled by Cargo would be identical to the code level of one manually written by a user. However, as one progresses with the writing of the code and thus the programme becomes more complex, Cargo will automatically and independently take care of the dependencies necessary for the programme to function, making the user experience much simpler and faster [6].

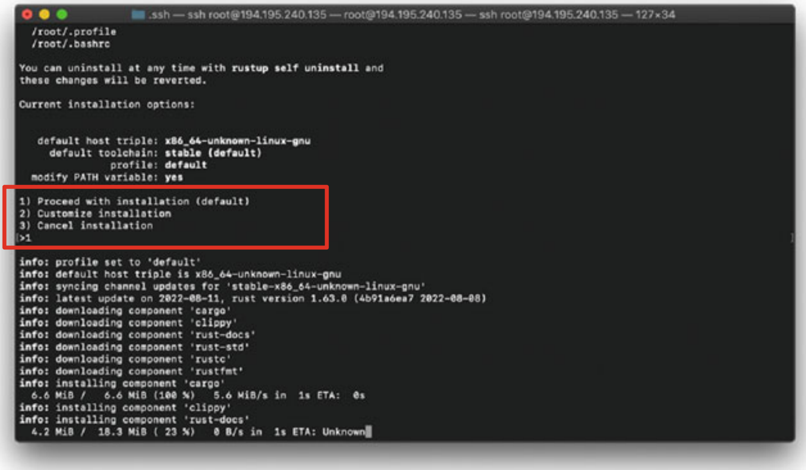
During the configuration of the Debian 11 machine, it was necessary to install these tools in order to correctly proceed with the creation of the token and NFTs on the Solana blockchain. As before using the SSH protocol and the curl command, Cargo has been installed via the following statement on the terminal:

curl https://sh.rustup.rs -sSf | sh.

The wizard allows customising the installation process by choosing between two options:

- Default installation
- Custom installation

As no customised experience is required for the project development, the default option has been chosen.



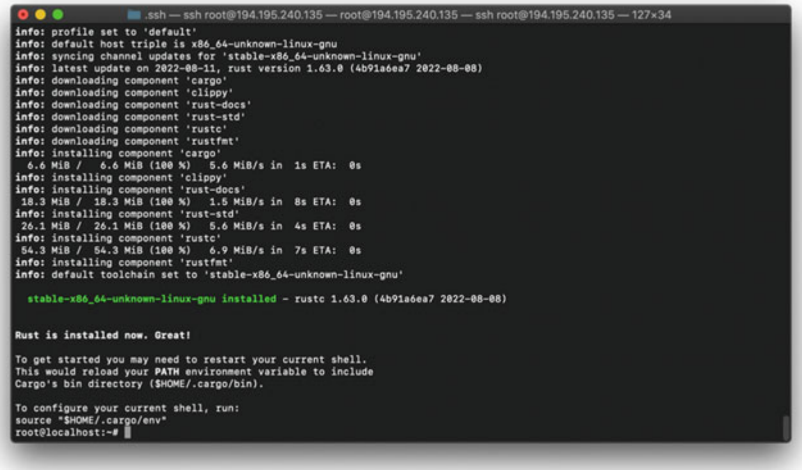
.ssh — ssh root@194.195.240.135 — root@194.195.240.135 — ssh root@194.195.240.135 — 127×34

```
  /root/.profile
  /root/.bashrc

You can uninstall at any time with rustup self uninstall and
these changes will be reverted.

Current installation options:


   default host triple: x86_64-unknown-linux-gnu
     default toolchain: stable (default)
               profile: default
  modify PATH variable: yes

1) Proceed with installation (default)
2) Customize installation
3) Cancel installation
>1

info: profile set to 'default'
info: default host triple is x86_64-unknown-linux-gnu
info: syncing channel updates for 'stable-x86_64-unknown-linux-gnu'
info: latest update on 2022-08-11, rust version 1.63.0 (4b91a6ea7 2022-08-08)
info: downloading component 'cargo'
info: downloading component 'clippy'
info: downloading component 'rust-docs'
info: downloading component 'rust-std'
info: downloading component 'rustc'
info: downloading component 'rustfmt'
info: installing component 'cargo'
  6.6 MiB /   6.6 MiB (100 %)   5.6 MiB/s in  1s ETA:  0s
info: installing component 'clippy'
info: installing component 'rust-docs'
  4.2 MiB /  18.3 MiB ( 23 %)   0 B/s in  1s ETA: Unknown
```

Figure 14 shows the message of successful installation of Rust and Cargo on the machine.

Next, three others development libraries were installed and imported via the linux apt install command, which are listed below:

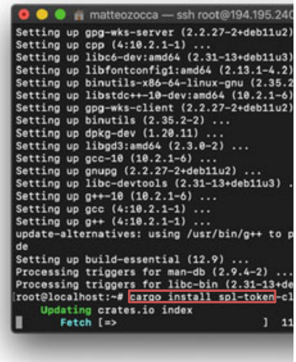
libudev-dev -y
libssl-dev pkg-config -y
build-essential –y



.ssh — ssh root@194.195.240.135 — root@194.195.240.135 — ssh root@194.195.240.135 — 127×34

```
info: profile set to 'default'
info: default host triple is x86_64-unknown-linux-gnu
info: syncing channel updates for 'stable-x86_64-unknown-linux-gnu'
info: latest update on 2022-08-11, rust version 1.63.0 (4b91a6ea7 2022-08-08)
info: downloading component 'cargo'
info: downloading component 'clippy'
info: downloading component 'rust-docs'
info: downloading component 'rust-std'
info: downloading component 'rustc'
info: downloading component 'rustfmt'
info: installing component 'cargo'
  6.6 MiB /   6.6 MiB (100 %)   5.6 MiB/s in  1s ETA:  0s
info: installing component 'clippy'
info: installing component 'rust-docs'
 18.3 MiB /  18.3 MiB (100 %)   1.5 MiB/s in  8s ETA:  0s
info: installing component 'rust-std'
 26.1 MiB /  26.1 MiB (100 %)   5.6 MiB/s in  4s ETA:  0s
info: installing component 'rustc'
 54.3 MiB /  54.3 MiB (100 %)   6.9 MiB/s in  7s ETA:  0s
info: installing component 'rustfmt'
info: default toolchain set to 'stable-x86_64-unknown-linux-gnu'

  stable-x86_64-unknown-linux-gnu installed - rustc 1.63.0 (4b91a6ea7 2022-08-08)


Rust is installed now. Great!

To get started you may need to restart your current shell.
This would reload your PATH environment variable to include
Cargo's bin directory ($HOME/.cargo/bin).

To configure your current shell, run:
source "$HOME/.cargo/env"
root@localhost:~#
```

Fig. 14 Successful installation of rust and cargo v 1.63.0



```
Setting up gpg-wks-server (2.2.27-2+deb11u2)
Setting up cpp (4:10.2.1-1) ...
Setting up libc6-dev:amd64 (2.31-13+deb11u3)
Setting up libfontconfig1:amd64 (2.13.1-4.2)
Setting up binutils-x86-64-linux-gnu (2.35.2
Setting up libstdc++-10-dev:amd64 (10.2.1-6)
Setting up gpg-wks-client (2.2.27-2+deb11u2)
Setting up binutils (2.35.2-2) ...
Setting up dpkg-dev (1.20.11) ...
Setting up libgd3:amd64 (2.3.0-2) ...
Setting up gcc-10 (10.2.1-6) ...
Setting up gnupg (2.2.27-2+deb11u2) ...
Setting up libc-devtools (2.31-13+deb11u3) .
Setting up g++-10 (10.2.1-6) ...
Setting up gcc (4:10.2.1-1) ...
Setting up g++ (4:10.2.1-1) ...
update-alternatives: using /usr/bin/g++ to p
de
Setting up build-essential (12.9) ...
Processing triggers for man-db (2.9.4-2) ...
Processing triggers for libc-bin (2.31-13+de
root@localhost:~# cargo install spl-token-cl
    Updating crates.io index
      Fetch [=>                              ]  11
```

Fig. 15 Entering the command for SPL installation

The process of machine configuration was concluded with the installation of the Solana Program Library (SPL), which is a library that enables the creation of tokens based on the Solana network. The assets created with SPL are able to benefit from the same advantages as the token itself, allowing them to be scalable, performant and fast in terms of transactions in the same way that Solana is.

For comparison with Ethereum, these assets use Solana's blockchain in the same way as ERC20 does with Ethereum. However, a small fee is charged in Solana tokens as the latter are needed to power each transaction and finalize the writing on the blockchain. This implies that a user must purchase SOLs (Solana Tokens) before making any transactions. They can be easily purchased from any exchanger such as Binance, Crypto.com, etc. This step will be discussed later in the project [7].

This operation has been performed done via Cargo command, Rust's package manager mentioned in the previous paragraphs, which allows the installation of the Solana Program Library via CLI. The command launched is as follows:

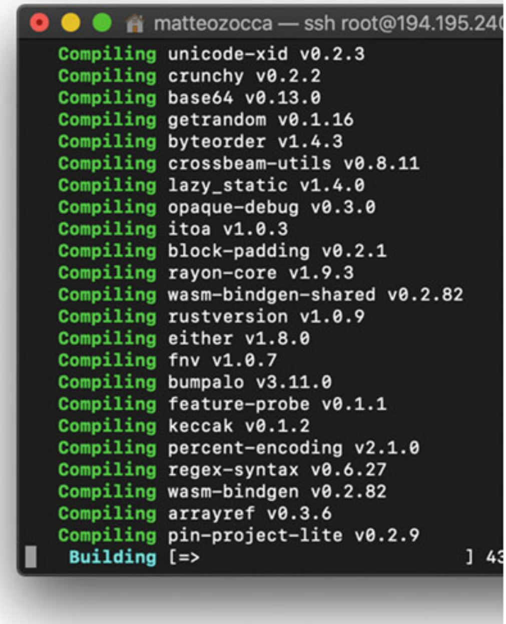
```
cargo install spl-token-cli
```

Figures 15 and 16 show the installation process of the Solana Program Library and display the command input and the ongoing installation of the various dependencies for SPL operation, respectively.

3.3 *Wallet Creation and Purchase of Solana Token from Binance*

In general, cryptocurrency Wallets are available in software or hardware versions. Although each type of Wallet works slightly differently, they are all designed to allow you to securely access your cryptocurrencies.

Fig. 16 Compilation of the various libraries and dependencies for SPL operation



```
   Compiling unicode-xid v0.2.3
   Compiling crunchy v0.2.2
   Compiling base64 v0.13.0
   Compiling getrandom v0.1.16
   Compiling byteorder v1.4.3
   Compiling crossbeam-utils v0.8.11
   Compiling lazy_static v1.4.0
   Compiling opaque-debug v0.3.0
   Compiling itoa v1.0.3
   Compiling block-padding v0.2.1
   Compiling rayon-core v1.9.3
   Compiling wasm-bindgen-shared v0.2.82
   Compiling rustversion v1.0.9
   Compiling either v1.8.0
   Compiling fnv v1.0.7
   Compiling bumpalo v3.11.0
   Compiling feature-probe v0.1.1
   Compiling keccak v0.1.2
   Compiling percent-encoding v2.1.0
   Compiling regex-syntax v0.6.27
   Compiling wasm-bindgen v0.2.82
   Compiling arrayref v0.3.6
   Compiling pin-project-lite v0.2.9
    Building [=>                           ] 43
```

What makes these wallets different from conventional ones is that they do not actually contain the cryptocurrencies, but exclusively the public and private key information needed to make cryptocurrency transactions. The actual cryptocurrencies are found on the blockchain [22].

In general, cryptocurrency wallets use two types of keys: public and private keys. Public keys function similarly to a bank account number. The public key is a long string of alphanumeric characters that can be shared with third parties, such as a cryptocurrency exchange, without compromising the security of the Wallet. This key allows transactions to be made to receive cryptocurrencies, often using an address associated to the Wallet, which represents a compressed version of that Wallet's public key.

Private keys, on the other hand, should never be revealed to anyone. Through your private key it is possible to access cryptocurrencies present on the blockchain. In other word, if someone were to be able to access your private keys, they would also have access to the cryptocurrencies in your Wallet.

Solana provides a specific tool to generate the two keys, satisfying the BIP39 implementation model during creation [28, 29]. As already mentioned, each wallet has its own private key, a 256-bit long code string that is difficult for the human mind to memorise. The BIP39 mnemonic phrase is a list of words from the English dictionary that, if entered and processed correctly, make it possible to obtain the private key, enabling the retrieval of a cryptographic wallet. In more detail, the process consists of associating each word with a set of randomly generated numbers using entropy, which, subjected to a PBKD2 function with the optional addition of a password, produce a 64-byte string called a seed. The seed makes it possible to create an extended master key for a deterministic hierarchical wallet obtaining the private key (See Fig. 17).

The Solana Program Library command launched by the CLI allows the creation of a wallet by fulfilling the BIP39 implementation model, but also the execution of a validator and the possibility of staking tokens (the act of locking cryptocurrencies to receive rewards). All these operations support the input of key pairs via seed phrases [28, 29].

The creation of a new Solana wallet was done through the SPL command, which generated the public key of the wallet and its seed phrase for retrieval. As can be seen in the Fig. 18, there are no Solana tokens on the account and therefore no operation can be performed.

The purchase of Solana was made through Binance. Founded in 2017, Binance is a company that operates a cryptocurrency exchange platform. It allows the purchase via FIAT coins (government-issued currency that is not backed by a physical commodity)

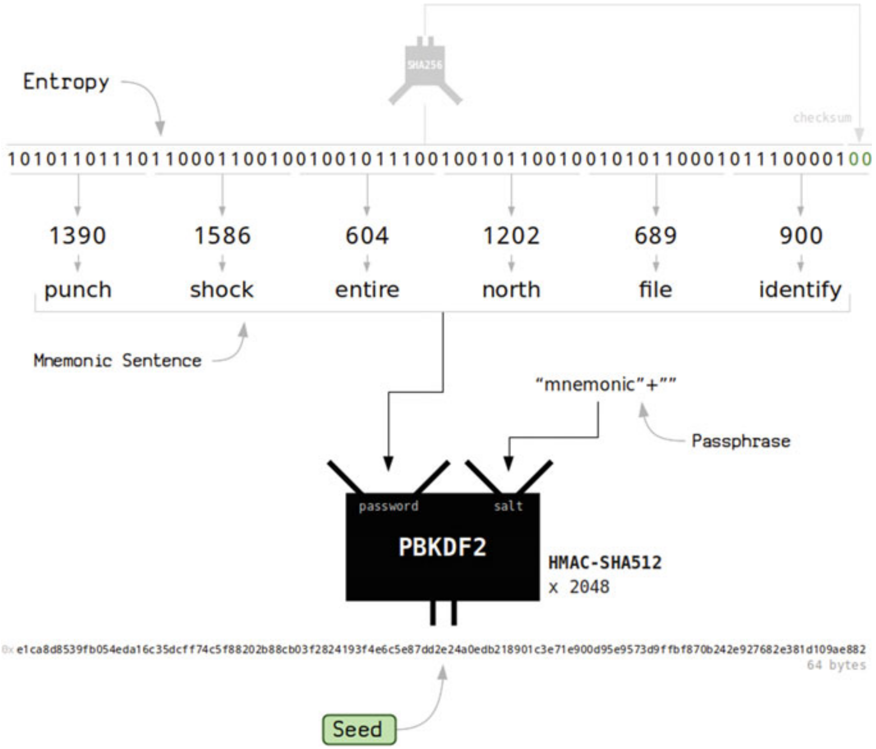
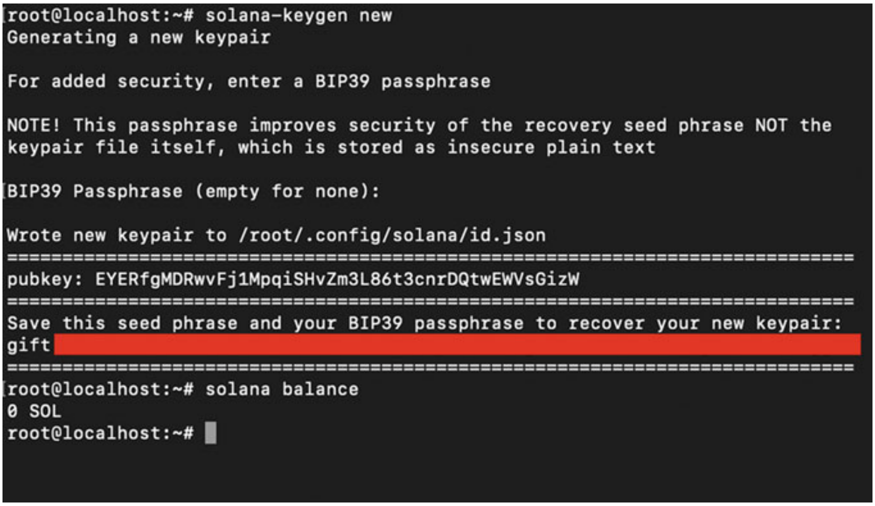


Fig. 17 Operation diagram of BIP39 [18]



```
root@localhost:~# solana-keygen new
Generating a new keypair

For added security, enter a BIP39 passphrase

NOTE! This passphrase improves security of the recovery seed phrase NOT the
keypair file itself, which is stored as insecure plain text

BIP39 Passphrase (empty for none):

Wrote new keypair to /root/.config/solana/id.json
=============================================================================
pubkey: EYERfgMDRwvFj1MpqiSHvZm3L86t3cnrDQtwEWVsGizW
=============================================================================
Save this seed phrase and your BIP39 passphrase to recover your new keypair:
gift [redacted]
=============================================================================
root@localhost:~# solana balance
0 SOL
root@localhost:~# ▌
```

Fig. 18 Creation of a new Solana wallet and balance control

of tokens and to perform staking operation that has been discussed above. As of May 2021, it recorded the world's largest digital asset market in terms of trading volume [19]. The purchase of Solana took place using the SOL/BUSD trading pair. The value recorded by Solana's token during the purchase was BUSD 31.13 per unit. The amount needed to feed the SPL transaction fees is minimal, and is around 0.005 per transaction. It follows that the quantity to be purchased should be around 0.10 SOL in order not to run into problems when conducting multiple transactions.

This quantity of Solana Token will then need to be transferred to the Wallet generated just above, to proceed with the creation of a Solana Token and NFTs that will then be associated with NFC tags. Figure 19 shows the purchase operation on the Binance platform of SOL tokens.

Once the tokens have been purchased, they are deposited on the Binance's personal Wallet. It is then necessary to transfer the newly obtained funds to the Wallet generated on the Debian 11 machine. To do this, Binance provides a feature for transferring money/cryptocurrencies from one Wallet to another, in the same way as when making a wire transfer between two banks. The only value needed is the address of the beneficiary, which in the Blockchain world is represented by the public key. The operation takes a few minutes to complete and is obviously carried out entirely via blockchain technology and without passing through any third party.

In the next figure, the data required to execute the transaction between the two accounts are entered. This means selecting the type of currency, entering the Wallet's public key data, setting the blockchain network on which the transaction is to take place, and deciding on the amount to be sent to the beneficiary.

In this scenario, the input data reports the above, the sending of a small amount (0.10 SOL) of Solana Token using the Solana blockchain since the related wallet

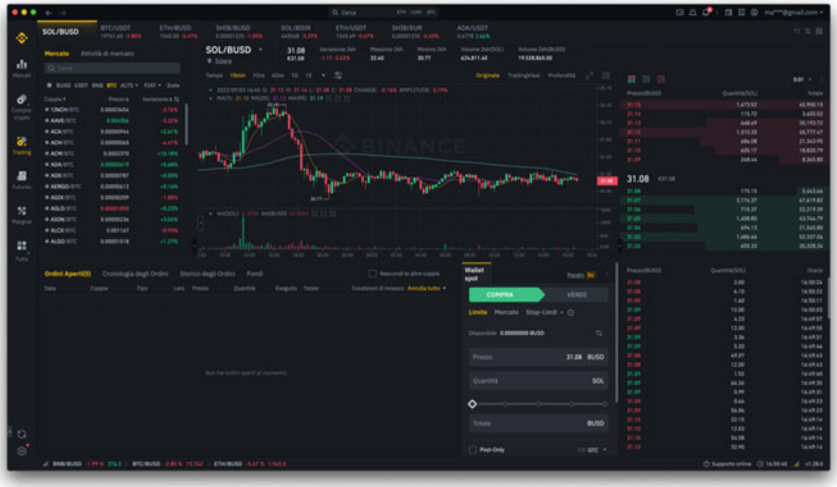
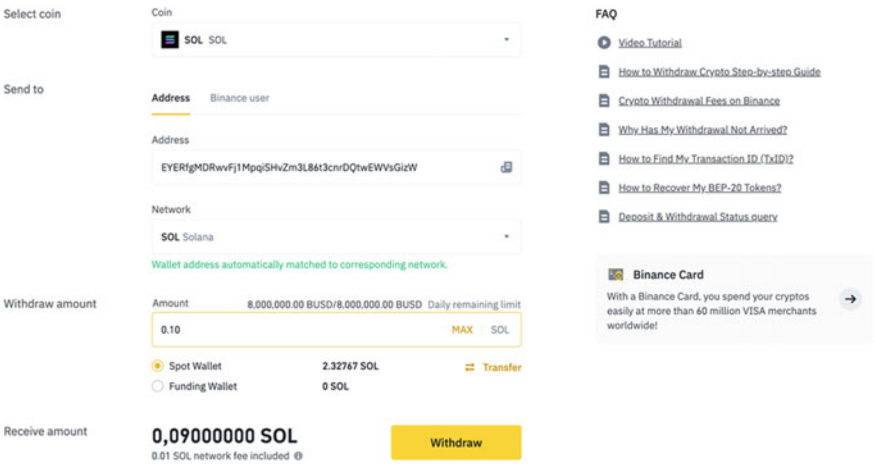


Fig. 19 Purchase of Solana tokens on Binance

belongs to the same network, and the input of the public key of the Wallet (EYERfgMDRwvFj1MpqiSHvZm3L86t3cnrDQtwEWVsGizW) generated with the Solana Program Library command.

Again, a small fee is charged to proceed with the operation (Fig. 20).

After waiting the required time for the transaction to be written inside a block and validated within the blockchain and then approved by the members of the ledger, the confirmation that the transaction was successful is obtained.



Select coin

Coin: SOL SOL

Send to

Address | Binance user

Address: EYERfgMDRwvFj1MpqiSHvZm3L86t3cnrDQtwEWVsGizW

Network: SOL Solana

Wallet address automatically matched to corresponding network.

Withdraw amount

Amount 8,000,000.00 BUSD/8,000,000.00 BUSD Daily remaining limit

0.10 MAX SOL

● Spot Wallet 2.32767 SOL ⇄ Transfer

○ Funding Wallet 0 SOL

Receive amount

0,09000000 SOL

0.01 SOL network fee included

Withdraw

FAQ

Video Tutorial

How to Withdraw Crypto Step-by-step Guide

Crypto Withdrawal Fees on Binance

Why Has My Withdrawal Not Arrived?

How to Find My Transaction ID (TxID)?

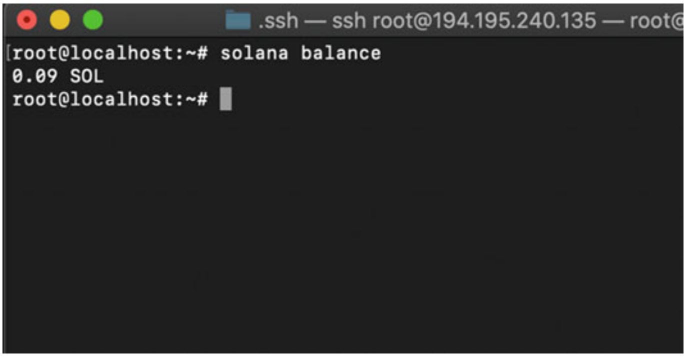
How to Recover My BEP-20 Tokens?

Deposit & Withdrawal Status query

Binance Card

With a Binance Card, you spend your cryptos easily at more than 60 million VISA merchants worldwide!

Fig. 20 Entering data on the Binance platform related to the transaction



```
[root@localhost:~# solana balance
0.09 SOL
root@localhost:~#
```

Fig. 21 Different wallet credit than in Fig. 18

Checking on the Debian 11 machine it is possible to see via command:

solana balance

The Wallet credit has risen to 0.09 SOL (0.10 SOL - 0.01 fee) (Fig. 21).

3.4 Creation of a Token Within Solana Blockchain

In the previous section, the prerequisites for the creation of a solana token were discussed, from the creation of a wallet to the purchase of SOL tokens to feed the operations that will be shown in the following paragraphs.

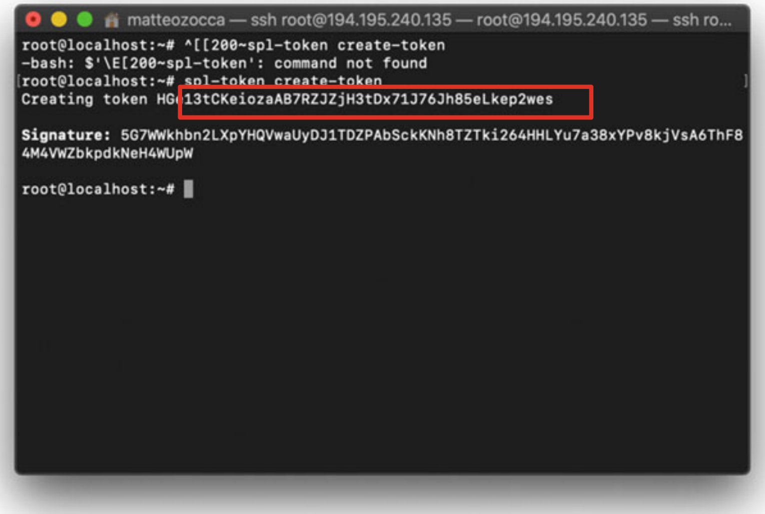
Although not necessary to achieve the objectives of this dissertation, the creation of a token allows the project to be given an identity by enabling the receipt of funding from external entities and creating its own currency for possible future developments. Creating a new token is done very easily using the Solana Program Library's create token command, as shown below.

spl-token create-token

As mentioned earlier, tokens created through the SPL interface are resources within the Solana ecosystem, meaning they benefit from the performance and scalability of the Solana network [7].

When a new token is created, its address is generated in order to identify it in the blockchain, as shown in Fig. 22.

After a new token is created, it is necessary to create an account that can act as a container for that currency. In Solana Network, when encountering the scenario of transferring tokens generated by the SPL, the sender's account and the beneficiary's account should not be the Wallet address, but respectively the two accounts associated with the token. The associated account therefore represents the container of that


matteozocca — ssh root@194.195.240.135 — root@194.195.240.135 — ssh ro...

```
root@localhost:~# ^[[200~spl-token create-token
-bash: $'\E[200~spl-token': command not found
root@localhost:~# spl-token create-token
Creating token HGc13tCKeiozaAB7RZJZjH3tDx71J76Jh85eLkep2wes

Signature: 5G7WWkhbn2LXpYHQVwaUyDJ1TDZPAbSckKNh8TZTki264HHLYu7a38xYPv8kjVsA6ThF8
4M4VWZbkpdkNeH4WUpW

root@localhost:~#
```

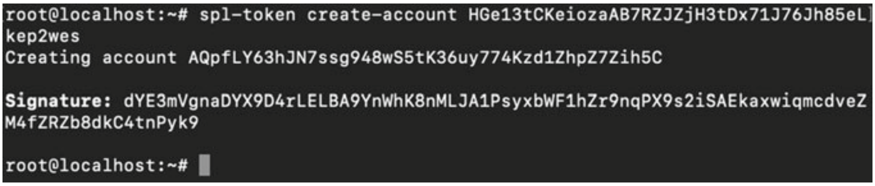
Fig. 22 Creating a new token with the Solana Token Library

token, as according to Solana's logic of operation, the transaction can be performed respecting these requirements.

According to Solana's official documentation [28, 29], this solution was implemented because a user could own several accounts of the same token, which therefore corresponds to the same mint, making it difficult for other transfer users to understand which among them is the actual address for receiving the currency, and above all, further complicating the management of the token. The desire to design an associated account allows the implementation of a deterministic method starting with the address of the user's main system and the address of the mint to generate a key that identifies the main account of the token in question. The latter is referred to as the Associated Token Account.

In addition, this method allows for more flexibility in the system, as a user can send the token created with SPL to a recipient even if the latter does not have a specific account for that mint and thus that token. If one does not have the associated account, an associated account will be created for the receiving accounts and a fee of 0.02 SOL will be charged to the recipient. For this to work properly, the wallet must have enough SOL.

If the recipient has to fund it first, this makes airdrop campaigns (a marketing move whereby coins are sent for free or in exchange for certain services to wallets in order to promote awareness of a new virtual currency) difficult, but also more generally speaking makes token transfers more mechanical. The Associated Token



```
root@localhost:~# spl-token create-account HGe13tCKeiozaAB7RZJZjH3tDx71J76Jh85eL
kep2wes
Creating account AQpfLY63hJN7ssg948wS5tK36uy774Kzd1ZhpZ7Zih5C

Signature: dYE3mVgnaDYX9D4rLELBA9YnWhK8nMLJA1PsyxbWF1hZr9nqPX9s2iSAEkaxwiqmcdveZ
M4fZRZb8dkC4tnPyk9

root@localhost:~#
```

Fig. 23 Creation of a new Associated Token Account

Account programme allows the sender to create the associated token account for the recipient so that the token transfer works.

Creating an address is always done using the SPL interface, and can be done via the following command:

spl-token create-account HGe13tCKeiozaAB7RZJZjH3tDx71J76Jh85eLkep2wes

The creation of a new Associated Token Account is associated with the address of the token that has just been created (Fig. 23).

All these operations mentioned above can be verified through Solana Explorer [8], the official Solana website that allows users to search for transactions, coins and accounts on the various Solana clusters.

A user can verify the successful creation of a transaction by consulting it.

As seen in the previous paragraphs, during the creation of a new token, an address is subsequently generated for it, which is useful for its identification within the blockchain. By entering this address into the search field of Solana Explorer, it is possible to obtain the coin's details.

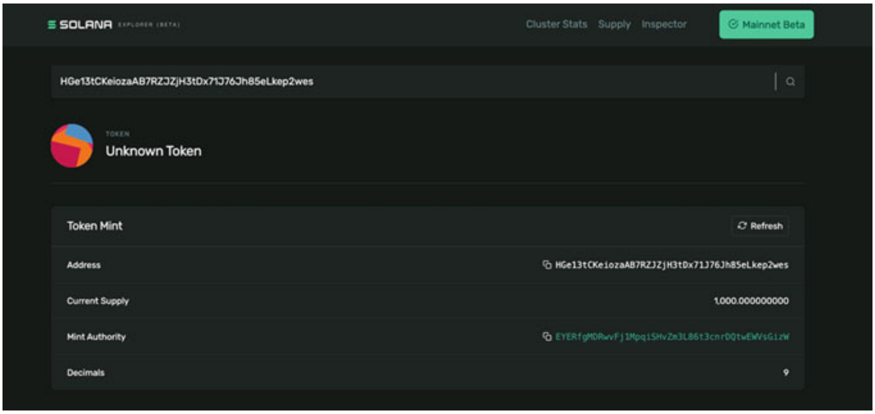
The information reported in the page are the Current Supply, which corresponds to the number of tokens that have been minted, the Mint Authority, which is indicated with the address of the account that can mint other coins, and decimals that represents the maximum number of digits that the Current Supply can reach (See Fig. 24).

Moreover, since Solana is a blockchain, it is possible to trace all history of transactions (Fig. 25).

According to the Solana documentation [30], it is possible to register the name of the token with its image within the Solana blockchain so that it is recognised in the Solana explorer. This operation requires quite some time to complete, and since it is not necessary for the purposes of the thesis, it has been omitted. More information can be found on the Github page.

3.5 *Creation of an NFT Within Solana Blockchain*

NFT stands for non-fungible digital token and represents a digital object that is not interchangeable. Fungible objects in the real world include banknotes: a 100 euro banknote will have the same value as another, swapping them gives the same object. Even the shares of a company are interchangeable. A work of art like Leonardo's



HGe13tCKeiozaAB7RZJZjH3tDx71J76Jh85eLkep2wes

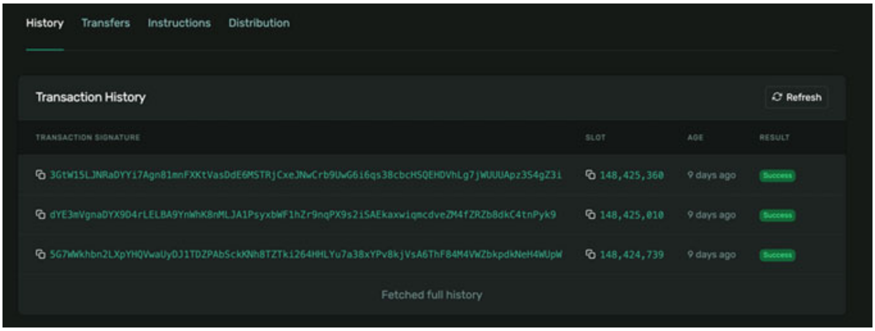
TOKEN

Unknown Token

Token Mint

Address	HGe13tCKeiozaAB7RZJZjH3tDx71J76Jh85eLkep2wes
Current Supply	1,000.000000000
Mint Authority	EYERfgMDRwvFj1MpqiSHvZm3L86t3cnrDQtwEWVsGizW
Decimals	9

Fig. 24 Token information. Note how the address within the search field corresponds to that in Fig. 22



Transaction History

TRANSACTION SIGNATURE	SLOT	AGE	RESULT
3GtW15LJNRaDYYi7Agn81mnFXKtVasDdE6MSTRjCxeJNwCrb9UwG6i6qs38cbcHSQEHDVhLg7jWUUUApz354gZ3i	148,425,360	9 days ago	Success
dYE3mVgnaDYX9D4rLELBA9YnWhK8nMLJA1PsyxbWF1hZr9nqPX9s2iSAEkaxwiqmcdveZM4fZRZb8dkC4tnPyk9	148,425,010	9 days ago	Success
5G7WWkhbn2LXpYHQVwaUyDJ1TDZPAbSckKNh8TZTki264HHLYu7a38xYPv8kjVsA6ThF84M4VWZbkpdkNeH4WUpW	148,424,739	9 days ago	Success

Fetched full history

Fig. 25 History of transactions each marked by the unique signature

Mona Lisa is a unique object. Reproductions may be sold, but the original will always retain a very high economic value.

Generally speaking, NFTs are mainly used to identify the ownership of digital works within the blockchain, in fact the common belief is to associate NFTs with the world of digital collectibles creation or exchange.

However, it is wrong to limit this new technology exclusively to this, the NFT represents a new approach to prove ownership of an asset, a kind of unique digital certificate that indicates the ownership of a product. This means that anything even in the real world can be represented through the non-fungible token, and their ownership through the NFT.

A prime example is the French brandy producer Hennessy (owned by the LVHM group, AURA's main supporter). For each bottle of Cognac it has associated a corresponding NFT. The bottles in question are high value, aged for some time in limited series (around 200 worldwide). At the time of purchase, the NFT copy of the bottle is purchased, which establishes its ownership. However, the actual bottle is not sent to the purchaser, but remains stored by Hennessy in its warehouse in pristine condition. If a buyer decides to consume this high-value bottle, the associated NFT will automatically be burnt and consequently the bottle will be sent, and it lose all its value. The important part is that a customer can choose to keep the NFT, so that it can be used as an investment asset, increasing its value over time, all while letting Hennessy store the bottle and without worrying about shipping [10].

This example was mentioned in order to comment on the use-case scenario covered by this research. Although in both cases, an NTF solution is implemented associated with a tangible physical product in the real world, in the first scenario only the NFT related to the bottle is sold and exchanged, but without the involvement of the latter. The second case treated in this research was, the user buys the luxury good or high fashion dress directly in the real world. This means that the actual product is traded and sold and not exclusively the NFT. For this reason, a method is needed to connect the two worlds, the real and the virtual, respectively, and it is thought that the application of an NFC tag could result in a viable solution which it will be discussed in more detail in Chap. 4.

The procedure for creating a new NFT on the Solana network is similar to that used when creating a new token. The interface to be used in the CLI is still the Solana Program Library, and the commands to be run are also the same, with the exception of a few things that will now be explained.

To create a new Non-Fungible Token comes using the create-token command, but unlike before a parameter is added indicating the number of digits the current supply can maximum have, in this case 0 since the NFT must be unique.

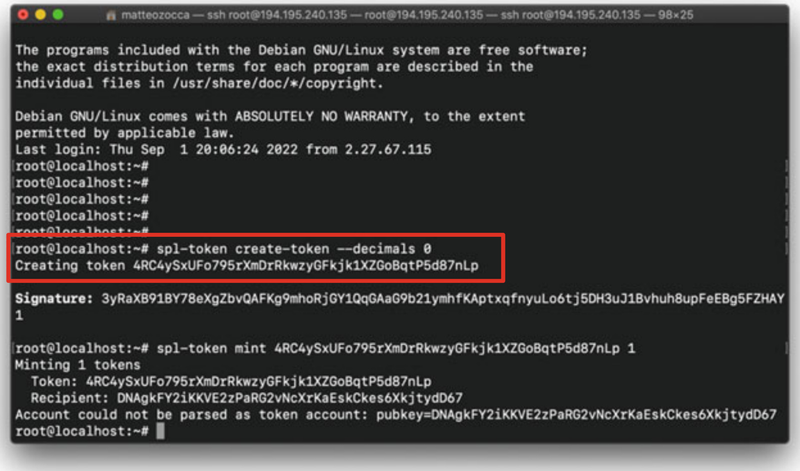
As can be seen in the lower part of Fig. 26, mint is not possible since there is no Associate Account Token related to that NFT. This means that the creation process respects the same order as that of creating a new token.

Therefore, it is necessary to create a new account related to the address of the NFT, mint only one NFT in the Associate Token Account, and then disable the minting capability of the latter (see Fig. 27).

Similar to the token created in the previous section, NFTs being present on the Solana network can also be tracked through Solana Explorer (Fig. 28).

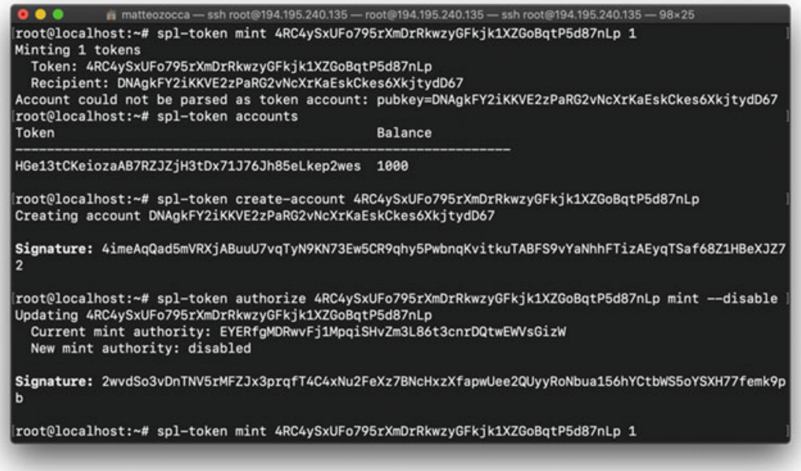
4 System and Technologies Used

In the previous chapter, an in-depth description of the simulation environment was provided, explaining step by step the procedures required for creating a new token and creating an NFT. This section will instead explain why the Solana Blockchain was chosen over Ethereum, how it is so high-performing, fast and inexpensive as far as fees are concerned, and above all, a small explanation of the nfc tags that will be used in the next chapter, necessary to associate the real luxury good with its NFC counterpart in the Solana network.


matteozocca — ssh root@194.195.240.135 — root@194.195.240.135 — ssh root@194.195.240.135 — 98×25

```
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Thu Sep  1 20:06:24 2022 from 2.27.67.115
root@localhost:~#
root@localhost:~#
root@localhost:~#
root@localhost:~#
root@localhost:~#
root@localhost:~# spl-token create-token --decimals 0
Creating token 4RC4ySxUFo795rXmDrRkwzyGFkjk1XZGoBqtP5d87nLp

Signature: 3yRaXB91BY78eXgZbvQAFKg9mhoRjGY1QqGAaG9b21ymhfKAptxqfnyuLo6tj5DH3uJ1Bvhuh8upFeEBg5FZHAY
1

root@localhost:~# spl-token mint 4RC4ySxUFo795rXmDrRkwzyGFkjk1XZGoBqtP5d87nLp 1
Minting 1 tokens
  Token: 4RC4ySxUFo795rXmDrRkwzyGFkjk1XZGoBqtP5d87nLp
  Recipient: DNAgkFY2iKKVE2zPaRG2vNcXrKaEskCkes6XkjtydD67
Account could not be parsed as token account: pubkey=DNAgkFY2iKKVE2zPaRG2vNcXrKaEskCkes6XkjtydD67
root@localhost:~# 
```

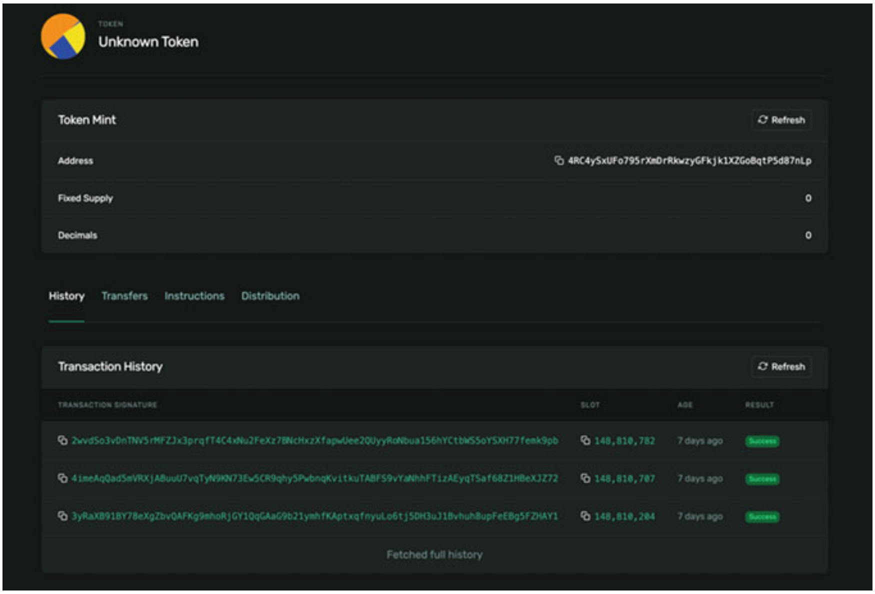
Fig. 26 Creation of a new NFT with corresponding address below


matteozocca — ssh root@194.195.240.135 — root@194.195.240.135 — ssh root@194.195.240.135 — 98×25

```
root@localhost:~# spl-token mint 4RC4ySxUFo795rXmDrRkwzyGFkjk1XZGoBqtP5d87nLp 1
Minting 1 tokens
  Token: 4RC4ySxUFo795rXmDrRkwzyGFkjk1XZGoBqtP5d87nLp
  Recipient: DNAgkFY2iKKVE2zPaRG2vNcXrKaEskCkes6XkjtydD67
Account could not be parsed as token account: pubkey=DNAgkFY2iKKVE2zPaRG2vNcXrKaEskCkes6XkjtydD67
root@localhost:~# spl-token accounts
Token                                         Balance
---------------------------------------------------------------
HGe13tCKeiozaAB7RZJZjH3tDx71J76Jh85eLkep2wes  1000

root@localhost:~# spl-token create-account 4RC4ySxUFo795rXmDrRkwzyGFkjk1XZGoBqtP5d87nLp
Creating account DNAgkFY2iKKVE2zPaRG2vNcXrKaEskCkes6XkjtydD67

Signature: 4imeAqQad5mVRXjABuuU7vqTyN9KN73Ew5CR9qhy5PwbnqKvitkuTABFS9vYaNhhFTizAEyqTSaf68Z1HBeXJZ7
2

root@localhost:~# spl-token authorize 4RC4ySxUFo795rXmDrRkwzyGFkjk1XZGoBqtP5d87nLp mint --disable
Updating 4RC4ySxUFo795rXmDrRkwzyGFkjk1XZGoBqtP5d87nLp
  Current mint authority: EYERfgMDRwvFj1MpqiSHvZm3L86t3cnrDQtwEWVsGizW
  New mint authority: disabled

Signature: 2wvdSo3vDnTNV5rMFZJx3prqfT4C4xNu2FeXz7BNcHxzXfapwUee2QUyyRoNbua156hYCtbWS5oYSXH77femk9p
b

root@localhost:~# spl-token mint 4RC4ySxUFo795rXmDrRkwzyGFkjk1XZGoBqtP5d87nLp 1
```

Fig. 27 Deactivating the mint of the Associate Token Account

Solana presents itself as a decentralised blockchain built to enable scalability and usability of decentralised applications (DApps).



Unknown Token

Token Mint

Address 4RC4ySxUFo795rXmDrRkwzyGFkjk1XZGoBqtP5d87nLp

Fixed Supply 0

Decimals 0

Transaction History

TRANSACTION SIGNATURE	SLOT	AGE	RESULT
2wvdSo3vDnTNV5rMFZJx3prqfT4C4xNu2FeXz7BNcHxzXfapwUee2QUyyRoNbua156hYCtbWS5oYSXH77femk9pb	148,810,782	7 days ago	Success
4imeAqQadSmVRXjABuuU7vqTyN9KN73Ew5CR9qhy5PwbnqKvitkuTABFS9vYaNhhFTizAEyqTSaf68Z1HBeXJZ72	148,810,707	7 days ago	Success
3yRaXB91BY78eXgZbvQAFKg9mhoRjGY1QqGAaG9b21ymhfKAptxqfnyuLo6tj5DH3uJ1BvhuhBupFeEBg5FZHAY1	148,810,204	7 days ago	Success

Fetched full history

Fig. 28 Note how the NFT is identified by checking that the value of decimals is zero

Some characteristics of Solana as a decentralised digital ecosystem are:

Solana's scalability and costs: the project developers, in explaining what Solana is, state that their decentralised network guarantees a cost per transaction of less than one cent (USD 0.01) for both developers and application users.

Speed without drops: the time to create a block on Solana's blockchain is just 400 ms, compared to 15 s for Ethereum, or two and a half minutes for the Litecoin blockchain, and compared to 10 min for Bitcoin. The designers also believe that as the speed of the hardware increases, the speed of their network will also increase further in the future.

Combined PoH and PoS consensus: Solana is based on a dual consensus model, on the one hand the proof-of-history (PoH) devised by its creator, Anatoly Yakovenko, which aims to guarantee greater scalability, and on the other hand the proof-of-stake (PoS) which with staking incentivised validators guarantees security on the blockchain.

Solana Cluster: the system of validators is divided into clusters and is called the Solana Cluster. The objective of this 'body' is to ensure that client transactions pass on the blockchain without interruption and at the same time guarantee the management and integrity of the Solana ledger. Multiple clusters can co-exist on the Solana blockchain.

4.1 Solana Consensus Algorithm

Proof-of-Stake and Proof-of-History (PoH) are combined in Solana to create a whole new hybrid consensus mechanism. PoH enables an extremely fast blockchain while maintaining its decentralised security.

On Solana, the SHA256 algorithm is used to hash all events and transactions. This function is then used to take an input and create a unique result that is very difficult to predict. The output of a transaction it is used as input for the next hash. As a result, the order of the transactions is updated in the hashed output.

This hashing operation produces a long unbroken chain of hashed transactions. Without the use of a traditional timestamp, this function generates a distinct, verifiable sequence of transactions that a validator adds to a block. Validators can quickly determine the elapsed time because hashing takes a certain amount of time to complete.

Assume we have three transactions, X, Y and Z. Each of these transactions is processed by Solana in order using its Proof-of-History consensus protocol. Then, the transaction and the function's internal clock are sent as input to PoH, so that it can generate the hash-encrypted version of the transaction, allowing it to be measured objectively:

PoH(X, TIMESTAMP 0) → hash: encrypted version of A on timestamp 0
PoH(Y, TIMESTAMP 1) → hash: encrypted version of B on timestamp 1
PoH(Z, TIMESTAMP 2) → hash: encrypted version of C on timestamp 2.

The special feature of this method is that it provides an objective measure, as each transaction is recorded with its timestamp. This implies that each transaction must have occurred, as is the order in which each transaction occurred. If, for example, transaction Y was entered at timestamp 0, the entire blockchain would be affected [33] (Fig. 29).

Because of this security objective, there is no need for humans to supervise the validation. This makes it much faster than PoW and PoS: in fact, Solana reaches a transaction speed of up to 50,000 transactions per second (TPS) where Bitcoin with Proof-of-Work reaches between 5 and 7 TPS and Ethereum with PoS reaches around 30 TPS. It is worth noting that Ethereum's Proof-of-Stake aims for a much higher TPS and will probably reach it in the future.

4.2 NFC—How It Works and Which Type to Use

NFC stands for Near Field Communication and means, literally, proximity communication. NFC is an evolution of RFID technology. It is also called RFID HF (High Frequency) because of its operating frequency of 13.56 MHz. NFC technology enables secure wireless connectivity between two devices, with the associated exchange of data.

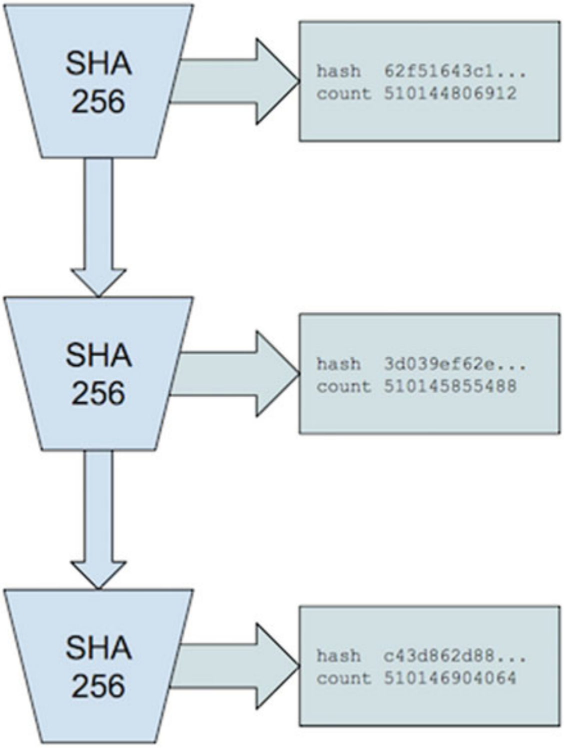


Fig. 29 Proof of history sequence [33]

NFC technology has 3 types of functionality:

1. The exchange of information via Peer-to-Peer (P2P) between 2 devices, safely and quickly. In the case of smartphones, simply bring them close and give the transfer command. Security is given precisely by the proximity (max. 3–4 cm) that the devices must maintain.
2. The simulation of a smart card, via the Host Card Emulation (HCE) protocol, also enables fast and secure payments with your smartphone.
3. The reading and writing of NFC tags, i.e. RFID transponders capable of storing information and interacting with NFC devices.

The NFC Data Exchange Format (NDEF), created by the NFC Forum specifically for programming NFC tags, consists of a number of distinct commands, known as ‘standard’ commands. In most cases, it is not necessary to install any kind of programme on a smartphone for it to read and execute these kinds of commands. iPhones are an exception. The following standard commands are:

- open link in general or query an API
- open any type of application
- sending or receiving text messages and email
- initiate a call

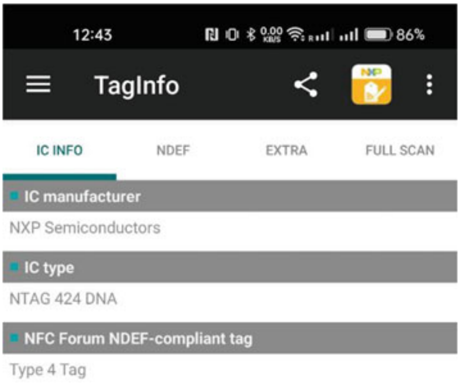
- show a text message
- save a V-Card contact
- start an application (does not work on iOS)

If the content of the chip is not protected by encryption, the content is ‘in the clear’, meaning that anyone scanning the tag with their smartphone, or an NFC reader can read the content. To defend against this type of attack, it is necessary to purchase a chip that supports encryption. Chips with this function are listed below, in ascending order of security of the supported cryptographic methods:

- MIFARE Classic (CRYPTO01—Not secure as it was hacked in 2008)
- MIFARE® DESFire EV1/EV2/Light (DES, 2K3DES, 3K3DES, AES)
- MIFARE Plus/ICODE® DNA (AES 128 bit)
- MIFARE Ultralight C (3DES)
- NTAG413 DNA/NTAG424 DNA (AES-based CMAC)

At the implementation level of this project, nine NTAG 424 DNA type tags were purchased at a price of around £9, as shown in Fig. 30 (each of them therefore cost around £1, but it is possible to find them for less, especially if one buys in bulk).

Fig. 30 9 tags 38 mm NFC Sticker Tag with White PVC NTAG 424 DNA



IC manufacturer

NXP Semiconductors

IC type

NTAG 424 DNA

NFC Forum NDEF-compliant tag

Type 4 Tag

Fig. 31 NFC tag information scanned via NPC's TagInfo application from Android phone

To get more information about the NTAG device, it is possible to download the official application from: Play Store: https://play.google.com/store/apps/details?id=com.nxp.taginfolite&hl=en_US&gl=US App Store https://apps.apple.com/us/app/nfc-taginfo-by-nxp/id1246143596 of NXP Semiconductors, the company that produces these two types of NFC tags (Fig. 31).

4.3 NTAG 424 DNA Versus NTAG 213 (Most Common)

Standard NFC chips, such as NXP's NTAG 213, allow data such as a URL link to be stored in the user's memory. Although these chips can be used to identify a product or item, there is nothing to prevent duplication of the data on another tag and in hundreds of counterfeit products. The code is static and never changes, and the same problem clearly occurs with QR codes (Fig. 32).

Authentication chips, such as NXP's NTAG 424, work differently: a unique dynamic code is generated with each scan, which means that the copied data will be old and out of date. This system offers a significantly higher level of protection against counterfeiting than standard NFC chips. To be clear, NFC authentication tags have been around for a long time and have been used in transportation and ticketing for many years. The difference lies in how the functionality can be accessed: the old chips encrypted the information inside the chip, and special codes, applications, or readers were required to access the data. The new generation of chips dynamically replaces the authentication data in the URL link presented when scanning the tag, which means that no special application or software is needed to read the tags and verify their authenticity.

When authentication chips are encoded, they store not only a link to the URL, but also a unique key. The unique key is hidden inside the memory and is not accessible. When the tags are scanned, an encryption algorithm takes the scan count, ID and

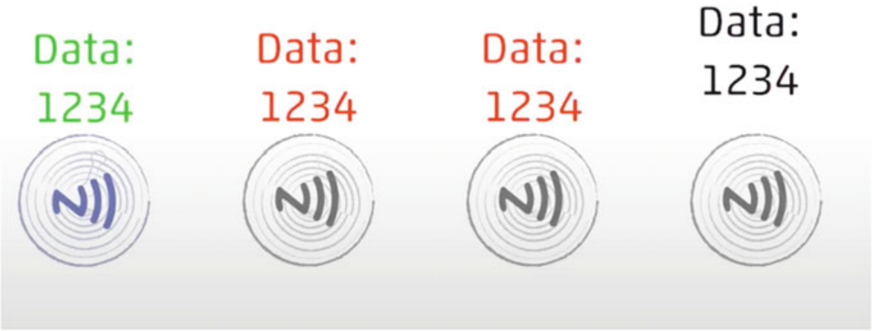


Fig. 32 Static data can be cloned to other NFC NTAG 213 tags [27]

possibly some other data from the chip, and combines it with the unique key to generate an authentication code. When encoding the tag, it is possible to set the key as a parameter within our URL, and that is therefore visible to the server. In other words, the chip during scanning, automatically processes the URL by dynamically replacing the authentication code. Note that the key itself is never displayed, only the result of the algorithm that uses it. This combination of tag, ID, scan count and authentication code can be verified on the destination server, which also stores a copy of the key and undertakes the same process. Once the scan count and then the corresponding authentication code have been used, the authentication server marks it as no longer valid, which means it cannot be used again. This happens with each scan, because as the scan count increases, the data used in the algorithm changes and a new unique authentication code is generated each time (Fig. 33).

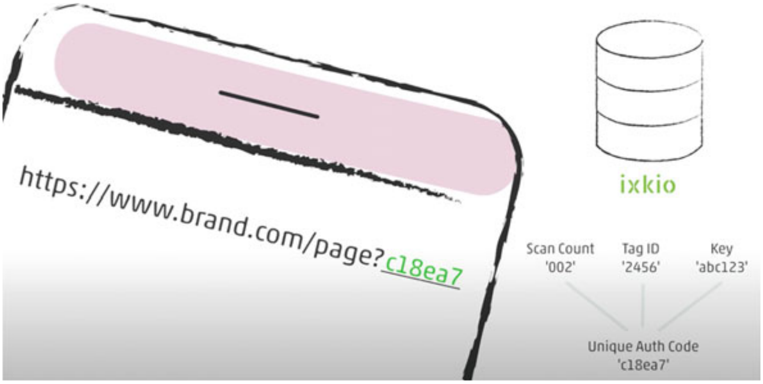


Fig. 33 NTAG 424 authentication diagram with the server [27]

4.4 Ixkio Platform

Ixkio is a pay-as-you-go NFC tag management platform designed to simplify the control of QR and NFC codes, allowing the user or company greater flexibility and scalability at all times. The platform is operated by Seritag, the world's leading NFC provider. Ixkio is designed to enable large-scale control of standard NFC tags, providing the necessary tools to support the management of up to 100,000 tags, but at the same time allowing it to scale at any time.

According to the official Ixkio website [17], some of the operations this platform provides are listed below:

- Redirection, Direct Response or API: Integrating Ixkio's services within the company's portal or application.
- Powerful rules system: Redirections or responses managed by creating ad hoc rules for each of them for both QR codes and NFC tags.
- Tamper and Auth: full support for the latest features of NFC tags, such as DNA authentication found in NTAG 424.
- Scan Tracking: Scan tracking functionality for each tag with scan counter information, last scan and more.
- Direct response: control of tag authentication or identification directly from the ixkio platform without implementing an infrastructure behind it.
- Limitless growth: Extreme scalability in adding additional tag slots when required.

As mentioned above, this service is chargeable and requires a monthly subscription that starts at £5 and can go up to £45 per month depending on the plan chosen and the services included. The plan selected is the basic £5 plan because it is considered sufficient to achieve the objectives of the thesis. The configuration of the service will be discussed in the next chapter, where it will be used to implement the anti-counterfeiting protection mechanism via the NFC tag.

5 NFC and NFT Anti-counterfeiting Mechanism

In the previous section, the services and technologies used in the implementation part of the research were discussed. In the following sections, the anti-counterfeiting mechanism will be developed step by step, discussing analytically and in depth its implementation and the realization of a simulation environment capable of protecting luxury goods from the counterfeit market.

The basic idea is as follows: initially set up links from Ixkio for authentication and identification of the NFC tag on the portal, set up redirection to the Solana Explorer page related to the NFC associated with the product (obviously this is a test environment, with more time and funding resources one could certainly customize the page related to the NFT and include information about the history of the product). Then programme the code URL on the NFC tag NTAG 424 and test its functionality. As a further experiment, it is possible to clone the contents of the NFC to test a counterfeiting attack and verify the results.

5.1 Configuring the Authentication Link Through Ixkio

In this initial step, the link for authenticating the NTAG 424 tag on the Ixkio portal is configured. This means that the link that will be generated will be exclusively to the tag with which it will be associated. Any possible clone or counterfeit tag, even if it were to reach into the content of the authentic tag and replicate it, will be blocked by the Ixkio platform and will not proceed with the redirection.

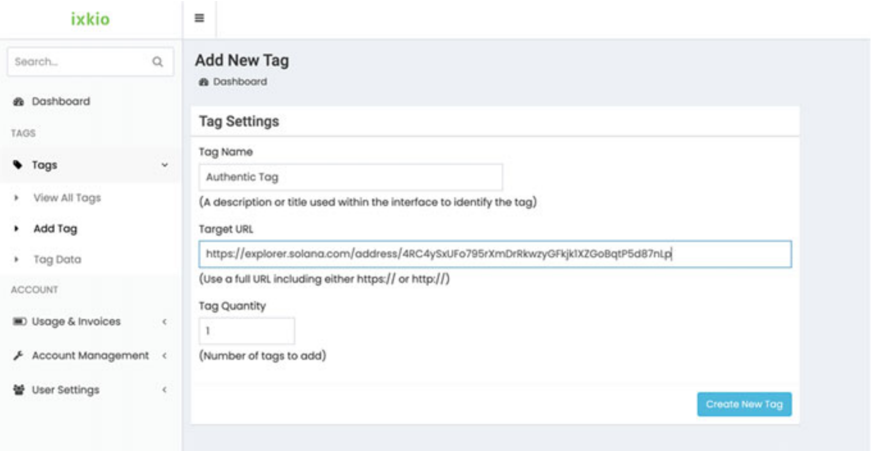
In order to configure a new encoded URL, Ixkio's Add Tag function is used.

As shown in Fig. 34, data is entered into the various text fields for the creation of a new Tag. The first field is for the name to identify the chip within the portal, which has been named 'Authentic Tag' for simplicity. The second field is the most important as it indicates the value to which the tag will point, i.e. the Target URL. Here again, for simplicity's sake, the Solana Explorer URL of the NFT created in Chap. 2 and shown in Fig. 28 has been inserted. However, a parenthesis must be opened, as future developments here may focus on the customisation of the NFT page associated with the physical product. This requires the setting up of APIs and Server backends capable of answering the https calls of the NTAG 424s, verifying their authentication, and finally sending them back to a customised page with all the information relating to the NFT, which is equivalent to the physical product but in the blockchain network. This series of operations, which are time-consuming and require considerable funding, have been skipped as they are out of the study context of this thesis. The development environment that will be proposed is similar to a real model for analysing the behaviour of this mechanism, and was therefore not elaborated on further due to time constraints. This discussion will be addressed in more detail towards the end of the dissertation.

Finally, the last field required is the number of tags to be overwritten, so that a link is generated for each of them.

The portal will then generate a link querying the Ixkio API by passing the NFT code as a parameter. This call will allow the tag to authenticate itself and receive the redirect on the NFT page.

All that remains now is to download the CSV file containing all the information to be programmed on NTAG 424 from the port. The information contained in the file is shown in Fig. 35, including the most important value, which is the encoded URL (Fig. 36).



Tag Settings

Tag Name

Authentic Tag

(A description or title used within the interface to identify the tag)

Target URL

https://explorer.solana.com/address/4RC4ySxUFo795rXmDrRkwzyGFkjk1XZGoBqtP5d87nLp

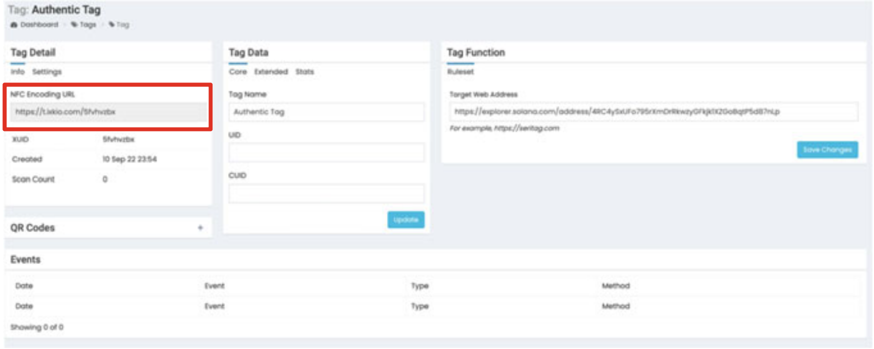
(Use a full URL including either https:// or http://)

Tag Quantity

1

(Number of tags to add)

Fig. 34 Page for entering new tag information



Tag Detail

NFC Encoding URL

https://t.ixkio.com/Sfvhvzbx

XUID	Sfvhvzbx
Created	10 Sep 22 23:54
Scan Count	0

Tag Data

Tag Name

Authentic Tag

UID

CUID

Tag Function

Target Web Address

https://explorer.solana.com/address/4RC4ySxUFo795rXmDrRkwzyGFkjk1XZGoBqtP5d87nLp

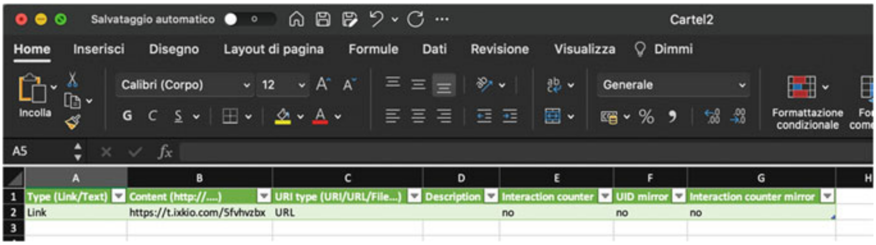
For example, https://seritag.com

Events

Date	Event	Type	Method
Date	Event	Type	Method

Showing 0 of 0

Fig. 35 Page with the tag details. The encoded URL generated by Ixkio is highlighted



	A	B	C	D	E	F	G
1	Type (Link/Text)	Content (http://....)	URI type (URI/URL/File...)	Description	Interaction counter	UID mirror	Interaction counter mirror
2	Link	https://t.ixkio.com/Sfvhvzbx	URL		no	no	no
3							

Fig. 36 Information contained within the csv file

5.2 Programming of NTAG 424 DNA

NFC is written using an application available free of charge in both the app store and the playstore (download link: https://play.google.com/store/apps/details?id=com). This application, also developed by NXP, allows NFC tags to be written and read without additional extensions directly from the phone. By uploading the CSV file, the data required for programming the NTAG 424 will be written.

The two images below show the steps to select tag writing via CSV file (Figs. 37 and 38).

At this point the CSV file generated just before by the Ixkio portal will be selected. The application will automatically load all the information in the file and it autonomy compiling the data. Note how the content is the Encoder dedicated to the tag itself (see Fig. 39).

Fig. 37 Application home screen

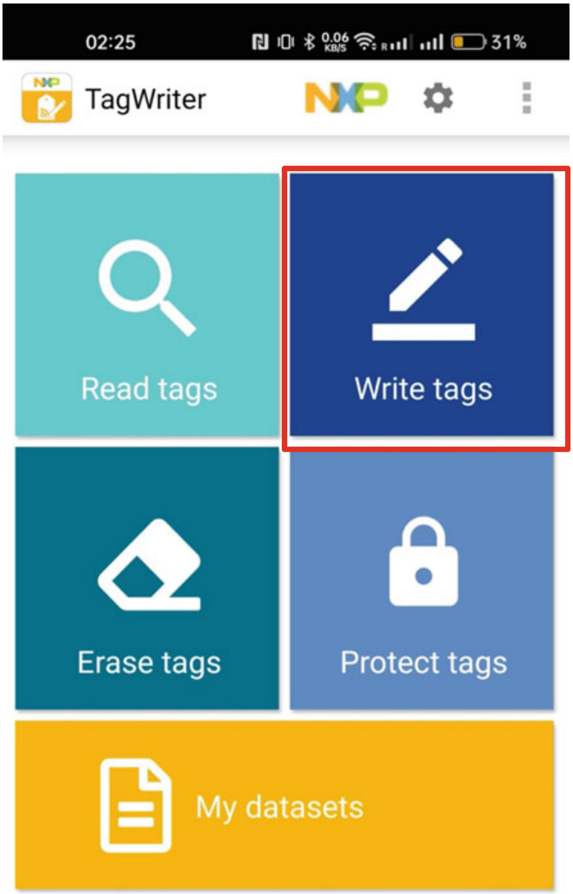
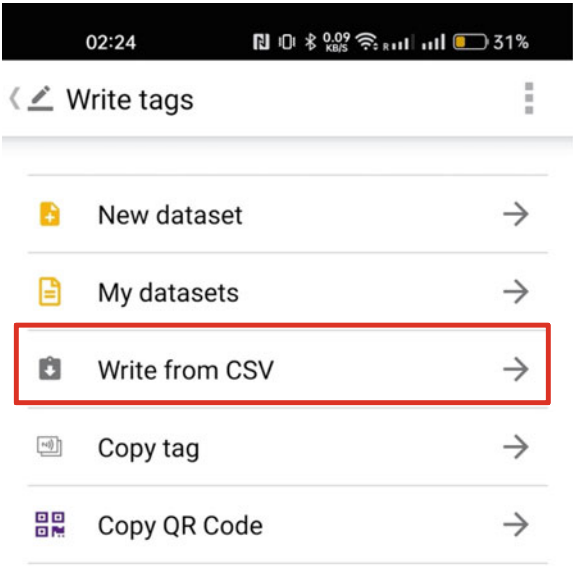


Fig. 38 Possible writing options



The last screen shows the outcome of writing the tag, indicating the content of the previous tag, which in this case is empty, and the newly overwritten content, which is equivalent to the Encoded URL (Fig. 40).

To actually verify the tag writing, an Iphone 13 without any kind of additional software but only with the NFC option enabled is used, and it is seen to be able to read the contents of the tag, automatically opening the link from safari (Figs. 41 and 42).

5.3 *Attempt to Cloning the Authentic NTAG 424 DNA*

Let assume that an attacker manages to read the content of the authentic tag and writes the Encoded URL on a new tag. The implemented system must prevent this type of attack, as it would be easy to clone a luxury good and make it appear authentic.

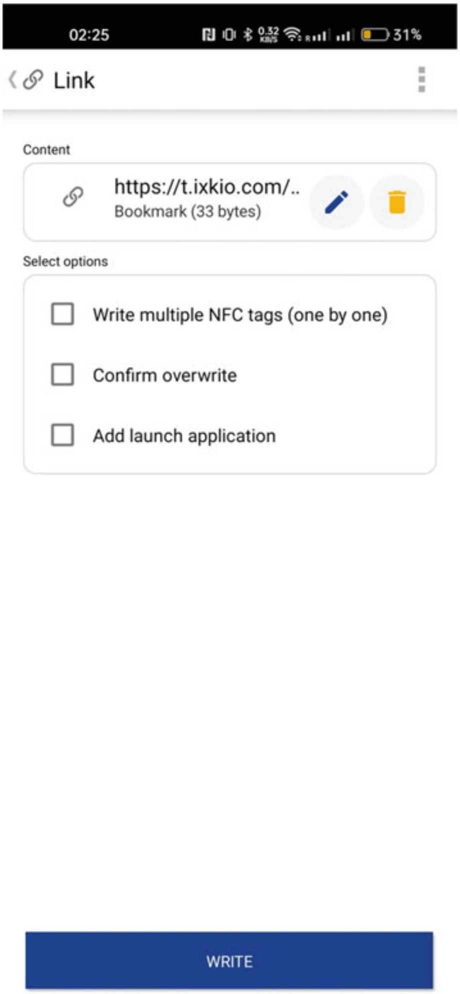
Cloning the content of an NFC 424 tag involves reading it first. This means using the TagWriter application but in read mode. The content of the chip can be read in plain text, and the link saved to write it to a new, non-authentic Tag.

As shown in Fig. 43, the plain-text encoded URL is present. An attacker can then write the following URL:

https://t.ixkio.com/5fvhvzbx

Into another NFC device. The attacker will therefore create a new dataset, select the link option, and overwrite the URL Encoding on the new NFC Tag (Figs. 44, 45 and 46 respectively).

Fig. 39 Data preview screen before writing



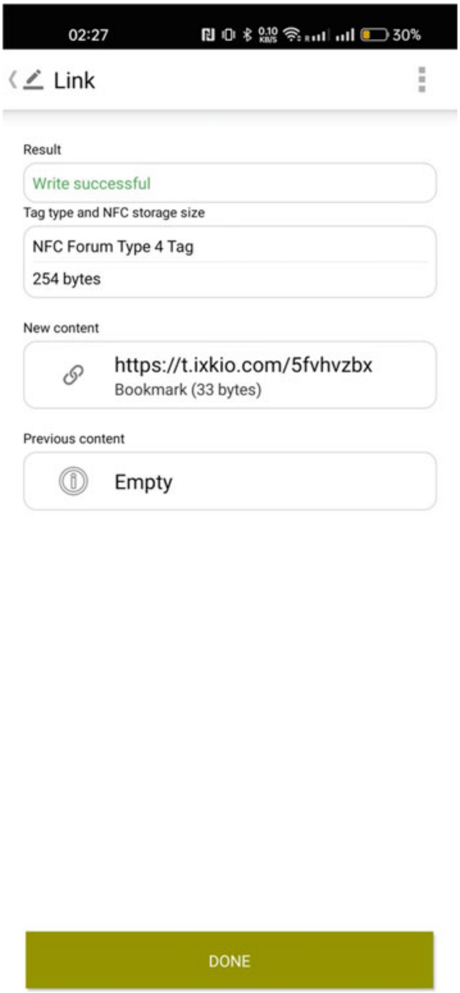
https://t.ixkio.com/..
Bookmark (33 bytes)

□ Write multiple NFC tags (one by one)
□ Confirm overwrite
□ Add launch application

A user who reads the inauthentic tag will not be able to view the Solana Explorer page of the NFT associated with the product, thus realising that the product is counterfeit and therefore a fake (Fig. 47).

As can be seen in Figs. 48 and 49, the URL is identical to the one configured in Fig. 40.

The Ixkio platform correctly blocked the redirection due to failed chip authentication.



Result

Write successful

Tag type and NFC storage size

NFC Forum Type 4 Tag

254 bytes

New content

https://t.ixkio.com/5fvhvzbx
Bookmark (33 bytes)

Previous content

Empty

Fig. 40 Tag writing summary

6 Full Implementation and Results

The final test consists of placing these two tags, the authentic and the cloned one on a dress. The tags can be incorporated into a dress easily, as there are different formats, both adhesive and non-adhesive, and they can also be resistant to washing. The experiment involves having two T-shirts, one belonging to a luxury brand and the other a counterfeit copy. With a bit of imagination, and also to simplify the experiment, a single T-shirt is used with two tags, the authentic one and the cloned one. The scenario remains the same, the outcome of the actual functioning of the NFC/NFT mechanism to protect against counterfeiting remains valid, even if it is a simulation environment (Fig. 50).

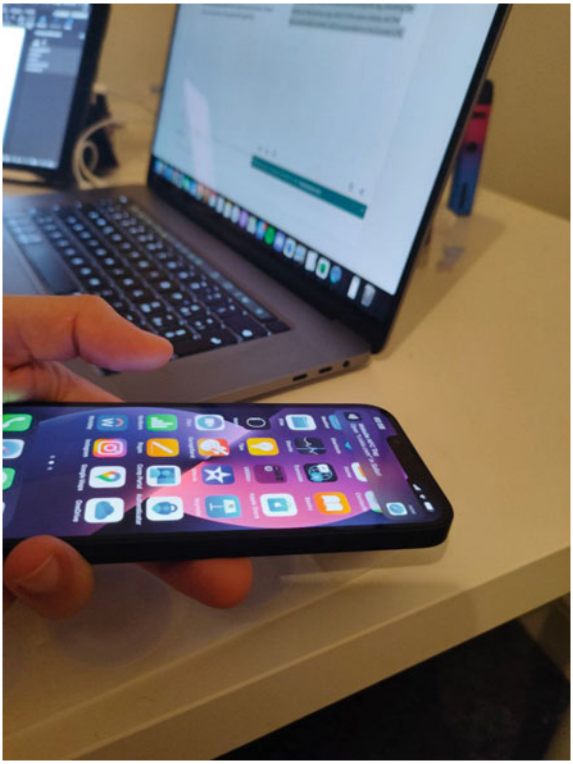


Fig. 41 The popup appears automatically by bringing the phone closer to the tag

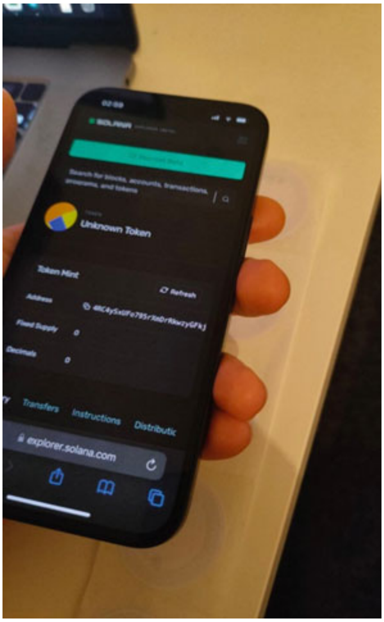
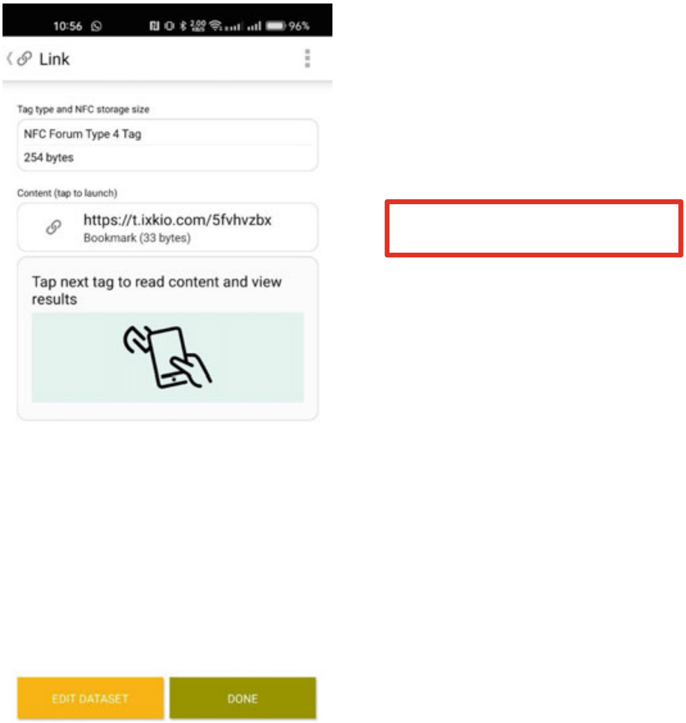


Fig. 42 Clicking on the popup directly opens safari to the NFT-related page of Solana Explorer. In all this, Ixkio acting as an intermediary, remains invisible to the user's eyes throughout the process



Tag type and NFC storage size

NFC Forum Type 4 Tag

254 bytes

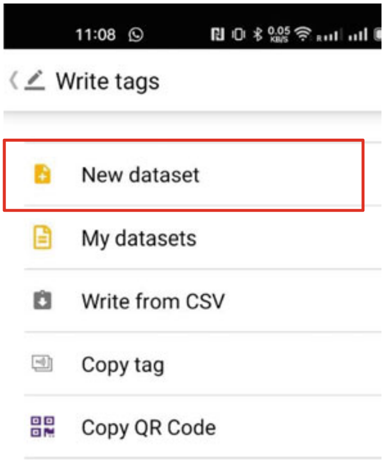
Content (tap to launch)

https://t.ixkio.com/5fvhvzbx
Bookmark (33 bytes)

Tap next tag to read content and view results

Fig. 43 Reading the authentic NFC tag

Fig. 44 Selecting a new dataset



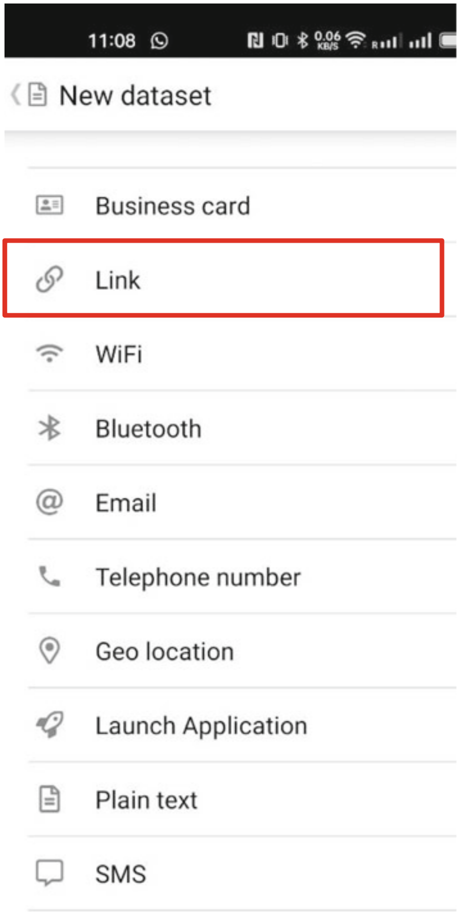
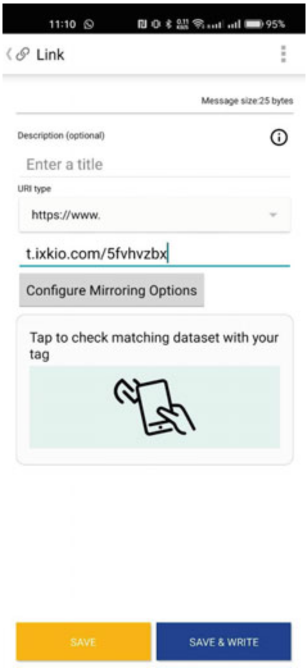


Fig. 45 Selecting of a new URL dataset mode

Thus, abstracting the experiment, the user has two T-shirts, each associated with an NFC tag. In other words, the two NFCs are placed on two different T-shirts, both aesthetically identical, and the user has to recognise the genuine product from the counterfeit one. The material, fabrics and embroidery are made in both T-shirts with great care and it is not possible to distinguish them.

The user places his or her phone on the tag associated with the authentic T-shirt, and actually verifies the presence of an NFT associated with it (Figs. 51 and 52).

In the first case, that of the authentic T-shirt, the link contained in the NFC tag is detected and, by clicking on the popup, the user has been redirected to the Solana Explorer page related to the NFT associated with the product. Everything worked correctly without any kind of problems (Figs. 53 and 54).



Message size:25 bytes

Description (optional)

Enter a title

URI type

https://www.

t.ixkio.com/5fvhvzbx

Tap to check matching dataset with your tag

Fig. 46 Writing of the encoded URL on the tag

In the second case, however, although the user's phone can detect the URL, upon opening from the browser, the user receives an error message caused by the server, which has not been found. This occurs because at the time of the request passed to the Ixkio API, the platform does not recognize the Tag and therefore does not forward the response to the user's phone.

As result, the user managed to identify the original product from the counterfeit one through this mechanism.

This research undertook to thoroughly analyse the various aspects of solving counterfeiting problems in luxury goods. The approach of using NFC and NFT tags in combination for the protection of a good proved to be valuable in many respects. However, certain caveats must be taken into account in order to consider it reliable and feasible in the real world. Through in-depth research into the analysis of the problem and the development of the simulation environment, a framework of best practices was drawn up to support future developments in the realisation of similar ecosystems focused on combating counterfeiting with these technologies.

The recommendations listed below can be considered good starting points for more substantial and elaborate projects, guidelines to support the practical implementation of the system thereby it can be considered safe and reliable. In other words, these are solutions adopted in the resolution of the proposed experiment,

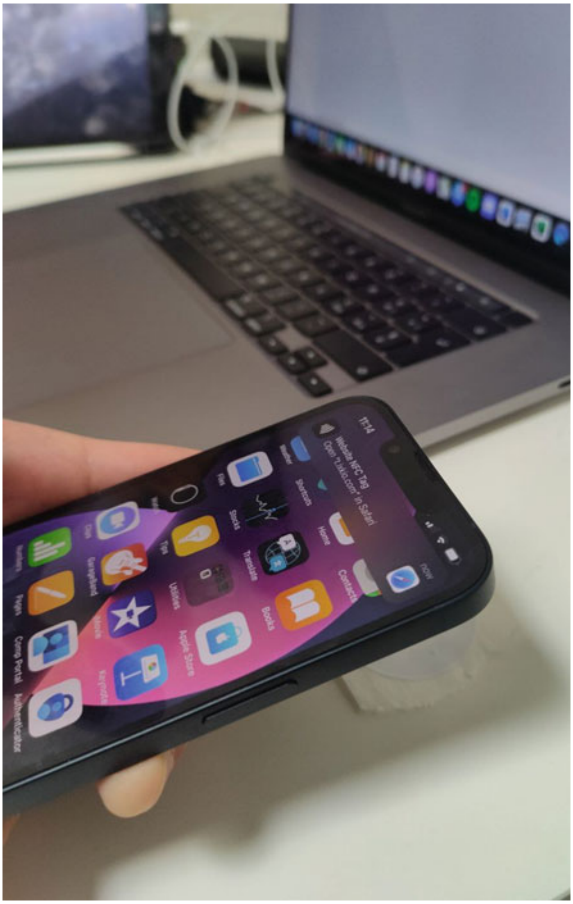
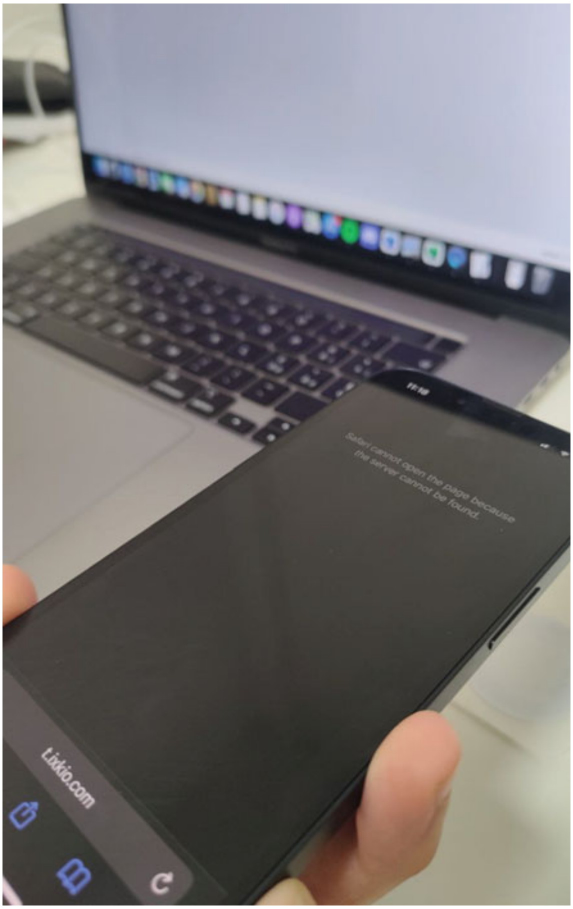


Fig. 47 Reading false NFC from Iphone 13

which are obviously relegated to a restricted context due to questions of time and funds, but which with a few adjustments can be considered valid for large-scale targeted projects.

Use authentication-protected tags: classic tags such as NTAG 210, NTAG 213 and NTAG 216 are not protected by encryption and therefore their content can be easily accessed and cloned on other products. This means that the use of encryption-protected tags such as NTAG 413 DNA and NTAG 424 (the one used in this project) is mandatory. In accordance with what was discussed in section above, a backend must be implemented in the system to save the non-accessible password of the Encrypted Tag, and then do all the necessary calculations to obtain the digest generated by the Tag at each scan, and authenticate it properly. The authentication of the NFC device



Safari cannot open the page because the server cannot be found.

Fig. 48 Safari is unable to open the Solana Explorer page

is a fundamental pillar for the security of the system, since a mismanagement of this procedure makes the correspondence between the NFC Tag and the NFT no longer unique, further worsening the degree of security. Two strangers might be unaware that their product points to the same NFT, leading them to believe that their luxury good is authentic.

Tag Protection: Although this aspect was not discussed in this research, the role of blocking tag overwriting plays a key role in protecting the system. This option, which is in fact a standard for most NFC produced by NXP and Mifare, ensures that a tag cannot be overwritten once the content has been inserted. This measure is very effective especially for all those devices that are easily accessible in public, such as luxury goods in shops.

Fig. 49 The link is identical to the authentic tag

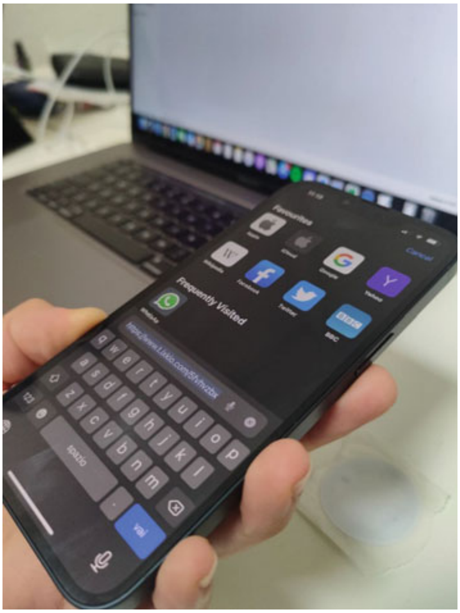
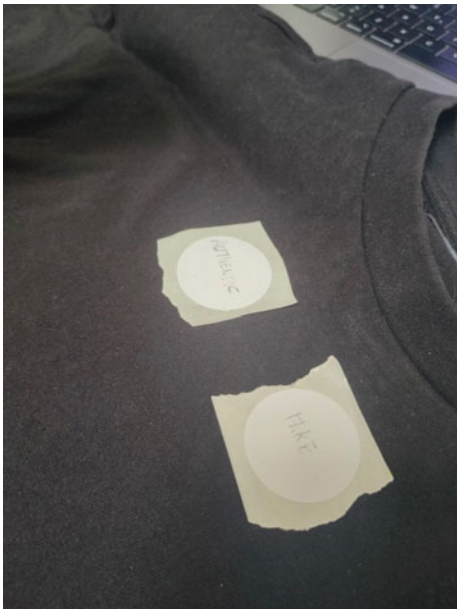


Fig. 50 T-shirt with two NFC tags: the first authentic and the second fake



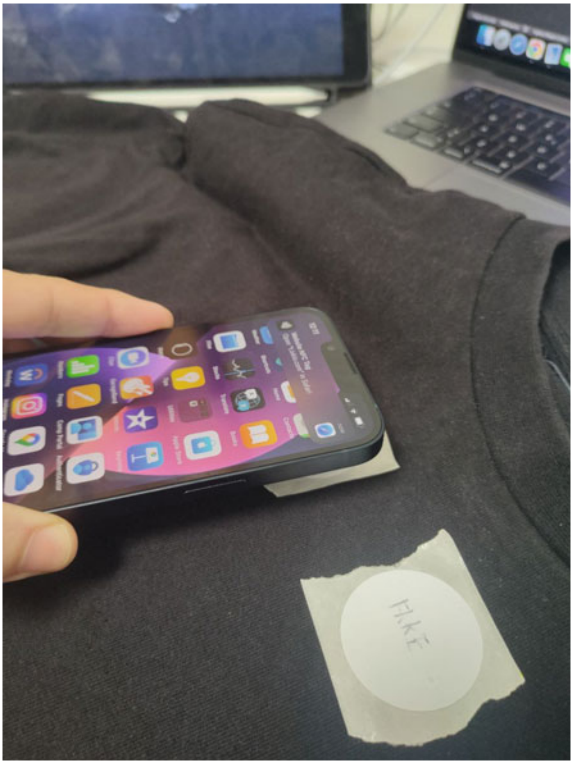


Fig. 51 The user approaches the phone to read the Authentic Tag

Logic of operation in the authentication process: This part was entrusted to the Ixkio platform, which also offers scanning and tracking services. However, especially when using uncoded tags, such as NXP's 213, verification is based on the UID (Unique IDentifier), which represents the unique number of the tag. The size of this field can vary from 4 bytes up to 7 bytes. For the latter, it is highly unlikely if not impossible to find two tags with the same UID, while for the former, it is already more likely. Moreover, with special devices it is possible to tamper with the UID of a tag, thus bypassing authentication. The authentication criteria must comply with what is said in Sect. 3.4, and must be used with Encrypted Tags, as recommended in point one of the framework.

NFT customization: registration of the NFT on Solana enables a better user experience of the entire ecosystem. Registering the name of the NFT on the Solana network, and setting up an image that represents the object it is associated with, staying true on color and shape, can help the user immediately understand whether the NFT is of the product in question. Otherwise, a substantial improvement would be to create a dedicated portal for NFTs that interfaces with Solana (or Ethereum depending on the project), containing all product information, from origin, to ownership transitions, etc.

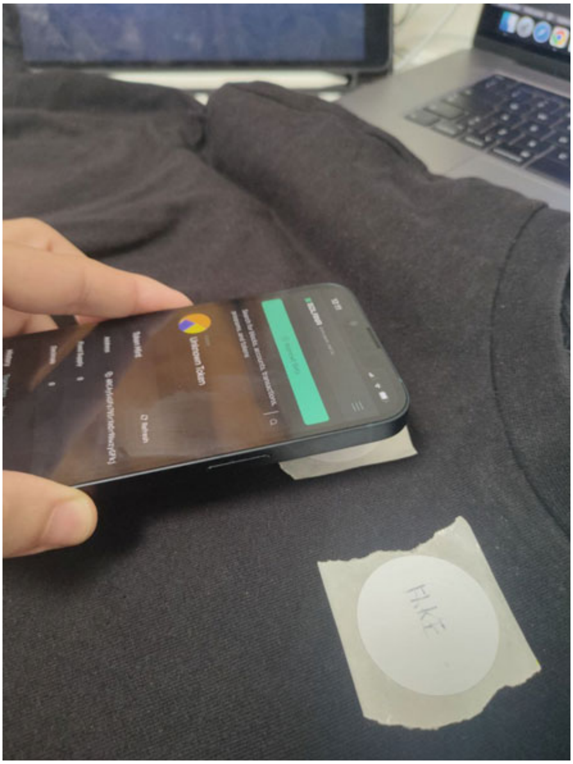


Fig. 52 The user is redirected to the page of the associated NFT

Integrity of data entered into the blockchain: it must be ensured that the people responsible for entering NFTs and thus product information are not operating with ulterior motives and that the data are not subject to tampering. The producing company must therefore implement a strict policy for controlling these parties to ensure the integrity of the data within the blockchain.

7 Conclusions and Future Work

Nowadays, there are several start-ups and consortia that have focused on implementing the following mechanism, but none of them contain information on how they are structured and how they analytically succeed in defending companies from the counterfeiting problem. The aim of this research is to fill the knowledge gap on this topic by setting up a functioning system and testing it in its configuration. It has proven to be functional in several respects, and with a few adjustments can be taken

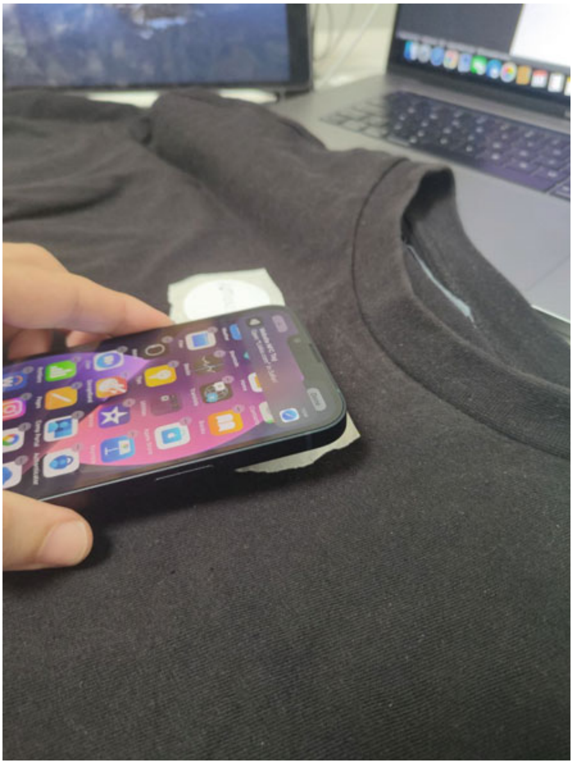


Fig. 53 The user approaches the phone to read the Fake Tag

to a larger scale. The system also allows it to be optimal for small and medium-sized companies, with an implementation cost that is not extremely high. Through the experiences made with the various experiments, best practices were drawn up: guidelines that can support the development of NFC/NFT anti-counterfeiting mechanisms. Future developments include a better study of NFC TAG authentication. In the research, this part was only dealt with theoretically, omitting the implementation, which was entrusted to the Ixkio platform. A further study to be undertaken is to export the model to the real world, monitoring its behaviour and keeping track of its functionality. Then, consult customers to assess the actual benefits and to obtain feedback aimed at improving the entire ecosystem.

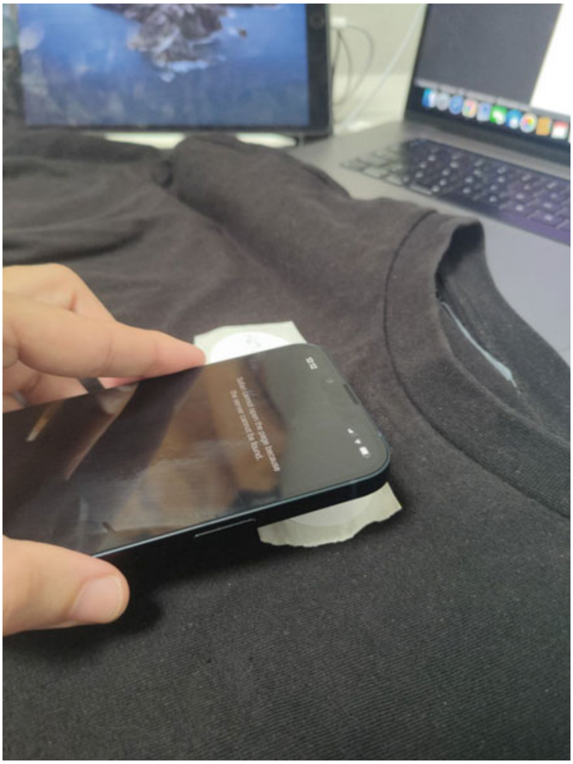


Fig. 54 The User gets an error message from Safari

References

1. AURA (2022) A revolution in the luxury industry. [Online] Available at: https://auraluxuryblockchain.com/. Accessed 10 July 2022
2. BCG (2019) Why luxury brands should celebrate the preowned boom. [Online] Available at: https://www.bcg.com/it-it/publications/2019/luxury-brands-should-celebrate-preowned-boom. Accessed 2022
3. Business of Fashion (2019) How luxury fashion learned to love the blockchain. [Online] Available at: https://www.businessoffashion.com/articles/technology/how-luxury-fashion-learned-to-love-the-blockchain/#:~:text=Amid%20growing%20concern%20about%20the,profit%20with%20the%20same%20goal. Accessed 10 July 2022
4. CNBC (2021) Cryptocurrency market value tops $2 trillion for the first time as ethereum hits record high. [Online] Available at: https://www.cnbc.com/2021/04/06/cryptocurrency-market-cap-tops-2-trillion-for-the-first-time.html. Accessed 10 July 2022
5. CNBC (2022) Alfa Romeo unveils new electric-hybrid SUV with NFT, blockchain technology. [Online] Available at: https://www.cnbc.com/2022/02/08/new-alfa-romeo-suv-equipped-with-nft-blockchain-technology.html. Accessed 10 July 2022
6. DocumentationRust (2022) Hello, Cargo!. [Online] Available at: https://doc.rust-lang.org/book/ch01-03-hello-cargo.html. Accessed 10 July 2022
7. Exodus (2022) Learn more about SPL tokens and the Solana ecosystem. [Online] Available at: https://support.exodus.com/article/1808-solana-ecosystem#supported-spl. Accessed 10 July 2021

8. Explorer (2022) Solana Explorer. [Online] Available at: https://explorer.solana.com/. Accessed 10 July 2022
9. Forbes (2019) Ford Motor Company launches blockchain pilot on IBM platform to ensure ethical sourcing of Cobalt. [Online] Available at: https://www.forbes.com/sites/rachelwolfson/2019/01/16/ford-motor-company-launches-blockchain-pilot-on-ibm-platform-to-ensure-ethical-sourcing-of-cobalt/?sh=535991c15a1d. Accessed 10 July 2022
10. Forbes (2022) Hennessy enters the NFT space with $226,000 release. [Online] Available at: https://www.forbes.com/sites/katedingwall/2022/01/10/hennessy-enters-the-nft-space-with-226000-release/. Accessed 10 Aug 2022
11. GBC (2018) The global brand counterfeiting report, s.l.: s.n
12. Globalnewswire (2022) Global luxury resale market report 2022: surge in the luxury goods E-commerce sales and increasing thrifters' demand for pre-owned luxury. [Online] Available at: https://www.globenewswire.com/en/news-release/2022/05/26/2451170/28124/en/Global-Luxury-Resale-Market-Report-2022-Surge-in-the-Luxury-Goods-E-commerce-Sales-and-Increasing-Thrifters-Demand-for-Pre-owned-Luxury.html#:~:text=The%20global%20luxury%20resale%2
13. Gray A (2018) How fake handbags fund terrorism and organized crime. s.l., s.n
14. IBM (2022) What is blockchain technology?. [Online] Available at: https://www.ibm.com/topics/what-is-blockchain. Accessed July 2022
15. ICF Yale (2018) The psychology behind why people buy luxury goods. [Online] Available at: https://www.investopedia.com/articles/personal-finance/091115/psychology-behind-why-people-buy-luxury-goods.asp. Accessed 10 July 2022
16. Insider (2021) Michael Dell says blockchain technology is 'underrated'. [Online] Available at: https://www.businessinsider.com/michael-dell-blockchain-is-underrated-but-will-pass-on-bitcoin-2021-10?r=US&IR=T. Accessed 10 July 2022
17. Ixkio (2022) Features. [Online] Available at: https://ixkio.com/. Accessed 10 Aug 2022
18. learn me bitcoin (2020) Mnemonic seed. [Online] Available at: https://learnmeabitcoin.com/technical/mnemonic. Accessed 10 July 2022
19. Ledesma L (2021) Binance extended crypto exchange dominance during may trading frenzy. [Online] Available at: https://www.coindesk.com/markets/2021/06/07/binance-extended-crypto-exchange-dominance-during-may-trading-frenzy/. Accessed 10 July 2022
20. Lim J (2021) Why luxury brands are embracing the resale revolution. [Online] Available at: https://www.theindustry.fashion/why-luxury-brands-are-embracing-the-resale-revolution/#:~:text=Estimated%20to%20be%20worth%20around,demand%20and%20digitisation%20of%20retail
21. Mansour K (2020) Early metrics-luxury brands using blockchain to fight counterfeiting. [Online] Available at: https://earlymetrics.com/luxury-brands-using-blockchain-to-fight-counterfeiting/. Accessed 10 July 2022
22. N26 (2021) What is a crypto wallet? [Online] Available at: https://n26.com/en-it/blog/what-is-a-crypto-wallet. Accessed 10 July 2022
23. Nakamoto S (2009) Bitcoin: a peer-to-peer electronic cash system. [Online] Available at: https://bitcoin.modeapp.com/bitcoin-white-paper.pdf
24. OECD (2016) Trends in trade in counterfeit and pirated goods. [Online] Available at: https://www.oecd.org/corruption-integrity/reports/trends-in-trade-in-counterfeit-and-pirated-goods. Accessed 1 July 2022
25. Precision (2022) Could blockchain revolutionize parcel shipping? [Online] Available at: https://www.fedex.com/content/dam/fedex/us-united-states/Compatible-Solutions/images/2019/Q2/Could_Blockchain_Revolutionize_Parcel_Shipping_V2_50457811.pdf
26. RUST (2022) A language empowering everyone to build reliable and efficient software. [Online] Available at: https://www.rust-lang.org/. Accessed 10 July 2022
27. Seritag (2022) NFC tag authentication explained. [Online] Available at: https://www.youtube.com/watch?v=ZFN881RKVZI. Accessed 10 Aug 2022
28. Solana Documentation (2022) Associated token account program. [Online] Available at: https://spl.solana.com/associated-token-account. Accessed 10 July 2022

29. Solana Documentation (2022) Paper Wallet. [Online] Available at: https://docs.solana.com/wallet-guide/paper-wallet. Accessed 10 July 2022
30. solana-labs/token-list (2022) Adding a new token. [Online] Available at: https://github.com/solana-labs/token-list. Accessed 10 July 2022
31. The Usenet Big-8 (2022) The Usenet Big-8 management board. [Online] Available at: https://www.big-8.org/wiki/Main_Page. Accessed July 2022
32. Walmart Global Tech (2022) Blockchain in the food supply chain—what does the future look like? [Online] Available at: https://one.walmart.com/content/globaltechindia/en_in/Tech-insights/blog/Blockchain-in-the-food-supply-chain.html
33. Yakovenko A (2017) Solana: a new architecture for a high performance blockchain v0.8.13. [Online] Available at: https://solana.com/solana-whitepaper.pdf. Accessed 10 Aug 2022

An Investigation into the State of Cybersecurity Preparedness with Respect to Operational Technology

Farouk Akrama and Hamid Jahankhani

Abstract The importance of software-level communication security in ICS is growing as these systems become more automated and connected to the outside world. This chapter provides a secure-by-design approach to ICS application development, where design-time abstractions known as secure links are used to meet criteria from security protocols like ISA/IEC 62443. Secure links are a proposed addition to an IEC 61499 design standard that makes it easy to integrate both lightweight and conventional security measures into software. Automatic compilation into completely IEC 61499-compliant software is possible for applications that use secure links. To keep up with this demand for greater adaptability. Nowadays, in the revolution of digitalization, automation plays significant role to achieve a sufficient level of security and reduce the use of both human resources and static processes. Therefore, it is crucial to model all security related capabilities and functionalities. In this chapter a unique requirements repository model for Industrial Control System that applies the LPGs (Labelled Property Graphs) to form and store standards based and system specific requirements using well-defined relationship types are highlighted. In addition, the researcher integrates the proposed requirements repository with the Industrial Control System design tools to determine requirements traceability. A wind turbine case study demonstrates the entire workflow within the proposed framework.

Keywords IEC 62443 · ISA/IEC 62443 International Electrotechnical Commission · ICS Industrial Control System · NIST National Institute of Standards and Technology

F. Akrama · H. Jahankhani (✉)
Northumbria University, London, UK
e-mail: Hamid.jahankhani@northumbria.ac.uk

H. Jahankhani and A. El Hajjar (eds.), *Wireless Networks*, Advanced Sciences
and Technologies for Security Applications,
https://doi.org/10.1007/978-3-031-33631-7_10

1 Introduction

Top-down analysis is not the only option, though; industry frameworks offer another perspective. A consensus amongst experts in a field is used to develop a "prototype" for a business in that field, and this is what industry frameworks give. In general, the frameworks identify typical functional and business process breakdowns that may correspond to capabilities. It may be more comprehensive and unbiased than a value chain tailored to a particular company. Naturally, every organisation will be unique due to its own specific set of circumstances and methods of operation, and these distinctions may provide a competitive edge in some sectors.

The capabilities of an industrial framework tend to coincide with their respective implementations in commercial enterprise software and outsourced services, which is a definite plus. A well-defined standard value chain should not be abandoned in favour of an industrial framework; rather, it can provide even more insight into the description of shared capabilities when used together. It is possible that a company's data model is part of the framework for its industry. This paper serves as a stepping stone to addressing security by design approaches by describing security capability levels and requirements across the Industrial Control System zones. Moreover, the paper examines why it is important to have a standard, enterprise-wide logical data model by following an adapted case study method. A safety critical wind turbine system was deployed and modelled to examine several security issues of monitoring and managing cybersecurity requirements in Industrial Control System. There are two primary arguments in favour of seriously considering the use of a structural data model early in the process of creating a CBA for such a given business. To begin with, the CBA transformation will be delayed and the cost of getting a model will be more than the cost of developing a suitable corporate logical data model. Second, there will be fewer data transformation issues when exchanging data between services because the framework data model will likely be similar with competitive software systems and technical service as well as regulatory requirements.

2 Literature Review

Different networks system like control processing, manufacturing of robotic system, automation system for both home and office, intelligent system on transportation and aircraft, spacecraft in advance. Sometime these types of network system are typically made up of a significant number of interconnected devices, the management of which can either be centralised or decentralised, depending on the requirements of the application. Routable data communications protocols like Ethernet (IEEE 802.3) and Wi-Fi are typically placed in homes and workplaces, but due to modern demands for adaptability, decentralisation, simple work for continuity, and reduced minimal cost for operations, their incorporation into network control systems has become increasingly common. Because of this shift, maintaining a high level of security within industrial control systems is now more vital than ever. Confidentiality is given the utmost priority in traditional information technology (IT) security regulations, while network availability receives the least amount of consideration [1]. In contrast, critical infrastructure ICSs and ISCI (ISA Security Compliance Institute) must always maintain both high availability and operational resilience. This is necessary for a variety of reasons, including those pertaining to the economy, the environment, the safety of humans, and the security of the nation. It is unacceptable, with regard to many different procedures, to suffer a decrease in performance for the sake of security [2]. In order to arrive at such a conclusion, a risk–benefit analysis must first be performed on each system. It is necessary to incorporate security safeguards in a manner that will preserve the integrity of the system both when it is functioning normally and when it is under attack from a computer network.

Alber and Prince [3] emphasised that industrial control system security needs to incorporate both network security and features of robust physical architecture (such as redundancy and physical adaptability) to maintain the appropriate level of system availability. A comprehensive risk assessment and methodical system engineering are the processes that are used to establish such requirements. Based on the concepts of precise measurement science, the Industrial Control System (ICS) testbed provides guidance on how to implement security in an ICS via the course of testing.

According to Green et al. [4], the purpose of the Industrial Operation System (ICS) Cyber Security Test Bed is to showcase the value of security in a variety of contexts, such as the management of a chemical plant, the dynamic assembly of complex parts with the help of robots, and the centralised management of vast WANs. As indicated, the testbed's major goal is to show how industrial control system security standards like NIST SP 800-82 can be applied to a networked control system and how the standards might affect the system's performance, if at all [5]. This test bed will also serve as a guide for implementing security measures without sacrificing efficiency. One of the testbed's secondary purposes is to assess how well industrial control systems function in the midst of a cyber-attack; this is important because no system can be rendered fully secure from network assaults [6]. The ability of systems to withstand attacks will be one of their primary concerns. The test bed will be available to universities, government organisations, and commercial businesses for the purpose of conducting research and evaluations on new technologies designed to improve remote monitoring systems and enhance procedures more resilient to attacks. A total of five years' worth of research will be supported by the testbed.

Numerous commercially available tools exist to safeguard systems built on top of industrial standards. Products like the CISCO Adaptive Protection Appliance (ASA) and the Tofino Protection Appliance are examples of NG firewall devices that offer a high standard of security and a plethora of security functions [7]. The primary purpose of these solutions is to prevent network perimeter exploits against programmable logic controllers (PLCs). However, these technologies do provide valuable network protection. The delay, the jitter, and the payload integrity of data packets are the metrics that make up this set. This means that each enclave's starting point for measurement will be based on deliberately generated delay, jitter, and noise, and that the performance of the processes under study would be analysed in relation to these factors [8], this document offers directions for the establishment of safe control systems for industrial machinery (ICS). This type of industrial control system (ICS) is widely used in manufacturing and similar fields. Industries that frequently employ ICS include the ones dealing with electricity, water, wastewater, oil and natural gas, transportation, chemicals, pharmaceuticals, paper products, food and beverages, and other types of discrete manufacturing (e.g., transportation equipment, aeronautical machinery, and long-lasting products) [9]. SCADA systems are typically used to control dispersed assets because of the centralised data gathering and performance monitoring that provide [10]. Controlling production systems in a localised region such as a factory through the use of supervisory and regulatory control is a typical use for distributed control systems (DCS). Programmable logic controllers (PLCs) are commonly employed to carry out regulatory control and perform discrete control for a wide range of applications. Control systems are crucial to the smooth running of the United States' essential infrastructures, which are increasingly interconnected and reliant on one another. Almost 85% of the nation's critical infrastructures are owned and operated by private enterprises [11], which must be taken into account. Postal Service mail sorting and air traffic control are just two instances of the aforementioned ICS that are also run by the federal government. This article provides a general introduction to ICS, describes common system topologies, discusses common security threats and vulnerabilities, and suggests solutions to reduce these risks. The following are examples of events that an ICS could potentially face: The flow of information over ICS networks being obstructed or slowed down, which could cause ICS to stop working, changes to alarm levels, instructions, or directives that could lead to the malfunction, shutdown, or destruction of machinery due to unauthorised tampering; cause harm to the environment; endanger people's safety [12]. Franceschett et al. [13] has highlighted that incorrect information relayed to operators of the system, with the intention of either disguising unlawful changes or prompting the operators to take activities that are not appropriate, both of which could have a variety of adverse outcomes. Alterations were made to ICS software or configuration settings, or malware was introduced into ICS software, any of which could have serious consequences. Creating an unsafe environment by interfering with safety systems that would otherwise keep people alive.

2.1 Industrial Control System (ICS)

The electric, water and sewage, oil and natural gas, chemical, pharmaceuticals, pulp and paper, foodservice, and discrete manufacturing industries are just some of the many that use ICS. The document presents a long number of strategies and approaches for protecting ICS, which is necessary given the wide variety of ICS and the wide range of risks and consequences that each form of ICS may provide. This paper is not meant to be used as a simple checklist to ensure the safety of any given system. Readers are urged to conduct a risk analysis of their systems and modify the suggested guidelines and remedies to match their unique security, business, and operational needs. The scope of use for the fundamental concepts for protecting control systems provided here keeps growing [14].

Industrial control system (ICS) is a broad term that includes several different types of control systems. These include supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other industrial automation configurations like Programmable Logic Controllers (PLC), which are often used in industrial sectors and critical infrastructures. An ICS is a group of control parts (such as electrical, mechanical, hydraulic, and pneumatic) that work together to reach a business objective. The process is the portion of the system that is mostly responsible for making the output. In the monitoring part of the system, you tell it what output or performance you want. Control can be done by machines alone or with a person in the loop. Systems can run in open-loop, closed-loop, or manual mode, depending on how it has been set up. In open-loop control systems, the output is monitored by the settings that have already been made. In closed-loop control systems, the output affects the input in a way that keeps the goal the same. When the system is in manual mode, it is completely controlled by people. The part of the system that is mostly responsible for making sure it stays in line with specifications is called the controller. A typical ICS may have many control loops, Human Machine Interfaces (HMIs), and secluded diagnostic testing and maintenance tools built with a variety of network protocols.

2.2 Comparing ICS and IT Systems Security

IT systems take care of data, while ICS control the nature of reality. ICS are distinct from traditional IT frameworks in many ways, such as having different threats and priorities. Some of these are a massive threat to people's health and safety, serious environmental damage, and significant financial loses like lost production and bad reputation on the economy of a specific country. ICS have different requirements for performance and reliability, and the use operating applications and systems that are not always common in an IT network environment. Security measures must be configured in a way which keeps the system's integrity both when it is running normally and when it is under attack.

At first, ICS did not have much in common with IT systems because it was separate systems with its own control protocols and hardware and software. Older proprietary technologies are being replaced by Wireless and Internet Protocol (IP) devices that are easy to find and don not cost much. This makes cybersecurity security flaws and incidents more likely. As ICS use IT solutions to improve corporate connectivity and remote access, and as it is designed and implemented using industry-standard computers, operating systems (OS), and internet protocol, it is started to look more like IT systems. This integration allows for new IT functionality, but it opens up ICS to the outside world much more than previous systems did. This makes it more important to secure such systems. Even though security mechanisms have been made to deal with all these security problems in normal IT systems, it must be used with extra care in ICS environments. In some cases, the ICS environment needs new security solutions that are made for it [15].

The following table demonstrate the key differences between IT and ICS security systems with the practice of cyber security.

Requirement	IT security system	ICS security system
Performance requirements	Non-real time, the key to a good response is uniformity Required is a high rate of processing Having a lot of delay and jitter might be fine in the event of an emergency, this interaction is less crucial There is scope for implementing highly restricted access control, to the point where security-related interactions are possible It is possible to create a level of access control that is tight enough to provide the requisite level of safety	Rapid reaction is necessary Low throughput is fine High levels of latency cannot be tolerated and/ or jitter It is crucial to act quickly in times of crisis There have to be tight controls on who can use ICS, but it does not mean, it should make it impossible for people and machines to work together
Availability (reliability) requirements	Reactions like restarting are appropriate Deficits in availability are often acceptable provided, it does not interfere with the system's functionality	Rebooting is not always an option, depending on process availability constraints It is possible that having duplicate systems is necessary due to availability needs Scheduled downtime needs to be prepared for days or weeks in advance Extensive pre-deployment testing is necessary for high availability

(continued)

(continued)

Requirement	IT security system	ICS security system
Risk management requirements	Keep data secure Maintaining data privacy and integrity is of the utmost importance In this case, data redundancy is less crucial, as brief outages pose little threat Delay in company operations is a major risk factor	The ability to manipulate the material universe First and foremost is ensuring the safety of the people involved, followed by safeguarding the actual process itself The ability to withstand failures is crucial, as even brief outages might not be tolerated Noncompliance with regulations, adverse effects on the environment, loss of life, property, or output is all potential catastrophes
System operation	In order to work with standard operating environments, systems have been built with the help of automated deployment tools, upgrades are a breeze	Various possibly proprietary, operating systems, many of which lack basic security features Due to the specific control algorithms and possibly updated hardware and software, patch management must be handled with care, and this is often the responsibility of software providers
Resource constraints	Systems are designed with ample capacity to accommodate the installation of optional software, such as security programs	In other cases, systems may lack the necessary storage space and processing power to properly implement security measures, as it was built to serve the needs of a specific manufacturing procedure
Communications	Protocols for regular communication Wire-based primarily with occasional wireless access Normal procedures for establishing and maintaining a network in the information technology industry	A wide variety of communication standards and proprietary protocols Networks are complicated and often call for the services of control engineers due to the wide variety of communication channels employed, including both hardwired and cellular options
Change management	When solid security policies and procedures are in place, updates to software are deployed promptly. Frequently, the processes are computerised	To prevent a control system's integrity from being compromised, software updates must be rigorously tested and rolled out in stages. It is common practise to schedule ICS outages several days or weeks in advance. ICS could be relying on unmaintained operating systems

(continued)

(continued)

Requirement	IT security system	ICS security system
Managed support	Afford a range of support methods	Single-vendor service support is the norm
Component lifetime	Approximately a 3–5-year lifespan	Ten- to fifteen-year lifespan
Components location	All parts are often stored in close proximity to one another	It may take a lot of time and energy to physically access an isolated, far-away, or difficult-to-reach component

2.3 *Risk Assessment and Management in ICS*

Risk management is an everyday occurrence for organisations. Financial risk, equipment failure risk, and risks to employee safety are just a few examples. Businesses need systems in place to help them assess the threats to their operations and determine the best course of action, taking into account internal and external priorities and restrictions. As part of routine business procedures, this risk management is carried out in an iterative, ever-evolving manner [16]. Traditionally, businesses that employ ICS have mitigated risk by adhering to sound safety and engineering principles. Most industries have long-standing practises of conducting safety evaluations, and it is often integrated into legislation. Management of the risks associated with information security adds an important dimension. Both physical and digital security risk assessments can make use of the risk assessment process and framework described in this section.

A company should implement a risk management process across the board, with a three-pronged strategy to handle risk at (i) the company level, (ii) the mission/business process level, and (iii) the information management level (IT and ICS). With the goal of ensuring that the organization's risk-related operations are continually improved and that all stakeholders with a vested interest in the organization's mission/business performance can effectively communicate with one another across all three levels, the risk assessment procedure is done out in an integrated fashion.

Frame, assess, respond, and monitor are the four steps in the process of risk management depicted in Fig. 1. These responsibilities overlap and require each other to be fulfilled effectively. As an example, the results from the monitoring part will be used in the framing part. Due to the dynamic nature of the business environment, managing risk must be an iterative procedure in which all phases involve ongoing actions. Keep in mind that these factors affect the control of any risk, whether it be financial, physical, safety, or informational.

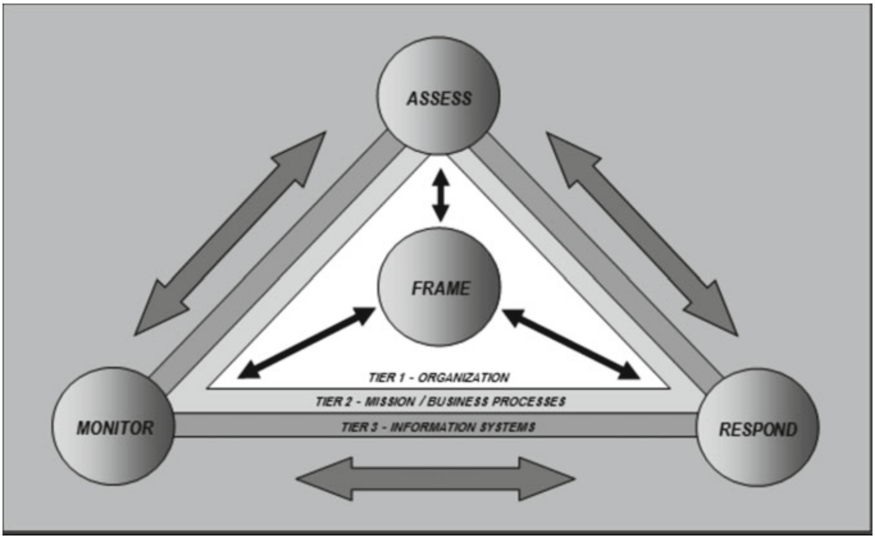

ASSESS
FRAME
TIER 1 - ORGANIZATION
TIER 2 - MISSION / BUSINESS PROCESSES
TIER 3 - INFORMATION SYSTEMS
MONITOR
RESPOND

Fig. 1 Risk assessment in different levels

2.4 *ICS-Specific Security Policies and Procedures*

The backbone of any reliable security system is its policies and procedures. Existing operational and management rules and processes should be linked with ICS-specific security procedures and policies whenever practicable. Consistent and up-to-date security protection against emerging threats is possible credits to policies and processes. Numerous suggestions for improving ICS information security policies may be found in the ICS overlay. After conducting a thorough risk assessment, the data security manager must evaluate the effectiveness of current security measures in mitigating threats to the ICS. Existing policies may need to be updated or replaced.

The organization's risk tolerance, or the level of risk it is willing to take, is determined and communicated by Tier 1 management. This information is used by the security manager to figure out how much of risk mitigation to implement in order to bring the remaining risk within acceptable bounds. An organisation can better minimise the risks posed by attacks if its security policies are based on a risk analysis and business modelling that establishes the organization's security priorities, classify assets, and identify business goals. In order to ensure that the rules are fully and correctly executed for the ICS, it is essential to create supporting procedures. Changes in policy, technology, and threats necessitate the documentation, testing, and continuous updating and improvement of security processes (Fig. 2).

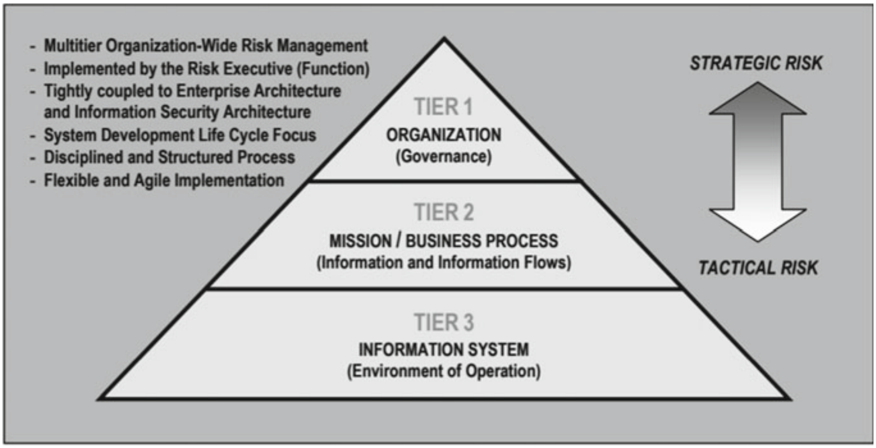

- Multitier Organization-Wide Risk Management
- Implemented by the Risk Executive (Function)
- Tightly coupled to Enterprise Architecture and Information Security Architecture
- System Development Life Cycle Focus
- Disciplined and Structured Process
- Flexible and Agile Implementation
TIER 1
ORGANIZATION
(Governance)
TIER 2
MISSION / BUSINESS PROCESS
(Information and Information Flows)
TIER 3
INFORMATION SYSTEM
(Environment of Operation)
STRATEGIC RISK
TACTICAL RISK

Fig. 2 NIST risk management system

2.5 ICS Security Risk Management Framework Implementation

From a more theoretical perspective, ICS risk management is just another risk that a company must consider. C management in charge of a particular mission or business operations must develop and implement a risk management plan in conjunction with the executive risk team at the company's highest priority. Information Security Risk Management is a Framework for assessing, mitigating, and migrating threats in today's organizations, missions, and Information Systems; NIST SP 800-39 having a point of view is essential to the success of any risk management initiative. When it comes to establishing and carrying out ICS global threat management and sharing information with enterprise management in support of effectively managing risks across the entire enterprise, the personnel involved to ICS apply their specialised subject matter knowledge, just as they do in the other task process areas. Implementing the framework for risk management is covered in NIST SP 800-37, guide for implementing the framework for risk management to Federal Information Systems. The next few paragraphs will briefly recap the procedure and then explain how to implement the RMF in an ICS setting.

There are several numbers of clearly defined organisational roles in the RMF process, each is responsible for a specific set of risk-related tasks within the organisation. It is important to note that many of the responsibilities outlined for risk management also exist in the ordinary life cycle of system development procedures. Processes in the RMF are carried out in parallel with, or as a part of, the system development life cycle (Fig. 3).

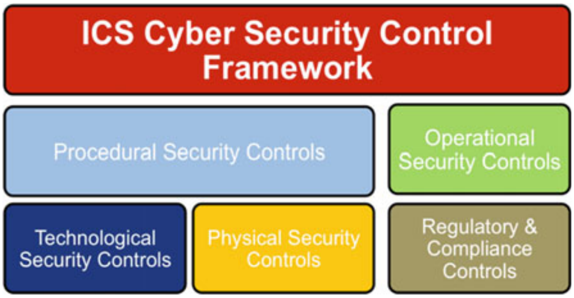

ICS Cyber Security Control Framework
Procedural Security Controls
Operational Security Controls
Technological Security Controls
Physical Security Controls
Regulatory & Compliance Controls

Fig. 3 ICS security framework with risk applied

3 ISA-99 Security

Cybersecurity Testbed verified the ISA/IEC-62443 principles and technological security standards. These criteria are similar to those found in NIST 800-82. Groups of related documents from the IEC series are displayed in Fig. 4. The documents in the 1-X series define the scope of the standard's application and explain why it was developed. The 2-X documents outline the necessities of an ICS security plan and how to put its policies and procedures into action. The 3-X series documentation outline the design criteria for solution providers and provides recommendations on various security solutions that may be relevant to an ICS integrator. Manufacturers of individual components are the primary targets of the 4-X series, which specifies the requirements they must meet in order to offer the vital functional hooks for a much more secure implementation. Meeting the standards is laid out in ISA/IEC-62443-3-3 [17].

3.1 Risk Management Framework (RMF) with Industrial Control System (ICS)

The steps necessary to implement RMF for ICS are outlined below. Each step of the procedure is outlined, and relevant NIST [18] documents are referenced. Although the following procedures are presented in a certain order, it can be performed in any order that is consistent with standard network and management development life cycle procedures.

3.1.1 Step 1: Classify Security Information System

Information system security classification is the most important step in RMF which include the process of categorising and labelling information based on its sensitivity level. This is done to protect the information from unauthorised access or disclosure. Information systems are usually classified into three categories: Confidential, Secret, and Top Secret.

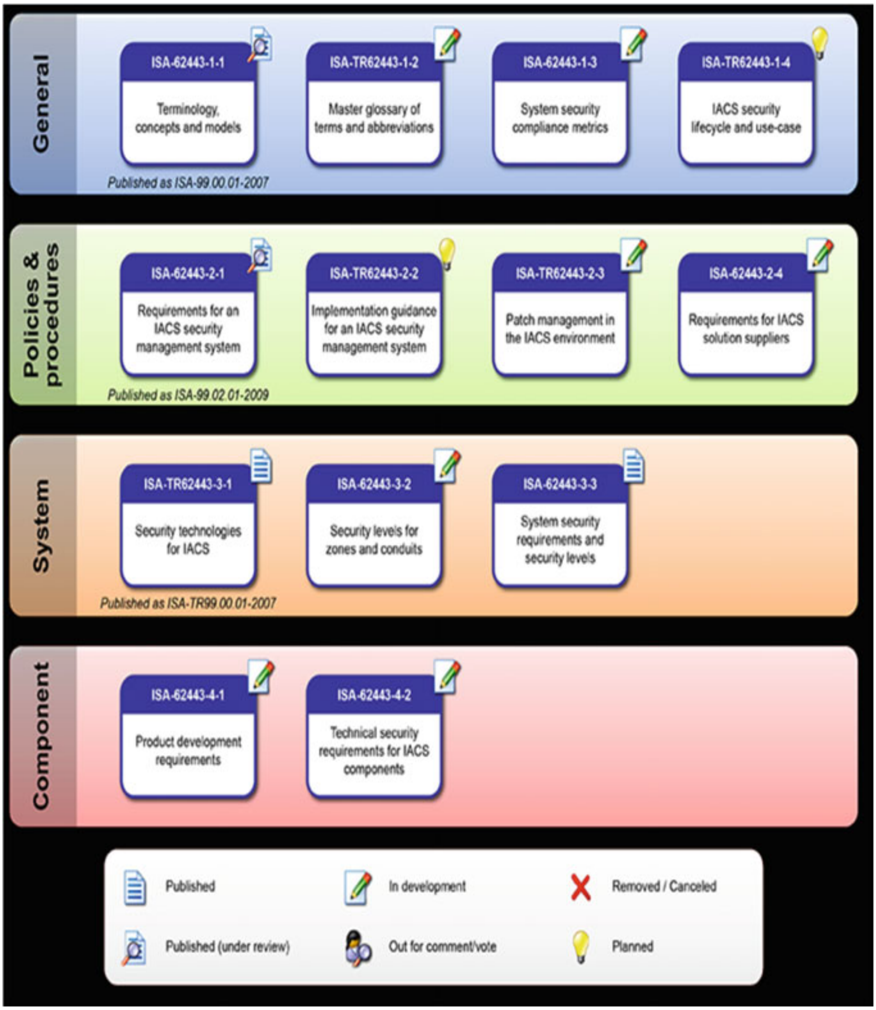

General
ISA-62443-1-1
Terminology, concepts and models
ISA-TR62443-1-2
Master glossary of terms and abbreviations
ISA-62443-1-3
System security compliance metrics
ISA-TR62443-1-4
IACS security lifecycle and use-case
Published as ISA-99.00.01-2007
Policies & procedures
ISA-62443-2-1
Requirements for an IACS security management system
ISA-TR62443-2-2
Implementation guidance for an IACS security management system
ISA-TR62443-2-3
Patch management in the IACS environment
ISA-62443-2-4
Requirements for IACS solution suppliers
Published as ISA-99.02.01-2009
System
ISA-TR62443-3-1
Security technologies for IACS
ISA-62443-3-2
Security levels for zones and conduits
ISA-62443-3-3
System security requirements and security levels
Published as ISA-TR99.00.01-2007
Component
ISA-62443-4-1
Product development requirements
ISA-62443-4-2
Technical security requirements for IACS components
Published
In development
Removed / Canceled
Published (under review)
Out for comment/vote
Planned

Fig. 4 ISA/IEC-62443 organization of standards documents

3.1.2 Step 2: Selection of Security Controls

The initial process of the set of requirements-based minimum security measures for the information system is part of this framework activity. The Federal Information Processing Standard 200 (FIPS 200) is a detailed document that illustrate a set of minimal security criteria for safeguarding federal data systems and the handled data in store, and in transport. These requirements span eighteen different security-related topics (Fig. 5).

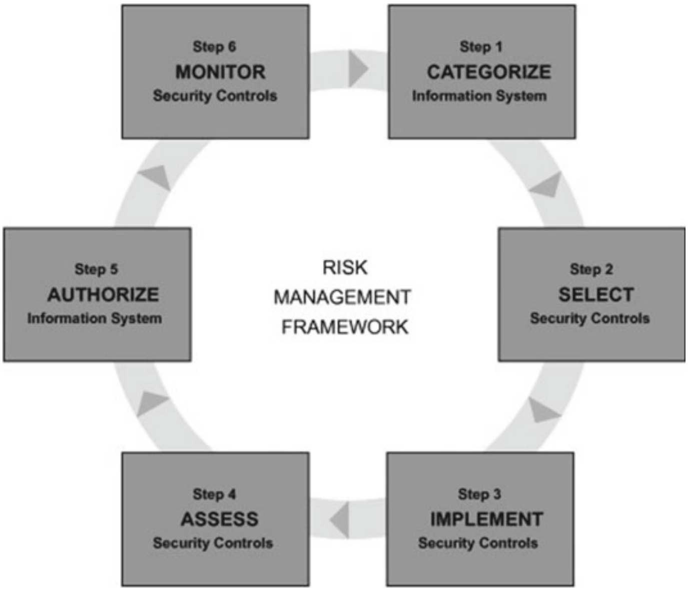


Fig. 5 Risk management framework step by step procedure

3.1.3 Step 3: Implement Security Controls

This process entails integrating new or existing security measures into an IT infrastructure. Both new development and legacy ICS can benefit from the adequate security selection approach outlined in this section.

Since new development systems do not yet exist, businesses doing initial security categorisations apply the cybersecurity selection procedure from the perspective of needs definition. The security controls outlined in the information system security plans act as a controlling and are meant to be integrated into the systems during in the Software development life cycle (SDLC) phases of design and implementation.

3.1.4 Step 4: Analyse Preventative Measures

Assessment of the information system's security measures is the process through which their efficacy in practise is measured. To verify that the security measures chosen from NIST SP 800-53 have been properly implemented, are functioning as intended, and have yielded the expected result in terms of meeting the system's security requirements, NIST has published NIST SP 800-53A to serve as a guide. NIST SP 800-53A aids in this endeavour by describing the assumptions of security assessments according to the FIPS 199 impact level, with the latter being based on assurance standards established in NIST SP 800-53.

3.1.5 Step 5: System of Authorised Data

A management decision is made to allow an information system to function and to accept the threat to agencies operations, federal assets, or personnel based on the application of an accepted set of security measures.

3.1.6 Step 6: Security Controls Monitoring

Monitoring and evaluating the efficacy of security measures is an ongoing process that keeps tabs on any updates to the data system that could affect such controls. Network security continuous monitoring is covered in detail by NIST SP 800-137.

4 Operational Technology Incident Response Plans

The term "operational technology" (OT) cybersecurity refers to the measures used to safeguard OT networks, systems, users, and data. The convergence of IT and OT to facilitate "big data" projects, combined with the growing importance of data gathering and analysis has necessitated a revaluation of cybersecurity best practises for defending OT environment.

The first Industrialisation in the 1700s marked the beginning of the era in which industrial controls became necessary. It takes generations to establish a regulator that could regulate the rate of steam—powered output and finally bring this new source of power under control, demonstrating just how challenging and critical the process of turning steam into useable energy was. Controls on complex processes have either prompted or been prompted by each industrial revolution.

4.1 Building a Business Case for OT Cybersecurity

The business case for keeping OT up to date is the same as it has been for and over 200 years; to get things done faster by improving productivity, safer by using sensors and other instruments to monitor the performance of various systems, and more efficiently for less cost, in addition to improve the ability to make more informed and efficient decisions. Throughout history, OT has become one of the most important ways to improve the quality of life and work. It has made it possible to provide treated drinking water, energy, and sewage treatment in a safe and cost-effective approach, as well as to many everyday life routines. Because of this, it should not be a surprise that OT features is being used by more people outside of its conventional industrial base. Businesses, governments, and sometimes even consumers are becoming more

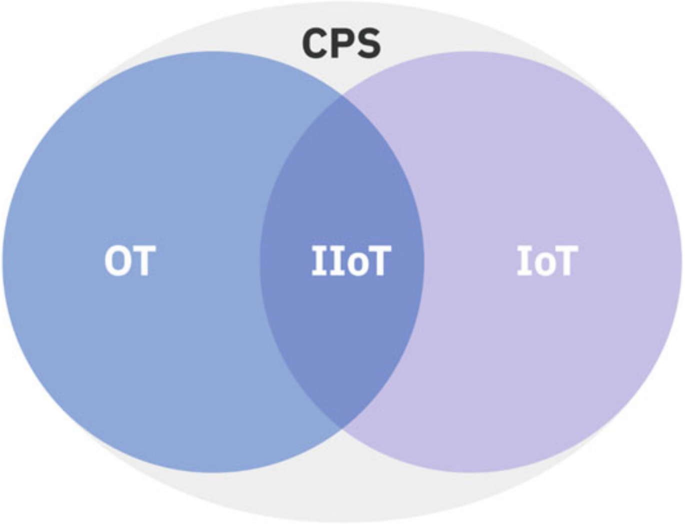


Fig. 6 Relationship among CPS, OT, IoT and IIoT

interested in the benefits of controlling and monitoring the physical environment. In the other hand, cybersecurity worries about OT are never higher because it is getting more complicated to keep OT systems secure (Fig. 6).

4.1.1 Concerns About Cybersecurity with the Integration of IT and OT

The widespread use of complex enterprise software, especially big data analytics, had also led organisations to integrate IT systems and OT infrastructure when industrial systems been connected with an IT network which makes possible to check on the performance and related of systems and equipment all the time via a life ERP dashboard. These benefits are very appealing, and it explain why involvement in IT/OT integration has grown expeditiously.

4.1.2 Importance of OT Cybersecurity

Traditional OT systems have a long list of security problems, such as the legacy equipment that lasts for decades; systems that cannot be patched, in addition to the lack of basic security features (user identification or encryption). In a perfect past, when these kinds of systems were "air-gapped" and completely isolated from the world at large these worries were thought to be acceptable risks. Complete isolation is almost impossible today, though, and organisations will need to use a combination of traditional IT information security products and services and OT-specific cybersecurity solutions to protect OT from new risks.

4.2 Purdue Model

Established in the middle of the 1990s, the Purdue Enterprise Standard architecture has gained widespread support in the business world as a means of comprehending the mandatory hierarchical system of OT systems. It is a part of the ANSI/ ISA-95 standard, that depicts how the various high-level parts of a typical control systems are linked to one another (ICS).

4.2.1 Purdue Model Levels

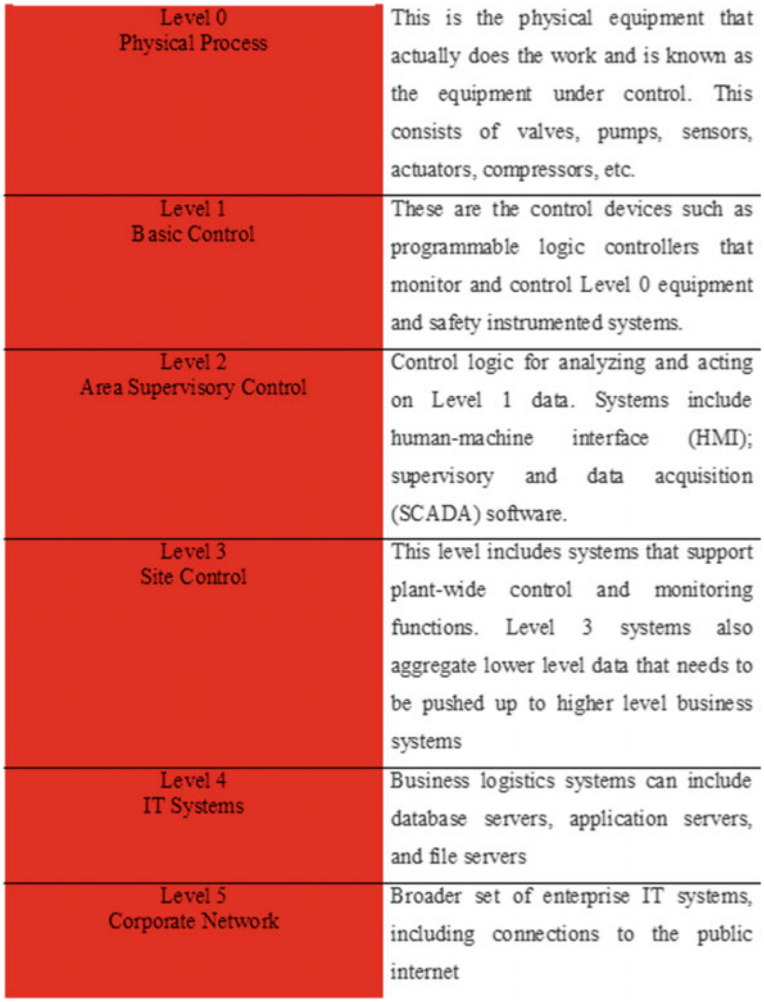
By outlining the model's foundational zones and tiers first, IT developments have made it much harder to implement the model's guidelines. Purdue's current model for OT and IT divides the two systems into three zones and six progressively more complex levels, from 0th level to 5th level (Fig. 7).

4.2.2 Purdue Model Zones

Typically, the levels are divided into three logical zones: an enterprise zone/ demilitarised zone (Levels 4 and 5), a manufacturing zone (Levels 0–3). This simplistic paradigm makes it easy to determine which systems must be in constant contact with one another. Although it was not designed to be a cybersecurity framework, it has been adopted by security experts as a means of creating more secure networks as the demand for increased communication between enterprise and manufacturing zones has grown (Fig. 8).

4.3 Cybersecurity Measures Tailored to OT

Complicating existing options is the fact that several typical IT cybersecurity technologies cannot be employed in OT contexts. Scanners designed to detect flaws in OT equipment, for instance, might cause major interruptions in production. Similarly, testing upgrades to security patches on backup systems is generally impossible in production scenarios. This is particularly troubling because technology with known vulnerabilities might be functioning for decades. Nevertheless, given the worries about system interruption, there is an intuitive reticence amongst operational teams to make modifications to their OT settings.



Level 0 Physical Process	This is the physical equipment that actually does the work and is known as the equipment under control. This consists of valves, pumps, sensors, actuators, compressors, etc.
Level 1 Basic Control	These are the control devices such as programmable logic controllers that monitor and control Level 0 equipment and safety instrumented systems.
Level 2 Area Supervisory Control	Control logic for analyzing and acting on Level 1 data. Systems include human-machine interface (HMI); supervisory and data acquisition (SCADA) software.
Level 3 Site Control	This level includes systems that support plant-wide control and monitoring functions. Level 3 systems also aggregate lower level data that needs to be pushed up to higher level business systems
Level 4 IT Systems	Business logistics systems can include database servers, application servers, and file servers
Level 5 Corporate Network	Broader set of enterprise IT systems, including connections to the public internet

Fig. 7 Prude model levels

4.4 Best Practices of OT Cyber Security

4.4.1 A Well-Defined Chain of Command Is Necessary for OT Cybersecurity's Adoption into Risk Management Plans

There must be a well-defined chain of command with specific roles and responsibilities in order to implement an OT security plan that receives adequate funding while complementing rather than undermining larger safety and reliability efforts. A Chief Safety Officer (CSO) should also have responsibility for both IT protection and OT security and should directly report to the Chief Operations Officer (COO); it will

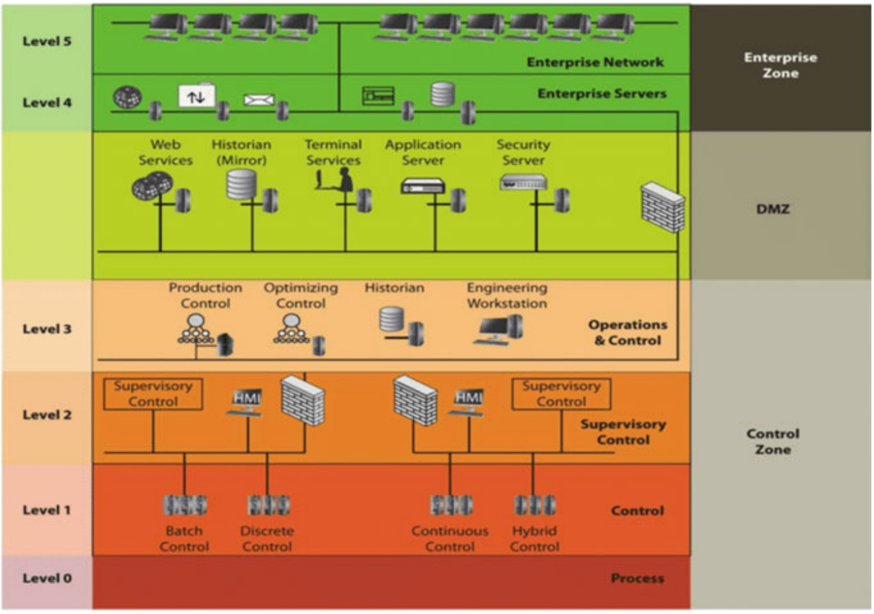


Fig. 8 Six Purdue enterprise reference architecture zones for OT

help to safeguard security expenditures and operational authority. The objective is for every company to have a responsible team for OT security working in the C-suite, and for it to be widely acknowledged that OT protection is an issue that increasingly merits board-level debate (Fig. 9).

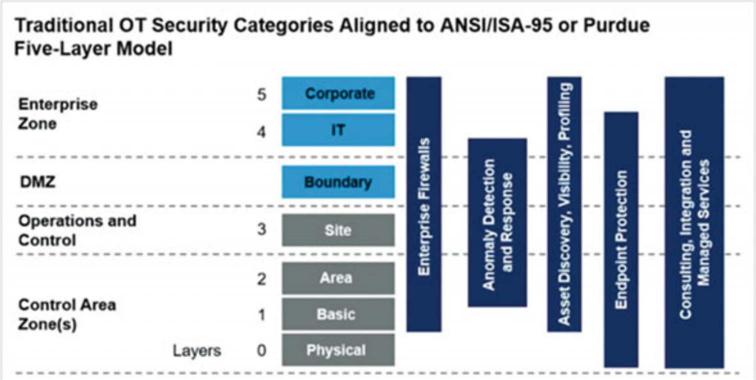

Traditional OT Security Categories Aligned to ANSI/ISA-95 or Purdue Five-Layer Model
Enterprise Zone
DMZ
Operations and Control
Control Area Zone(s)
Layers
5
4
3
2
1
0
Corporate
IT
Boundary
Site
Area
Basic
Physical
Enterprise Firewalls
Anomaly Detection and Response
Asset Discovery, Visibility, Profiling
Endpoint Protection
Consulting, Integration and Managed Services

Fig. 9 Purdue 5 layer model with traditional OT security

4.4.2 The Importance of Multi-disciplinary Teams

The National Institute of Standards and Technology (NIST) suggests assembling a multidisciplinary OT cybersecurity team with representation from management, physical security, information technology, and control system operation. It is crucial, for operational staff to understand the potential implications on systems from OT cybersecurity related activity.

4.4.3 Procedures Suggested by the Computer Security Industry Association

CIS Critical Security Protocols and the CISA Suggested Cybersecurity Practices, both are beneficial for organisations to start up a set of security baseline. CISA suggests ten best practises at a high level:

- To verify, rank, test, and deploy ICS security updates.
- Keep your system's information and settings in a safe place.
- Recognise, reduce, and protect all network links to ICS.
- Maintain constant vigilance in evaluating the safety of ICS, protocols, and connections.
- It is important to turn off any protocols, ports, and services that are not in use.
- Incorporate strong configuration management standards and activate all applicable security mechanisms.
- Use whitelisting to restrict which programs can access sensitive data and antivirus software's to keep harmful code from even getting installed.
- Make sure all managers and employees in charge of industrial control systems have taken a course on cyber safety.
- Keep an incident management plan up-to-date and test it.
- Secure ICS hosts and networks using a risk-based, defense-in-depth strategy.

4.4.4 Design Principles of NCSC

CISA recommends the UK National Cyber Security Centre's (NCSC) Design Principles and Operational Technology for organisations that want to start from the ground up. Here is a summary of the NCSC's design principles:

- Set up the context before creating a system.
- Make it hard to compromise.
- Make it hard to disrupt.
- Make it easier to find compromises.
- Lessen the effect of compromise.

4.4.5 CIS Critical Security Controls

The CIS 20 Controls are a good starting point for cybersecurity, and it can be changed to fit ICS and IoT network. The controls are put into three groups: basic, foundational, and organisational. According to Boehm [19], the top five critical security controls in ICS are:

CIS Control #1: Inventory of Hardware Assets and Control of Them.

CIS Control #2: List and Management of Software Assets.

CIS Control #3: Continuous Assessment and Repair of Vulnerabilities.

CIS Control #4: Use of Supervisory Privileges in a Managed Way.

CIS Control #5: Software and hardware on mobile devices, notebook computers, workstations, and servers can be set up to be secure.

4.4.6 How to Use Gartner's Flexible Security Model to Protect OT Cyberspace

Cybersecurity is often described as a process. It should also be continuous and change over time, which is why Gartner made the Adaptive Security Architecture (ASA). Traditional IT security was mostly about finding threats and stopping them, but the ASA prototype adds forecasting and response to make a cycle. The model can be broken down into four stages:

Predict—This involves identifying potential threats or vulnerabilities through risk assessments and AI intelligence gathering. By predicting potential risks, organizations can better prepare for and mitigate them.

Respond—This involves having a strategy for how to handle a security breach or incident or when it happens and consider other essential measures to minimise the impact of the incident.

Prevent—This involves implementing measures to prevent security incidents from occurring in the first place which include implementing security controls as well as educating users and employees about cyber security best practices.

Detect—This involves monitoring for events of a security incident and detecting it as fast as probable. This can include monitoring tools and protocols to identify and respond to security incidents in a timely manner.

PRPD strategy was first proposed by MITRE (ATT&CK) and Lockheed Martin (Cyber Kill Chain). And it aims to protect organizations from harm by predicting and preventing potential security incidents and responding effectively when it does occur. By learning more about early signs of an attack, it is easier to predict, which helps with strategy and makes other parts of the cycle easier.

4.4.7 Cyber Threat Awareness in OT

Participating in cyber threat awareness programmes, like the U.S. Department of Homeland Security's ICS-CERT and the Industrial Control System Information Sharing and Analysis Center's ICS-ISAC, is another important best practise for spotting threats early on.

4.4.8 Cybersecurity in OT

CISA gives each organisation a risk assessment document that tells them to do the following things:

- Ensure that VPNs and other remote management systems are fully patched.
- Improve system monitoring so that unusual activity can be caught early, and an alert sent.
- Use multi-factor authentication.
- Ensure that all machines have firewalls, anti-malware, and intrusion protection software installed and properly set up.
- Ensure continuity of operational processes or contingency planning are up to date.
- Raise awareness of IT support options for employees who work from home.
- Update incident response strategies to consider changes in the workforce in a distributed environment.

4.5 Preparedness and Response to Incidents: The NIST Framework

The United States Department of Commerce's National Institute of Standards and Technology (NIST) is a non-profit organisation that develops and publishes norms and guidelines for several fields of IT. The Information Technology Laboratory (ITL) at NIST creates benchmarks and tests for the IT industry, including data protection. An important framework for incident handling and response (IR) was created by ITL, Computer Security Incident Management Guide.

The NIST incident handling process is an iterative activity with built-in opportunities for learning and improvement in the pursuit of optimal security. There are four main phases preparation; detection and analysis; containment, eradication, and recovery; and post-event activity.

4.6 Plan for Incident Response (IR)

Incident management is an organisational process that lets people respond to cyber-attacks quickly and effectively. The incident response procedure involves finding an attack, figuring out how bad it is and how important it is, investigating and stopping it, putting things back to normal, and taking steps to make sure it does not happen again.

Furthermore, an incident response plan (IRP) is a written list of the steps that should be taken during each phase of a response to an incident. It should have rules for defining roles and responsibilities, plans for communication, and standard protocols for how to respond.

4.7 Key Roles of a Team that Responds to an Incident

An incident response team is crucial for carrying out an incident response plan. Full-time personnel or teams may be responsible for these tasks in a large firm, whereas in a smaller one, staff juggling many responsibilities may be asked to step up. The following are essential roles within the team:

When an event happens, it is the responsibility of at least two individuals to approve the incident response strategy and coordinate the necessary actions. After then analysts in this field are responsible for reviewing alerts, determining the likelihood of occurrences, and conducting preliminary investigations into the scale of attacks. Researchers in the field of threats are tasked with supplying further details about a given threat by sifting through data from many sources (the internet, threat intelligence feeds, security tools, etc.) to piece together a complete picture. Others who have a vested interest include executives, board members, human resources professionals, public relations experts, and top-level security personnel like Chief Information Security Officer (CISO).

4.8 ICS Implementation for NIST SP 800-73-3

4.8.1 Limiting Who May Access the Industrial Control System (ICS) Network and What They Can Do on It

Separate authentication techniques and credentials are provided for users on the corporate and ICS networks, and demilitarised zone (DMZ) network architecture is used to block communication between the two types of networks. The ICS should also have a multi-layered network architecture, with the most crucial communications occurring at the highest security and reliability layer [20].

4.8.2 Limiting Who Can Go In and Out of the ICS Infrastructure

Physically tampering with the ICS's components without authorization could cause serious problems; Use of locks, contactless cards, and security staff are only few of the many possible physical access restriction methods that should be considered.

4.8.3 Reducing the Risk of Attack on Individual ICS Components

Disabling unused ports and services, restricting ICS user permissions to only what is necessary for each position, keeping a close eye on the audit trail, and using security controls like antivirus and file integrity checking software whenever possible are all part of this strategy to avoid, hinder, predict, and mitigate malware.

4.8.4 Carrying Out Normal Operations Under Trying Circumstances

To achieve this goal, the ICS must be built with redundancy in mind. When a component fails, it shouldn't trigger a chain reaction that affects other parts of the system or create unnecessary traffic on the Industrial Control System (ICS) or other networks.

4.8.5 Accidental System Restores

Problems will always arise, which is why it is necessary to have a plan to respond to them. One of the most important aspects of an effective security programme is the speed with which a system may be restored after an attack or breach has taken place.

In order to analyse and lower risk to an industrial control system, it is essential for a cross-functional cyber security team to exchange their different domain expertise and experience. After that, proper ICS security measures can be implemented. The cyber security team should consist of at least one person from management, one from IT, one from control engineering, one from control system operations, one from the field of information and computer security, and one from the field of physical protection. In order to maintain consistency and ensure that all bases are covered, the cyber security team ought to confer with the vendor of the system's controller or integrator. Full responsibility and accountability for the ICS's cyber security should rest with site management (such as the facility superintendent) or the company's CIO or CSO. When designing a cyber security plan for an ICS, it is essential to take "defense-in-depth" into account. This strategy entails stacking many security measures so that the failure of any one layer has minimal effect on the system as a whole [21].

4.9 Key Components of Industrial Framework

Key components include the following:

Control Loop—A control loop consists of actuators such control valves, breakers, switches, and motors, and the transmission of variables. Other types of controller hardware include PLCs. The sensors send the controlled variables to the controller so that it can make the appropriate adjustments. The controller is responsible for interpreting the signals and generating the associated controlled variables, which are then transmitted to the actuators, based on the set points [22]. Alterations to the process brought on by disturbances result in the generation of new sensor signals that, once again, are sent to the controller to identify the condition of the process.

Human–Machine Interface (HMI)—Both operators and engineers rely on HMIs to keep tabs on controller settings, such as set points and control algorithms. The HMI also displays real-time data and information about the past performance of the process.

Tools for Remote Inspection and Repair—Tools for diagnosis and upkeep are used to spot and correct malfunctions before it causes serious damage, and to get back up and running after an accident with reference to the standard IEC 62443 [23].

4.10 Industry Framework

Another method for conducting top-down analysis is provided by industry frameworks. Industry frameworks offer archetypal designs of businesses operating within a given industry, and it arrange the basis of an agreement reached by representatives from that industry. Normalised functional and business process breakdowns that may map to capabilities are typically defined by these frameworks. It might provide greater granularity and impartiality than a value chain that is exclusive to a business. Not surprisingly, individual circumstances or the way a company chooses to conduct its operations and business needs can make each entity distinctive, and these distinctions can serve as a foundation for achieving a competitive advantage in particular markets.

One of the benefits of an industry framework is that contains capabilities typically align with implementations of capabilities in commercial corporate applications and outsourcing services. This is one of the advantages of an industry framework. The use of an industry framework does not imply that a conventional value chain that is well-defined should be abandoned; rather, the two working together define greater insight for the definition of shared capabilities [24].

4.10.1 Authentic, Real-Time, Safety-Certified Kernels

A considerable number of built-in safety mechanisms are available with the SCIOPTA 61508 kernel and IEC 61499, which are a pre-emptive multi-tasking high performance real-time kernel. SCIOPTA is an excellent alternative for use in applications that must conform to stringent safety criteria since it employs a kernel that directly passes messages. This makes it an ideal candidate for use in such applications [25].

4.10.2 Safety Certified Data Transfers

By performing checksum validation on message data areas, the SCIOPTA kernel is able to monitor the movement of data between processes. The workload of the creator of safety software is significantly reduced thanks to these verified functions. When it can be delegated this responsibility to the kernel, the overall development time and costs are cut down significantly.

A header, a data region that can be any size, and an end-mark that is validated by the kernel make up the SCIOPTA message and ETFA [26]. The sender, owner, and addressee of the message all have their respective process IDs included in the message's header.

4.10.3 No Shared Memory

Traditionally, shared memory has been used as the inter process communication protocol in real-time operating systems. Users are responsible for assigning semaphores to specific data areas and kinds, as well as implementing semaphore protection for shared memory.

No form of shared memory is needed in a SCIOPTA-based system. Direct communication provides a safer method of transmission. Information is packaged in messages, and the kernel is responsible for their security by managing data ownership.

4.10.4 Controlled Storage of Information

SCIOPTA modules can be used to organise and manage a collection of related processes. Each module has the potential to have a maximum of 128 pools available to store SCIOPTA messages. Modules and pools might share the same section of memory or be located in different sections. Using a Memory Management Unit and the SCIOPTA Memory Management System (SMMS), full memory protection can be attained (MMU) [27].

4.10.5 Certified by TÜV

SCIOPTA has been given approval for use in systems up to SIL3 by the TÜV in Munich in accordance with IEC61508/EN50128 [28].

4.11 IEC 61508

IEC 61508 is the name of the international standard that focuses on safety-related systems that mix electrical, electronic, and/or programmable electronic (E/E/PE) instruments and devices. The full title of the standard is the International Electrotechnical Commission Standard for Safety-Related Systems that Combine Electrical, Electronic, and/or Programmable Electronic [29].

Despite its origins in the automation and process control industry, IEC 61508 is finding increasing acceptance in other sectors, like the automotive and medical industries, where safety and dependability are of paramount importance.

The 7 Parts of IEC 61508

- IEC 61508-1 Defines common requirements.
- IEC 61508-2 States all the safety-related systems requirements.
- IEC 61508-3 Gives software requirements.
- IEC 61508-4 Defines all the definitions and abbreviations.
- IEC 61508-5 Some techniques for determining the level of safety integrity.
- IEC 61508-6 By using IEC 61508-2 and -61508-3 correctly gives some suggestions.
- IEC 61508-7 Defines an outline of methods and procedures.

4.11.1 Market Guide for Operational Technology Security

The convergence of IT, IoT, and OT environments has increased the complexity and vulnerability of previously isolated OT/ICS networks and newly designed cyber-physical systems (CPSs). As a result, there is a necessity for an all-encompassing, automated approach to asset discovery, risk assessment, and helping to avoid downtime. "*By 2025, 70% of asset-intensive organizations will have converged their security functions across both enterprise and operational environments*"—by Gartner [30].

Report to Discover

- The factors that are driving the transition of the OT security market from a focus on OT networks to a focus on CPS assets.
- Market dynamics such as increasing threats, exposing vulnerabilities, a continuous skills deficit, and growing laws, directives, and frameworks.

- Suggestions for "anchoring security efforts to operational resilience" in the face of growing threats, by implementing an integrated security strategy that goes beyond legacy OT systems.

4.12 Differentiation Between ISO/IEC/IEC 62443, NIST Cybersecurity Framework, and ISO/IEC 27001

A set of standardised risk mitigating strategies is needed in order to take a methodical approach to the implementation of a cyber security programme. These strategies should be developed through the collaborative efforts of regulatory institutions, industry associations, government agencies, and technology specialists. Organizations are able to not only reduce the risks to an acceptable level with the assistance of a single well-defined procedure or a combination of procedures that are also well-defined, but they are also able to track the progress, evaluate any gaps that exist between the current and targeted security levels, and improve the overall efficiency of their security system.

International standards like as ISO-27001, NIST Cyber security Framework, and ISA/IEC 62443 are a few illustrations of those that are extensively used and widely embraced. These standards offer a comprehensive guidance and absolute effectiveness in safeguarding IT and OT systems.

4.12.1 ISO-27001

Beginning around the turn of the millennium, several independently developed industry standards began to converge into what is currently known as the ISO set of guidelines for security management of information. The International Organization for Standardization (ISO) is now widely recognised as one of the most thorough standards for establishing and maintaining an effective information security management system. Information security is the primary focus of the ISO-27001 standard, and it helps businesses prioritise and solve their needs for keeping data private, secure, and accessible [31].

A plan-do-check-act cycle, which is more often known as the PDCA cycle, lies at the core of it. This cycle can trace its origins back to quality assurance in production contexts (Fig. 10).

The cycle of plan-do-check-act can provide assistance in establishing the framework of the organisation, defining the scope and objectives, determining the requisite competence, and creating a written policy. This is supplemented further by the evaluation of risks, the planning of treatments, the selection of available controls, and the

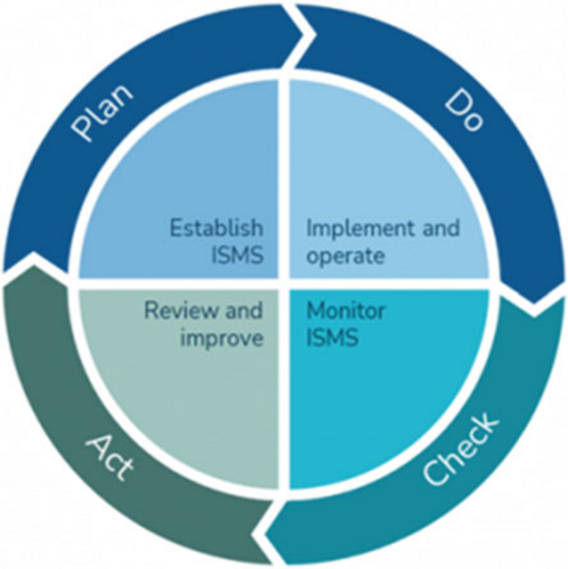


Fig. 10 PDCA cycle for quality assurance

implementation of those controls [32]. In addition, constant innovations and improvements are able to fulfil the ongoing demand for risk reduction. In a nutshell, ISO-27001 provides businesses with a step-by-step guide that assists in effectively implementing the necessary security capabilities and minimising risks using an approach that is iterative and scalable for successive degrees of development.

The Need for OT Security Standards

IT and OT systems are often different in terms of the technological nature and scope of their operations. Murray et al. [33] stated in their work that the approach to security that is taken with an OT system needs to be adapted to the specific demands of that system. Since many of the controls that were implemented to manage the security of IT systems are not relevant to OT systems, a distinct set of industry standards is required in order to satisfy the safety needs and limit the risks that are connected with them. Both the NIST Common Security Framework (CSF) and the ISA/IEC 62443 standard were developed expressly for the for the sake of establishing guidelines to ensure the security of industrial control and automation systems.

4.12.2 ISA/IEC 62443

By deriving from the controls defined in ISA/IEC 62443 delves even further into the particulars of the application process. The set of standards known as ISA/IEC 62443 provides a framework for managing and securing operational technology (OT) systems, as well as for monitoring and preventing potential attacks in the future. It enables organisations to identify their assets and keep track of their asset inventory, to group assets with similar security requirements into zones, and to define conduits for the establishment of a secure communication channel within and among these zones. Afterwards, the zones exposure to danger is evaluated, and the proper levels of security are implemented there. Controls are decided upon and put into place in accordance with the predetermined levels of safety that are associated with each zone. In light of raising concerns over the safety of industrial control systems, the International Society of Automation (ISA) has established norms to guarantee their security; Using the knowledge of experts in industrial automation and control systems, the Industrial Systems Association (ISA) developed a set of standards (ISA/IEC 62443) to detect and eliminate any security flaws (IACS) [34].

ISA 62443 is a set of standards, technical papers, and supporting materials whose overarching goal is to create a flexible framework that permits addressing current and future vulnerabilities in IACS and applying essential mitigations in a methodical, defensible manner. Standards, technical reports, and other supporting materials can all be found inside ISA 62443. It is imperative to have a clear understanding of the purpose of the ISA 62443 series, which is to create extensions to enterprise security that adapt the needs for business IT systems and integrate them with the particular requirements for robust availability that are needed by IACS [34].

According to Fachot [35], the main sections of the series are as follows:

- General (62443-1): This category contains items that discuss themes that are present throughout the entirety of the sequence.
- Policies and regulations (62443-2): The components of this set pay special attention to the rules and regulations surrounding the protection of IACS.
- Requirements for the System (62443-3): The elements that make up the third group are those that deal with requirements for the method.
- Requirements for components (62443): More specific and precise requirements for the development of IACS products are covered in the fourth and final group of elements.

The following sections of the standard demonstrate a detailed definition of the security requirements across the software development life cycle (SDLC) for industrial control systems:

- **ISA-62443-3-3**—Specific operational and technological criteria for IACS safety are established in this sequel. Within the scope of the standard's definitions are located seven sets of foundational requirements (FR), as well as four tiers of security levels (SL). The level of security that must be maintained by the system is established through the use of risk analysis. System requirements, or SRs, can vary widely depending on the amount of security desired. The standard defines SRs by referring to the applicable FRs in various places. Some of the SRs contain modifications to the requirements that apply to all the SLs, while others only apply to a subset of the SLs.

- **ISA-62443-4-2**—Includes detailed descriptions of embedded parts, network parts, host parts, and software parts, and more. The standard consists of a total of seven fundamental requirement groups and four security level groups (SL-Cs). This standard's requirements are derived from ISA-62443-3-3 (system security requirements); however, they are more narrowly focused on parts of the control system rather than the entire system [36].

In addition to ISA 62443, there is also NIST Special Publication 800-82, which is an alternate framework. In compliance with the Federal Information Security Modernization Act (FISMA) that was passed in 2014, the National Institute of Standards and Technology (NIST) designed and developed this [37].

4.12.3 NIST 800-82 Standard

Guidelines for National Institute of Standards and Technology Cyber security offers asset owners a comprehensive roadmap for securing operational technology (OT) systems in their organisations. It is basically built to assist companies in streamlining the required processes, defining and prioritising the security level for both existing risks and anticipated hazards, and managing the budget in accordance with these considerations [38]. Users of the NIST Cyber Security Framework are given general guidance toward the implementation of cyber security measures that are in keeping with the framework's five basic functions (Fig. 11).

Among the many different NIST standards, the NIST 800-53 and the NIST 800-82 are two that stand out as particularly important. While NIST 800-53 is utilised across the industry for the purpose of managing the cyber security needs of information systems, NIST 800-82 is utilised for the purpose of managing the privacy and security controls of operational technology (OT) systems. Through the use of an "overlay," which is made possible by NIST 800-82, businesses are able to modify certain controls from NIST 800-53 so that they better meet the requirements of OT. The written recommendations of the NIST provide an overview that is both comprehensive and detailed of all the security capabilities of these standards.

Stouffer et al. [39] found a guide for ensuring the security of industrial control systems may be found in the Special Publication 800-82 that was published by the National Institute of Standards and Technology. It is feasible, as stated in the executive summary of Publication 800-82, to consider it an "overlay" to Publication 800-53. Guidelines for applying the security measures detailed in NIST Special

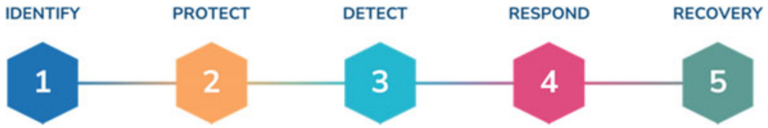


Fig. 11 NIST cybersecurity framework's five functions

Publication (SP) 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, have been developed by the National Institute of Standards and Technology (NIST) in collaboration with the community of ICS professionals working in the public and private sectors. A significant number of the controls in Appendix F of NIST SP 800-53 can be directly applied to ICS as written, however, many of these controls also require ICS-specific interpretation and/or augmentation [10].

In fact, NIST SP 800-82 cites multiple other NIST SPs throughout the document and offers "ICS-specific Recommendations and Guidance" for every possible scenario.

The Importance of Security Policies

The lifetime of control systems includes not only the creation, testing, and release of systems and software, but also the accompanying rules and procedures. The absence of a security policy in and of itself might create conditions that are conducive to the introduction of vulnerabilities in industrial control systems.

To define roles and duties, provide direction for programme implementation, and outline how violations will be handled, a thorough and well-documented security policy is required. One of the most important factors that determines whether a security programme is successful is the level of support and governance that it receives from management. In-depth discussions on policies and procedures are presented in both ISA/IEC 62443 and NIST SP 800-82; however, the two documents take somewhat dissimilar approaches to the subject matter [40].

This subject is covered in depth by the IC4F and 62443-2 category, which is organised into four subparts that focus primarily on developing a management system for cybersecurity is suitable for IACS settings [41]. This is also known as an IACS security programme or, more generally, an IACS security management system, according to the standard. These two terms are synonymous with one another. Moreover, the requirements for a successful IACS security system are outlined in the first part (62443-2-1), and assistance for developing such a system is provided in the second part (62443-2-2) of this document. Although, the third section (62443-2-3) details the best practises for the system's patch and change management, while section four (62443-2-4) restates the security programme criteria with an emphasis on the responsibilities of IACS service providers [42].

The National Institute of Standards and Technology's Special Publication 800-82 is another helpful reference for drafting and implementing policies and procedures. In fact, it devotes an entire section in Appendix C to the topic of detecting vulnerabilities and predisposing factors that are related to the absence of policies and procedures.

4.13 *Selecting the Right Standard/Framework for OT Cybersecurity*

Responses from a variety of industrial verticals to a survey conducted by SANS and titled "SANS ICS/OT survey 2021" revealed an interesting combination of OT Cybersecurity standards. The top 5 standards that control systems are mapped to are NIST CSF, ISA/IEC-62443, NIST 800-53, and NIST 800-82, and ISO 27001 [43]. There are also a few standards that are unique to the industry, such as the NERC CIP, as well as standards that are unique to the region, such as the NIS Directive and the Qatar's ICS security standard [44] (Fig. 12).

In most cases, a combination of these standards will be utilised in order to meet the specific requirements of certain business. These requirements might be affected by the region or the overall environment in which the company operates, in addition to other conditions or goals connected to your specific organizational context. It is possible that the implementation of these standards could successfully establish a cyber-secure industrial environment. This would make it possible for OT defenders to combat threats, while identifying areas-of-emphasis for the protection of a critical infrastructure in a vividly streamlined manner. The ISA/IEC 62443 standard and the NIST SP 800-82 standard provides exhaustive coverage and direction for industrial control system (ICS) security respectively [45]. Despite the presence of other

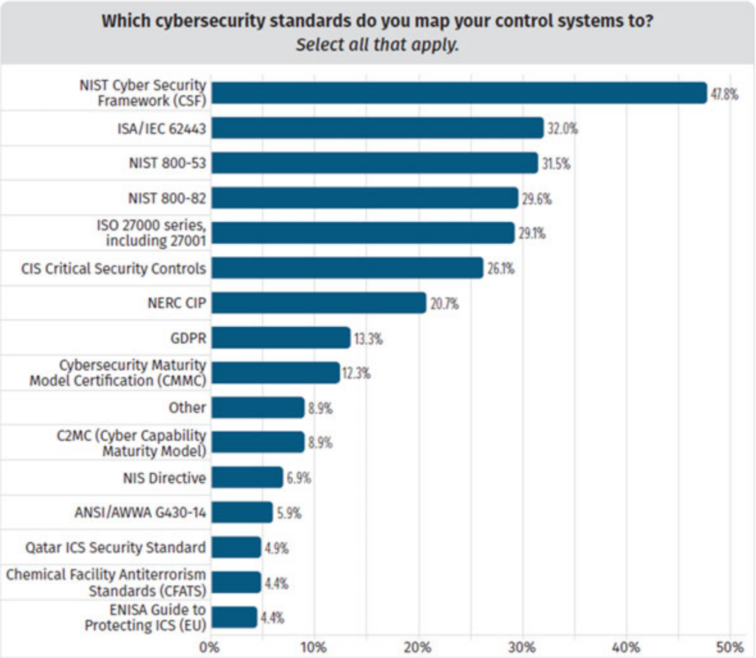


Fig. 12 Top utilised ICS international cybersecurity frameworks

security standards, initiatives, and best practises in this field, these two frameworks have gained the most traction and attention. Because connected systems are always susceptible to new risks, it is necessary to take a multi-faceted approach in order to counteract the many dangers. The implementation of a security framework is one way to assist enterprises in moving toward a more holistic strategy [45].

The choice of a framework will, in many instances, be determined by the industry and the accompanying regulatory drivers, which may require a particular framework. Therefore, because various regulators may need various organizational structures and each framework has a plethora of knowledge concerning the safeguarding of industrial control systems. For instance, organizations in the public sector are typically expected to adhere to the NIST standards.

5 Research Methodology

This part offers detailed of how the study was performed along with method used.

5.1 Research Process

The research process indicates to the process conducted by researchers to develop and put in writing feasible research. This often involves identifying, finding, evaluating, and analysing various information research related facts and information.

5.2 Research Methodology

Research methodology describes the methods' systematic analysis that be appropriate to a research field. Particularly, it is the phase where the researchers consider several models and methods that will be used in their studies. Irny and Rose [46] stated that Research methodology generally involves hypothesis, phases theoretical model and quantitative or qualitative techniques.

In this study, the results are established based on open-source data; mix methodology model is used: the qualitative and quantitative methods are used to investigate the available datasets required for the classifier training. Literature review was retrieved from online archives, such as: Google Scholar, Web of Science, Science Direct, and IEEE Xplore and so on. Additionally, news, articles, books, related industry descriptive reports and articles initiated by cybersecurity professionals in career were also utilised to enhance the background research. As mentioned earlier, the dataset chosen greatly affects the performance of the classifier. The dataset should be of moderate size and high quality so that the feature extraction procedure can train the algorithm efficiently.

5.3 Data Collection and Data Analysis

Researcher must determine the applicable methods and techniques to implement for the data collection and analysis phase. The date used to conduct this research secondary data that collected from several open-source online archives.

5.4 Legal and Ethical Consideration

Proposed study has to comply with relevant ethical and legal issues. The author has to take into consideration the academic policies and guidelines extremely and adhere to the academic codes of conduct for the duration of the research establishment. Research actions, events and elements involving data analysis methods, data collection and theoretical and practical studies all be required to fulfil with legal guidelines.

The research mechanisms, activities approach, Internet and computer uses must comply with legal obligations and responsibilities in the United Kingdom Computer Misuse Act 1990 (legislation.gov.uk),

The collected data will be used exclusively for this project and will be erased after use. Only data in English language will be compiled and evaluated and must obey with and the GDPR and DPA (2018) (Legislation.gov.uk).

6 Proposed Architecture for Automation Energy System Applying the IEC 62443 Standard

Cyber-attacks on critical infrastructure systems like Secondary Distribution Automation (SDA) systems have been in the news frequently as of late. The immaturity of their security architecture makes them vulnerable to cyberattacks. Because of the potential for significant financial losses, the potential loss of intellectual property, and the catastrophic damage to the company's reputation on the market, securing these systems from attacker actions has been an increasing area of focus. To approach the cybersecurity problem of these important systems comprehensively, an analysis based on the international standard IEC 62443 is warranted. For Industrial Automation Systems, this specification represents a worldwide consensus on the best security procedures (IACS). To protect against attacks from numerous directions, IEC 62443 employs a system called defence in depth, which has a variety of security layers and predetermined degrees of security. The aim of this proposed work is to test the implementation of the IEC 62443 Standard in a representative SDA energy system and to raise the level of security maturity in such installations to an acceptable level.

The International Electrotechnical Commission (IEC) 62443 was developed by the ISA (the International Society of Automation) as a set of standards, technical

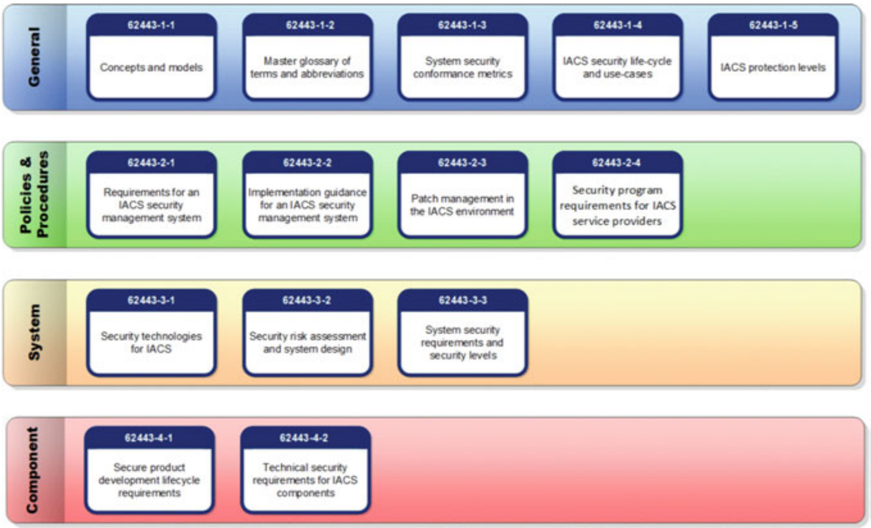

General
62443-1-1
Concepts and models
62443-1-2
Master glossary of terms and abbreviations
62443-1-3
System security conformance metrics
62443-1-4
IACS security life-cycle and use-cases
62443-1-5
IACS protection levels
Policies & Procedures
62443-2-1
Requirements for an IACS security management system
62443-2-2
Implementation guidance for an IACS security management system
62443-2-3
Patch management in the IACS environment
62443-2-4
Security program requirements for IACS service providers
System
62443-3-1
Security technologies for IACS
62443-3-2
Security risk assessment and system design
62443-3-3
System security requirements and security levels
Component
62443-4-1
Secure product development lifecycle requirements
62443-4-2
Technical security requirements for IACS components

Fig. 13 IEC 62443-standard

reports, and other materials that define the steps necessary to implement electronically secure Industrial Automation and Control Systems (IACS), in order to meet all concerned with entirely forms of industrial automation, application, control, and key infrastructure, including but not limited thereto SCADA, power plants, transmission lines, distribution networks, utilities for gas, water, oil, etc. This technical definition focuses on cyber security, which encompasses hardware, software, networks, and configuration settings.

As demonstrated in Fig. 13, IEC 62443 Standard covers a wide range of stakeholders involved in the manufacturing, design, deployment, and industrial automation management and control systems, including end users. The four main sections of IEC 62443 are “General,” “Policies and Procedures,” “System,” and “Component.” It is crucial to notice that while some things have been published already, others are still in the process of being created, evaluated, or planned.

6.1 Using IEC 62443-Based Safety Systems

6.1.1 Segmentation of Network

To safeguard a network, segmentation of network is a potent defence strategy. The essential concept is to place network components that require a similar level of security within the same zone and then to limit access to that zone in both a physical and logical manner. Network segmentation reference proposes a network separation that creates three distinct network zones [47]:

Trusted Zone—In order to meet the Trusted Zone's special communication requirements, further precautions must be taken. As a result, a firewall surrounds it, and trustworthy process networks are a part of it. In this context, "Trusted Zone" refers to the areas around the Control Zone, the Control Centre, and the primary Substations.

Demilitarised Zone (DMZ)—Between the safe area and the dangerous area is where the DMZ is set up. This is the area where all outside connections to the security zone are monitored and managed. When located inside the Command Centre or primary substations, the service PC is considered to be in a Demilitarised Zone (DMZ), which adds another degree of security for off-site personnel.

Untrusted Network—The security measures of the "untrusted network" are either undefined or insufficient.

6.1.2 Interfaces, Conduits and Data Flow

Human Machine Interfaces (HMIs) or physical interfaces can be used for the solution components' interaction. IEC 62443 requires, in general, that any vulnerable or unused interfaces be turned off. Safely connecting devices requires categorising IP-based communication protocols according to their purpose; Operation entails all protocols principally required for the operational functioning of the power utility. Various IEC and NTP standards are good examples; Engineering covers all processes that are implemented to manage product setup, upkeep, and problems. All engineering equipment is a good example; And lastly remaining protocols are classified under the "support" heading, the Simple Network Management Protocol (SNMP) and other remote access protocols are a couple of [13].

With the goal of protecting the integrity of data transmitted between different networks in mind, two methods have been established. First is secures data transmission between the SDA Control Area and the Control Centre/Basic Substation using Virtual Private Network (VPN) between gateways. Since just part of the communication line will be secured, this method is considered "bare minimum" security. Secondly is the communication channel between devices in the SDA control area and network devices in the Control Centre/Basic substation is safeguarded by a Virtual Private Network (VPN) using Internet Protocol Security (IPSec). By implementing that, secure communications end-to-end will be optimised.

6.1.3 Controlling Identity and Permitting Entry

The topology of the network within the design mandates two access methods, distant access (through DMZ) and public access in the field, for maintenance and engineering purposes. Services PCs are used to verify user identities in both environments, however after a project is handed over, it is advised that DMZ access be limited further.

6.1.4 Hardening to Lessen Vulnerability to Attack

To put system hardening into action, it must ensure that all unnecessary service's ports and connections are closed or deactivated on all network nodes (including switches, routers, RTUs, and computers). In other words, all engineering protocols and tools are mapped, and only those that are necessary for keeping the system running are allowed to be turned on.

A protected repeater is a crucial part of an IEC 62443-compliant secure solution. There is an absolute need for Hardening in this scenario. Blocking unused ports and using a MAC address filters to restrict access to the network to authorised devices are two examples of the precautions used to provide a sufficient level of security. Disabling Telnet remote access and HTTP, two examples of services and protocols known to be vulnerable, is a good place to start.

6.1.5 Security Against Malware and Other Attacks on OT Systems

Some generic and preferable product qualities were taken into account to ensure the system's continued functioning: digitally signed firmware that can continue to operate normally under attack; validation mechanisms to ensure that only valid setup commands and blog posts with the correct syntax are accepted; firmware that has been subjected to extensive security testing during development; firmware that can function normally regardless of whether or not it is connected to the internet. All these safeguards make it feasible to protect against firmware tampering, Denial of Service (DoS) attacks, unexpected product behaviour, and unauthorised modifications to the system's configuration.

To prevent devices from being exploited as a vector for propagating system viruses, anti-malware software is now required to be installed on all service PCs. It is expected in the strategy that the IT and industrial networks are partitioned at the control centre level to lessen the attack surface.

6.1.6 System Monitoring

It is vital to build a monitoring system in order to keep track of what is going on in the platform, such as unusual equipment actions (e.g., attempts to configure changes or erroneous logins) and the behaviour of your network (suspect packages and protocols). At the level of the control centre, it makes appropriate to implement a "Logging" server to receive such data. The syslog protocol can be used to send and map cyber security data to a SIEM or to transmit data from internal locations on the equipment using a normal distribution protocol (such as DNP3) to a SCADA system.

7 Data Analysis and Critical Discussions

7.1 Case Study

"Tracing security requirements in industrial control systems using graph databases for wind turbine cases."

Because there are numerous numbers of different system and security standards, it is crucial to record the interdependencies and hierarchies between them. As a result, the current techniques for specifying security requirements fail to adequately capture such structure, which in turn complicates currently existing and traceability and extends the time and money needed to construct certified ICS. This paper proposes a novel paradigm for ICS requirements repositories, one that makes use of LPGs (Labelled Property Graphs) to chain store both demands for standards-based and system-specific, with the latter being organised according to predefined relationship types. Finally, the document achieves the requirements traceability by integrating the proposed requirements database with ICS tools during the design phase. A wind turbine scenario study highlights the promote efficiency in our system. These papers illustrate that utilising labelled property graphs inevitably results in a solid requirements traceability matrix, although, its present adaptable requirements change management process that can be used to accommodate future modifications to both the development and certification processes.

There must be security in place for all the crucial parts used in ICS deployments. IEC 62443 is one of many ICS-specific security standards, provides stringent yet generic security criteria. Such requirements' applicability to a given project is not always obvious and can often be difficult to parse. Multiple organisations must reach consensus on a common set of product-centric security requirements in order to move forward with the certification process for security standards. Therefore, in a safety certification program, all parties (users, vendors, and certifying bodies) must reach consensus on a security needs engineering strategy that is practical for them. It is crucial to maintain the security of the entire process by correctly mapping required functionality to security standards requirements.

Modelling and implementing a security wind turbine system allowed researchers to examine the challenges inherent in monitoring and monitoring security requirements in ICS.

7.2 *Contribution of This Research Work*

The key contributions of this research are as follows:

1. With an emphasis on requirements structure and linkages, the papers demonstrate a unique repository approach that maintains the IEC 62433-4-2 specific security and Cyber Security Requirements Specification (CRSC) as Labelled Parameter Graphs (LPGs) in various subsets.
2. The papers propose and illustrate a method for integrating the repositories with Industrial Control System design tools in order to facilitate end to end supplies traceability.

7.3 *Detail Study on Safety–Critical Wind Turbine ICS Standards*

To illustrate the use of the repository and the related traceability procedure, a case study of a safety–critical Industrial Control System wind turbine is implemented. The wind turbine system makes use of a master–slave configuration of many Programmable Logic Controllers (PLCs). The nacelle's slave PLCs take orders from a master PLC located at the wind turbine's foundation. In addition, the PLCs send data to the control system, which in turn sends the information to SCADA or an enterprise system. Due to its central role in regulating the wind turbine's mechanical operations, the data exchange between the master and slave Programmable logic controllers is of the utmost importance. An attacker can compromise the control device system by injecting a rogue instrument in the middle of both the master and slave PLCs, blocking the nacelle and pitch gears from functioning properly. For an ICS to function, there must be reliable lines of communication between all its parts.

7.3.1 Step 1: Generation of Requirement Graph

The CSRS's recommendations for protecting wind turbines are incorporated into the case study.

Each requirement and sub-requirement, such as CRa, CRb, AR, IRa and IRb is treated as a node in the LPG that is generated from these specifications. This method of organising the security standards from several specification papers aids in drawing attention to the connections between the various levels of these hierarchical needs. To ensure that each system's CSRS graph is distinct, the LPGs are developed in isolation from one another. However, the same safety adjusted accordingly can be utilised with different CSRS graphs. In addition, the structure of the requirements is dependent on the specific CSRS graph [48].

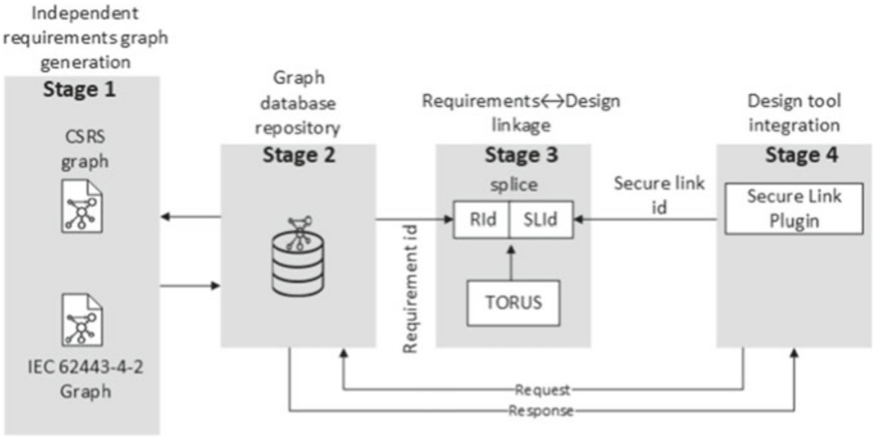


Fig. 14 Process overview of creating an LPG security requirements repository

7.3.2 Step 2: Repository for Graph Database

An LPG's organisation makes it possible to store and manage the repository more effectively. The relations between data are produced and put in storage for the duration of the database building step, which is a major benefit of utilising LPG. Complete needs can be queried from the repository using a variety of graph patterns including trees, chains, chain sets, and forests. In addition, the properties of nodes and edges in an LPG can be used to filter the result sets. Here, the graph database tool's has created querying features to use. It could be seen the entire chain of dependencies between each criterion under a security umbrella. As an added bonus, the proposed repository's numerous partitions are highly reusable by both manufacturers and the ICS developer community (Fig. 14).

7.3.3 Step 3: Requirement to Design

TORUS is an application for tracing requirements to their implementation, and it does so by employing splices. Splice meta data in TORUS keeps the repository link alive with a need identifier from the wind turbine system's CSRS. Traceability between the security repository's requirements and the design phase is facilitated by TORUS's integration with the repository.

7.3.4 Step 4: Design Tool with Security

The integration of secure connections and TORUS with a need's repository is briefly introduced in this secure-by-design technology for ICS. However, this article demonstrated the concept's actual applicability and consolidate it. Therefore, End-to-end requirements traceability is realised by encrypting the safe bond and the wind turbine Cyber Security Requirements Specification necessary identifiers in a TORUS splice. The verification and certification of security requirements is aided by the visible and complete traceability matrix produced by the proposed repository concept.

7.4 IEC 62443-4-2 Property Graph

Using the Neo4j graph database tool, it explains how the formalism can be put into practise in meeting the security standards laid out in IEC 62443-4-2 [49]. As demonstrated an LPG specification of FR3, one of the seven FRs in the specification, which is the foundation for realising the ICS integrity objective, FR3 is selected due for its pertinency for security integrity needs IRa and IRb for the wind turbine system, as shown in Table 1. IRa demands data integrity in the middle of both the wind turbine PLCs and peripherals, whereas IRb involves security integrity of data among master and slave PLCs. In cooperation are related to system integrity requirement FR3 as defined by IEC 62443-4-2 (Fig. 15).

Table 1 Wind turbine security requirements

Goal	RID	Example of security requirement (SR) of wind turbine PLCs	Security level
Confidentiality	CR	The master and slave PLCs shall ensure the confidentiality of the data in transmission and at rest	
	CRa	Data communication between master and slave PLCs shall use appropriate encryption algorithms	SL-C 2
	CRb	Critical parameters shall be not be persisted on the master and slave PLCs in order to ensure the confidentiality of data for discharged devices from the system	SL-C 4
Authentication	AR	Any access to the PLC (master/slave) shall be provided after appropriate authentication based on role-based identification	SL-C 1
Integrity	IR	The system shall ensure the integrity of ingress and outguess data	
	IRa	Communication between master PLC and external components shall use appropriate methods to ensure the integrity of the data	SL-C 4
	IRb	Communication between master and slave PLCs shall support communication integrity checks	SL-C 4

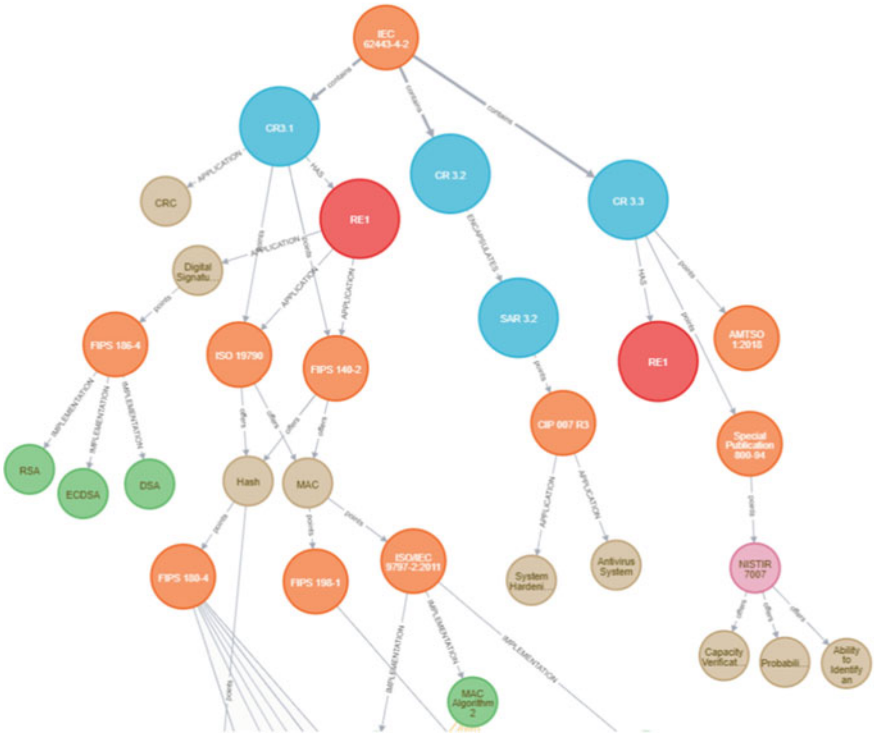


Fig. 15 Integrity property graph produced by Neo4j

7.5 Implementation of Security Standards

A single Neo4j above graph file includes the wind turbine case study's IEC 62443-4-2 and Cyber Security Requirements Specification parameter graphs, functioning the same as a logical repository [49]. Using Cypher queries, the author generated two distinct property graphs. A CSRS wind turbine's property described in Fig. 16, is generated using the Cipher query in Listing 1. Similar queries can also be used to construct the IEC 62443-4-2 graph. For instance, SL-C:4 on line 4 of Listing 2 describes the above label the edge of CR3.1 and its RE1. These are essential for sorting out the security standards. To reach CR3.1's desired level of capability security, level 4, this aids in defining a route to the necessary cryptographic primitives. The query fragment shown in Listing 2 is too long to be displayed in full here.

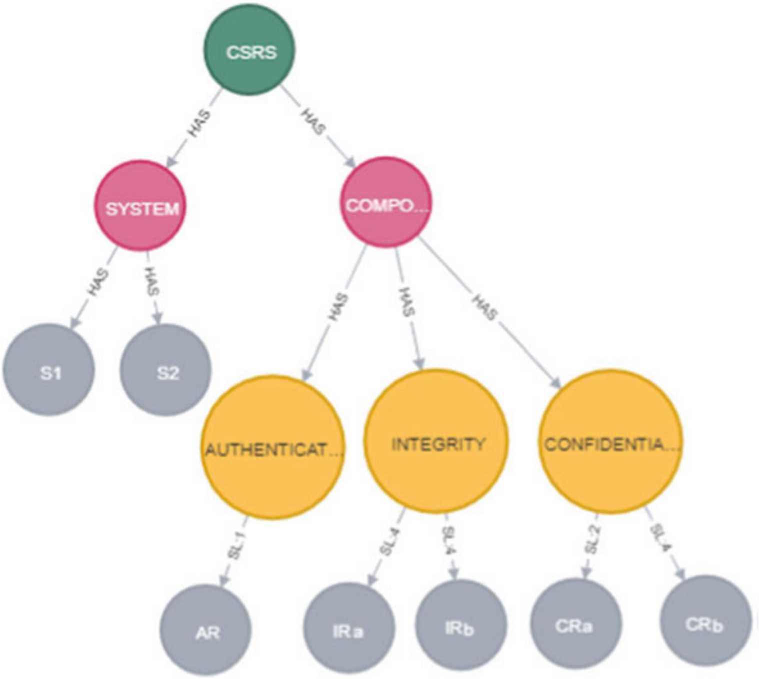


Fig. 16 A CSRS graph of a wind turbine system created in Neo4j

Listing 1

```
CREATE (cr:CSRS{name:"CSRS"})-[:HAS]->
 (co:COMPONENT{name:"COMPONENT"}),
(cr)-[:HAS]->(sy:SYSTEM{name:"SYSTEM"}),
(sy)-[:HAS]->(:LEAF{name:"S1"}),
(sy)-[:HAS]->(:LEAF{name:"S2"}),
(co)-[:HAS]->(con:CONFIDENTIALITY
{name:"CONFIDENTIALITY"}),
(co)-[:HAS]->(auth:AUTHENTICATION
{name:"AUTHENTICATION"}),
(co)-[:HAS]->(inte:INTEGRITY
{name:"INTEGRITY"}),
(con)-[:SL-C{type:2,name:"SL-C:2"}]->
(:CON_REQ{name:"CRa"}),
(con)-[:SL-C{type:4,name:"SL-C:4"}]->
(:CON_REQ{name:"CRb"}),
(auth)-[:SL-C{type:1,name:"SL-C:1"}]->
   (:AUTH_REQ{name:"AR"}),
(integ)-[:SL-C{type:4,name:"SL-C:4"}]->
   (:INT_REQ{name:"IRa"}),
(integ)-[:SL-C{type:4,name:"SL-C:4"}]->
   (:INT_REQ{name:"IRb"})
```

Listing 2

```
CREATE (s6244311)-[:contains]->(fr3),
(fr3)-[:points]->(s6244342),
(s6244342)-[:contains]->(cr31),
(cr31)-[:HAS {SL-C:4}]->(cr31RE1),
(cr31RE1)-[:APPLICATION]->(sISO19790),
(cr31RE1)-[:APPLICATION]->(sFIPS1402),
(cr31RE1)-[:APPLICATION]->(mDigitalSig),
(mDigitalSig)-[:points]->(sFIPS1864)
```

Another aspect of Neo4j that works well with our planned repository is its ability to execute and store a series of searches in a specific database. When a query is run, its results are stored in the database, opening the door to the possibility of saving several views of the data for later use. The graph database also stores the individual entities that resulted from the IEC 62443-4-2 FR3 and the wind turbine CSRS required inquiries in the listings. Thus, both graphs can be merged, in other word, the information can be obtained using additional Cypher queries. For instance, according CSRS, IRa, a security criterion for wind turbines, must be provided at SL-C 4. Recommendations for carrying out the security standards specified in IEC 62443-4-2 are existing in a structure of LPG nodes, which are stored in the repository that the report offer. This set of rules covers the use of common security methods and the corresponding cryptographic primitives. The existing set of rules is not comprehensive; for example, the IEC 62443-4-2 norm only specifies a small subset of the possible standard encryption protocols and procedures. For the library to be utilised in large-scale industrial control system (ICS) projects, the standard's LPG graphs must be exhaustive.

Ultimately. secure connection and repository act like anchors in the structure of cybersecurity algorithms/methods represented by the leaf nodes of the property graph of IEC 62443 in the repository and implementation of that functional block within the IEC 61499 Industrial Control System application. complement each other. To each protected connection is recognized by a unique identifier indicating to it [48].

End-to-end traceability of security requirements combines repositories with design patterns to enforce communication security constraints via secure connections [50], and the requirements traceability engine TORUS [51].

8 Conclusions

Establishing safe and reliable control systems in industrial settings is the focus of this article (ICS). Typical examples of these ICS can be found in the process control sectors, and they include SCADA systems, DCSs, and PLCs (among other control system types). This document gives an introduction to ICS and common system architectures, details common security threats and vulnerabilities, and suggests safeguards to implement to reduce those risks.

At first, ICS were separate networks that used their own control protocols and hardware and software that were not shared with other networks, bearing little resemblance to the more common IT networks. Many ICS elements were not linked to any kind of information technology network or system and were instead kept in specially guarded rooms. Internet Protocol (IP) components that are easy to find and inexpensive are gradually replacing proprietary products, which raises the stakes for cyberattacks. The increasing use of computers, operating systems (OS), and network protocols from the IT industry in the design and implementation of ICS has led to a convergence between the two types of systems.

Because of the critical role that cybersecurity plays in ensuring the safe and reliable functioning of today's industrial processes, ICS cybersecurity programmes must constantly be integrated into larger ICS safety and security plans at both construction plants and corporate cybersecurity programmes. Control systems are vulnerable to intrusion from a wide variety of causes, including as hostile nations, terrorist groups, individual employees, malevolent intruders, complications, accidents, natural disasters, and even intentional or inadvertent activities by insiders. Availability and integrity are the top priorities in ICS security, followed by confidentiality.

To organise and consolidate CSRS and IEC 62443-4-2 standard requirements, this paper suggests a decentralised LPG system requirement repository with several partitions. In order to help determine which standard cryptographic primitives are needed to implement a security needs, a formal specification of the IEC 62443-4-2 expanded requirement structure is provided. When the repository is used in conjunction with design patterns to record communication security restrictions via secure links and a requirements management engine like TORUS, full-stack security requirements traceability can be attained. The document also shows how the repository can be used to facilitate a process for adapting to new or altered needs. Using graph-query languages to query the repository is what makes the difference, further, to examine what this means for the security testing process and how the repository can be used.

References

1. Norwich University (2019) IT vs. OT: comparing two vital information security concepts. Norwich University. Online. Available at: https://online.norwich.edu/academic-programs/resources/it-vs-ot. Accessed: 2 Sept 2022
2. Kuppusamy E, Mariappan K (2021) Integration of operation technology (OT) and information technology (IT) through intelligent automation in manufacturing industries. In: Advances in manufacturing technology XXXIV: proceedings of the 18th international conference on manufacturing research, incorporating the 35th national conference on manufacturing research, 7–10 Sept 2021. University of Derby, Derby, UK. IOS Press
3. Alber B, Prince A (2021) The structure of OT typologies. Chapter 1: introduction to property theory
4. Green B, Derbyshire R, Knowles W, Boorman J, Ciholas P, Prince D, Hutchison D (2020) {ICS} testbed tetris: practical building blocks towards a cyber security resource. In: 13th USENIX workshop on cyber security experimentation and test (CSET 20)
5. US Homeland Security (2022) Cybersecurity, cybersecurity | Homeland security. Available at: https://www.dhs.gov/topics/cybersecurity. Accessed: 8 Sept 2022
6. Ani UPD, Watson JM, Green B, Craggs B, Nurse JR (2021) Design considerations for building credible security testbeds: perspectives from industrial control system use cases. J Cyber Secur Technol 5(2):71–119
7. Anwar RW, Abdullah T, Pastore F (2021) Firewall best practices for securing smart healthcare environment: a review. Appl Sci 11(19):9183
8. IECEE Publication (2022) Rules of procedure—CB scheme of the IECEE for mutual recognition of test certificates for electrotechnical equipment and components (CB scheme) and its related services: statement of test results—Energy Efficiency Testing Service (E3) Global Motor Energy Efficiency (GMEE) Program Industrial Cyber Security Program. IECEE documents | Rules, operational documents and guides. Available at: IECEE 02—rules of procedure. Accessed: 13 Sept 2022
9. Knapp ED, Langill J (2014) Industrial network security: securing critical infrastructure networks for smart grid, SCADA, and other industrial control systems. Syngress
10. Stouffer K et al (2015) Guide to industrial control systems (ICS) security. CSRC. Available at: https://csrc.nist.gov/publications/detail/sp/800-82/rev-2/final. Accessed: 13 Nov 2022
11. Hayden E (2019) 4 steps to critical infrastructure protection readiness: TechTarget, security. TechTarget. Available at: http://www.techtarget.com/searchsecurity/tip/252465638/4-steps-to-critical-infrastructure-protection-readiness. Accessed: 26 Sept 2022
12. Boyer SA (2010) SCADA: supervisory control and data acquisition, 4th edn. ISA—International Society of Automation, Research Triangle Park
13. Franceschett AL, de Souza PR, de Barros FLP, de Carvalho VR (2019) A holistic approach—how to achieve the state-of-art in cybersecurity for a secondary distribution automation energy system applying the IEC 62443 standard. In: 2019 IEEE PES innovative smart grid technologies conference-Latin America (ISGT Latin America). IEEE
14. Ehrlich M et al (2019) Secure and flexible deployment of industrial applications inside cloud-based environments: semantic scholar. In: 2019 24th IEEE international conference on emerging technologies and factory automation (ETFA). Available at: https://www.semanticscholar.org/paper/Secure-and-Flexible-Deployment-of-Industrial-inside-Ehrlich-Trsek/e73f3d815cbf1c3f1ae437908cc39dbb37befb00. Accessed: 24 Dec 2022
15. Conklin WA (2016) IT vs. OT security: a time to consider a change in CIA to include resilienc. In: 2016 49th Hawaii international conference on system sciences (HICSS). IEEE
16. Joint Task Force Transformation Initiative (2011) Managing information security risk: organization, mission, and information system view. CSRC. Available at: https://csrc.nist.gov/publications/detail/sp/800-39/final. Accessed: 22 Sept 2022
17. Team E (2021) Understanding IEC 62443. IEC. Available at: https://www.iec.ch/blog/understanding-iec-62443. Accessed: 12 Sept 2022

18. ITL NIST (2018) About the RMF–NIST risk management framework: CSRC. CSRC. Available at: https://csrc.nist.gov/projects/risk-management/about-rmf. Accessed: 12 Nov 2022
19. Boehm A (2018) Take security to the next level with the top 5 CIS critical security controls, Ivanti. Ivanti. Available at: https://www.ivanti.com/blog/take-security-to-the-next-level-with-cis-critical-security-controls. Accessed: 21 Oct 2022
20. Cooper D (2021) NIST test personal identity verification (PIV) cards version 2
21. Abdelghani T (2019) Implementation of defense in depth strategy to secure industrial control system in critical infrastructures. Am J Artif Intell 3(2):17–22
22. Dutta N, Tanchak K, Delvadia K (2020) Modern methods for analyzing malware targeting control systems. In: Recent developments on industrial control systems resilience. Springer, Cham, pp 135–150
23. Culot G et al (2019) Addressing industry 4.0 cybersecurity challenges: semantic scholar. IEEE Eng Manag Rev. Available at: https://www.semanticscholar.org/paper/Addressing-Industry-4.0-Cybersecurity-Challenges-Culot-Fattori/ddefa2b96bdf6e9dc66ffc373ef5fd216b662574. Accessed 30 Sept 2022
24. Ehrlich M et al (2019) Figure 1 from automated processing of security requirements and controls for a common Industrie 4.0 use case: semantic scholar. In: 2019 international conference on networked systems (NetSys). Available at: https://www.semanticscholar.org/paper/Automated-Processing-of-Security-Requirements-and-a-Ehrlich-Gergeleit/51d9b30acce66178804333c960d20ee638887988/figure/0. Accessed 5 Oct 2022
25. Hahm O, Baccelli E, Petersen H, Tsiftes N (2015) Operating systems for low-end devices in the internet of things: a survey. IEEE Internet Things J 3(5):720–734
26. Raymundo Belleza R, de Freitas Pignaton E (2018) Performance study of real-time operating systems for internet of things devices. IET Softw 12(3):176–182
27. Zakaria HM (2022) Security of IoT: sine logistic map, S-box, and Tan-Bessel function
28. Steinert LF (2022) Safety critical, high-performance systems based on COTS multicore processors for industrial and aerospace applications. Doctoral dissertation, Technische Universität München
29. IEC (2010) What is IEC 61508? 61508 Association. Available at: https://www.61508.org/knowledge/what-is-iec-61508.php. Accessed: 26 Dec 2022
30. DRAGOS (2022) 10 ways asset visibility builds the foundation for OT cybersecurity. Available at: https://cdn.cyberscoop.com/asset-visibility-builds-OT-cybersecurity-foundation.pdf. Accessed 21 Oct 2022
31. Lopes IM et al (2019) How ISO 27001 can help achieve GDPR compliance. In: 2019 14th Iberian conference on information systems and technologies (CISTI). IEEE
32. Singgrit P, Pamuji GC (2020) The use of ISO 27001 framework for government's online E-monitoring system implementation. Int J Educ Inf Technol Others 3(3):556–563
33. Murray G, Johnstone MN, Valli C (2017) The convergence of IT and OT in critical infrastructure
34. Hohenegger A (2019) Die common criteria und IEC-62443. Deutscher IT-Sicherheitskongress
35. Fachot M (2020) IEC 62443 standards—a cornerstone of industrial cyber security. Etech. Available at: https://etech.iec.ch/issue/2020-04/iec-62443-standards-a-cornerstone-of-industrial-cyber-security#:~:text=The%20IEC%2062443%20series%20of%20Standards%20is%20organized,4%20Components%20%28IEC%2062443-4.%2A%20%E2%80%93%20both%20parts%20published%29. Accessed: 27 Oct 2022
36. ISA (2020) Security lifecycles in the ISA/IEC 62443 series. ISA.org. Available at: https://21577316.fs1.hubspotusercontent-na1.net/hubfs/21577316/2022%20ISA%20Website%20Redesigns/ISA%20Secure/Files%20Repository%20For%20Learning%20Center/Articles%20Page/ISAGCA-Security-Lifecycles-whitepaper.pdf. Accessed: 27 Oct 2022
37. Gupta S (2020) Assuring compliance with government certification and accreditation regulations. In: Cloud computing security
38. Brandao Filho SB, Cesar CDAC (2022) A secure method for industrial IoT development. SN Comput Sci 3(2):173
39. Stouffer K, Pease M, Tang C, Zimmerman T, Pillitteri V, Lightman S (2022) Guide to operational technology (OT) security (No. NIST Special Publication (SP) 800-82 Rev. 3 (Draft)). National Institute of Standards and Technology

40. Syafrizal M, Selamat SR, Zakaria NA (2020) Analysis of cybersecurity standard and framework components. Int J Commun Netw Inf Secur 12(3):417–432
41. Hohenegger A, Krummeck G, Baños J, Ortega A, Hager M, Sterba J, Kertis T, Novobilsky P, Prochazka J, Caracuel B, Sanz AL (2021) Security certification experience for industrial cyberphysical systems using common criteria and IEC 62443 certifications in certMILS. In: 2021 4th IEEE international conference on industrial cyber-physical systems (ICPS). IEEE
42. Téglásy BZ, Katsikas S, Lundteigen MA (2022) Standardized cyber security risk assessment for unmanned offshore facilities. In: Proceedings of the 3rd international workshop on engineering and cybersecurity of critical systems
43. Grove C (2021) Surprising findings in the SANS 2021 OT/ICS cybersecurity survey. Nozomi Networks. Available at: https://www.nozominetworks.com/blog/surprising-findings-in-the-sans-2021-ot-ics-cybersecurity-survey/. Accessed: 2 Nov 2022
44. Jones N (2019) International policy: pitfalls and possibilities. In: Cyber security: threats and responses for government and business
45. Stouffer K et al (2022) Guide to operational technology (OT) security. CSRC. Available at: https://csrc.nist.gov/publications/detail/sp/800-82/rev-3/draft. Accessed: 4 Nov 2022
46. Irny S, Rose A (2005) Designing a strategic information systems planning. Issues Inf Syst VI(1)
47. BouSaba C (2019) Implementing a DeMilitarized zone using holistic open source solution. In: 2019 ASEE annual conference and exposition
48. Tanveer A et al (2022) Tracing security requirements in industrial control systems using graph databases—software and systems modeling. Springer, Berlin. Available at: https://doi.org/10.1007/s10270-022-01019-8?code=4e726f40-5d33-456d-abf4-ffac84231bc8&error=cookies_not_supported. Accessed: 14 Dec 2022
49. Lal M (2015) Neo4j graph data modeling. Packt Publishing Ltd., UK
50. Tanveer A, Sinha R, Kuo MM (2020) Secure links: secure-by-design communications in IEC 61499 industrial control applications. IEEE Trans Ind Inf 17(6):3992–4002
51. Sinha R, Dowdeswell B, Zhabelova G, Vyatkin V (2018) Torus: scalable requirements traceability for large-scale cyber-physical systems. ACM Trans Cyber Phys Syst 3(2):1–25