Wireless Personal Communications (2022) 124:1557–1592
https://doi.org/10.1007/s11277-021-09420-0

A Survey on Internet-of-Things Security: Threats and Emerging Countermeasures

Dorsaf Swessi[1] · **Hanen Idoudi**[1]

Accepted: 14 November 2021 / Published online: 5 January 2022

Abstract
Internet of things (IoT) is a world wide network and set of paradigms that are intended to allow communications between anything, anytime and anywhere. However, connected objects are in most cases vulnerable due to their constrained resources and the inherent IoT environment conditions, basically, the dynamic aspect, the heterogeneity, and the open and wireless medium of communication. Securing the IoT networks is still an open and challenging issue and the majority of traditional security mechanisms designed so far for Internet doesn't satisfy IoT security requirements. Recently, the use of emergent technologies such as Artificial Intelligence mechanisms, Blockchain and IoTA as a promising solutions to solve security and privacy problems has shown a yield remarkable performance. In this paper we outline the security requirements proposed for the IoT. We provide a comprehensive taxonomy of the major security issues based on IoT architecture, attack implications and application areas. Furthermore, we tabulate and map the different countermeasures used to solve these threats taking into account new advances in security approaches. Finally, we discuss and compare the enumerated countermeasures for IoT security.

Keywords Internet of things (IoT) · Security · IoT threats · Attack implications · Emerging countermeasures

1 Introduction

The Internet of Things (IoT) is among the most developing technologies that have piqued the interest of academic and industry researchers [17]. It was firstly proposed in 1999 by Kevin Ashton and officially introduced in 2005 by the International Telecommunication Union (ITU) [1]. IoT is considered as a global network that enables the communication between anything in the world anytime and in anyplace by assigning a unique identity to each thing [1]. Furthermore, it comprises a wide variety of applications, including smart cities, smart buildings smart grids, healthcare, manufacturing, intelligent transportation,

✉ Dorsaf Swessi
dorsaf.swessi@ensi-uma.tn

Hanen Idoudi
Hanen.Idoudi@ensi-uma.tn

[1] National School of Computer Science (ENSI), University of Manouba, Manouba, Tunisia

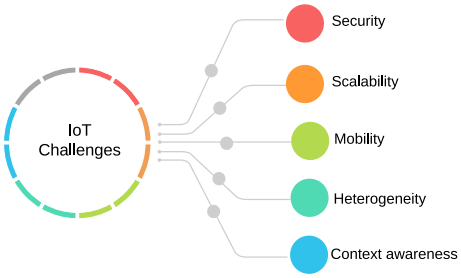

Fig. 1 IoT challenges

and so on. The most popular IoT application areas in 2020 are presented by IoT-analytics.[1] It is reported that till 2020,[2] there are about 31 billion connected devices worldwide and, every second, 127 new IoT devices are connected, with estimates forecasting 75 billion of connected things by 2025. In addition, Social IoT (SIoT) is also an emerging concept in which IoT combines with social networks and devices may be shared between people via the Internet [33].

Along with the challenges confronted by the Internet, IoT faces significant and special challenges including a massive number of connected devices, heterogeneity of the exchanged data, scalability, mobility, and resources limitation, summarized in Fig. 1, making it more complex than other networks and bringing new vulnerabilities. In October 2016, millions of users were prevented from access to over 1200 websites including Twitter, Netflix, and Spotify, among others. Due to the wide-scale Distributed Denial of Service (DDoS) attack, Mirai [110] which is still expanding its techniques to target more devices. Likewise, a group of security researchers was capable to attain absolute control of a Jeep SUV by utilizing a firmware update vulnerability through the vehicle's Controller Area Network (CAN) bus [84].

Securing such networks is quite challenging, and the majority of traditional security methods deployed for the Internet so far do not meet IoT security requirements. To prevent particular threats, many academics attempted to adapt existing security solutions to IoT, like lightweight cryptographic algorithms or hash functions, key management systems, and secure routing. However, such security measures cannot offer robust security against a broad range of security threats. Emerging technologies like artificial intelligence (AI), Blockchain, IoTA, and context awareness are being utilized as promising solutions to address security and privacy concerns in IoT. Therefore, a mix of various technologies is adopted to solve additional security problems and provide a safer IoT environment.

Recently, many surveys addressed IoT security challenges. In [51], authors classified security issues and solutions with regard to the IoT layered architecture and explained how Blockchain may solve many IoT security concerns. Authors in [4, 42] categorized the various security and privacy problems based on the four layers of IoT architecture and discussed the use of Blockchain and Machine Learning methods and their role in improving the degree of security in IoT. Further, authors in [1, 6, 11, 67] addressed the security threats linked with the various layers of IoT architecture and provided several security countermeasures. In contrast, Yang et al. [108] presented a categorization of IoT security measures based on IoT architecture without categorizing the different

[1] https://iot-analytics.com/top-10-iot-applications-in-2020.
[2] https://securitytoday.com/articles/2020/01/13/the-iot-rundown-for-2020.

Table 1 Recent surveys in IoT security

Year	Authors	Attacks classification	IoT Specific	Security requirements		Countermeasures	
			Attacks	Classic	Specific	Classification	Emerging
2015	Rwan et al. [11]	3 Layers architecture	–	✓	–	✓	–
2017	YuchenYang et al. [108]	4 Layers architecture	–	–	–	✓	–
2017	Minhaj et al. [51]	3 Layers architecture	-	✓	✓	✓	✓
2018	Yang Lu et al. [67]	4 Layers architecture	–	–	–	✓	✓
2018	Ahanger et al. [1]	IoT applications	✓	✓	–	–	–
2018	kouicem et al. [56]	IoT applications	✓	✓	-	✓	✓
2019	Hassija et al. [42]	4 Layers architecture	–	–	–	–	✓
2019	Inayat et al. [6]	4 Layers architecture	–	–	–	–	–
2020	Al-Garadi et al. [101]	4 Layers architecture	–	–	–	✓	✓
–	Our proposed survey	Attack implications Security requirements 4 Layers architecture Application areas	✓	✓	✓	✓	✓

threats and constraints. Additionally, authors in [56] broad overview of security issues related to IoT applications and design. They also categorized and analyzed the advantages of emerging methods such as Blockchain and Software-Defined Networking (SDN) in terms of flexibility and scalability.

As indicated in Table 1, the majority of these studies focused on classifying classical security threats and challenges and offering traditional solutions or some emerging approaches without a clear classification that discuss new relevant techniques that might bring significant benefits in terms of security and privacy.

In this study, we provide a comprehensive and up-to-date survey of security issues, attacks and countermeasures in IoT. We take a different direction than previous works by giving a clear classification of the majority of IoT classical and specific security issues on the basis of attack implications and compromised security requirements in each layer of IoT architecture. We utilize the four layers of IoT architecture for our new classification of IoT attacks and show up the importance of the support layer security. Additionally, each IoT application area is characterized by its own challenges, resulting in unique security requirements, leading to various threats that necessitate specialized and adaptive security solutions. Therefore, we categorize the main security countermeasures into classical and intelligent solutions, and we highlight and analyze existing

and emerging IoT security solutions that have not been covered in previous works. Our work's primary contributions can be summarized as follows.

- An explanation of the different security requirements that improve the security of the IoT infrastructure.
- A parametric analysis and classification of both classical and specific IoT security issues according to IoT architecture, attack implications and security requirements.
- Detailed and realistic recommendations to improve the IoT security.
- Taxonomy and categorization of the different countermeasures used to solve IoT threats.
- A discussion and a comparison of the enumerated countermeasures.

The remainder of our article is arranged as follows. The following section gives the key enabling security requirements in IoT. A classification of IoT classical and specific threats according to their implications and compromised security requirements in each layer of IoT architecture is discussed in Sect. 3. Section 4 describes in detail the main classical and intelligent countermeasures, as well as the benefits they provide in terms of security and privacy.

2 Security Requirements in IoT

Security encompasses all strategies aimed at preserving, restoring, and ensuring the security of information in computer systems against attacks. IoT inherits all security requirements as a network, but it also has numerous constraints and limitations in terms of resources and devices, computational and power resources, which defines additional challenges. Various security criteria must be considered for a secure IoT deployment, as detailed below.

2.1 Classical Security Requirements

2.1.1 Confidentiality

Any node in the IoT network has the risk of a confidentiality breach, which may include sending sensitive data to surrounding nodes or unauthorized users [1]. A suitable confidentiality mechanism is needed to guarantee that data and user privacy are safe and that they are only accessible and communicated to authorized users [51].

2.1.2 Integrity

IoT integrity issues result in data tampering by adversaries and communication problems. Integrity is associated with maintaining the credibility and veracity of data [1].

2.1.3 Non-repudiation

It is associated with the authentication of a legitimate user in order to get access to the requested service [1]. This concern is associated with three properties of IoT, namely:

autonomy, pervasiveness, and ubiquity. It guarantees that the sender of the message cannot deny having sent the message in the future [56].

2.1.4 Availability

The most frequent availability risks are denial of service (DoS) attacks and bottleneck scenarios. The goal of ensuring availability is to provide genuine users with rapid access to data, services, and devices in both normal and crisis conditions [1].

2.2 A A A

2.2.1 Authentication

Unauthentic users may obtain access to the network and read, alter, or delete data, as well as damage the entire system, by tampering with control and sensing data [1]. Authentication implies that each node in the IoT Network should be able to identify and authenticate other nodes.

2.2.2 Authorization

An unauthorized adversary can easily eavesdrop or alter sensitive data and inject malicious information, etc. Authorization ensures that only genuine and authorized nodes have access to systems or data [51].

2.2.3 Accountability

Accounting for resource consumption entails assigning specific responsibilities to each node for data assurance and ensuring that each node's activities can be traced uniquely to it [51].

2.3 Specific Security Requirements

2.3.1 Resources Efficiency

It ensures that the intruder will be unable to carry out attacks on IoT architecture that may lead to increased resource usage due to duplicate or faked service requests [51]

3 Attacks Classification

The IoT is expected to connect any object from any external or internal network to communicate with other objects directly via the Internet. Additionally, the IoT Data flows via many nodes, through different networks and in different arias, which may expose its sensitive information to numerous attacks, alterations, external intrusions, data theft, unauthorized access, and even the destruction of the whole IoT system.

Table 2 IoT classical attacks classification

Security issues	Affected layers				Implications							Security requirements								References
												Classical				AAA			Specific	
	Perception	Network	Support	Application	Disruption	DoS/DDoS	Privacy violation	Res consumption	Spoofing	Bottleneck	Eavesdropping	Confidentiality	Integrity	Non-repudiation	Availability	Authentication	Authorization	Accountability	Resources efficiency	
Node capturing/tampering	✓					✓	✓					✓	✓			✓	✓			[2, 67]
Malicious data injection	✓			✓		✓						✓	✓			✓	✓			[42, 67]
Jamming adversaries	✓	✓			✓	✓						✓			✓					[51]
Initialization and configuration	✓				✓	✓	✓					✓								[22, 51]
Replay attack	✓	✓			✓	✓	✓	✓				✓			✓	✓	✓		✓	[1, 58, 67, 104]
Booting attack	✓					✓						✓							✓	[42]
Timing attack	✓					✓						✓								[2, 67, 96]
Eavesdropping	✓	✓									✓	✓	✓	✓		✓				[42, 63]
Mass node authentication	✓	✓					✓									✓				[111]

Table 2 (continued)

Security issues	Affected layers				Implications							Security requirements								References
												Classical				AAA			Specific	
	Perception	Network	Support	Application	Disruption	DoS/DDoS	Privacy violation	Res consumption	Spoofing	Bottleneck	Eavesdropping	Confidentiality	Integrity	Non-repudiation	Availability	Authentication	Authorization	Accountability	Resources efficiency	
Trace back submitter	✓						✓				✓	✓								[108]
Firmware updates	✓					✓						✓								[42]
Replay and duplication attacks		✓			✓	✓		✓							✓				✓	[44, 52]
Buffer reservation attack		✓				✓		✓											✓	[44]
Routing attack		✓			✓	✓	✓				✓	✓				✓				[3, 42, 61, 67]
Access attack		✓				✓	✓					✓			✓					[42]
DoS/DDoS/PDoS attacks	✓	✓	✓	✓		✓									✓					[1, 42, 54, 58]
Data transmission attack		✓					✓					✓								[42]

Table 2 (continued)

Security issues	Affected layers				Implications							Security requirements								References
												Classical				AAA			Specific	
	Perception	Network	Support	Application	Disruption	DoS/DDoS	Privacy violation	Res consumption	Spoofing	Bottleneck	Eavesdropping	Confidentiality	Integrity	Non-repudiation	Availability	Authentication	Authorization	Accountability	Resources efficiency	
Network congestion problems		✓										✓				✓				[111]
Malicious insider		✓					✓				✓	✓	✓							[62]
Botnet attack		✓				✓					✓	✓	✓		✓					[42, 64, 108]
Man-in-the-middle attack		✓	✓				✓				✓	✓			✓	✓				[42, 88]
SQL injection attack			✓				✓					✓								[31, 87, 109]
Signature wrapping attack			✓				✓				✓	✓	✓							[42, 59]
Cloud-based IoT attacks			✓				✓					✓			✓		✓			[41, 51, 67,73]
Secure on boarding			✓				✓				✓	✓								[42]

Table 2 (continued)

Security issues	Affected layers				Implications							Security requirements								References
												Classical				AAA			Specific	
	Perception	Network	Support	Application	Disruption	DoS/DDoS	Privacy violation	Res consumption	Spoofing	Bottleneck	Eavesdropping	Confidentiality	Integrity	Non-repudiation	Availability	Authentication	Authorization	Accountability	Resources efficiency	
Middleware security		✓	✓	✓	✓	✓	✓									✓				[51]
Authentication and communication		✓	✓				✓					✓				✓				[37, 86]
Session establishment and resumption			✓				✓									✓				[46, 77]
Interoperability & portability		✓	✓				✓					✓		✓						[6]
Business continuity and disaster recovery			✓		✓	✓									✓					[6]
Single point failure			✓			✓									✓					[42, 51, 85]

Table 2 (continued)

Security issues	Affected layers				Implications							Security requirements								References
												Classical				AAA			Specific	
	Perception	Network	Support	Application	Disruption	DoS/DDoS	Privacy violation	Res consumption	Spoofing	Bottleneck	Eavesdropping	Confidentiality	Integrity	Non-repudiation	Availability	Authentication	Authorization	Accountability	Resources efficiency	
Tenants security			✓				✓				✓	✓				✓				[6]
Phishing attacks			✓	✓			✓					✓			✓					[67]
Linux malware				✓		✓	✓					✓					✓			[108]
Malicious scripts/ malware attacks				✓		✓	✓					✓	✓		✓		✓			[67, 108]
CoAP security with internet				✓		✓				✓		✓				✓				[93]
Insecure interfaces				✓	✓	✓	✓					✓								[51]
Insecure software/ firmware		✓	✓	✓	✓	✓	✓					✓								[51]
Mass-data vulnerability				✓		✓						✓								[2]

Table 2 (continued)

Security issues	Affected layers				Implications							Security requirements								References
												Classical				AAA			Specific	
	Perception	Network	Support	Application	Disruption	DoS/DDoS	Privacy violation	Res consumption	Spoofing	Bottleneck	Eavesdropping	Confidentiality	Integrity	Non-repudiation	Availability	Authentication	Authorization	Accountability	Resources efficiency	
Software vulnerability				✓		✓						✓								[2]

3.1 Classical Attacks

IoT inherits many network vulnerabilities and threats from the Internet. Table 2 contains a taxonomy of these IoT security attacks, as well as publication references for each one. As explained below, our categorization varies from conventional layered architecture in that we classified the issues based on their implications and violated security requirements in each layer. We utilized a four-layer architecture rather than the standard three-layer architecture to clarify the categorization and highlight the necessity of support layer security.

3.1.1 Perception Layer

Due to the constrained resources of the IoT devices and the dynamic nature of the IoT network, there are several attacks and implications on the perception layer.

3.1.2 Disruption

Many attackers may exploit the insecure initialization and configuration of the IoT nodes by breaching privacy, disrupting network functions and corrupting confidentiality and availability of the system [22, 51]. In jamming adversary attack, the attacker produces radio frequency signals without following a specific protocol and emits them continuously or based on the channel's activity to interfere with legitimate wireless communications, which disrupt the network operations and completely blocks the communication between the legitimate node [51, 107]. Furthermore, replay attacks can be made by spoofing, altering, and replaying the identity information of the IoT nodes or by malicious Sybil nodes that use fake or multiple identities for a single node, resulting in network performance and integrity degradation and data privacy violations [1, 51, 67].

3.1.3 Denial of Services

Because of the nature of IoT nodes, many threats may cause the denial of services of the whole system. In Booting attack, the adversary tries to attack the devices when they are being restarted. Since the security mechanisms are not activated during the boot process [42]. Moreover, after tampering a node, the attacker can easily alter sensitive data, inject malicious data, force the node to perform unintended functions, or gain access to the entire IoT system [42, 67, 96]. Also, the Timing attack can be generated by analyzing the time required for executing the encryption algorithm and obtaining the encryption key's information [42, 67, 96]. Another DoS attack is the Permanent or Phlashing denial of services (PDoS)[3] which destroys the IoT device via hardware sabotage.

3.1.4 Privacy Violation

Many attacks can affect the confidentiality, authentication, availability, and authorizations by violating the privacy of the nodes like node capturing/tampering attacks [2, 42, 67] where the attacker capture the whole node or part of its hardware, replace it with a malicious node or connect directly to it, and that may appear to be part of the IoT system

[3] https://www.datafoundry.com/blog/what-is-a-permanent-dos-pdos-attack.

but controlled by the attacker. Therefore, a malicious data injection attack can be made. Because of the limited resources of devices, gateways are used to download and install firmware updates, implying that a vulnerable version of the firmware might destroy the system [42]. In addition, many nodes in IoT systems suffer from authentication issues, and the network communication requires authentication purposes only, hence affecting the system's performance [42, 67, 111].

3.1.5 Eavesdropping

The eavesdropper can deploy a sensor near the IoT nodes or use some sniffing tools such as "Packet sniffer" to sense the same data or sniff the traffic in the wireless proximity network then capture the data during transmission or authentication processes, which harms its confidentiality, integrity, and authentication [42, 63].

3.2 Security Recommendations

To detect malicious nodes and take actions to avoid further deterioration of the service, it is recommended to use a localized fault detection algorithm to identify the malicious nodes, a decentralized intrusion detection system, intrusion detection probability in both homogeneous and heterogeneous networks, and a multi-layer-based intrusion detection system for sleep deprivation attacks [17, 51]. To protect the legitimate nodes of backdoor authentication, data breach, eavesdropping, or data injection [42], it is essential to use end-to-end encryption, ID authentication, cryptographic algorithms, and key management mechanisms (Like Rabin's Scheme, NtruEncrypt, and Elliptic Curve Cryptography (ECC)) [63]. While sensing in IoT applications, cryptographic mechanisms, anonymous data aggregation, and data reporting protocols are needed to avoid trace back submitters [108]. And a modern chip is required to prevent Side-channel attacks [42]. It is also essential to secure the boot process, software/firmware updates, and set data transmission rates between nodes [42, 51]. As well as abstain from unnecessary interfaces, software/firmware access to the Universal Serial Bus (USB) [42]. Hardware-based Trusted Platform Modules (TPM), and testing/debugging tools are crucial too [51]. Moreover, signal strength measurements and channel estimation, computing packet delivery ratio, encoding packets with error-correcting codes, and changing frequencies and locations must be employed to avoid threats like replay and jamming attacks. [1, 51, 67].

3.2.1 Network Layer

Because of the large number of nodes, the massive amount of data transmission, and the heterogeneous environment, the network layer faces various threats, as explained further down.

3.2.2 Disruption

Disruption in the network layer may be created via routing attacks in which the attacker attempts to manipulate routing information and spread it in the network to generate routing loops, advertise bogus routes, generate error messages, or drop network traffic [42, 51, 67]. A wormhole attack can disrupt the encrypted traffic by producing a tunnel between a compromised node and an external attacking device to bypass the IoT security protocols.

While a Sinkhole attacker reveals an artificially shortest routing path and attracts devices to flow traffic through it, then performs malicious network activities. Combining these two attacks can have severe implications, such as eavesdropping, privacy violations, and denial of service [42, 51].

3.2.3 Denial of Services

DoS attacks originating from or on IoT nodes are a grave concern due to their limited configuration and the heterogeneity and complexity of IoT networks. Thus the adversary can easily flood the target servers with a massive number of unnecessary requests [42] result in exhausting resources, overburdened network unavailable services to legitimate users [6].

3.2.4 Privacy Violation

A malicious insider is an internal attacker who violates legitimate nodes' privacy by intentionally modifies and extracts information from the IoT network. In addition, with access attacks, an unauthorized adversary gains access to the IoT network and may remain undetected in the network for an extended period of time in order to steal important data or information rather than causing network damage [42, 62].

3.2.5 Eavesdropping

Low-Power and Lossy Networks (RPL) are subject to a variety of attacks launched by compromised nodes in the network, which may lead to eavesdropping on the whole network traffic and exhausting the nodes' energy [51].

3.2.6 Resources Consumption

An attacker can easily exhaust IoT resources with replay or duplication attacks by duplicating fragments or replicating the packet fragment fields, which may lead to resource depletion, slower processing of valid packets, and even devices restarting [44, 52]. Moreover, an attacker may employ a buffer reservation attack to exploit allocated buffer space for re-assembly by delivering incomplete packets, resulting in a resource drain and buffer overflows [44].

3.3 Security Recommendations

For communication vulnerabilities, it is necessary to use a timestamp, nonce options, and fragment verification through hash chains for fragmentation attacks [51]. A split buffer approach that requires complete transmission of fragments is important to prevent buffer reservation attacks [44]. While extending IPv6 Low power Wireless Personal Area Networks (6LoWPAN) that enables Internet Protocol Security (IPSec) communication with IPv6 devices is needed. It is also essential to employ end-to-end security, hashing, and signature-based authentication using ECC-based signatures [51] without the need for a reliable gateway [108]. Likewise, rank verification via hash chain function, trust management, network activity analysis, Intrusion Detection Systems (IDS), key management, graph traversals, and signal strength measurement are all crucial [51].

3.3.1 Support Layer

The support layer's goal is to serve as an abstraction layer between the network and application layers. However, it is equally vulnerable, and any security flaw or significant overhead of securing communication may expose it to a wide variety of attacks. Some of them are listed below.

3.3.2 Denial of Services

A damaged or injected virtual machine in IoT cloud can affect other virtual machines or attack the whole system. There are several forms of attacks that may occur, like the Cloud Flooding attack in which the attacker sends several queries to a service in a continuous loop to expand the load on the cloud servers, thus denial of services, privacy violation as well as confidentiality, availability and authorization issues [41, 51, 67, 73].

3.3.3 Privacy Violation

The middleware layer suffers from several attacks that breach identity and location privacy. A malicious cloud service vendors where IoT services are deployed can easily access transmitted confidential information. Furthermore, an adversary may insert malicious SQL queries (SQLi) into services to get sensitive data from any legal node or even modify database records [42].

3.3.4 Eavesdropping

A Man-In-The-Middle (MITM) attacker could manipulate the broker or eavesdrop node's keying material and control all communication without the knowledge of the nodes or during the gateway's onboarding process [42]. Additionally, by exploiting the Simple Object Access Protocol (SOAP) vulnerabilities, the attacker bypasses the Extensible Markup Language (XML) signature mechanism and may gain control, insert malicious code and modify eavesdropped messages to access the legitimate node's service requests and collect sensitive information [42, 88].

3.4 Security Recommendations

For middleware communication and to prevent MITM attacks, it is vital to use end-to-end encryption, robust key exchange mechanisms, symmetric key-based encryption, and security policies [42, 51, 88]. Also, hybrid, fuzzy extractor long-lived secret key authentications, software-based Advanced Encryption Standard (AES), TPM employing Rivest-Shamir-Adleman (RSA), and Secure Hash Algorithm SHA1/AES are essential [51]. Advanced protocols and software/hardware [67], distributed logs, and symmetric homomorphic mapping are utilized to identify irregular activities [51]. Implementing cloud Security Alliance (CSA) standards, policies, and requirements for continuous cloud Audits is required for cloud-based threats [6]. Furthermore, secure virtualization technologies, tenant separation, and data encryption should be employed to ensure the confidentiality and integrity of customer information [6]. It is also suggested to set up the IoT network from a central location, store control messages at several locations, and secure packet forwarding for delay tolerant networks, and secure Constrained Application Protocol (CoAP) utilizing

ECC [42, 51]. Lastly, data loss prevention technologies, database activity monitoring, and data fragmentation are also recommended to safeguard and detect data migration from the cloud [41, 73].

3.4.1 Application Layer

The application layer threats are mainly concerned with the applications executing on IoT as discussed as follows.

3.4.2 Denial of Services

Relay Chat (IRC), an application layer protocol that allows text-based communication, is vulnerable to Internet Relay Chat Network Virtual Terminal Protocol (IRCTelNet) malware, which compromises the node by brute-forcing its Telnet ports and infecting the operating system. As a result, the device became a slave of the botnet network to launch massive DDoS attacks [64, 108].

3.4.3 Privacy Violation

Malicious script and malware attacks may severely affect data privacy. An attacker can control access and steal data or shut down the system when the user executes a malicious script in gateways [67]. In addition, the attacker can inject malware onto the system via viruses, worms, trojan horses, and spyware in order to deny service, modify data, and steal private data [67].

3.4.4 Bottleneck

Linux malware attacks may hook IoT devices into botnets and get shell access through the default password of TelNet or Secure Shell (SSH) accounts, causing delayed processes, file deletion, and even the installation of further malware on the system [64, 108] Moreover, The CoAP messages follow a specific unsecured format defined in RFC-7252, which may lead to bottleneck, authentication and confidentiality problems [51].

3.4.5 Eavesdropping

The code with languages such as JSON, XML, SQLi, and XSS and insecure software/firmware updates are vulnerable and could be a gate for eavesdroppers. Phishing attacks are made by an adversary who employs infected emails or phishing sites to compromise the user's credentials, such as login credentials or credit card information and accesses the whole IoT system, which may lead to severe damage [67].

3.5 Security Recommendations

It is crucial to combine Transport Layer Security (TLS), Datagram TLS (DTLS), secured Hypertext Transfer (HTTPS) with firewalls, CoAP mapping, Mirror Proxy (MP), and Resource Directory protocols to secure the application layer. TLS-DTLS tunneling and message filtering through 6LoWPAN Border Router (6LBR) are also essential [51]. Another critical security measurement is to guarantee regular security updates of software/

firmware, the usage of file signatures, and encryption with validation [51]. Moreover, weak passwords must be prevented, and the interface must be tested for software tool vulnerabilities (SQLi and XSS) [51].

3.6 Specific Attacks for IoT

Due to the inherent heterogeneity of the IoT systems, scalability, high mobility, resource limitation, and the vast spectrum of IoT applications, many new security challenges and issues face the IoT systems. In this section we describe specific security attacks, faced by major IoT applications, as illustrated in Table 3.

3.6.1 Smart Cities, Smart Homes

Smart cities and smart homes are one of the most critical applications of the IoT ecosystem. It offers an effective environment for resource management, thus improving the quality of services such as water distribution, pollution reduction, and traffic congestion. The large amount of the integrated devices from different applications combined with the lack of communication standards leads to heterogeneity, scalability, and data management issues. As a result, attackers may exploit these weaknesses to compromise data confidentiality, authentication, availability, and integrity. Several smart cities threats are presented below.

Social Engineering: it is the knowledge of utilizing social interactions as a technique to convince and deceive a victim into complying with the attacker's request in order to gather sensitive information [35]. It is a psychological attack that attacks the IoT users via devices rather than their devices.

Physical deterioration: Because IoT nodes often operate in exterior and outdoor environments, the attacker has the ability to physically destroy it [108].

Insecure RFID: due to RFIDs' weak radio frequency signals, the attacker may corrupt them with noise signals or sniff the target tag's Electronic Product Key (EPC) to use it to transmit malicious data or to program it to another tag to obtain access to the system or cause a denial of services [11, 112].

Hello Flood attack: Several protocols assume that when a device receives a Hello packet, the sender is within its radio range and considers it a neighbor. Therefore a Hello flood attacker may utilize a high-powered transmitter to mislead IoT nodes into believing it is a neighbor and falsely broadcast the information to all the other devices [1]. Thus, cause denial of services, privacy and non-repudiation violation.

BlackHole, GreyHole attacks: An external adversary attempts to disrupt nodes communications by compromising a node and refusing to transmit incoming packets or pretending to have the shortest route and then drops, holds, or passes them. As a result, the availability of services is jeopardized [5].

Sleep deprivations attack: Because of the limited resources, IoT Sensors adopt sleep mode to save energy. An attacker can drain the battery by executing endless loops code, depriving it of the sleep mode, or intentionally boosting the power usage of the nodes [17, 51].

3.6.2 Manufacturing

IoT has a significant impact on the industry as well. The Industrial Internet of Things (IIoT) integrates IoT emerging techniques with industry mechanisms to provide an intelligent

Table 3 IoT specific attacks classification

Security issues	Affected layers				Implications							Security requirements								References
												Classical				AAA			Specific	
	Perception	Network	Support	Application	Disruption	DoS/DDoS	Privacy violation	Res consumption	Spoofing	Bottleneck	Eavesdropping	Confidentiality	Integrity	Non-repudiation	Availability	Authentication	Authorization	Accountability	Resources efficiency	
Physical deterioration	✓					✓						✓				✓			✓	[108]
Side-channel attack	✓						✓					✓	✓			✓				[42, 57, 67]
Sleep deprivation attack	✓					✓		✓											✓	[17, 42, 51]
Insecure RFID	✓	✓				✓	✓				✓	✓				✓				[11]
Insecure neighbor discovery		✓				✓			✓							✓				[51]
Selective forwarding attack		✓			✓	✓						✓	✓							[1, 70]
Hello flood attack		✓				✓					✓	✓		✓						[1, 50]
Social Engineering				✓			✓					✓	✓							[35]

Table 3 (continued)

Security issues	Affected layers				Implications							Security requirements								References
												Classical				AAA			Specific	
	Perception	Network	Support	Application	Disruption	DoS/DDoS	Privacy violation	Res consumption	Spoofing	Bottleneck	Eavesdropping	Confidentiality	Integrity	Non-repudiation	Availability	Authentication	Authorization	Accountability	Resources efficiency	
Black-Hole, Grey-Hole		✓			✓							✓	✓		✓					[5]
Stealthy sensor attack	✓				✓	✓														[99]
SCADA modbus attacks		✓				✓							✓	✓		✓				[99]
Supply chain attacks	✓			✓		✓						✓								[99]
Ransom-ware attacks				✓	✓							✓	✓		✓					[101]
Proximity attack	✓				✓	✓						✓	✓							[57]
Same-Nonce attack	✓							✓			✓	✓	✓				✓		✓	[57]
Hidden vehicle attack		✓							✓				✓	✓		✓				[7]

Table 3 (continued)

Security issues	Affected layers				Implications							Security requirements								References
												Classical				AAA			Specific	
	Perception	Network	Support	Application	Disruption	DoS/DDoS	Privacy violation	Res consumption	Spoofing	Bottleneck	Eavesdropping	Confidentiality	Integrity	Non-repudiation	Availability	Authentication	Authorization	Accountability	Resources efficiency	
Location tracking			✓										✓							[7]
Fuzzy attack		✓			✓	✓									✓				✓	[15, 100]
Accelerator attack	✓				✓	✓									✓				✓	[100]
Illusion attack		✓			✓								✓							[7]
Rushing attack		✓			✓		✓				✓	✓	✓							[5]
Coward attack		✓		✓	✓		✓		✓		✓		✓	✓		✓				[65]

industrial ecosystem capable of improving production by offering potential solutions for automating the manufacturing process and efficiently controlling the production chain. Maintaining IIoT's security is challenging due to a lack of standards, resource constraints, and scalability problems, thus jeopardising the system's availability, integrity, confidentiality, and authenticity. In this section, we will demonstrate some of the IIoT security issues.

Stealthy sensor attack: After launching a MITM attack, the attacker may modify sensors and actuators configurations such as exaggerating certain values in order to alter the functioning of particular mechanisms that may affect the system's functioning [99].

SCADA modbus attacks: Vulnerabilities in the SCADA network Modbus protocol, such as implementation problems, enable an unauthorized intruder to launch a DoS or DDoS attack by sending request or response settings containing erroneous values to a data field on the system [99].

Supply chain attacks: due to the participation of many manufacturers in the construction and assembly of device components, a vendor may add backdoor channels, viruses, or provide defective chips in their products. Unfortunately, this maliciously injected code may be executed without being noticed or controlled [99].

3.6.3 Healthcare

Patients' bodies are implanted with smart objects to monitor and track their physiological conditions. The Internet of Healthcare Things (IoHT) or The Internet of Medical Things (IoMT) integrates IoT mechanisms in the healthcare sector to sense, actuate, and gather information about the patient health state to transmit it to the authorized individuals in order to supervise its health status. This type of communication between healthcare objects and objects with hospitals servers must be adequately secured and assure its authentication, confidentiality and integrity security requirements because any security threat can harm the patient's life. It also comes with many challenges like resources limitation and mobility of wearable objects and heterogeneous environments.

Ransomware attacks: one of the most significant healthcare-related attacks in which target medical systems become useless unless a ransom is paid. This attacks is more concerned with applications and data rather than device hardware and may lead to operations disruption, loss of patient data, and reputation damage. In addition, Ransomware attacks have a severe effect on the system's integrity, availability, and confidentiality and have many variants like Scareware, BadRabbit, WannaCry, and Petya-Esque attacks [101].

Selective forwarding attack: A variant of the Blackhole attack in which the attackers gain control of one or more nodes so that one of them drops a malicious packet while the others assist in covering up the attack. It results in packet loss or incomplete data transmission, putting the patient's life at risk, as well as denial of services and data integrity problems [1, 70].

Proximity attacks: Due to the lack of rigorous security mechanisms in the Near Field Communication (NFC) standard, an attacker using basic antennae may cause data breaches, signal manipulation, privacy violations, and denial of service [57]. Furthermore, Proximity Inductive Coupling Card (PICC) attacks may be carried out by pairing devices and exploiting their protocol challenge response requests with the help of a malicious NFC reader and an emulated PICC [57].

Side-channel attack: An adversary may attack the encryption techniques based on information like power consumption, time usage, and electromagnetic radiation of sensor nodes [42, 67]. Encrypted RFID implementations are susceptible to this attack due to their

inadequate active and passive systems [57]. Furthermore, shutting off equipment or disrupting service may cause RFID systems failure, putting the patient's safety at risk [57].

Same-Nonce attack: An attacker may exploit the ZigBee and Ultra-Wideband (UWB) vulnerabilities to generate incorrect access control settings or a power failure [57]. Consequently, the systems will clear the access control list and share the same nonce and security key for two consecutive messages. Thus, by XORing these two successive cipher messages, the attacker may retrieve partial data [57].

3.6.4 Transportation Systems

The Internet of Vehicles (IoV) is a revolutionary concept in Intelligent Transportation Systems (ITS) that integrates the existing capabilities of Vehicular Ad-hoc Networks (VANETs) with the Internet of Things to enable Vehicle-to-everything (V2X) communications. Vehicle-to-Infrastructure (V2I), Vehicle-to-Vehicle (V2V), and Vehicle-to-Device (V2D), as well as Vehicle-to-Pedestrian (V2P), Vehicle-to-Grid (V2G), and Vehicle-to-Sensors (V2S) are all V2X communication variants. Besides that, IoV is distinguished by dynamic topological structures, large network scale, and high mobility, leading to increased security issues that threaten the authentication, confidentiality, non-repudiation, and availability of the entire system. In this section we enumerates several IoV attacks.

Hidden vehicle attack: also known as GPS spoofing or location bogus attacks that generate misleading position alerts to cause accidents [7]. This attack manipulates the mobility data which affects authentication, integrity and non-repudiation security requirements.

Location tracking: following a GPS spoofing, or collecting shared locations between legitimate nodes, an internal or external adversary may follow the vehicle's location or route threatening the privacy of the vehicle's driver [7].

Fuzzy attack: an injection attack in which bogus random data is injected into the vehicle's internal CAN bus to corrupt the electronic control units (ECUs) [15]. It may cause unpredictable unit behavior, malfunctions, and failures such as accelerator impotence, heating and lighting issues, and navigation system troubles [100].

Accelerator attack: an advanced timing opaque attack proposed by ORNL [100] alters the vehicle's entire state, rendering it undetectable by a frequency-based IDS. Instead of compromising the normal target ID or timing, this attack targets a vehicle model-specific vulnerability that disrupts the ECUs and disables the cruise control [100]. Consequently, the car driver loses control, and the vehicle accelerates at a constant speed, regardless of accelerator pedal level, cruise control parameters, or whether the car is in drive or reverse mode [100].

Illusion attack: also known as position forging/falsification attack, occurs when an adversary transmits timely coordinated erroneous traffic alerts with falsified locations, creating car accidents, traffic congestion, or emergency braking [7]. This can be due to GPS antennas and GPS clock vulnerabilities which harms the data integrity.

Rushing attack: also called sudden attack, a novel sort of denial of services attack that has a direct and severe impact on the functioning of routing protocols [5]. During the route discovery phase, the attacker captures and immediately re-sends the road requests (RREQ) with zero delay from the source car to the destination cars, so that the destination vehicles accepts the rushed request (because it arrived first) and delete the original legitimate request because it considers it as a copy [5].

Coward attack: an attacker may dynamically modify his attacking plan after determining whether the declared wrong location will be detected, ensuring that no security system

would notice its attack [65]. Nonetheless, if the attacker suspects that a nearby security system would detect his misbehavior, he will temporarily cease or reduce his attack. This attack may be performed against the VANET's location verification protocol, resulting in system disruption, privacy breaches, as well as data integrity, non-repudiation, and authentication issues [65].

4 Security Countermeasures Classification

It is challenging to ensure IoT security because of the restrictions and limitations of resources that introduce additional concerns. Therefore, it is desirable to achieve security at a low cost and support context-awareness computing. This section categorizes the security solutions in two main approaches: classical and intelligent countermeasures.

4.1 Classical Countermeasures

It is true that traditional countermeasures, with some modifications, could be used to support the resource limitation of IoT objects; however, this is not a goal in and of itself but rather a constraint that must be addressed when designing and implementing protocols for data encryption or device authentication in IoT. Several traditional security solutions are mentioned below.

4.1.1 Protocols

Standard communication and routing protocol are insecure by design; that is why it should be wrapped with security protocols such as TLS and DTLS for communication and IPSec for routing [51]. These standards are not designed for IoT but developed to support it. For example, TLS 1.3 [28] reduces the handshake process and resource consumption over its previous versions.

4.1.2 End-to-End Encryption

Its aim is to ensure that data sent by the source node is reliably received by the destination node and should be undecryptable at any other stage [51] and without the intervention of a third party. Moreover, It is based on cryptographic algorithms, hash functions, and a signature algorithm, and it provides a solution to various threats caused by the employment of multiple encryption methods at various levels and protocols in an IoT system [42]. Authors in [36] suggested a lightweight solution for the post-quantum secure public-key Sign/Verify approach, which can maintain IoT technology's end-to-end security. For appropriate end-to-end security, it is also preferable to encrypt data using AES.

4.1.3 Cryptographic Algorithms

Several cryptographic algorithms have been developed or modified to support IoT environments, including symmetric key cryptographic algorithms like Data Encryption Standard eXtended Lightweight (DESXL), which is a lightweight version of the DESX algorithm, one of the most commonly used variants of DES and asymmetric key cryptographic algorithms such as the Nth degree truncated polynomial ring (NTRU) which is an alternative

to RSA encryption and ECC encryption, etc. Indeed, the authors in [24] proposed a new lightweight Identity-based Encryption (IBE) based on ECC encryption, bilinear map, and hash function that gains the advantage of IBE by using unforgeable string related to the user identity as public key without the need of certificates thereby eliminating its costly and heavy resource consumption.

4.1.4 Cryptographic Hash Functions

A one-way function that takes data of any length and generates a fixed size hash and the most often used hash function in IoT is SHA-256. In addition, The Merkle tree [71] is extensively utilized owing to the multiple levels of hashing that increase data security. It is a complete data structure and a hash binary tree used to rapidly summarize and confirm the integrity of large amounts of data, where the leaf nodes store the data, and the roots represent the data's hash values [55, 79, 103].

4.1.5 Signature Algorithms

Digital signature methods are intended to give an electronic equivalent to handwritten signatures used to establish unique digital signatures that enable data integrity, authentication, and non-repudiation [95]. The Elliptic Curve Digital Signature Algorithm (ECDSA) is one of the most widely used digital signatures algorithms in IoT [82].

4.1.6 Anonymity, Unlinkability and Traceability Techniques

These strategies rely on data suppression, randomization, or cloaking to prevent unauthorized access. Otgonbayar et al. [75] introduced a novel algorithm that kanonymizes IoT data streams produced by several IoT devices. Nonetheless, authors in [23] suggested the use of zero-knowledge proof (ZKP), which allows one party (prover) to demonstrate to another party (verifier) some property by proving its possession of some information without disclosing it in order to ensure the privacy of users' data and properties. Moreover, to reduce the resource usage caused by ZKP, they recommended combining it with ECC [23, 56].

4.1.7 Key Management Systems

They are essential for credentials and keys negotiation between nodes in order to secure the data flow. Several key management strategies are examined and compared systems in terms of their suitability for IoT contexts [89]. Further, Public-key infrastructure (PKI) allows users to securely interact across a network while verifying their authenticity [89].

4.2 Intelligent Countermeasures

Using traditional security measures for IoT often provide low power consumption mechanisms but lacks flexibility and unadaptable to specific IoT contexts. Therefore, new security mechanisms must be defined to guarantee the support of IoT devices' limited resources and all the specific security needs of IoT systems. In recent years, many novels and intelligent security countermeasures have been proposed to tackle IoT's environment requirements; some of them are mentioned below.

4.2.1 Blockchain

Researchers consider Blockchain technology as a major enabling technology that will play a significant role in monitoring, controlling, and, most crucially, securing IoT nodes [51]. There are two types of Blockchain: permissionless (or public) ones that support a massive number of nodes and are open to anyone to join, such as Bitcoin, and permissionned (or private) ones that are constrained to a specific group of participants and provide more privacy and access control, such as Hyperledger and Rippel Blockchain [42, 51, 83]. The most valuable aspects of Blockchain are its decentralized architecture and distributed nature, which makes security solutions more resistant to DoS attacks [56] and can provide secure data storage, effective access control, and removes the risk of a single point of failure [42]. Besides, Blockchain employs ECC and SHA-256 hashing to provide robust cryptographic proof for data authenticity, and integrity [12, 42] and the pseudonyms that do not reveal the identities of the nodes. Another aspect is the security of transactions, which are signed by the node and must be verified and approved by miners, making it nearly unattainable to forge or alter transactions that have already been stored in the Blockchain [56]. In addition, Blockchain can assist in creating a tamper-resistant, allowing all devices to access the same data more consistently and reliably [56]. As well as Blockchain smart contracts, which are programs created by users and automatically performed by smart objects that may provide decentralized authentication and authorization rules and conditions in order to offer unique and multiparty authentication to an IoT node [51, 56]. Latterly, several Blockchain-based strategies have been suggested to address various IoT security and privacy challenges. The first IoT platform based on Blockchain, called ADEPT (Autonomous Decentralized Peer-To-Peer Telemetry), was developed by IBM in 2013 [13]. To deal with the challenging scalability and reliability issues in smart cities, authors in [18] suggested a multi-layer security architecture that incorporates Blockchain as a distributed database layer. In [53], Blockchain was proposed as a solution to the SSH public key management problem; indeed, a new block holding the public key is added to the Blockchain each time a key is added, changed, or revolved. Authors in [34] proposed an HTTPS protocol based on Blockchain because of its peer-to-peer architecture that removes intermediate nodes and secure transactions that are kept in the Blockchain. Hashemi et al. [40] suggested a distributed and decentralized data storage system for exchanging data in IoT environments that uses Blockchain to administer access control and separate data management and data storage. A Blockchain-based framework was proposed in [14] to allow industrial IoT nodes to interact with the cloud for analysis and storage as well as to conduct secure transactions with the Blockchain network. In [20, 27, 48], authors demonstrated that smart contacts for Blockchain might enable and support the autonomous workflow and the sharing of services across IoT devices.

4.2.2 IoTA

IoTA, released in 2016, is an open, decentralized, and permissionless Distributed Ledger Technology (DLT) that delivers real-time micro-transactions, an efficient, reliable, lightweight, and free system, and built explicitly for resource-constrained IoT devices [30, 56, 83, 92]. Unlike Blockchain, the main benefit of IoTA is the removal of transaction costs and the lowering of processing time [30]. Moreover, instead of Blockchain's blocks, chains, and miners, IoTA employs a peer-to-peer system known as "Tangle" [80], which is a novel data structure based on a Directed Acyclic Graph (DAG): a data structure that goes in a single

direction without looping back on itself [16, 47]. In addition, each node is a transaction, and in order to be added to the Tangle, it must approve two other transactions by conducting a small amount of "Proof-of-Work" (PoW) [79] and a Markov Chain Monte Carlo algorithm is used to select the non-approved yet transactions (called tips) that will be presented for approval in the Tangle [16]. This platform has been utilized in several research projects for IoT applications. Shabandri et al. [92] utilized the IoTA protocol to enable machine-to-machine (M2M) data transactions for IoT sensors using Blockchain, allowing for reliable data exchange and promoting data monetization economy in sensor networks. Meanwhile, authors in [60] presented a distributed sensor node system that uses the IoTA protocol to gather securely, store, exchange, and analyze field data by employing IoTA protocol capabilities that enable M2M data and value transactions (data monetization). Furthermore, for improving privacy in Tangle transactions, a novel decentralized mixing protocol for the IoTA ledger that combines decryption mixnets with multi-signatures is proposed in [91].

4.2.3 Artificial Intelligence

AI offers several essential and extensively used methods, which are inspired by nature or human behaviors, such as Artificial Neural Network (ANN), genetic algorithms, or swarm behaviors such as artificial swarm intelligence [8]. Many researchers believed that adopting AI approaches might improve the effectiveness of security solutions, such as intrusion detection systems, to limit the harm caused by attacks on IoT networks. Alrajeh et al. [9] introduced an energy harvesting system based on an ANN algorithm to identify energy depletion attacks, particularly flooding attacks that produce DoS in a cluster-based Wireless Sensor Network (WSN). In [78] an ANN method based on Multi-Layer Perceptron (MLP) for identifying abnormal behaviors in IoT systems such as Blackhole and Grayhole attacks. A three-layer authentication technique based on a deep neural network (DNN) that conducts activity recognition and human authentication are presented in [94]. Many studies have proposed Q-learning mechanisms, including the Multi-Agent Reinforcement Learning (MARL) algorithm and optimal channel accessing strategy in multi-channel dynamic environments that avoid jamming attacks [39, 84], cloud-based malware detection strategy [106] and PHY-authentication method for spoofing attack detection [105]. Furthermore, Support Vector Machine (SVM) can be used to detect network intrusion and prohibit unauthorized users from IoT resources depletion [10, 76]. In [19] authors applied the K-NN strategy to solve the issue of unsupervised outlier detection in WSNs, which provides flexibility in defining outliers while using less energy.

4.2.4 Trust Management

In the literature, trust management methods have been researched in various areas, and they played an important position in IoT to ensure trustworthy data collection, context awareness, enhanced privacy and flexibility, and handle uncertainty issues during IoT objects communication [81]. In this respect, authors in [25] presented an adaptive trust management method for dynamic and social IoT systems wherein the distribution of trust values of IoT devices is the fundamental concept. In [66] another trust management mechanism is suggested, based on node behavior detection by evaluating recommended trust and statistical history trust. Furthermore, a novel trust computational approach that offers a robust way to calculate trust within a few iterations for thousands of objects based on three trust parameters reputations, recommendations, and knowledge to evaluate the trustworthiness

of IoT nodes improves the effectiveness and performance compared to other methods has been suggested in [69]. Moreover, in [74] proposes a reputation-based trust management method for SIoT, in which objects can establish social relationships autonomously by computing the trustworthiness of an object depending on experiences and perceptions of common trusted entities before distributing information and services only to it. In other work, Lize et al. [38] implemented a three layers (perception, core, and application) IoT architecture for trust management control system in which each one is managed by precise trust management based on multi-service and self-organization routing, and the final decision is made based on the collected trust data and requester policy.

4.2.5 FOG Computing

There are many environments from which IoT may benefit to improve its security. For example, FOG computing may process data produced by IoT nodes locally for better management [56], and it serves as a security layer between end-users to the IoT system that detects and mitigates anomalous behaviors before they are sent. The authors in [98] suggested using a fog computing environment to execute a robust centralized architecture for the end-to-end incorporation of an IoT-based healthcare system. As an intermediary layer, fog may aid in the security of authentication and authorization during end-node communication and data transmission across remote healthcare systems. Furthermore, [68] presents a lightweight privacy preserving data collection strategy for Fog computing IoT in which the fog device may filter incorrect data locally, making it robust against fake external data injection attacks.

4.2.6 Software Defined Networking

SDN is another effective method for addressing some problems in IoT environments. Its primary aim is to isolate the network control system from the data so that an SDN controller conducts control choices rather than devices [49, 56]. In [21] authors developed an OpenFlow based SDN architecture in which gateways dynamically scan network traffic to detect compromised or malicious entities by recognizing attacks, thus take an appropriate mitigation measure. As well, Salman et al. [90] proposed an SDN identity based authentication architecture for IoT in which the SDN controller is in charge of access control by providing an authentication certificate for the gateway, making it robust to masquerade, MITM and replay attacks.

4.2.7 Context Awareness

Due to the heterogeneous, low-powered, and dynamic nature of the IoT environment, static security measures are inefficient and require many resources; that's why security solutions should be adaptable to the context in which IoT objects evolve. A context is the set of conditions under which an entity is used. It can be the time interval occupied by the object, the spatial context such as the object's location (geographical or logical location), the software and hardware environment, or any information such as the temperature, the level of the battery, the level of sensitivity against attacks, and the trustworthiness of the object [56]. Mauro et al. [29] introduced an adaptive security method for Energy Harvesting WSNs (EH-WSNs) in which each node may dynamically adjust its security settings such as cryptographic primitives or encryption key size based on its energy level and notify

its neighbors about it. In the same concept of an energy-aware security method, the authors of [97] proposed a solution that reduces the amount of sent packets to just necessary packets when the device's battery level is low. Furthermore, an adaptive security mechanism based on the reliability of devices is introduced in [43]. Whereby each node periodically calculates the level of trust of its neighbors based on its experiences, observations, and recommendations to determine whether it authenticates each of its neighbors or not. Authors in [33, 110] presented an adaptative security solution based on Markov game theory that assists in making appropriate security decisions depending on the computational cost and power consumption of IoT nodes.

4.2.8 Hybridization Solutions

Recently, the hybridization of two or more techniques has been suggested in the literature to improve IoT security. LIN et al. [64] developed a classified model that combines Artificial Fish Swarm Algorithm (AFSA) and Support Vector Machine (SVM) to detect essential traits in a botnet attack pattern. Authors in [45] provided a three-tier hybrid model for attack detection. The first of which is a signature-based technique that uses the blacklist notion to filter known attacks, the second of which is an anomaly detector that utilizes the white list concept to differentiate between normal and malicious traffic that passed through the first tier, and the third of which uses the SVM to identify unknown attacks. A decentralized cybersecurity architecture for IoT networks based on Blockchain, AI and SDN, is described in [85]. SDN analyzes traffic data and identifies attacks, Blockchain provides decentralized intrusion detection to reduce "single point of failure," and fog and mobile computing allow attack detection at the fog node while mitigating storage, computation, and latency limitations.

4.3 Discussion

Table 4 compares security countermeasures depending on IoT challenges and security needs. It is worth noting that the proposed security countermeasures are ineffective in all areas and/ or cannot meet all security criteria. IoT security strategies based on adapting traditional security countermeasures, including security protocols, cryptographic algorithms, or hash functions, are mainly aimed at or propose low "power, storage, and computation-cost" solutions. Still, they lack flexibility and scalability and are therefore unsuitable for the current context. Due to its distributed structure, Blockchain, on the other hand, seems to be a viable option in terms of scalability and heterogeneity. Fortunately, some challenges associated with Blockchain IoT application must be addressed, such as miner hashing power and private key management with limited randomness, which can be compromised by adversaries [51]. As well as bandwidth consumption due to the excessive number of generated transactions that can provoke a time latency problem for real-time applications [56, 83]. IoTA, on the other hand, optimizes transaction costs and lowers processing time [30]. However, one of its major drawbacks is the usage of PoW for security, which forces transaction producers to pay money for electricity and chips [32]. It also does not allow smart contracts that do not require transaction order finality, even though there is no incentive for new transactions to confirm these more complicated transactions since they take more computation to substantiate [32].

Meanwhile, AI methods, due to their robustness, adaptability to the environment, and flexibility, may improve the performance of security solutions. However, certain AI

Table 4 Security countermeasures classification

Counter measures	IoT challenges				Security requirements								References
					Classical				AAA			Specific	
	Heterogeneity	Mobility	Scalability	context awareness	Confidentiality	Integrity	Non-repudiation	Availability	Authentication	Authorization	Accountability	Resources efficiency	
Classical countermeasures													
Protocols	–	–	±	±	+	+	±	+	+	+	±	±	[28, 51, 56]
End-to-end encryption	–	–	–	–	+	+	+	+	+	±	±	±	[36, 42, 51]
Cryptographic algorithms	–	–	±	–	+	+	–	+	+	±	–	±	[24]
Cryptographic Hash functions	–	–	–	–	–	+	–	–	+	–	–	±	[55, 79, 103]
Digital signature	–	–	–	–	–	+	+	–	+	–	–	±	[95]
Anonymity-unlinkability-traceability	–	–	–	-	+	–	+	–	–	+	–	±	[23, 75]
Key management	–	–	±	–	+	+	+	+	+	±	+	±	[6, 89]
Intelligent countermeasures													
Blockchain	+	±	+	±	±	+	±	+	+	+	+	–	[12–14, 18, 20, 27, 34, 40, 42, 51, 53, 56, 83]

Table 4 (continued)

Counter measures	IoT challenges				Security requirements								References
					Classical				AAA			Specific	
	Heterogeneity	Mobility	Scalability	context awareness	Confidentiality	Integrity	Non-repudiation	Availability	Authentication	Authorization	Accountability	Resources efficiency	
IoTA	+	+	+	±	+	+	±	+	+	+	+	+	[16, 30, 47, 56, 60, 83, 91, 92]
Artificial intelligence	+	±	+	+	+	+	±	+	+	+	±	±	[8–10, 19, 39, 76, 78, 84, 94, 105, 106]
Trust management	+	±	−	+	+	±	+	−	−	+	+	±	[25, 38, 66, 74, 81, 69]
FOG computing	+	±	±	−	±	±	±	+	±	+	−	+	[56, 68, 98]
Software Defined Networking	+	±	+	−	±	+	±	±	+	+	−	±	[21, 49, 56, 90]
Context awareness	+	+	+	+	±	±	±	±	±	±	±	+	[29, 33, 43, 56, 97, 102, 110]
Hybridization Solutions	+	+	+	+	+	+	+	+	+	+	+	+	[21, 45, 85]

In this table a comparison of the countermeasures presented previously based on IoT security challenges and requirements is provided. The following notations are used to assess the level of satisfaction of each one: + good; ± average (it can deal with it); – bad

methods suffer from high computing cost and complexity, as well as regular required updates [72]. In contrast, trust management techniques may provide privacy, context awareness, and adaptability, but they need a significant amount of power consumption, and processing [81]. Furthermore, while fog computing can provide practical solutions to many limitations such as bandwidth consumption, resource limitations, and latency issues [26], it can also result in policy violations, and malicious activities on fog nodes or IoT devices since proper intrusion detection and data privacy mechanisms are not implemented [42]. SDN strategies are distinguished by their agility, dynamism, and flexibility. They can minimize computing costs and resource usage, but due to their centralized design, they cannot cope with scalability problems effectively [49, 56]. Last but not least, hybridization solutions of several mechanisms have shown better performance that capitalizes on the benefits of each component while correcting the limits of each.

5 Conclusion

The Internet of Things is a revolutionary technology that has drawn attention all over last decade. However, because of its heterogeneity, dynamic nature, wireless environment, various application fields and ongoing development, it faces several security issues. Despite all the researches that have been done so far, securing such environment is still an open challenge especially with the continuously new defined use cases and technologies that integrated to the IoT ecosystem. In this paper, we reviewed IoT security threats and the so far suggested countermeasures for IoT security. First and foremost, we highlighted the essential enabling security needs, particularly those applied in IoT. Following that, we evaluated and categorized the most critical security issues based on IoT architecture, attack implications, IoT application fields, and security requirements, as well as their possible security recommendations. We distinguished clearly the classical attacks that face IoT and the new specific vulnerabilities that come with IoT use cases and applications. Literature-proposed security countermeasures include both traditional solutions such as cryptographic methods and security protocols and intelligent solutions such as Blockchain, AI, and IoTA. We point out that the hybridization of multiple methodologies offers better performance and protection of IoT systems against a wide range of security attacks and threats. Finally, we compared and discussed various solutions in terms of IoT challenges and security requirements. IoT security continues to face many unresolved problems despite all proposed solutions due to the growing and dynamic IoT ecosystem.

Author Contributions Not applicable.

Declarations

Funding Not applicable.

Availability of Data and Material Not applicable.

Conflicts of interest Not applicable.

Code Availability Not applicable.

References

1. Khan, M. A., & Salah, K. (2018). IoT security: Review, blockchain solutions, and open challenges. *Future Generation Computer Systems, 82,* 395–411.
2. Hassija, V., Chamola, V., Saxena, V., Jain, D., Goyal, P., & Sikdar, B. (2019). A survey on IoT security: Application areas, security threats, and solution architectures. *IEEE Access, 7,* 82721–82743.
3. Roman, R., Alcaraz, C., Lopez, J., & Sklavos, N. (2011). Key management systems for sensor networks in the context of the internet of things. *Computers and Electrical Engineering, 37*(2), 147–159.
4. Otgonbayar, A., Pervez, Z., & Dahal, K. (2016). Toward anonymizing iot data streams via partitioning. In *2016 IEEE 13th international conference on mobile ad hoc and sensor systems (MASS)* (pp. 331–336). IEEE.
5. Ahanger, T. A., & Aljumah, A. (2018). Internet of things: A comprehensive study of security issues and defense mechanisms. *IEEE Access, 7,* 11020–11028.
6. Antonakakis, M., April, T., Bailey, M., Bernhard, M., Bursztein, E., Cochran, J., et al. (2017). Understanding the mirai botnet. In *26th USENIX security symposium (USENIX Security 17)* (pp. 1093–1110).
7. Yang, Y., Wu, L., Yin, G., Li, L., & Zhao, H. (2017). A survey on security and privacy issues in internet-of-things. *IEEE Internet of Things Journal, 4*(5), 1250–1258.
8. Lu, Y., & Da Xu, L. (2018). Internet of things (iot) cybersecurity research: A review of current research topics. *IEEE Internet of Things Journal, 6*(2), 2103–2115.
9. Chae, S. H., Choi, W., Lee, J. H., & Quek, T. Q. (2014). Enhanced secrecy in stochastic wireless networks: Artificial noise with secrecy protected zone. *IEEE Transactions on Information Forensics and Security, 9*(10), 1617–1628.
10. Bhattasali, T., & Chaki, R. (2011). A survey of recent intrusion detection systems for wireless sensor network. In *International conference on network security and applications* (pp. 268–280). Springer.
11. Mahmoud, R., Yousuf, T., Aloul, F., & Zualkernan, I. (2015). Internet of things (IoT) security: Current status, challenges and prospective measures. In *2015 10th international conference for internet technology and secured transactions (ICITST)* (pp. 336–341). IEEE.
12. Xiao, L., Greenstein, L. J., Mandayam, N. B., & Trappe, W. (2009). Channel-based detection of sybil attacks in wireless networks. *IEEE Transactions on Information Forensics and Security, 4*(3), 492–503.
13. Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of things: The road ahead. *Computer Networks, 76,* 146–164.
14. Liao, C. H., Shuai, H. H., & Wang, L. C. (2018). Eavesdropping prevention for heterogeneous Internet of Things systems. In *2018 15th IEEE annual consumer communications and networking conference (CCNC)* (pp. 1–2). IEEE.
15. Zhao, K., & Ge, L. (2013). A survey on the internet of things security. In *2013 Ninth international conference on computational intelligence and security* (pp. 663–667). IEEE.
16. Kim, H. (2008). Protection against packet fragmentation attacks at 6LoWPAN adaptation layer. In *2008 International conference on convergence and hybrid information technology* (pp. 796–801). IEEE.
17. Hummen, R., Hiller, J., Wirtz, H., Henze, M., Shafagh, H., & Wehrle, K. (2013). 6LoWPAN fragmentation attacks and mitigation mechanisms. In *Proceedings of the sixth ACM conference on Security and privacy in wireless and mobile networks* (pp. 55–66).
18. Ahmed, F., & Ko, Y. B. (2016). Mitigation of black hole attacks in routing protocol for low power and lossy networks. *Security and Communication Networks, 9*(18), 5143–5154.
19. Le, A., Loo, J., Lasebae, A., Vinel, A., Chen, Y., & Chai, M. (2013). The impact of rank attack on network topology of routing protocol for low-power and lossy networks. *IEEE Sensors Journal, 13*(10), 3685–3692.
20. Kolias, C., Kambourakis, G., Stavrou, A., & Voas, J. (2017). DDoS in the IoT: Mirai and other botnets. *Computer, 50*(7), 80–84.
21. Kozlov, D., Veijalainen, J., & Ali, Y. (2012). Security and privacy threats in IoT architectures. In *BODYNETS* (pp. 256–262).
22. Li, S., & Da Xu, L. (2017). Securing the internet of things. *Syngress*.
23. Mathur, A., Newe, T., & Rao, M. (2016). Defence against black hole and selective forwarding attacks for medical WSNs in the IoT. *Sensors, 16*(1), 118.
24. Kaur, P., & Gurm, J. S. (2016). Detect and prevent HELLO FLOOD attack using centralized technique in WSN. *International Journal of Computer Science Engineering and Technology, 7*(8), 379–381.
25. Lin, K. C., Chen, S. Y., & Hung, J. C. (2014). Botnet detection using support vector machines with artificial fish swarm algorithm. *Journal of Applied Mathematics*, 2014, 1–9.

26. Roman, R., Najera, P., & Lopez, J. (2011). Securing the internet of things. *Computer, 44*(9), 51–58.
27. Zhang, Q., & Wang, X. (2009). SQL injections through back-end of RFID system. In *2009 International symposium on computer network and multimedia technology* (pp. 1–4). IEEE.
28. Dorai, R., & Kannan, V. (2011). SQL injection-database attack revolution and prevention. *Journal International Communication and Technology, 6,* 224.
29. Razzaque, M. A., Milojevic-Jevric, M., Palade, A., & Clarke, S. (2015). Middleware for internet of things: A survey. *IEEE Internet of Things Journal, 3*(1), 70–95.
30. Kumar, J., Rajendran, B., Bindhumadhava, B. S., & Babu, N. S. C. (2017). XML wrapping attack mitigation using positional token. In *2017 International conference on public key infrastructure and its applications (PKIA)* (pp. 36–42). IEEE.
31. Hashizume, K., Rosado, D. G., Fernández-Medina, E., & Fernandez, E. B. (2013). An analysis of security issues for cloud computing. *Journal of Internet Services and Applications, 4*(1), 5.
32. Nagaraju, K., & Sridaran, R. (2012). A survey on security threats for cloud computing. *International Journal of Engineering Research and Technology (IJERT), 1*(7), 1–10.
33. Granjal, J., Monteiro, E., & Silva, J. S. (2014). Network-layer security for the internet of things using TinyOS and BLIP. *International Journal of Communication Systems, 27*(10), 1938–1963.
34. Raza, S., Duquennoy, S., Chung, T., Yazar, D., Voigt, T., & Roedig, U. (2011). Securing communication in 6LoWPAN with compressed IPsec. In *2011 International conference on distributed computing in sensor systems and workshops (DCOSS)* (pp. 1–8). IEEE.
35. Park, N., & Kang, N. (2016). Mutual authentication scheme in secure internet of things technology for comfortable lifestyle. *Sensors, 16*(1), 20.
36. Ibrahim, M. H. (2016). Octopus: An edge-fog mutual authentication scheme. *IJ Network Security, 18*(6), 1089–1101.
37. Ali, I., Sabir, S., & Ullah, Z. (2019). Internet of things security, device authentication and access control: A review. arXiv:1901.07309.
38. Shelby, Z., Hartke, K., & Bormann, C. (2014). The constrained application protocol (CoAP). RFC 7252. https://doi.org/10.17487/RFC7252
39. Ahmadi, P., Islam, K., Maco, T., & Katam, M. (2018). A survey on internet of things security issues and applications. In *2018 International conference on computational science and computational intelligence (CSCI)* (pp. 925–934). IEEE.
40. Kouicem, D. E., Bouabdallah, A., & Lakhlef, H. (2018). Internet of things security: A top-down survey. *Computer Networks, 141,* 199–221.
41. Atzori, M. (2017). Blockchain-based architectures for the internet of things: A survey. SSRN 2846810.
42. Biswas, K., & Muthukkumarasamy, V. (2016). Securing smart cities using blockchain technology. In *2016 IEEE 18th international conference on high performance computing and communications; IEEE 14th international conference on smart city; IEEE 2nd international conference on data science and systems (HPCC/SmartCity/DSS)* (pp. 1392–1393). IEEE.
43. Kokoris-Kogias, L., Gasser, L., Khoffi, I., Jovanovic, P., Gailly, N., & Ford, B. (2016). Managing identities using blockchains and CoSi. In *9th Workshop on hot topics in privacy enhancing technologies (HotPETs 2016)* (No. POST TALK).
44. Gaurav, K., Goyal, P., Agrawal, V., & Rao, S. L. (2015). IoT transaction security. In *Proceedings of the 5th international conference on the internet of things (IoT)*, Seoul, Korea (pp. 26–28).
45. Hashemi, S. H., Faghri, F., Rausch, P., & Campbell, R. H. (2016). World of empowered IoT users. In *2016 IEEE first international conference on internet-of-things design and implementation (IoTDI)* (pp. 13–24). IEEE.
46. Bahga, A., & Madisetti, V. K. (2016). Blockchain platform for industrial internet of things. *Journal of Software Engineering and Applications, 9*(10), 533–546.
47. Christidis, K., & Devetsikiotis, M. (2016). Blockchains and smart contracts for the internet of things. *IEEE Access, 4,* 2292–2303.
48. Brody, P., & Pureswaran, V. (2014). Device democracy: Saving the future of the internet of things. *IBM*.
49. Antonopoulos, A. M. (2014). *Mastering Bitcoin: Unlocking digital cryptocurrencies*. O'Reilly Media, Inc.
50. Divya, M., & Biradar, N. B. (2018). IOTA-next generation block chain. *International Journal of Engineering and Computer Science, 7*(04), 23823–23826.
51. Shabandri, B., & Maheshwari, P. (2019). Enhancing IoT security and privacy using distributed ledgers with IOTA and the Tangle. In *2019 6th International conference on signal processing and integrated networks (SPIN)* (pp. 1069–1075). IEEE.
52. Janečko, T., & Zelinka, I. (2018). Impact of security aspects at the IOTA protocol. In *International conference on intelligent information technologies for industry* (pp. 41–48). Springer.
53. Bartolomeu, P. C., Vieira, E., & Ferreira, J. (2018). IOTA feasibility and perspectives for enabling vehicular applications. In *2018 IEEE globecom workshops (GC Wkshps)* (pp. 1–7). IEEE.

54. Quasim, M. T., Khan, M. A., Algarni, F., Alharthy, A., & Alshmrani, G. M. M. (2020). Blockchain Frameworks. In *Decentralised internet of things* (pp. 75–89). Springer.
55. Lamtzidis, O., & Gialelis, J. (2018). An IOTA based distributed sensor node system. In *2018 IEEE globecom workshops (GC Wkshps)* (pp. 1–6). IEEE.
56. Sarfraz, U., Alam, M., Zeadally, S., & Khan, A. (2019). Privacy aware IOTA ledger: Decentralized mixing and unlinkable IOTA transactions. *Computer Networks, 148,* 361–372.
57. Popov, S. (2016). The tangle. cit. on, 131.
58. Florea, B. C. (2018). Blockchain and Internet of Things data provider for smart applications. In *2018 7th Mediterranean conference on embedded computing (MECO)* (pp. 1–4). IEEE.
59. Chen, W. (2012). An IBE-based security scheme on internet of things. In *2012 IEEE 2nd international conference on cloud computing and intelligence systems* (Vol. 3, pp. 1046–1049). IEEE.
60. Chatzigiannakis, I., Pyrgelis, A., Spirakis, P. G., & Stamatiou, Y. C. (2011). Elliptic curve based zero knowledge proofs and their applicability on resource constrained devices. In *2011 IEEE eighth international conference on mobile ad-hoc and sensor systems* (pp. 715–720). IEEE.
61. Koo, D., Shin, Y., Yun, J., & Hur, J. (2017). An online data-oriented authentication based on Merkle tree with improved reliability. In *2017 IEEE international conference on web services (ICWS)* (pp. 840–843). IEEE.
62. Wang, J., Li, M., He, Y., Li, H., Xiao, K., & Wang, C. (2018). A blockchain based privacy-preserving incentive mechanism in crowdsensing applications. *IEEE Access, 6,* 17545–17556.
63. Pohrmen, F. H., Das, R. K., & Saha, G. (2019). Blockchain-based security aspects in heterogeneous internet-of-things networks: A survey. *Transactions on Emerging Telecommunications Technologies, 30*(10), e3741.
64. Merkle, R. C. (1980). Protocols for public key cryptosystems. In *1980 IEEE symposium on security and privacy* (pp. 122–122). IEEE.
65. Bull, P., Austin, R., Popov, E., Sharma, M., & Watson, R. (2016). Flow based security for IoT devices using an SDN gateway. In *2016 IEEE 4th international conference on future internet of things and cloud (FiCloud)* (pp. 157–163). IEEE.
66. Alrajeh, N. A., & Lloret, J. (2013). Intrusion detection systems based on artificial intelligence techniques in wireless sensor networks. *International Journal of Distributed Sensor Networks, 9*(10), 351047.
67. Pourghebleh, B., Wakil, K., & Navimipour, N. J. (2019). A comprehensive study on the trust management techniques in the internet of things. *IEEE Internet of Things Journal, 6*(6), 9326–9337.
68. Chen, R., Bao, F., & Guo, J. (2015). Trust-based service management for social internet of things systems. *IEEE Transactions on Dependable and Secure Computing, 13*(6), 684–696.
69. Jayasinghe, U., Truong, N. B., Lee, G. M., & Um, T. W. (2016). Rpr: A trust computation model for social internet of things. In *2016 International IEEE conferences on ubiquitous intelligence and computing, advanced and trusted computing, scalable computing and communications, cloud and big data computing, internet of people, and smart world congress (UIC/ATC/ScalCom/CBDCom/IoP/SmartWorld)* (pp. 930–937). IEEE.
70. Nitti, M., Girau, R., Atzori, L., Iera, A., & Morabito, G. (2012). A subjective model for trustworthiness evaluation in the social internet of things. In *2012 IEEE 23rd international symposium on personal, indoor and mobile radio communications-(PIMRC)* (pp. 18–23). IEEE.
71. Gu, L., Wang, J., & Sun, B. (2014). Trust management mechanism for Internet of Things. *China Communications, 11*(2), 148–156.
72. Liu, Y. B., Gong, X. H., & Feng, Y. F. (2014). Trust system based on node behavior detection in internet of things. *Journal on Communications, 5,* 8–15.
73. Alrajeh, N. A., Khan, S., Mauri, J. L., & Loo, J. (2014). Artificial neural network based detection of energy exhaustion attacks in wireless sensor networks capable of energy harvesting. *Ad Hoc Senser Wireless Networks, 22*(1–2), 109–133.
74. Rae, J. S., Chowdhury, M. M., & Jochen, M. (2019). Internet of things device hardening using shodan. io and ShoVAT: A survey. In *2019 IEEE international conference on electro information technology (EIT)* (pp. 379-385). IEEE.
75. Xiao, L., Li, Y., Han, G., Liu, G., & Zhuang, W. (2016). PHY-layer spoofing detection with reinforcement learning in wireless networks. *IEEE Transactions on Vehicular Technology, 65*(12), 10037–10047.
76. Gwon, Y., Dastangoo, S., Fossa, C., & Kung, H. T. (2013). Competing mobile network game: Embracing antijamming and jamming strategies with reinforcement learning. In *2013 IEEE conference on communications and network security (CNS)* (pp. 28–36). IEEE.
77. Xiao, L., Li, Y., Huang, X., & Du, X. (2017). Cloud-based malware detection game for mobile devices with offloading. *IEEE Transactions on Mobile Computing, 16*(10), 2742–2750.
78. Alsheikh, M. A., Lin, S., Niyato, D., & Tan, H. P. (2014). Machine learning in wireless sensor networks: Algorithms, strategies, and applications. *IEEE Communications Surveys and Tutorials, 16*(4), 1996–2018.

79. Ozay, M., Esnaola, I., Vural, F. T. Y., Kulkarni, S. R., & Poor, H. V. (2015). Machine learning methods for attack detection in the smart grid. *IEEE Transactions on Neural Networks and Learning Systems, 27*(8), 1773–1786.
80. Pavani, K., & Damodaram, A. (2013). Intrusion detection using MLP for MANETs.
81. Shi, C., Liu, J., Liu, H., & Chen, Y. (2017). Smart user authentication through actuation of daily activities leveraging WiFi-enabled IoT. In *Proceedings of the 18th ACM international symposium on mobile ad hoc networking and computing* (pp. 1–10).
82. Branch, J. W., Giannella, C., Szymanski, B., Wolff, R., & Kargupta, H. (2013). In-network outlier detection in wireless sensor networks. *Knowledge and Information Systems, 34*(1), 23–54.
83. Hwang, T. S., Lee, T. J., & Lee, Y. J. (2007). A three-tier IDS via data mining approach. In *Proceedings of the 3rd annual ACM workshop on Mining network data* (pp. 1–6).
84. Cremers, C., Horvat, M., Hoyland, J., Scott, S., & van der Merwe, T. (2017). A comprehensive symbolic analysis of TLS 1.3. In *Proceedings of the 2017 ACM SIGSAC conference on computer and communications security* (pp. 1773–1788).
85. Rathore, S., Kwon, B. W., & Park, J. H. (2019). BlockSecIoTNet: Blockchain-based decentralized security architecture for IoT network. *Journal of Network and Computer Applications, 143,* 167–177.
86. Chiang, M., & Zhang, T. (2016). Fog and IoT: An overview of research opportunities. *IEEE Internet of Things Journal, 3*(6), 854–864.
87. Mishra, P., Varadharajan, V., Tupakula, U., & Pilli, E. S. (2018). A detailed investigation and analysis of using machine learning techniques for intrusion detection. *IEEE Communications Surveys and Tutorials, 21*(1), 686–728.
88. Thota, C., Sundarasekar, R., Manogaran, G., Varatharajan, R., & Priyan, M. K. (2018). Centralized fog computing security platform for IoT and cloud in healthcare system. In Fog computing: *Breakthroughs in research and practice* (pp. 365–378). IGI global.
89. Lu, R., Heung, K., Lashkari, A. H., & Ghorbani, A. A. (2017). A lightweight privacy-preserving data aggregation scheme for fog computing-enhanced IoT. *IEEE Access, 5,* 3302–3312.
90. Salman, O., Abdallah, S., Elhajj, I. H., Chehab, A., & Kayssi, A. (2016). Identity-based authentication scheme for the Internet of Things. In *2016 IEEE Symposium on Computers and Communication (ISCC)* (pp. 1109–1111). IEEE.
91. Kalkan, K., & Zeadally, S. (2017). Securing internet of things with software defined networking. *IEEE Communications Magazine, 56*(9), 186–192.
92. Di Mauro, A., Fafoutis, X., & Dragoni, N. (2015). Adaptive security in odmac for multihop energy harvesting wireless sensor networks. *International Journal of Distributed Sensor Networks, 11*(4), 760302.
93. Taddeo, A. V., Mura, M., & Ferrante, A. (2010). Qos and security in energy-harvesting wireless sensor networks. In *2010 International conference on security and cryptography (SECRYPT)* (pp. 1–10). IEEE.
94. Hellaoui, H., Bouabdallah, A., & Koudil, M. (2016). Tas-iot: trust-based adaptive security in the iot. In *2016 IEEE 41st conference on local computer networks (LCN)* (pp. 599–602). IEEE.
95. Wang, E. K., Wu, T. Y., Chen, C. M., Ye, Y., Zhang, Z., & Zou, F. (2015). Mdpas: Markov decision process based adaptive security for sensors in internet of things. In *Genetic and evolutionary computing* (pp. 389–397). Springer.
96. Frustaci, M., Pace, P., Aloi, G., & Fortino, G. (2017). Evaluating critical security issues of the IoT world: Present and future challenges. *IEEE Internet of things journal, 5*(4), 2483–2495.
97. Zhang, X., Upton, O., Beebe, N. L., & Choo, K. K. R. (2020). IoT Botnet forensics: A comprehensive digital forensic case study on Mirai Botnet servers. *Forensic Science International: Digital Investigation, 32,* 300926.
98. Ghosh, S., Misoczki, R., & Sastry, M. R. (2019). Lightweight post-quantum-secure digital signature approach for IoT motes. *IACR Cryptology, 2019,* 122.
99. Shinder, D. L., & Cross, M. (2008). *Scene of the cybercrime*. Elsevier.
100. Liu, B., Chiang, J. T., Haas, J. J., & Hu, Y. C. (2010). Coward attacks in vehicular networks. *ACM SIGMOBILE Mobile Computing and Communications Review, 14*(3), 34–36.
101. Al-Garadi, M. A., Mohamed, A., Al-Ali, A. K., Du, X., Ali, I., & Guizani, M. (2020). A survey of machine and deep learning methods for internet of things (IoT) security. *IEEE Communications Surveys & Tutorials, 22* (3), 1646–1685.
102. Qu, F., Wu, Z., Wang, F. Y., & Cho, W. (2015). A security and privacy review of VANETs. *IEEE Transactions on Intelligent Transportation Systems, 16*(6), 2985–2996.
103. Xu, W., Trappe, W., Zhang, Y., & Wood, T. (2005). The feasibility of launching and detecting jamming attacks in wireless networks. In *Proceedings of the 6th ACM international symposium on Mobile ad hoc networking and computing* (pp. 46–57).

104. Vytarani Mathane and P.V. Lakshmi, (2021). Predictive analysis of ransomware attacks using context-aware AI in IoT systems. *International Journal of Advanced Computer Science and Applications (IJACSA), 12*(4), 240–244.
105. Verma, M. E., Iannacone, M. D., Bridges, R. A., Hollifield, S. C., Kay, B., & Combs, F. L. (2020). ROAD: the real ORNL automotive dynamometer controller area network intrusion detection dataset (with a comprehensive CAN IDS dataset survey and guide). arXiv:2012.14600.
106. Barletta, V. S., Caivano, D., Nannavecchia, A., & Scalera, M. (2020). Intrusion detection for in-vehicle communication networks: An unsupervised kohonen som approach. *Future Internet, 12*(7), 119.
107. Alnasser, A., Sun, H., & Jiang, J. (2019). Cyber security challenges and solutions for V2X communications: A survey. *Computer Networks.*
108. Ali Alheeti, K. M., Gruebler, A., & McDonald-Maier, K. (2016). Intelligent intrusion detection of grey hole and rushing attacks in self-driving vehicular networks. *Computers, 5*(3), 16.
109. Ghasemi, M., Saadaat, M., & Ghollasi, O. (2019). Threats of social engineering attacks against security of Internet of Things (IoT). In *Fundamental research in electrical engineering* (pp. 957–968). Springer.
110. Koutras, D., Stergiopoulos, G., Dasaklis, T., Kotzanikolaou, P., Glynos, D., & Douligeris, C. (2020). Security in IoMT communications: A survey. *Sensors, 20*(17), 4828.
111. Tsiknas, K., Taketzis, D., Demertzis, K., & Skianis, C. (2021). Cyber threats to industrial IoT: A survey on attacks and countermeasures. *IoT, 2*(1), 163–188.
112. Lee, J., Lin, W., & Huang, Y. (2014). A lightweight authentication protocol for Internet of Things, 2014 International Symposium on Next-Generation Electronics (ISNE), pp. 1-2.

Dorsaf Swessi is a Ph.D student in computer science under the supervision of professor Hanen Idoudi in the National school of computer sciences (ENSI) at University of Manouba, Tunisia. She received her B.sc and M.sc in computer sciences from the Faculty of Science of Bizerte at University of Carthage, Tunisia. Her doctoral work explores the intelligent security of the Internet of things which is based on the use of emerging security countermeasures that are able to detect all kinds of anomalies including unknown and zero-day attacks.

Hanen Idoudi is a professor and senior researcher in Computer Science at University of Manouba, Tunisia. She received her HDR (Habilitation a Diriger des Recherches) in 2017 from the University of Toulouse-Jean Jaures (France) and her Ph.D degree from the University of Rennes 1, France. Her technical and research skills include IoT communications protocols and architecture, networking protocols, Security, and Blockchain. She served as chair and committee member of several international technical and scientific conferences and journals. She is a Senior IEEE Member, an ISOC IGF ambassador and ICANN fellow.