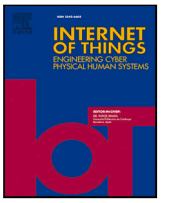
Internet of Things 23 (2023) 100888

Contents lists available at ScienceDirect

Internet of Things

journal homepage: www.elsevier.com/locate/iot



Review article

A review of the security vulnerabilities and countermeasures in the Internet of Things solutions: A bright future for the Blockchain ☆

Hossein Pourrahmani [a,*], Adel Yavarinasab [b], Amir Mahdi Hosseini Monazzah [c,d], Jan Van herle [a]

[a] Group of Energy Materials, École Polytechnique Fédérale de Lausanne, Sion 1951, Switzerland
[b] School of Biomedical Engineering, Life Sciences Institute, University of British Columbia, Vancouver, BC V6T 1Z3, Canada
[c] School of Computer Engineering, Iran University of Science and Technology, Tehran, Iran
[d] School of Computer Science, Institute for Research in Fundamental Sciences (IPM), Tehran, Iran

ARTICLE INFO

Keywords:
Blockchain
IA
IoT
Security countermeasures
Security vulnerabilities

ABSTRACT

The current advances in the Internet of Things (IoT) and the solutions being offered by this technology have accounted IoT among the top ten technologies that will transform the global economy by 2030. IoT is a state-of-the-art paradigm that has developed traditional living into a high-tech lifestyle. The current study aims to provide a comprehensive review and analysis of the existing cybersecurity attacks and vulnerabilities in IoT, offering suitable countermeasures with a focus on describing the impact of emerging technologies on IoT devices and protocol layers. The main vulnerabilities across different layers of the IoT reference model are discussed and categorized, and suitable countermeasures (such as separating IT and IoT network traffic, enhancing physical security, implementing encryption and secure messaging protocols, etc.) are suggested. In addition, the hardware, communication, application, web, and cloud vulnerabilities are introduced, then the corresponding safeguards and protections are presented. Furthermore, Information Assurance (IA) has been deliberately defined and the adoption of the NIST framework and IA model is recommended as a metric to ensure security for IoT solutions considering the five pillars of availability, integrity, authentication, confidentiality, and non-repudiation. Finally, Blockchain technology, known for its use in securing cryptocurrencies, is suggested to facilitate secure data exchange, identification, authentication, and communication for IoT devices by various avenues including ensuring the integrity of sensor data, eliminating the need for intermediaries, reducing costs, and enabling direct addressability of IoT devices.

1. Introduction

Internet of Things (IoT) is defined as a trend where many embedded devices use communication services that have been introduced by the internet protocols. These devices, often referred to as "smart objects", operate autonomously within the environment without direct human interaction, serving as distinct components with specific functionalities. In 2020, for the first time, out of 21.7 billion active connected devices worldwide, the number of IoT devices surpassed non-IoT connections, and it is

☆ This project has received funding from the European Union's Horizon 2020 research and innovation program under the Marie Sklodowska-Curie grant agreement No. 754354.

* Corresponding author.
E-mail addresses: Hossein.pourrahmani@epfl.ch (H. Pourrahmani), adel.yavarinasab@ubc.ca (A. Yavarinasab), monazzah@iust.ac.ir (A.M.H. Monazzah), jan.vanherle@epfl.ch (J. Van herle).

https://doi.org/10.1016/j.iot.2023.100888
Received 11 April 2023; Received in revised form 16 June 2023; Accepted 1 August 2023
Available online 5 August 2023

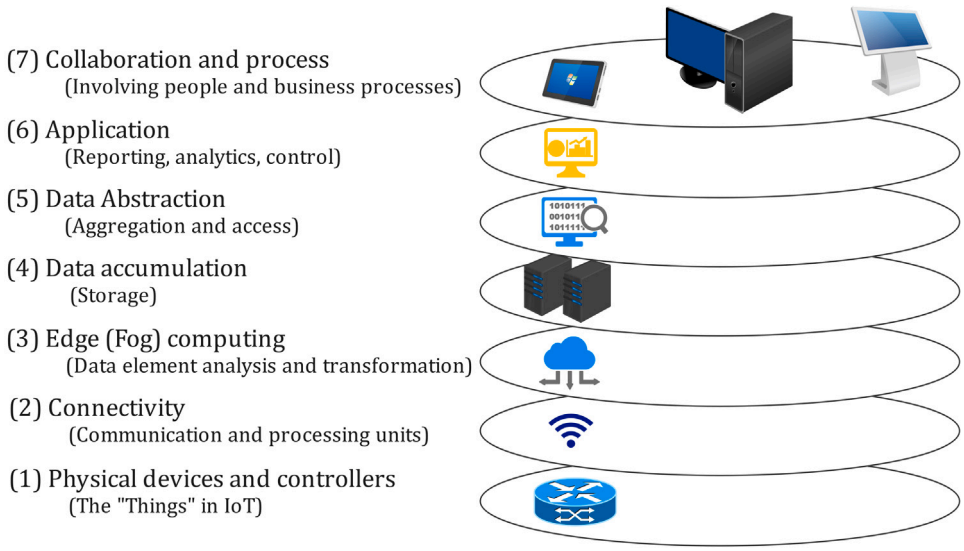


Fig. 1. A schematic of IoT reference model.

expected that by 2025, almost 4 IoT devices will be available per person on average (more than 30 billion connections) [1]. The IoT industry is reported to grow by $49. 04 billion during 2022–2026, accelerating at a compound annual growth rate (CAG) of $27.48 during the forecasted period [2]. While the recent progress in the Internet of Things (IoT) solutions has enabled the shift from conventional modes of operation to a new, technologically advanced approach, it is crucial to give deliberate consideration to the security aspects of these solutions.[3]. For a large amount of generated data (Big data) by IoT devices, big data should be managed, secured, and analyzed [4]. However, ensuring the security of the big data considering the volume [5], variety [6], and velocity [7] is an ongoing challenge. In his "Future Crimes" book, author Marc Goodman recounts the story of a 23-year-old college student who, in 2000, manipulated the stock market by posting a fake press about the Emulex Corporation, a Nasdaq-traded manufacturer. In 16 min, 2.3 million shares were traded, resulting in Emulex's losing $2.2 billion in market capitalization [8]. The evolving nature of cyber-attacks has rendered them increasingly adaptable and intricate in their pursuit of targeted objectives, thereby heightening our vulnerability to a greater extent than before. A Microsoft study shows a 1,070 percent increase just in ransomware attacks between July 2020 and June 2021 [9]. In order to formulate an effective cybersecurity strategy, there exists a pressing requirement for individuals, corporations, and governments to prioritize the protection of their respective identities, customers, and the overall well-being of citizens [10]. In essence, manufacturers are particularly vulnerable to cyberattacks due to their substantial intrinsic value, making them attractive targets for malicious activities.

The main difference in the type of challenges in the IoT domain in comparison to other Information Technology (IT) environments is their dimensions [11]. Numerous Internet of Things (IoT) devices, which are physically interconnected to the internet, exhibit inadequate security measures in place. This is a matter of significant concern due to the potential vulnerabilities and risks associated with such devices [12]. In this regard, physical security should be considered in addition to data security in IoT devices [13]. The forging of the network statistics and file access records has directed the researchers to develop the first energy auditing and analytics-based IoT monitoring system using a deep learning model [14]. Additionally, preventing IoT devices from vandalism is considered a type of physical security [15]. The type of selected components for IoT solutions should be selected based on the infrastructure facility of a region to provide physical security as well [16]. In addition to ensuring physical security, it is imperative to guarantee the security of the interconnected network, cloud infrastructure, and applications. Safeguarding the entire ecosystem of connected devices, networks, and software applications is essential for maintaining the integrity, confidentiality, and availability of data and services. A survey of over 250 manufacturing security leaders and practitioners worldwide showed that only 25% of companies have more than 60% of their cloud data encrypted [17].

When developing an Internet of Things (IoT) solution, it is common to utilize the IoT reference model as a framework for design [18], which is shown in Fig. 1. Security measures should ensure the safety of the utilized hardware/software for each of the components that are connected to the IoT network [19]. Additionally, the security of the processes in each level of the IoT reference model, illustrated by Fig. 1, and the communications between each level should be provided [20]. In addition to the poor physical security, the major vulnerabilities in IoT systems are the insecure web interfaces [21], like, insufficient authentication/authorization [22], insecure network services [23], lack of transport encryption/integrity verification [24], privacy concern [25], insecure cloud interface [26], insecure mobile interface [27], insufficient security reconfigurability [28], and insecure software/firmware [29].

Fig. 2 depicts ten essential parameters that necessitate careful consideration for ensuring the security of IoT devices across various scales. [30]. Here, IoT devices refer to the sensors, actuators, controllers, and gateways, which demand either operating systems or

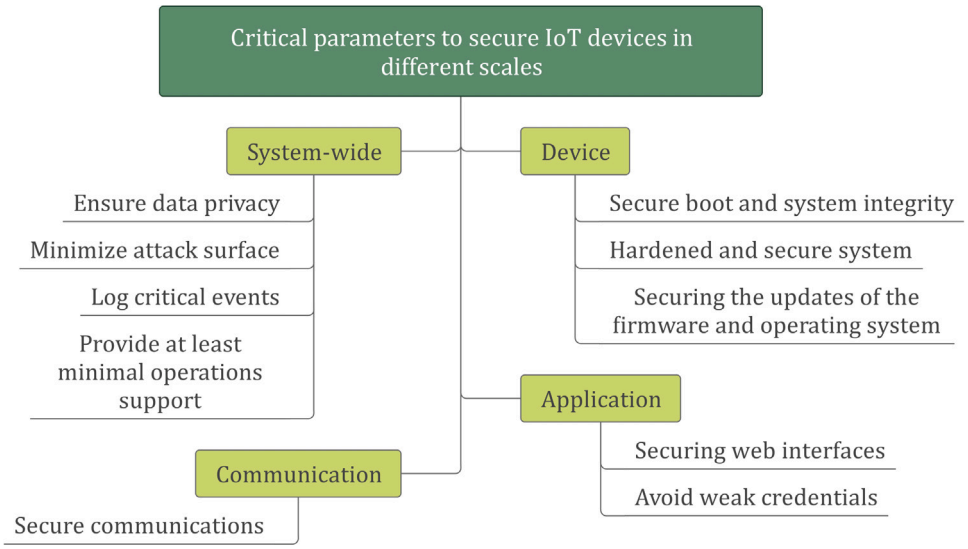


Fig. 2. The main critical parameters to ensure the security of IoT devices in different scales.

application programs to operate. Regarding Fig. 1, it should be noted that in the fifth layer, the boot and system integrity should be secured using hardware components such as Trusted Platform Modules (TPM) [31]. Additionally, the system should not run unnecessary network services in the sixth layer to further secure the system [32]. In the seventh layer, the firmware and operating system updates should be secured as well [33].

The current study aims to provide a comprehensive review of the security challenges and vulnerabilities in IoT solutions across various technologies. The study also provides some countermeasures to avoid or prevent possible security attacks. The information assurance model (encompassing security services, security countermeasures, and information states, with confidentiality, availability, integrity, authentication, and non-repudiation) in addition to the common frameworks and protocols is presented as a solution to cybersecurity concerns in IoT technologies. Finally, it has been suggested that Blockchain technology can hold significant promise for enhancing security in IoT devices by leveraging its decentralized and immutable nature to secure data exchange and enable identification and authentication [34]. By bridging the existing gaps in research concerning comprehensive references for potential cybersecurity attacks and their corresponding mitigation strategies, this study serves as a valuable resource for ensuring the security of IoT solutions.

The flow of the current paper is to first present the possible security vulnerabilities in different layers of the IoT reference layer followed by the existing countermeasures to prevent possible security attacks in Section 2. Then, the possible vulnerabilities and countermeasures for IoT hardware are introduced in Section 3. Section 4 covers the vulnerabilities of communication, application, and web/cloud infrastructures that are utilized in IoT applications. In Section 5 several methods to ensure IoT applications security will be explored. Finally, Section 6 concludes the paper.

2. Security challenges and requirements of IoT devices

In this section, the main cybersecurity attacks for IoT devices are identified to ensure the security of IoT devices [35]. The following sections will give a more detailed description of the possible vulnerabilities in each layer of the IoT reference model (see Fig. 1). However, it should be noted that this particular section focuses exclusively on renowned instances of cybersecurity attacks.

2.1. The main cybersecurity attacks in IoT devices

Thus far, the main cyber-attacks in IoT solutions are considered to be: Botnet [36], man-in-the-Middle [37], data and identity theft [38], code injection [39], and distributed denial of service (DDoS) [40]. In a Botnet attack, the attackers will obtain control of internet-enabled devices (including computers, tablets, etc.) without the permission of the owners to perform particular tasks [41]. Fig. 3 illustrates a conceptual schematic of the Botnet attack. As an example of the Botnet attack, the Mirai malware in 2016 changed the operation of the IoT devices working with Linux to remote-controlled bots that could be used as a part of a botnet in a distributed attack.

In the Man-in-the-Middle (MitM) attack, the communication between the nodes will be intercepted to steal information such as authentication credentials [42]. In this regard, the attacker will gain control of the messages and be able to distribute false information [43]. An example of MitM in the IoT domain can be the usage of fake sensor data to destroy physical assets and business operations. Fig. 4 shows the concept of the MitM in cybersecurity. As a famous example of the MitM, 2.5 million Equifax website costumers were directed to a fake website.

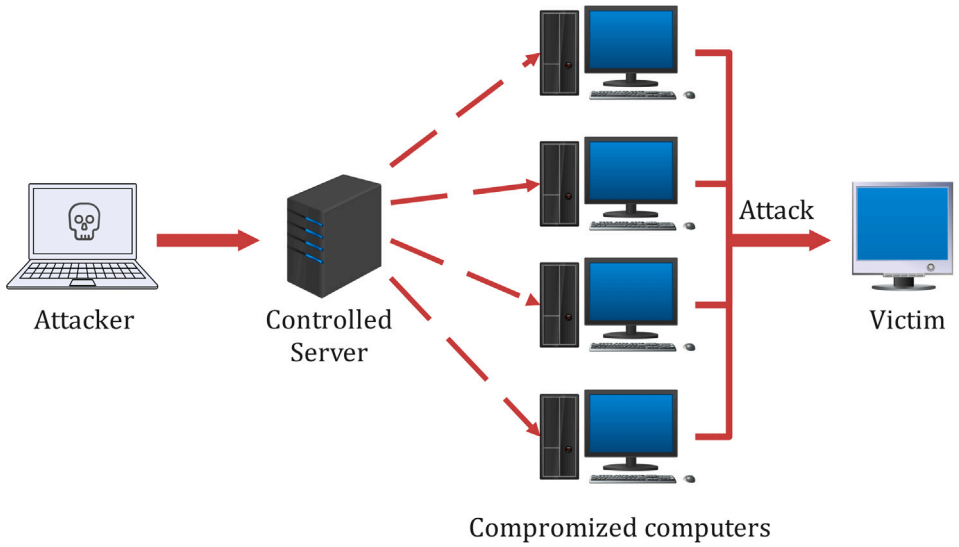


Fig. 3. A schematic of the Botnet attack.

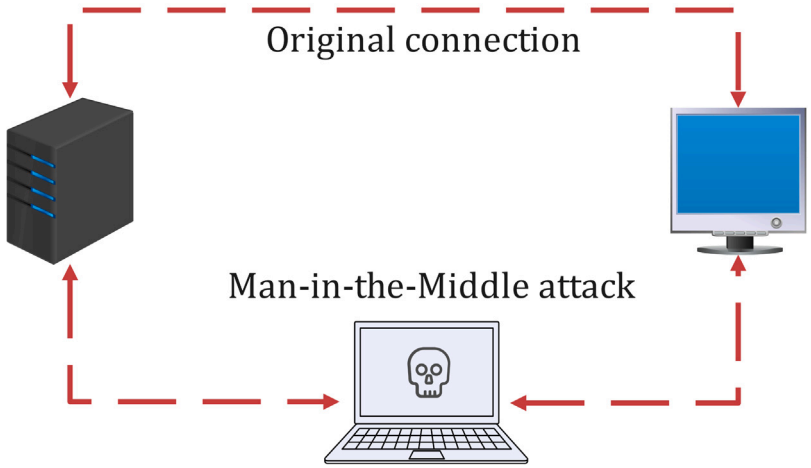


Fig. 4. The conceptual schematic of the Man-in-the-Middle (MitM) attack.

Considering data and identity theft type attacks, personally identifiable information (PII) can be a target for hackers and should be protected [44]. Data and identity theft usually occur on five occasions. On the first occasion, a person does not control the PII such as the leak of information in the governmental agencies, and medical/financial providers. On the second occasion, the financial PII can be pilfered through physical and electronic channels. The legal selling of PII by some businesses and using similar passwords for different online accounts are the other vulnerabilities for identity theft on are third and fourth occasions, respectively [45]. Finally, on the last occasion, the attacker may file someone's tax return and give controlled addresses for inevitable refunds. In this type of attack, the attacker usually obtains a list of emails and makes a generic contact to direct the user to a fake website/login page. It is also possible that the attacker distributes a phishing message and obtains the credentials.

It is common to use Extensible Markup language (XML) or Structured Query Language (SQL) databases to store the obtained data by IoT devices. However, these databases are prone to code injection attacks, which are injecting malicious codes into a computer program by spoofing the identity and acquiring the administration of the server [46]. The most famous example of code injection goes back to the Ghost Shell group, which is a cybersecurity activist company. In this example, more than 30 million accounts were hacked using SQL injection.

Another type of attack is the Denial of Service (DoS) which interrupts the services to the users and devices through an overwhelming quantity of traffic or maliciously formatted packets [47]. In the former, the attacker will send a massive amount of data at a non-controllable rate, which results in crashing the system, while the latter sends maliciously formatted packets that

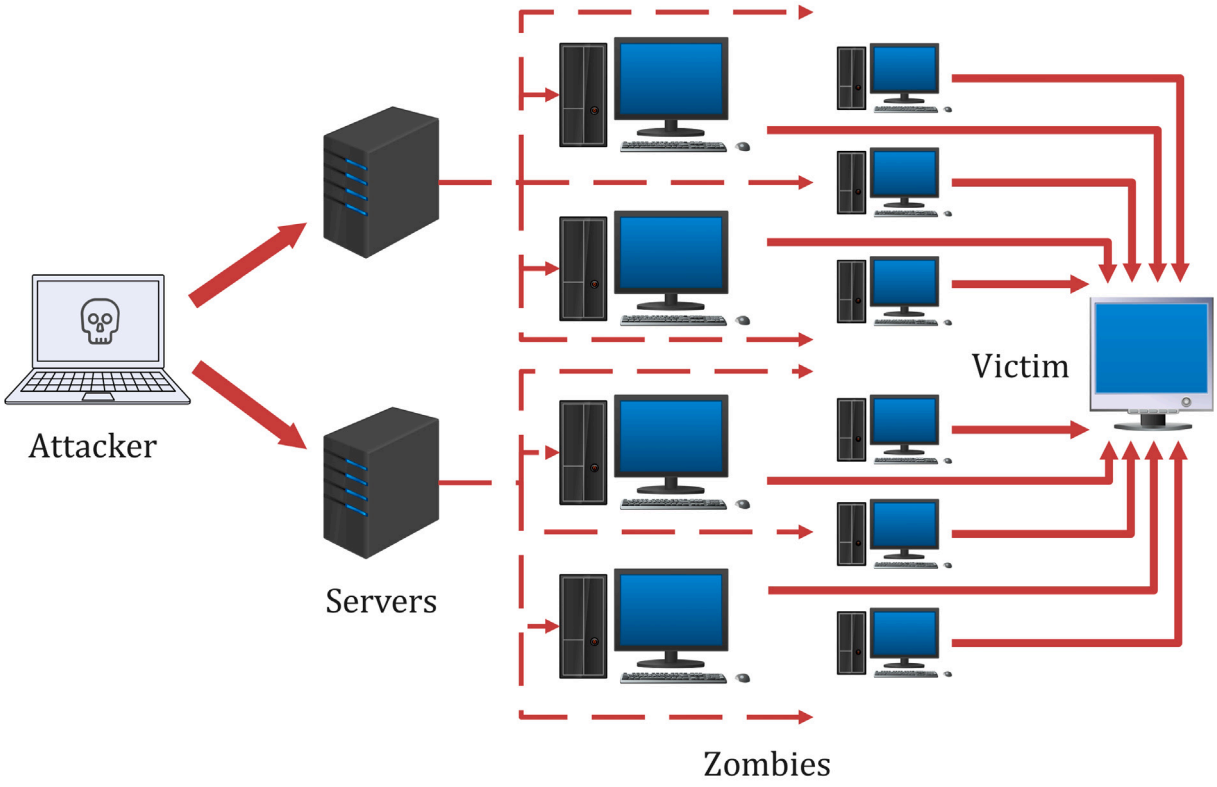


Fig. 5. A conceptual schematic of the Distributed Denial of Service (DDoS) attack.

Table 1
The list of vulnerabilities and attack surfaces to secure IoT devices.

Attack surfaces	Details
Hardware sensors	The locations of the sensors should be selected deliberately to avoid physical damage.
Device memory	Can be accessed and exposed to sensitive data since a lot of devices are manufactured with default credentials.
Physical interfaces	Because data storage can be done using removable cards. In this regard, the card can be removed, stolen, or duplicated.
Firmware	Backdoor accounts and encryption keys are the vulnerabilities of the firmware.
Firmware update mechanisms	Non-encrypted, not signed, and malicious updates can be considered as an attack to threaten IoT devices.

will not be possible to be controlled by the receiver. In DoS, the PII will not be stolen, but access to the services will be denied. If the DoS attack is being originated from multiple sources, then a DDoS attack is occurring, which is shown in Fig. 5. The concept of a DDoS attack is to use malicious programs to infect devices, which are known as zombies [48]. A handler system will control the zombies and decides when a Botnet can be created. There are quite more examples of DDoS attacks, such as the GitHub attack in 2018, the Six Banks attack in 2012, the Spamhaus attack in 2013, etc.

2.2. Security requirements of IoT devices

As illustrated in Fig. 2, the security of IoT devices will be ensured as long as the security of the devices, communication, and applications are provided [49]. Devices, such as sensors, actuators, etc. demand application programs to operate, and the data will be transferred over the network from the devices to the application programs. The Open Web Application Security Project (OWASP) [50] has recently provided the vulnerabilities and attack surfaces to secure IoT devices as indicated in Table 1.

The major parts of IoT devices are the Central Processing Units (CPUs), memory, and physical ports [51]. CPUs can be either Reduced Instruction Set Computing (RISC) or Complex Instruction Set Computing (CISC) [52]. The novel CPUs also benefited from both the RISC and CISC at the same time. RISC processors are more appropriate for IoT components rather than those of CISC. RISC processors are cheaper, generate less heat, and use less power as they have a lower number of transistors [53]. On the other hand, CISC processors can perform several operations with a single instruction by more transistors [54]. The main providers of

CISC processors are Intel and Advanced Micro Devices (ADM) while Advance RISC Machine (ARM) and Microprocessor without Interlocked Pipeline Stages (MIPS) are the main architectures of the RICS processors [55].

The memory of IoT devices is usually SD or MicroSD cards, Non-Volatile Memory, Embedded Multimedia Card, and Volatile Memory [56]. A dedicated space in the memory should be given for processing data, storing data, and firmware. SD cards can store the obtained data from the sensors or the operation of the system. The SD cards should be protected from detachment to prevent the leakage of the data. The concept of non-volatile memory means the ability to retain the stored information when there is no power supply such as Erasable Programmable Read-Only Memory (EPROM) [57] and Electrically Erasable Programmable Read-Only Memory (EEPROM) [58]. Embedded Multimedia Card (eMMC) [59], which is a type of non-volatile memory, can be used as a removable component. The advantage of using Volatile Memory is to store the temporary data during the device run-time. Examples of Volatile Memory are Static Random Access Memory (SRAM) [60], and Dynamic Random Access Memory (DRAM) [61]. The disadvantage of Volatile Memory is losing the data after shutting down the system.

In addition to the memory and CPU, the physical ports of IoT devices such as USB and Ethernet should be secured. If the attacker accesses the Joint Test Action Group (JTAG), which is a protocol for testing and debugging, the related data about the firmware and micro-controller can be obtained in addition to the possibility of loading malicious firmware on the device [62]. Some vulnerabilities exist in Serial Peripheral Interface (SPI), which is a protocol for short-distance communication between multiple devices [63]. This protocol is faster than Universal Asynchronous Receiver–Transmitter (UART) and Inter-Integrated Circuit (I2C), which are also prone to security attacks [64]. In I2C, the transferred data between the micro-controller and the EEPROM chips should be protected, while the shell access to the UART can be considered as a security flaw [65].

2.3. Access control

To ensure the security of IoT devices, physical security should be considered [66]. In many systems, IoT devices are located in remote areas which makes it challenging to implement physical security measures [67]. IoT devices are prone to be stolen, physically damaged, or disabled/removed. In this regard, securing the perimeters, video surveillance, tamper-proof housing, and disabling devices for tampering can be considered as solutions [68]. Additionally, the access control as an authentication procedure can be applied as follows:

- Mandatory access control (MAC)
  As a common military approach, the users will obtain access based on the security level clearance [69].
- Discretionary access control (DAC)
  This method enables access to the data following the ownership and the access control list (ACL) to introduce the rules for individuals/groups [70].
- Non-discretionary access control or Role-based access control (RBAC)
  This method gives access to the individuals based on the defined roles in an organization [71].
- Attribute-based access control (ABAC)
  This method gives access to the data following the defined permissions for the attributes of the resource, the user, and the environmental factors such as the time of access [72].
- Least privilege access control (LPAC)
  Allows access to defined resources at a specific time that has been clarified in advance [73].

To enable the management of the identity and access to the secured data, an identity, and access management (IAM) system should be implemented. Fig. 6 shows the IAM protocol flow based on the standardized OAuth 2.0 authorization framework [74] for IoT devices. As IoT communication also involves Machine-To-Human (M2H) and Machine-To-Machine (M2M), Identity Resource Management (IRM) should be considered in addition to IAM.

In addition to the devices and the application programs, the networks should be secured. The common network access protocols are the IEEE 802.3 Ethernet [75], IEEE 802.11 WiFi [76], IEEE 802.15.4 [77], LPWAN [78], Cellular [79]. Encryption can also help data confidentiality by applying defined algorithms. In this regard, different types of IoT wireless manufacturers have considered encryption in IoT wireless standards. For example, Zigbee, which offers low power and data rate communications for 10–100 meters uses basic encryption, while Long-Range (LoRa), as a long-range communication (up to 10 km), enjoys better encryption in comparison to Zigbee.

3. Hardware vulnerabilities and countermeasures

In an IoT system, the security of the utilized components is of important in all aspects including firmware, software, and network. The critical hardware security threats are Hardware Trojans (HT) [80] and Side-Channel Analysis (SCA) [81] in Integrated Circuits (IC).

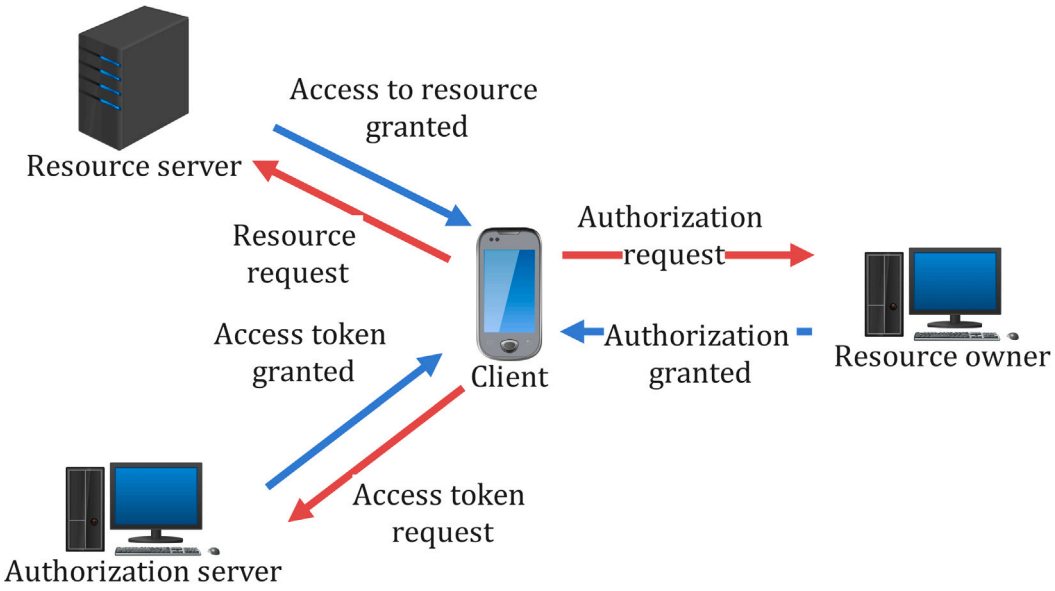


Fig. 6. A schematic of the identity and access management (IAM) protocol flow.

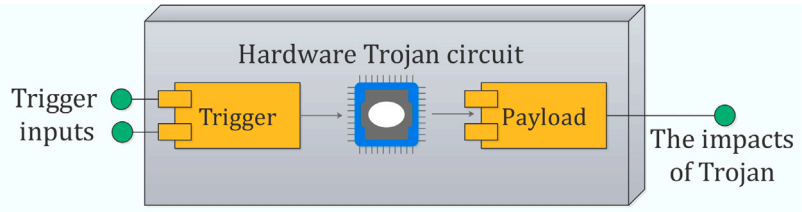


Fig. 7. A simplified schematic of the Hardware Trojan (HT) with its components.

3.1. Hardware Trojan (HT)

A malicious change at any step of manufacturing a chip is considered as an HT [82]. HT can simply happen with a small modification in the IC, which disturbs the operation of the chip [83]. The attacker can disturb the chip's operation by adding a backdoor that sniffs out the encryption keys and transfers the chip's data to other devices [84]. Fig. 7 illustrates a simplified version of an HT attack, where the HT is triggered by sensors, internal logic states/counter values, and input patterns [85]. In Fig. 7, the payload of an HT is the corresponding activity of the Trojan when it has been triggered.

In general, HT attacks are either based on trigger or payload methodologies [86]. In Trigger, the HT triggers a malicious functionality by reading the target circuit [87], however, in Payload, the HT executes the malicious function by writing to the target circuit as described in Fig. 8.

- Trigger HT
  The digitally triggered HT can be either combinational or sequential [88]. In the combinational digital trigger, a rare situation will be used to trigger the HT. In the sequential digital trigger, the HT will be executed by the sequence or a series of continuous operations. The synchronous standalone counters are examples of sequential digital triggers. In this condition, the trigger is a synchronous counter with k-bits that cause the changes in the output when the counter reaches $2^{(k-1)}$. In this attack, once the trigger is deactivated, the value of the digital signal will be shown without any change, however, the corresponding digital signal will be inverted if the trigger is activated.
- Payload HT
  In the payload HT mechanisms, the attacks can be further categorized as digital and analog [89]. Digital Trojans can either change the logical parameters at payload nodes or modify the contents of memory locations. Analog Trojans will directly change the performance, power, and noise margin of the circuit. In addition to hardware-based attacks, the payload HT can lead to software-based attacks such as privilege escalation, login backdoors, and password theft.

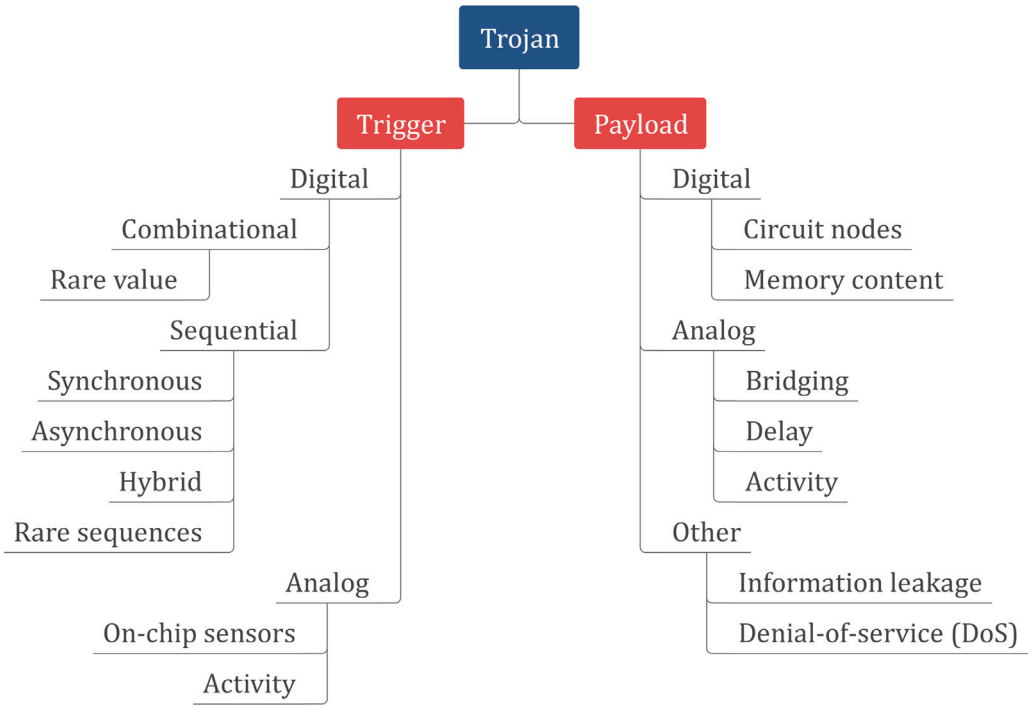


Fig. 8. Different types of HT attacks and their methodologies.

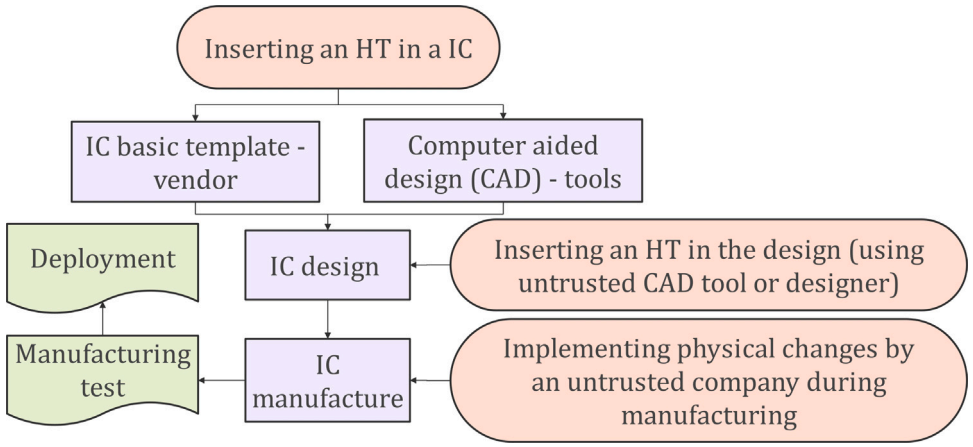


Fig. 9. The life cycle of an integrated circuit and the possibilities of an attacker to implement the HT.

3.2. HT countermeasures

The HTs are common in having malicious intent and trying not to be detected by post-manufacturing test processes [90]. The Trojans are usually passive for a long time that the circuit is being used and the attackers usually try to implement more than only one HT in a circuit [91]. Fig. 9 demonstrates the life cycle of an integrated circuit and the possibility of an attacker implementing the HT in the IC.

The existing countermeasures are usually divided into three general groups Trojan detection, design for security, and run-time monitoring methods [92]. Fig. 10 illustrates the classification of the existing countermeasures for the HT attacks. In general, the detection of HT can be either destructive or non-destructive. In the former, the reverse engineering approaches will be used to de-package an IC and analyze the structure using Chemical Mechanical Polishing (CMP) followed by Scanning Electron Microscopy (SEM) [93]. In this methodology, only one IC sample will be used and the reconstruction using SEM will be done since the sample cannot be used later after performing the analysis.

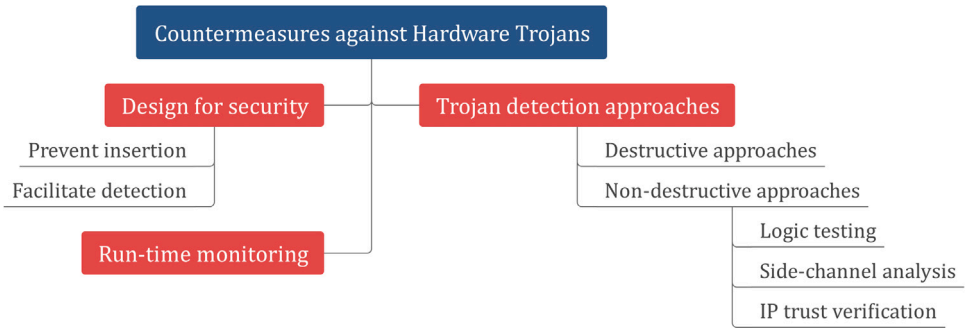


Fig. 10. The classification of the countermeasures for HT attacks.

In the non-destructive methods, different approaches in the pre-silicon and post-silicon stages will be used to analyze the IC and detect the HTs [94]. In pre-silicon analyses, the IC will be compared with a completely specified model of the IC. In the post-silicon analyses, logic testing and side-channel analysis are usually used [95]. Logic testing, which is a robust method under process noise and efficient for detecting ultra-small HTs, triggers the HT by test vectors and monitors the corresponding impacts to the output ports. Logic testing suffers from the existing challenges for large Trojan detection and generating test vectors [96]. In the side-channel analysis (SCA), however, the test vectors are easy to be generated and there are no challenges for large Trojans [97]. This method makes a comparison between the supply current and path delays to the specified reference values, hence the possible faults in the design will be recognized. The existing challenges in the side-channel analysis are detecting ultra-small Trojans and being vulnerable to process noise.

As an HT countermeasure mentioned in Fig. 10, security design is important to detect threats in advance. In this regard, devising security plans such as Trojan Insertion Prevention and Trojan Detection Facilitation are considered. In the former, it is common to use methods of obfuscation and Layout-filler. In the obfuscation [98], the functionality of the circuit design would be concealed by obtaining key passwords for the operation of IC in normal conditions; otherwise, the system undergoes the obfuscation mode. In the layout filler, all the free spaces on the circuit will be occupied by filler cells to prevent the possible insertion of HTs by attackers. In the Trojan detection facilitation, on-chip embedded components will be used to detect the HTs.

In Fig. 10, the SCA countermeasure is considered a post-silicon non-destructive solution for HT attacks. However, the system may go for an SCA attack [99], which is analyzing the side-channel signals for cryptography devices to calculate the secret keys. This happens by the existence of physically observable phenomena caused by the operation of the microelectronic components [100]. SCA attacks can be divided into three main types of Simple Power Analysis (SPA) [101], Differential Power Analysis (DPA) [102], and Correlation Power Analysis (CPA) [103]. In a SPA attack, which can be considered as a data collection technique rather than an attack, monitor the power usage of the microelectronic devices and estimate the performed operations by the component such as AES (Advance Encryption Standard) [104]. DPA attack visually estimates the power traces and electrical activity of the devices [105], while a CPA attack can predict the passwords by measuring the encrypting device's power usage during the data encryption process [106].

4. Communication, application, web/cloud vulnerabilities

4.1. The main cybersecurity attacks in IoT devices

The role of communication channels is to transfer the obtained data by the sensors, actuators, etc. to the applications and vice versa [107]. As the data in motion demands safety, providing security measures is of significance in the communication layer. In general, communication in IoT devices can be done using either mesh or star topologies (see Fig. 11). In the mesh topology, IoT devices send the information to other IoT devices until reaching the IoT gateway, while in the star topology, the data are sent directly to the IoT gateway, which limits the potential coverage of the network area.

The most commonly utilized protocols in IoT solutions are Bluetooth and WiFi, which are accompanied by security concerns. The connection to the utilized hot spot in WiFi protocol demands minimum configurations and enables the attackers to potential threats. In this regard, it is suggested to follow the IEEE 802.15.4 protocol [77] for Machine-to-Machine (M2M) communication, which is common in IoT solutions. This protocol aimed to provide personal area networks (PAN) but it is also possible to extend the usage to the Wireless Sensor Network (WSN) as well. The IEEE 802.15.4 protocol consists of Media Access Layer (MAC) and Physical Layer (PHY). The former integrates channel access management, device addressing, and device association/disassociation while the latter enables the activation/deactivation of a radio transceiver, data coding, modulation, and error correction. The main functionalities in the IEEE 802.15.4 protocol are Full Function Devices (FFD), Personal Area Network (PAN) Coordinators, and Reduced Function Devices (RFD).

One of the concerns about the security of the network in IoT devices is related to IP addresses [108]. In IoT solutions, each IoT node has access to the network and it may create threats due to the existing vulnerabilities. IoT gateway and the enterprise

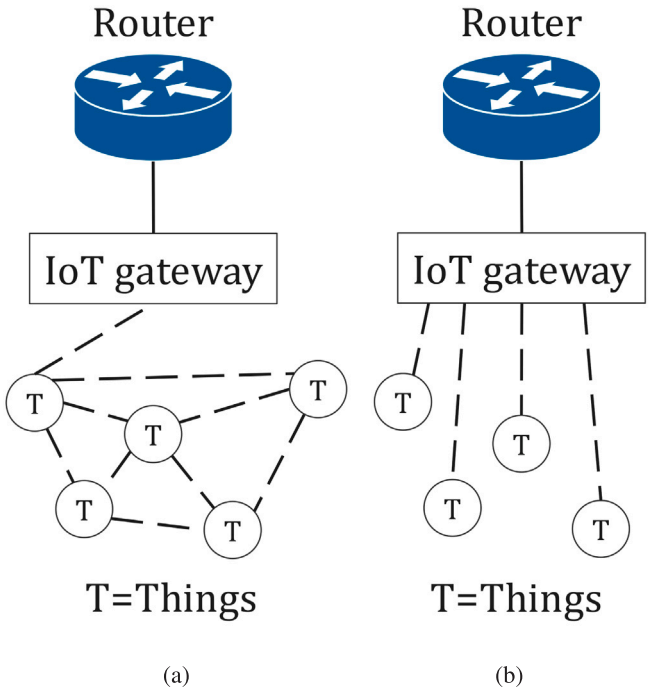


Fig. 11. The existing communications topologies in IoT devices; (a) Mesh topology, (b) Star topology.

IT network are also prone to security attacks [109]. The existing IP-related attacks are the DoS, DDoS, Internet Control Message Protocol (ICMP) attack, Address spoofing, Man-in-the-Middle (MitM), and session hijacking attacks. In DoS attacks, attackers prevent the users to access the data, similarly, in a DDoS attack, multiple machines reduce the accessibility of the users [110]. The concept of ICMP messages was to send diagnostic messages, however, attackers can use ICMP to scan the sub-nets and hosts on a protected network. In the session hijacking, the attacker obtains the possibility to control the physical network to use a MitM attack to access the web server. In address spoofing attacks, the IP address in a packet will be changed to another IP address, while the MitM attack involves positioning the attacker between the source of the data and the destination.

The first step to reduce network vulnerabilities is to implement a robust wireless protocol [111], which only permits legitimate devices and users. The transport of the data should be also protected using cryptography approaches. As mentioned before, the IEEE 802.15.4 protocol [77] can be used to further improve security in IoT solutions. Additionally, the traffic isolation and zoning method can be considered an efficient approach to control security in IoT solutions [112]. Fig. 12 shows an example of this method in an industrial IoT architecture, in which firewall implementation and zoning of the network prevent the possible attacks in one domain to be extended to other domains and the entire network. This method enables the formation of smaller zones of trust that ensure access control at levels 3 and 4.

4.2. Application layer vulnerabilities

Any related vulnerability such as a design flaw or implementation bug related to the security of the application can be considered as an application vulnerability [113]. The detection of application vulnerabilities is possible using an application penetration tester, port scanner, and code cracker [114]. The most exposed vulnerabilities can be considered username enumeration, weak passwords, account lockout, lack of multi-factor authentication, and insecure 3rd party components.

In the past, physical access was needed for the attacker, while nowadays, the devices can be detected on the network and exploited their vulnerabilities. The common local exploits are the DoS, cloning, firmware replacement, and extraction of security parameters [115]. In cloning, a duplicate physical device can be created and run similar software/firmware [116], while firmware replacement means the replacement of a malicious update for a device instead of the original version [117]. The common exploits in the communication protocols are the MitM, eavesdropping attacks, SQL injection (SQLi), and routing attacks. In an Eavesdropping attack, the communication between multiple devices can be intercepted and the security keys can be used [118], while in the SQLi, the attacker will usually find a flaw in the SQL application to enable the theft and authorized access [119]. The routers are usually used by small businesses and residential homes, hence owners may not give enough attention to the security alarms and the routers may remain unpatched and open to attack. In a routing attack, a rouge routing device will be placed on the network and modifies the routing packets to maliciously change the routing table.

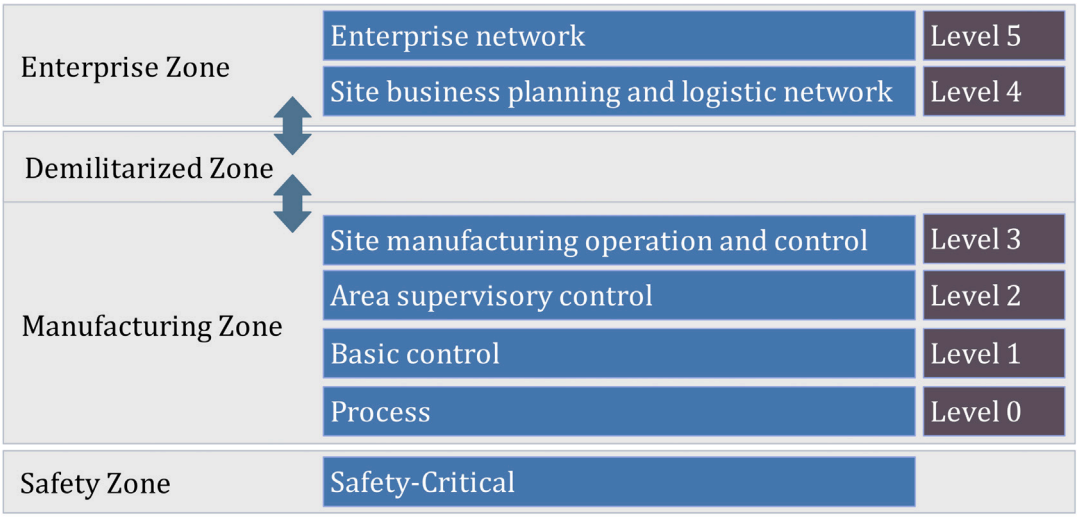


Fig. 12. A schematic of the traffic isolation and zoning method as an approach to managing the security in IoT solutions.

4.3. Web/cloud layer vulnerabilities

The storage, collection, and analysis of the data in the cloud have raised concerns to provide security for the cloud. The security for the cloud can be achieved using web application scanners, static analysis, and run-time protection [120]. The common web and cloud vulnerabilities are injection, XML external entities (XXE), sensitive data exposure, broken access control, and broken authentication [121]. In an injection attack, a malicious code will be injected into the program to control the database and website remotely. XXE happens when the XML input contains a reference to an external entity that is processed by a weakly configured XML parser. Sensitive data exposure is also a result of inappropriate encryption. To secure the cloud-based web interfaces, the following approach is suggested:

- Analyzing the web/cloud applications, web interfaces, and API interfaces for possible security vulnerabilities.
- Applying strong passwords
- Applying an account lockout mechanism to avoid brute-force attacks.
- Implementing two-factor authentication.
- Utilizing transport encryption, such as SSH and Secure Socket Layer 3.0 (SSL).
- Testing for SQLi, cross-site scripting (XSS), and cross-site request forgery (CSRF) vulnerabilities.
- Suggesting the users change the credentials after a period.

The existence of weak passwords has raised concerns in IoT solutions [122]. The common types of password attacks are brute force, dictionary attacks, password sniffing and cracking, and rainbow tables. In brute force, the attacker tries to use many possible passwords with the hope of finding the correct one [123]. The dictionary attack is similar to brute force, but the guesses for the password are based on all the strings in a pre-arranged listing that have more chances to succeed [124]. Password sniffing and cracking aims at finding hashed passwords using protocol analyzers that can intercept authentication traffic [125]. Also, rainbow tables contain hashed passwords and their equivalent plain text [126]. These tables are published/sold so that an attacker can be able to guess the passwords. Overall the existing vulnerabilities in different layers of the IoT reference model can be summarized as indicated in Fig. 13.

5. The methods to ensure the security for IoT solutions

To better follow the required privacy regulations in a business, it is necessary to follow a comprehensive framework [127,128]. In this regard, the National Institute of Standards and Technology (NIST) [129] defined a cybersecurity framework by five core functions that are shown in Fig. 14 The idea is to know the cybersecurity risks in the “Identify” step followed by utilizing proper safeguards in the “Protect” step. Then, the occurred cybersecurity events can be detected in the “detect” step, which enables the appropriate response in the “respond” step. After the cybersecurity incidents, the services can come back to their initial state by recovering in the “Recover” state.

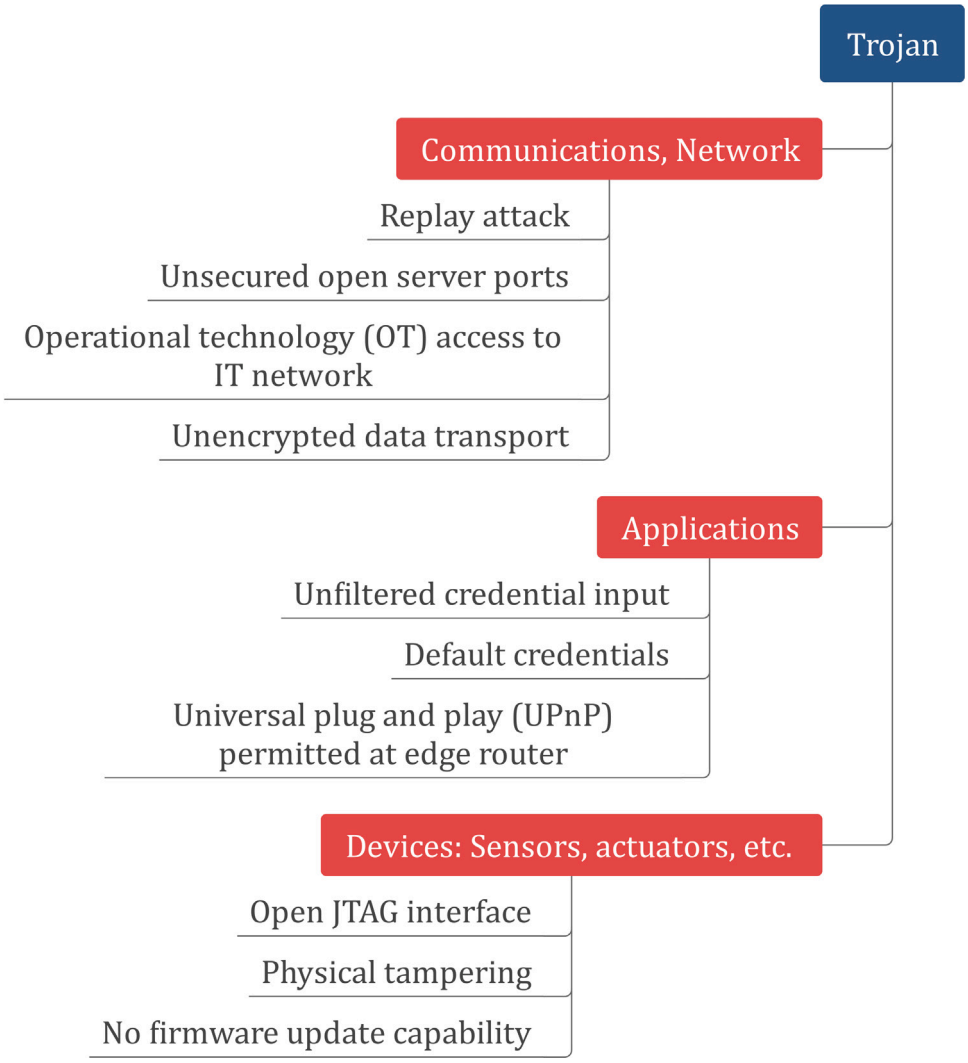


Fig. 13. A summary on the existing vulnerabilities in the communication, application, web/cloud layers of IoT reference model.

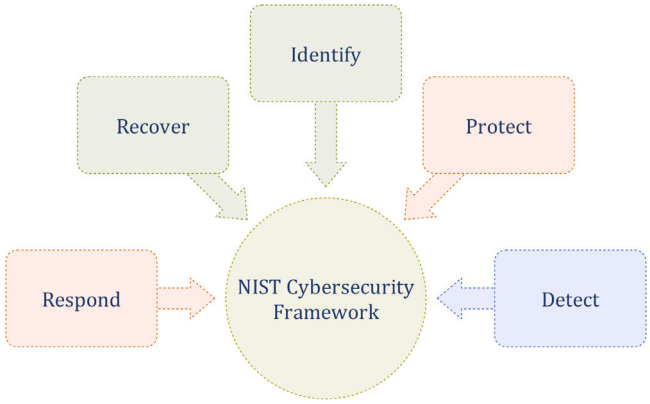


Fig. 14. The defined cybersecurity framework by NIST [129].

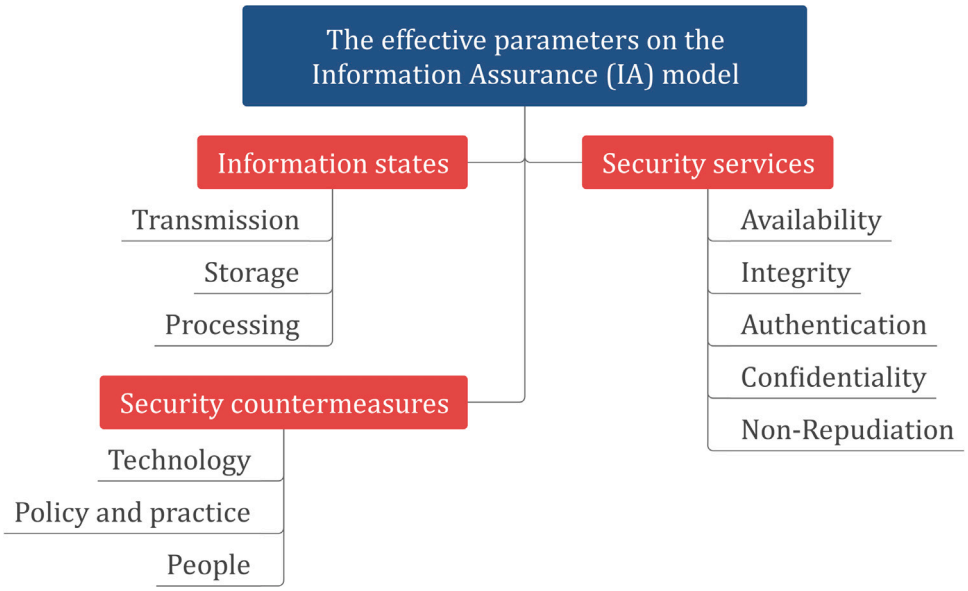


Fig. 15. A schematic of the main effective parameters in the information assurance model.

5.1. Information assurance (IA)

The definition by the National Security Agency (NSA) clarifies information assurance (IA) as a series of regulations to provide security for the data by ensuring availability, integrity, authentication, confidentiality, and non-repudiation [130]. In other words, IA can be presented by three main factors, which are security services, security countermeasures, and information states, considering time as the fourth parameter [131]. Fig. 15 illustrates the main effective parameters of the IA model to help the security experts for IoT applications.

5.1.1. Security services

As presented in Fig. 15, the security services can be divided into five main parameters of Confidentiality, Integrity, Availability, Authentication, and Non-Repudiation [132]. It is noteworthy to mention that the first three parameters are known as the CIA triad which relates to controlling information access/disclosure, preventing improper addition/ modification/ destruction of data, and ensuring the accessibility of the information, respectively.

- Confidentiality
  The parameter controls and protects private data from unauthorized entities [133]. As wireless data transmission is the main method of transferring data in IoT applications, the information is more in danger in comparison to the wired network. The cryptography methodology can be considered an efficient method to secure the confidentiality of the data [134]. In this regard, data encryption, authentication, and access control, which are cryptography methods, can be used. All the cryptography methods prevent unauthorized users to access the data using encoding in the encryption method and checking the access requests by the AAA framework in the authentication and access control methods.
- Availability
  Availability indicates the timely, reliable access of information or services to authorized entities [135]. In IoT applications, cybersecurity events result in interrupting the data availability, hence preventing access to IoT devices. The availability of the information can be ensured using system redundancy, system backups, enhanced system resiliency, equipment maintenance, up-to-date operating software, and in-advance plans to recover quickly from unforeseen incidents.
  In IoT applications, high availability, which is the agreed level of operational performance that reduces the unavailability of the system as much as possible, is of importance [136]. In this regard, it is necessary to use improves performance and reduce downtime by removing a single point of failure using hot stand-by devices, redundant components, and multiple pathways, by providing reliable crossover using power supplies and redundant backups, and by detecting failures as they occur using a robust monitoring system.
- Integrity
  Integrity verifies the quality of data by ensuring the accuracy, relevance, consistency, and reliability of the information in every operational procedure including data capture, storage, retrieval, updating, and transfer [137]. The usage degree in an organization and the type of gathered information determine the level of data integrity. The main levels of data integrity are classified as low, medium, high, and critical.

The healthcare and financial records can be considered as an example of the critical level. At this level, the data are validated, tested, and verified to ensure trustworthiness [138]. The organizations' databases are at a high level, where the data are validated and will be checked to provide trustworthiness. Online sales and search engines use Mid-level integrity with negligible verification. At this level, the data is not trustworthy entirely and the information has been collected using publicly posted forms. Blogs and personal posting sites are also being considered for the low level, in which the data may not be verified and a low level of trust exists in the content of the data.

- Authentication
  Authentication ensures the validity of a transmission, message, originator, or individual's authorization to receive determined types of data [139]. Bio-metric/password logins are considered authentication methods. The authentication in the IA demands detecting any possible limitations in the authentication system and removing them.
- Non-Repudiation
  In this service, the sender and the receiver of the data will be notified about the delivery of the information in which the former will receive the proof of delivery and the latter will have the proof of the sender's identity [140]. The IA demands establishing a network infrastructure to analyze the transmissions of the information with very low errors.

5.1.2. Security countermeasures

As the second dimension of the IA, the security countermeasures can be presented in the three main divisions of the technologies, operational policies and practices, and education and awareness [141].

- Technologies
  The main developed technologies in this division are software-based, hardware-based, network-based, and cloud-based technology countermeasures [142]. Software-based technology countermeasures are the installed programs on the devices to protect the operating systems, databases, and services such as firewalls, network scanners, protocol analyzers, etc., while hardware-based technology countermeasures are devices that deal with the protection of information. Virtual Private Networks (VPN) and Network Access Control (NAC) are examples of network-based technology countermeasures, while virtual security appliances are developed on a cloud virtual environment [143].
- Operational policies and practices
  In each organization, the policies or the operation should be deliberately selected to protect the system from cybersecurity threats [144]. The cybersecurity policy should clearly define the authentication, password, remote access, network maintenance, incident handling, and acceptable use policies.
- Education and awareness
  Increasing the security knowledge about efficient procedures and policies is needed as a countermeasure for possible cybersecurity threats [145]. It is suggested to provide special training for the employees who have access to confidential data, and IT professionals to use the appropriate technology to enhance the reliability and security of information services.

5.1.3. Information states

At a specific time in a system, the data can be considered as stored (data at rest), in transmission (data in transit), or the process (data in the process).

- Data at rest
  Providing the security and the management of the data in the storage is a challenging task especially in local storage, although easier to configure [146]. Generally, the main storage types are Direct Attached Storage (DAS), Redundant Array of Independent Disk (RAID), Network Attached Storage (NAS), Storage Area Network (SAN), and Cloud Storage. In DAS, which is a type of local storage, the storage is closer to the computing devices. In IoT applications, DAS is in the domain of Fog computing. RAID is an array of hardware that ameliorate the performance and fault tolerance, while NAS shares the data among the network users in addition to providing storage services. SAN enables different servers to utilize centralized storage by a high-speed interface, and cloud storage is being widely used by IoT appliances to store and characterize the data.
- Data in transit
  The main methods to transmit data between different devices are sneaker nets, wired networks, and wireless networks. Sneaker net, which is physical transmission utilizing a removable device, is widely being used in rural areas with no network connection. Once the network is available, either wired or wireless networks can be used in which wired transmission is through copper or fiber optic wires. In all these transmission methods, ensuring security is of importance [147].
- Data in process
  The input/output, modified, and computation data are considered as the data in the process. The modification of the data can be done through users, processes, or events such as equipment failure or cybersecurity attacks. If the data in process is being affected by the cybersecurity attacks and equipment failures, severe damages are foreseen, hence concentrated efforts should be made to prevent the cybersecurity attacks at this stage [148].

Table 2
The twelve cybersecurity domains defined by the ISO/IEC 27000.

Cybersecurity domain	Description
Risk assessment	As a first step in the risk management process, it clarifies the quantitative and qualitative value of risk to a specific situation or recognized threat.
Security policy	A document that regulates the access of the data and defines the existing constraints.
Organization of information security	The governing model established by an organization for data security.
Asset management	The inventory of a categorized scheme for data assets.
Human resource security	This domain deals with the joining, moving, and leaving of an employee within an organization.
Physical and environmental security	The protection of physical assets within an organization.
Communications and operations management	The management of technical security controls.
Information systems acquisition, development, and maintenance	The integration of security into applications.
Access control	The existing restrictions to access the network, system, etc.
Information security incident management	How to expect and respond to data security breaches.
Business continuity management	The protection, maintenance, and recovery of processes within a business.
Compliance	Ensuring conformance with the data security policies, standards, and regulations.

5.2. Cybersecurity management

The IA enables the cybersecurity authorities to detect security vulnerabilities and select the countermeasures, however, a system should be developed to manage the ensure the implementation of the IA. The required framework has been developed by the International Organization for Standardization (ISO)/ International Electrochemical Commission (IEC) 27000 [149]. The ISO/IEC 27000 standard defines the following twelve cybersecurity domains presented in Table 2 based on the implementation of an information security management system (ISMS).

5.3. Blockchain and IoT security

Despite the existence of numerous proposed solutions aimed at enhancing security for IoT devices across various layers, such as the application, network, and devices themselves, it is argued that the future of IoT security lies within the realm of Blockchain technology.[150]. Currently, Blockchain technology is extensively employed to ensure the security of cryptocurrencies. However, its potential extends beyond this domain, as it can also be leveraged for data exchange in IoT devices, along with other applications depicted in Fig. 16. In Blockchain, digital records (i.e. blocks) are linked to each other, while being secured by cryptography principles (i.e. chain), and are distributed across multiple computers not owned by any single entity [151].

The usage of Blockchain can enable IoT solutions to overcome the existing limitations to provide security as follows [152]:

- Securing the obtained measurements by the sensors and preventing malicious information.
- Enabling identification, authentication, and securing the data communication for IoT devices.
- Exchanging the data between IoT sensors directly in a secure condition.
- A distributed ledge eliminates a single source of failure within the IoT ecosystem.
- As the intermediary roles will not be needed in the Blockchain, the implementation of IoT devices and the communication of IoT devices will cost less.
- IoT devices are directly addressable with Blockchain, which provides an immutable history of connected devices for trust and transparency.

Additionally, the usage of Blockchain addresses more space than the conventional methods. In comparison to IPv6, that is benefiting from 128-bit address space, the Blockchain enjoys 160-bit address space. In this regard, Blockchain is capable to dedicate space for around 1.46×10^{48} IoT devices in offline conditions to supply Global Unique Identifier (GUID). The usage of Blockchain also eliminates centralized authority, which improves the security of IoT devices. Moreover, Blockchain is also able to supply 4.3 billion addresses in comparison to IPv6. Addressing the space for IoT devices through Blockchain will also enable many IoT devices that are not a good fit to be run with IPv6 stacks due to low memory capacity.

The implementation of the IoT will also resolves the current problems considering the ownership of the IoT devices from the manufacturer, supplier, retailer, and consumer. Blockchain has shown capabilities to provide authorized identity registration, ownership tracking of products, and maintaining the connection between transactions. In this regard, Blockchain is capable to ensure the decentralized management and tracking of IoT devices in every step of a device's life cycle.

6. Conclusion

The presented review article aimed to provide a comprehensive source to identify and describe the main cybersecurity attacks in IoT devices, emphasizing their significance in ensuring the security of IoT solutions. These attacks pose serious threats to the

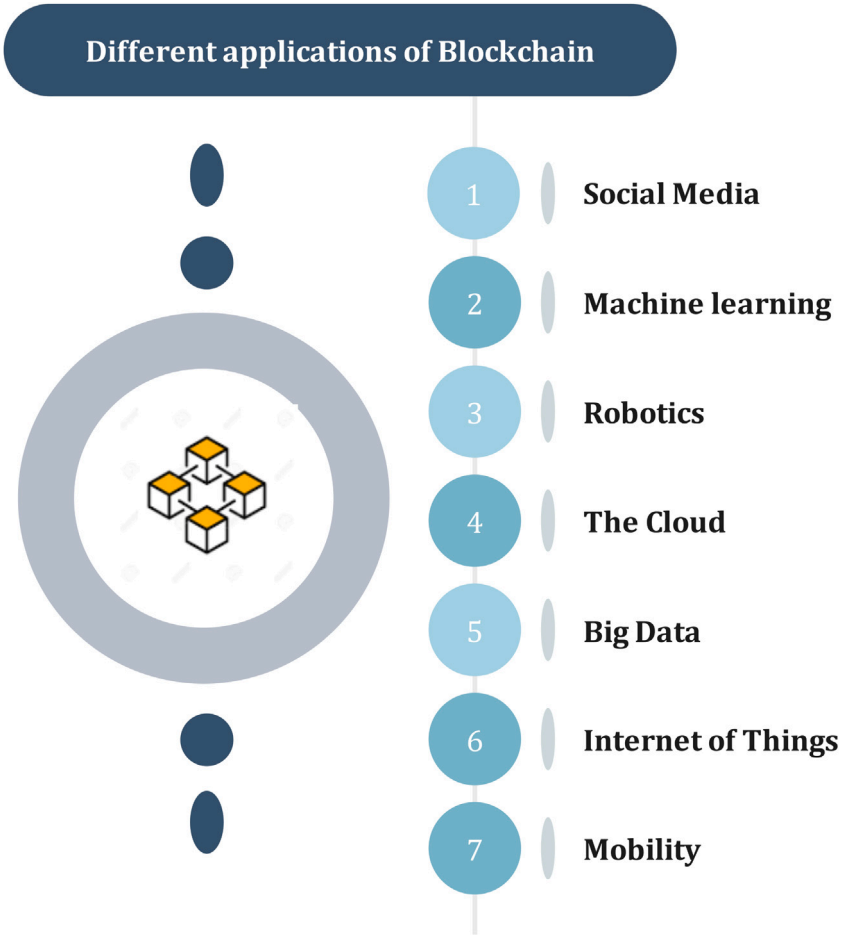


Fig. 16. The possible usage of Blockchain to provide security in different domains.

integrity, confidentiality, and availability of IoT devices and their data. In this regard, all the existing vulnerabilities in the different layers of the IoT reference model were highlighted, and suitable countermeasures were offered to mitigate these vulnerabilities to protect IoT devices and the broader IoT ecosystem. To ensure the security of the IoT solution, it was suggested that by adhering to the NIST framework and implementing IA measures, organizations can effectively safeguard sensitive information, mitigate cybersecurity threats, and maintain the trust of stakeholders in today's digital landscape. As a novel topic in the cybersecurity of IoT systems, Blockchain was also suggested for future development in this domain. By linking digital records through cryptographic principles and distributing them across multiple computers, Blockchain can eliminate the need for intermediaries, reduces costs, and can provide a resilient and transparent system. Additionally, it is proposed that Blockchain enables secure measurement acquisition, prevents malicious information, and establishes an immutable history of connected devices for trust and transparency in the IoT ecosystem. To mitigate the adverse effects of cybersecurity attacks, a comprehensive strategy can be proposed to effectively counteract various threats, including spoofing, tampering, repudiation, information disclosure, denial of service, and escalation of privilege. These strategies aim to prevent these malicious activities and safeguard the integrity, confidentiality, availability, and authenticity of the system.

- It is essential to assess the feasibility of updating devices intended for use in IoT systems and ensure that their firmware is kept up-to-date for future upgradability.
- Outdated and unsupported software and hardware components should be identified and replaced with updated versions of application software.
- Organizations should implement a clear separation between IT and IoT network traffic.
- The physical security of the devices in IoT systems is of high importance and the possible opportunity for attackers to tamper or destroy those devices should be minimized. The access control should be checked deliberately at well.
- The network traffic should be encrypted with high precision and secure messaging protocols should be utilized.

- The security of the network is a joint project between the personnel of the network security and the organization that is responsible to configure and maintain the security of the system. In this regard, engaging both parties in the security of IoT devices is crucial.
- The resource limitations of IoT devices are the main obstacle to improving the security of these devices. The cryptographic algorithms are constrained to operate within IoT resources. In this regard, the protocols in this field should be updated.
- Considering the large variety of IoT devices' power demand, a multi-layer security framework is required to cover the heterogeneity of the devices. Thus, special standardization of resources will be needed to provide intelligence for the secure framework.
- With regard to the heterogeneous IoT devices, the IoT paradigm will be vulnerable to single points of failure. Hence, concentrated efforts should be made to ensure the IoT elements for mission-critical applications.

By implementing robust measures and employing such strategies, organizations can significantly reduce the vulnerabilities and risks associated with cybersecurity attacks, thereby enhancing the overall security posture of their systems.

Declaration of competing interest

The authors declare the following financial interests/personal relationships which may be considered as potential competing interests: This project has received funding from the European Union's Horizon 2020 research and innovation program under the Marie Sklodowska-Curie grant agreement No. 754354.

Data availability

Data will be made available on request.

Acknowledgment

This project has received funding from the European Union's Horizon 2020 research and innovation program under the Marie Sklodowska-Curie grant agreement No. 754354.

References

[1] L. Knud Lasse, in: IoT Analytics (Ed.), Controversy in the Maldives, 2020, Available: https://iot-analytics.com/state-of-the-iot-2020-12-billion-iot-connections-surpassing-non-iot-for-the-first-time/.
[2] C. Perera, Internet of Things Research and Teaching: Vision and Mission Annual Report (2022) (Ph.D. thesis), Cardiff University, 2023.
[3] W. Iqbal, H. Abbas, M. Daneshmand, B. Rauf, Y.A. Bangash, An in-depth analysis of IoT security requirements, challenges, and their countermeasures via software-defined security, IEEE Internet Things J. 7 (10) (2020) 10250–10276.
[4] A.K. Gupta, R. Johari, IOT based electrical device surveillance and control system, in: 2019 4th International Conference on Internet of Things: Smart Innovation and Usages, IoT-SIU, IEEE, 2019, pp. 1–5.
[5] D.B. Rawat, R. Doku, M. Garuba, Cybersecurity in big data era: From securing big data to data-driven security, IEEE Trans. Serv. Comput. 14 (6) (2019) 2055–2072.
[6] V. Janjic, J. Bowles, A.F. Vermeulen, A. Silvina, M. Belk, C. Fidas, A. Pitsillides, M. Kumar, M. Rossbory, M. Vinov, et al., The serums tool-chain: ensuring security and privacy of medical data in smart patient-centric healthcare systems, in: 2019 IEEE International Conference on Big Data, Big Data, IEEE, 2019, pp. 2726–2735.
[7] T. Teoh, Y. Zhang, Y. Nguwi, Y. Elovici, W. Ng, Analyst intuition inspired high velocity big data analysis using PCA ranked fuzzy k-means clustering with multi-layer perceptron (MLP) to obviate cyber security risk, in: 2017 13th International Conference on Natural Computation, Fuzzy Systems and Knowledge Discovery, ICNC-FSKD, IEEE, 2017, pp. 1790–1793.
[8] M. Goodman, Future Crimes: Inside the Digital Underground and the Battle for Our Connected World, Random House, 2015.
[9] D.W. Pullin, Cybersecurity: positive changes through processes and team culture, Front. Health Serv. Manag. 35 (1) (2018) 3–12.
[10] C. Brumfield, B. Haugli, Cybersecurity Risk Planning and Management, Wiley Data and Cybersecurity, 2022.
[11] V.S. Shah, Fragmented architecture of IoT services to edge relationship between dimensions of electronic commerce, in: 2016 International Conference on Engineering & MIS, ICEMIS, IEEE, 2016, pp. 1–7.
[12] D. Shin, K. Yun, J. Kim, P.V. Astillo, J.-N. Kim, I. You, A security protocol for route optimization in DMM-based smart home IoT networks, IEEE Access 7 (2019) 142531–142550.
[13] S. Green, I. Ciçek, C.K. Koç, Continuous-time computational aspects of cyber-physical security, in: 2016 Workshop on Fault Diagnosis and Tolerance in Cryptography, FDTC, IEEE, 2016, pp. 59–62.
[14] F. Li, Y. Shi, A. Shinde, J. Ye, W. Song, Enhanced cyber-physical security in internet of things through energy auditing, IEEE Internet Things J. 6 (3) (2019) 5224–5231.
[15] X. Yang, L. Shu, Y. Liu, G.P. Hancke, M.A. Ferrag, K. Huang, Physical security and safety of iot equipment: A survey of recent advances and opportunities, IEEE Trans. Ind. Inform. 18 (7) (2022) 4319–4330.
[16] A.-K.A. Waleed, V. Kharchenko, D. Uzun, O. Solovyov, IoT-based physical security systems: Structures and PSMECA analysis, in: 2017 9th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, Vol. 2, IDAACS, IEEE, 2017, pp. 870–873.
[17] D. Lis, M. Arbter, M. Spindler, B. Otto, An investigation of antecedents for data governance adoption in the rail industry—Findings from a case study at Thales, IEEE Trans. Eng. Manage. (2022).
[18] A. Bassi, M. Bauer, M. Fiedler, T. Kramp, R. Van Kranenburg, S. Lange, S. Meissner, Enabling Things to Talk, Springer Nature, 2013.
[19] D. Hanes, G. Salgueiro, P. Grossetete, R. Barton, J. Henry, IoT Fundamentals: networking Technologies, Protocols, and Use Cases for the Internet of Things, Cisco Press, 2017.
[20] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, B. Sikdar, A survey on IoT security: application areas, security threats, and solution architectures, IEEE Access 7 (2019) 82721–82743.

[21] Z. Qi, Y. Wu, F. Hang, L. Xie, Y. He, A secure real-time internal and external network data exchange method based on web service protocol, in: 2020 International Symposium on Computer Engineering and Intelligent Communications, ISCEIC, IEEE, 2020, pp. 184–187.

[22] V. Kumar, N. Malik, J. Singla, N. Jhanjhi, F. Amsaad, A. Razaque, Light weight authentication scheme for smart home iot devices, Cryptography 6 (3) (2022) 37.

[23] I.A. Oyewumi, ISAAC: The Idaho Cyber-Physical System Smart Grid Cybersecurity Testbed, University of Idaho, 2019.

[24] S.K. Kavuri, G.R. Kancherla, B.R. Bobba, Data authentication and integrity verification techniques for trusted/untrusted cloud servers, in: 2014 International Conference on Advances in Computing, Communications and Informatics, ICACCI, IEEE, 2014, pp. 2590–2596.

[25] L. Xu, N. Pombo, Human behavior prediction though noninvasive and privacy-preserving internet of things (iot) assisted monitoring, in: 2019 IEEE 5th World Forum on Internet of Things, WF-IoT, IEEE, 2019, pp. 773–777.

[26] M.A. Helmiawan, I. Fadil, Y. Sofiyan, E. Firmansyah, Security model using intrusion detection system on cloud computing security management, in: 2021 9th International Conference on Cyber and IT Service Management, CITSM, IEEE, 2021, pp. 1–5.

[27] J.J. Wang, Wideband wide-scan millimeter-wave phased arrays for enhanced security/privacy and performance in 5G mobile wireless, in: 2017 IEEE International Symposium on Antennas and Propagation & USNC/URSI National Radio Science Meeting, IEEE, 2017, pp. 1471–1472.

[28] A. Roukounaki, S. Efremidis, J. Soldatos, J. Neises, T. Walloschke, N. Kefalakis, Scalable and configurable end-to-end collection and analysis of IoT security data: towards end-to-end security in IoT systems, in: 2019 Global IoT Summit, GIoTS, IEEE, 2019, pp. 1–6.

[29] N. Redini, A. Machiry, R. Wang, C. Spensky, A. Continella, Y. Shoshitaishvili, C. Kruegel, G. Vigna, Karonte: Detecting insecure multi-binary interactions in embedded firmware, in: 2020 IEEE Symposium on Security and Privacy, SP, IEEE, 2020, pp. 1544–1561.

[30] N. Neshenko, E. Bou-Harb, J. Crichigno, G. Kaddoum, N. Ghani, Demystifying IoT security: an exhaustive survey on IoT vulnerabilities and a first empirical look on internet-scale IoT exploitations, IEEE Commun. Surv. Tutor. 21 (3) (2019) 2702–2733.

[31] D. Lu, R. Han, Y. Shen, X. Dong, J. Ma, X. Du, M. Guizani, xTSeH: A trusted platform module sharing scheme towards smart IoT-ehealth devices, IEEE J. Sel. Areas Commun. 39 (2) (2020) 370–383.

[32] M.R. Nosouhi, K. Sood, M. Grobler, R. Doss, Towards spoofing resistant next generation iot networks, IEEE Trans. Inf. Forensics Secur. 17 (2022) 1669–1683.

[33] S. Siboni, V. Sachidananda, Y. Meidan, M. Bohadana, Y. Mathov, S. Bhairav, A. Shabtai, Y. Elovici, Security testbed for Internet-of-Things devices, IEEE Trans. Reliab. 68 (1) (2019) 23–44.

[34] A.P. Singh, N.R. Pradhan, A.K. Luhach, S. Agnihotri, N.Z. Jhanjhi, S. Verma, U. Ghosh, D.S. Roy, et al., A novel patient-centric architectural framework for blockchain-enabled healthcare applications, IEEE Trans. Ind. Inform. 17 (8) (2020) 5779–5789.

[35] S. Rizvi, A. Kurtz, J. Pfeffer, M. Rizvi, Securing the Internet of Things (IoT): A security taxonomy for IoT, in: 2018 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/12th IEEE International Conference on Big Data Science and Engineering, TrustCom/BigDataSE, IEEE, 2018, pp. 163–168.

[36] F. Hussain, S.G. Abbas, I.M. Pires, S. Tanveer, U.U. Fayyaz, N.M. Garcia, G.A. Shah, F. Shahzad, A two-fold machine learning approach to prevent and detect IoT botnet attacks, IEEE Access 9 (2021) 163412–163430.

[37] G.R. Andreica, L. Bozga, D. Zinca, V. Dobrota, Denial of service and man-in-the-middle attacks against IoT devices in a GPS-based monitoring software for intelligent transportation systems, in: 2020 19th RoEduNet Conference: Networking in Education and Research, RoEduNet, IEEE, 2020, pp. 1–4.

[38] C. Faircloth, G. Hartzell, N. Callahan, S. Bhunia, A study on brute force attack on T-mobile leading to SIM-hijacking and identity-theft, in: 2022 IEEE World AI IoT Congress, AIIoT, IEEE, 2022, pp. 501–507.

[39] L. Luo, Y. Zhang, C. White, B. Keating, B. Pearson, X. Shao, Z. Ling, H. Yu, C. Zou, X. Fu, On security of TrustZone-M-based IoT systems, IEEE Internet Things J. 9 (12) (2022) 9683–9699.

[40] M. Nascimento, J. Araujo, A. Ribeiro, Systematic review on mitigating and preventing ddos attacks on IoT networks, in: 2022 17th Iberian Conference on Information Systems and Technologies, CISTI, IEEE, 2022, pp. 1–9.

[41] M. Waqas, K. Kumar, A.A. Laghari, U. Saeed, M.M. Rind, A.A. Shaikh, F. Hussain, A. Rai, A.Q. Qazi, Botnet attack detection in Internet of Things devices over cloud environment via machine learning, Concurr. Comput.: Pract. Exper. 34 (4) (2022) e6662.

[42] N. Sivasankari, S. Kamalakkannan, Detection and prevention of man-in-the-middle attack in iot network using regression modeling, Adv. Eng. Softw. 169 (2022) 103126.

[43] A. Ashenafi, A Model to Detect MiTM Attack in IoT Networks: A Machine Learning Approach (Ph.D. thesis), St. Mary's University, 2022.

[44] M. Mukhandi, F. Damião, J. Granjal, J.P. Vilela, Blockchain-based device identity management with consensus authentication for IoT devices, in: 2022 IEEE 19th Annual Consumer Communications & Networking Conference, CCNC, IEEE, 2022, pp. 433–436.

[45] N. Kumar, J.K. Samriya, Secure data validation and transmission in cloud and IoT through ban logic and KP-ABE, Int. J. Sens. Wirel. Commun. Control 12 (1) (2022) 79–87.

[46] J. Thomé, L.K. Shar, L. Briand, Security slicing for auditing XML, XPath, and SQL injection vulnerabilities, in: 2015 IEEE 26th International Symposium on Software Reliability Engineering, ISSRE, IEEE, 2015, pp. 553–564.

[47] S. Rachmadi, S. Mandala, D. Oktaria, Detection of DoS attack using AdaBoost algorithm on IoT system, in: 2021 International Conference on Data Science and Its Applications, ICoDSA, 2021, pp. 28–33.

[48] R. Arthi, S. Krishnaveni, Design and development of IOT testbed with DDoS attack for cyber security research, in: 2021 3rd International Conference on Signal Processing and Communication, ICPSC, 2021, pp. 586–590.

[49] K.-Y. Lam, S. Mitra, F. Gondesen, X. Yi, ANT-centric IoT security reference architecture—Security-by-design for satellite-enabled smart cities, IEEE Internet Things J. 9 (8) (2022) 5895–5908.

[50] N.M. Min, V. Visoottiviseth, S. Teerakanok, N. Yamai, OWASP IoT top 10 based attack dataset for machine learning, in: 2022 24th International Conference on Advanced Communication Technology, ICACT, 2022, pp. 317–322.

[51] K. Ishibashi, N. Sugii, K. Kobayashi, T. Koide, H. Nagatomi, S. Kamohara, SOTB technology, which enables perpetually reliable CPU for IoT applications, in: 2015 Fourth Berkeley Symposium on Energy Efficient Electronic Systems, E3S, 2015, pp. 1–3.

[52] M.N. Ince, J. Ledet, M. Gunay, Building an open source linux computing system on RISC-V, in: 2019 1st International Informatics and Software Engineering Conference, UBMYK, 2019, pp. 1–4.

[53] G. Leplus, O. Savry, L. Bossuet, Insertion of random delay with context-aware dummy instructions generator in a RISC-V processor, in: 2022 IEEE International Symposium on Hardware Oriented Security and Trust, HOST, 2022, pp. 81–84.

[54] M.N.M. Najib, D.A. Ramli, Analysis of smart IoT portal based on advanced RISC machines (ARM) processor for fanless heat maintenance, in: N.M. Mahyuddin, N.R. Mat Noor, H.A. Mat Sakim (Eds.), Proceedings of the 11th International Conference on Robotics, Vision, Signal Processing and Power Applications, Springer Singapore, Singapore, 2022, pp. 612–617.

[55] J. Jung, B. Kim, J. Cho, B. Lee, A secure platform model based on ARM platform security architecture for IoT devices, IEEE Internet Things J. 9 (7) (2022) 5548–5560.

[56] U. Saeed, M.A. Khuhro, M. Waqas, N. Mirbahar, Mehran Univ. Res. J. Eng. Technol. 41 (3) (2022) 113–119, Available: https://search.informit.org/doi/10.3316/informit.629770127992220.

[57] D.M. Rajagopal, A. Pathak, N. Khare, Ultra wide voltage range one time programmable EPROM circuit for portable applications, in: 2020 IEEE International Symposium on Circuits and Systems, ISCAS, 2020, pp. 1–4.

[58] A.C. Bento, L.A.T. Mantovani, J.C. Gomes, M. Galdino, WiFi and EEPROM experiment with nodemcu12e and nextion tft for IoT projects, in: 2019 10th International Conference on Computing, Communication and Networking Technologies, ICCCNT, 2019, pp. 1–6.

[59] S. Vasile, D. Oswald, T. Chothia, Breaking all the things—A systematic survey of firmware extraction techniques for IoT devices, in: B. Bilgin, J.-B. Fischer (Eds.), Smart Card Research and Advanced Applications, Springer International Publishing, Cham, 2019, pp. 171–185.

[60] J.R. Dinesh Kumar, C. Ganesh Babu, V.R. Balaji, K. Priyadharsini, S.P. Karthi, Performance investigation of various SRAM cells for IoT based wearable biomedical devices, in: G. Ranganathan, J. Chen, A. Rocha (Eds.), Inventive Communication and Computational Technologies, Springer Singapore, Singapore, 2021, pp. 573–588.

[61] N.A. Anagnostopoulos, T. Arul, Y. Fan, C. Hatzfeld, J. Lotichius, R. Sharma, F. Fernandes, F. Tehranipoor, S. Katzenbeisser, Securing IoT devices using robust DRAM PUFs, in: 2018 Global Information Infrastructure and Networking Symposium, GIIS, 2018, pp. 1–5.

[62] G. Vishwakarma, W. Lee, Exploiting JTAG and its mitigation in IOT: A survey, Future Internet 10 (12) (2018) Available: https://www.mdpi.com/1999-5903/10/12/121.

[63] W. Liu, J. Zhou, Research and implementation of IoT secure element testing software based on SPI interface, in: 2021 3rd International Academic Exchange Conference on Science and Technology Innovation, IAECST, 2021, pp. 252–255.

[64] D. D'Alessandro, W. Gunderson, E. Staten, Y.K. Donastien, P. Rodriguez, R. Bailey, Integrating modularity for mass customization of IoT wireless sensor systems, in: 2021 Systems and Information Engineering Design Symposium, SIEDS, 2021, pp. 1–5.

[65] B. Jeevan, P. Sahithi, P. Samskruthi, K. Sivani, Simulation and synthesis of UART through FPGA zedboard for IoT applications, in: 2022 International Conference on Advances in Computing, Communication and Applied Informatics, ACCAI, 2022, pp. 1–7.

[66] S.A. Chaudhry, K. Yahya, F. Al-Turjman, M.-H. Yang, A secure and reliable device access control scheme for IoT based sensor cloud systems, IEEE Access 8 (2020) 139244–139254.

[67] M.U. Aftab, Y. Munir, A. Oluwasanmi, Z. Qin, M.H. Aziz, Zakria, N.T. Son, V.D. Tran, A hybrid access control model with dynamic COI for secure localization of satellite and IoT-based vehicles, IEEE Access 8 (2020) 24196–24208.

[68] H. Liu, D. Han, D. Li, Fabric-IoT: A blockchain-based access control system in IoT, IEEE Access 8 (2020) 18207–18218.

[69] C.B. Mwakwata, H. Malik, M. Mahtab Alam, Y. Le Moullec, S. Parand, S. Mumtaz, Narrowband Internet of Things (NB-IoT): From physical (PHY) and media access control (MAC) layers perspectives, Sensors 19 (11) (2019) Available: https://www.mdpi.com/1424-8220/19/11/2613.

[70] G. Jeong, S. Hong, Current reused CMOS RF-DAC for IoT applications, Microw. Opt. Technol. Lett. 63 (12) (2021) 2991–2996, Available: https://onlinelibrary.wiley.com/doi/abs/10.1002/mop.33019.

[71] A. Thakare, E. Lee, A. Kumar, V.B. Nikam, Y.-G. Kim, PARBAC: Priority-attribute-based RBAC model for Azure IoT cloud, IEEE Internet Things J. 7 (4) (2020) 2890–2900.

[72] S. Bhatt, R. Sandhu, ABAC-CC: Attribute-based access control and communication control for Internet of Things, in: Proceedings of the 25th ACM Symposium on Access Control Models and Technologies, SACMAT '20, Association for Computing Machinery, New York, NY, USA, 2020, pp. 203–212, http://dx.doi.org/10.1145/3381991.3395618.

[73] I.A. Kamil, S.O. Ogundoyin, Lightweight privacy-preserving power injection and communication over vehicular networks and 5G smart grid slice with provable security, Internet of Things 8 (2019) 100116, Available: https://www.sciencedirect.com/science/article/pii/S2542660518302063.

[74] D. Hardt, The OAuth 2.0 authorization framework, 2012, Request for Comments, 6749, RFC 6749, RFC Editor. Available: https://www.rfc-editor.org/info/rfc6749.

[75] E. Chatzoglou, G. Kambourakis, C. Kolias, Empirical evaluation of attacks against IEEE 802.11 enterprise networks: The AWID3 dataset, IEEE Access 9 (2021) 34188–34205.

[76] A.M. Al Naamany, A. Al Shidhani, H. Bourdoucen, IEEE 802.11 wireless LAN security overview, Int. J. Comput. Sci. Netw. Secur. 6 (5B) (2006) 138, Available: https://cir.nii.ac.jp/crid/1571980075939355904.

[77] L.-H. Yen, W.-T. Tsai, The room shortage problem of tree-based ZigBee/IEEE 802.15.4 wireless networks, Comput. Commun. 33 (4) (2010) 454–462, Available: https://www.sciencedirect.com/science/article/pii/S0140366409002783.

[78] S. Chacko, D. Job, Security mechanisms and vulnerabilities in LPWAN, in: IOP Conference Series: Materials Science and Engineering, Vol. 396, No. 1, IOP Publishing, 2018, 012027, http://dx.doi.org/10.1088/1757-899X/396/1/012027.

[79] A.I. Gardezi, Security in Wireless Cellular Networks, Wash. Univ. St Louis St Louis, 2006.

[80] S. Bhunia, M.S. Hsiao, M. Banga, S. Narasimhan, Hardware Trojan attacks: Threat analysis and countermeasures, Proc. IEEE 102 (8) (2014) 1229–1247.

[81] M. Devi, A. Majumder, Side-channel attack in Internet of Things: A survey, in: J.K. Mandal, S. Mukhopadhyay, A. Roy (Eds.), Applications of Internet of Things, Springer Singapore, Singapore, 2021, pp. 213–222.

[82] R.S. Chakraborty, S. Narasimhan, S. Bhunia, Hardware Trojan: Threats and emerging solutions, in: 2009 IEEE International High Level Design Validation and Test Workshop, 2009, pp. 166–171.

[83] Z. Chen, Hardware Trojan designs on BASYS FPGA board (Virginia tech), in: CSAW Embed. Syst. Chall., 2008.

[84] X.T. Ng, Z. Naj, S. Bhasin, D.B. Roy, J.-L. Danger, S. Guilley, Integrated sensor: A backdoor for hardware Trojan insertions? in: 2015 Euromicro Conference on Digital System Design, 2015, pp. 415–422.

[85] W. Zhou, C. Cao, D. Huo, K. Cheng, L. Zhang, L. Guan, T. Liu, Y. Jia, Y. Zheng, Y. Zhang, L. Sun, Y. Wang, P. Liu, Reviewing IoT security via logic bugs in IoT platforms and systems, IEEE Internet Things J. 8 (14) (2021) 11621–11639.

[86] S. Koley, P. Ghosal, Addressing hardware security challenges in Internet of Things: Recent trends and possible solutions, in: 2015 IEEE 12th Intl Conf on Ubiquitous Intelligence and Computing and 2015 IEEE 12th Intl Conf on Autonomic and Trusted Computing and 2015 IEEE 15th Intl Conf on Scalable Computing and Communications and Its Associated Workshops, UIC-ATC-ScalCom, 2015, pp. 517–520.

[87] S. Mitra, H.-S.P. Wong, S. Wong, The Trojan-proof chip, IEEE Spectr. 52 (2) (2015) 46–51.

[88] J. Dofe, J. Frey, Q. Yu, Hardware security assurance in emerging IoT applications, in: 2016 IEEE International Symposium on Circuits and Systems, ISCAS, 2016, pp. 2050–2053.

[89] A. Sengupta, S. Kundu, Guest editorial securing IoT hardware: Threat models and reliable, low-power design solutions, IEEE Trans. Very Large Scale Integr. (VLSI) Syst. 25 (12) (2017) 3265–3267.

[90] K.G. Liakos, G.K. Georgakilas, S. Moustakidis, N. Sklavos, F.C. Plessas, Conventional and machine learning approaches as countermeasures against hardware Trojan attacks, Microprocess. Microsyst. 79 (2020) 103295, Available: https://www.sciencedirect.com/science/article/pii/S0141933120304543.

[91] J. Graf, W. Batchelor, S. Harper, R. Marlow, E. Carlisle, P. Athanas, A practical application of game theory to optimize selection of hardware Trojan detection strategies, J. Hardw. Syst. Secur. 4 (2) (2020) 98–119.

[92] X.-T. Ngo, V.-P. Hoang, H.L. Duc, Hardware Trojan threat and its countermeasures, in: 2018 5th NAFOSTED Conference on Information and Computer Science, NICS, 2018, pp. 35–40.

[93] E. Kim, G. Woo, T. Kim, In-situ monitoring hydrodynamic pressure distribution during chemical mechanical polishing, in: 2019 II Workshop on Metrology for Industry 4.0 and IoT, MetroInd4.0&IoT, 2019, pp. 235–239.

[94] S. Guo, J. Wang, Z. Chen, Y. Li, Z. Lu, Securing IoT space via hardware Trojan detection, IEEE Internet Things J. 7 (11) (2020) 11115–11122.

[95] A. Sayakkara, N.-A. Le-Khac, M. Scanlon, Leveraging electromagnetic side-channel analysis for the investigation of IoT devices, Digit. Investig. 29 (2019) S94–S103, Available: https://www.sciencedirect.com/science/article/pii/S1742287619301616.

[96] F. Rozie, I. Syarif, M.U.H. Al Rasyid, Design and implementation of intelligent aquaponics monitoring system based on IoT, in: 2020 International Electronics Symposium, IES, 2020, pp. 534–540.

[97] Q. Pan, J. Wu, A.K. Bashir, J. Li, J. Wu, Side-channel fuzzy analysis-based AI model extraction attack with information-theoretic perspective in intelligent IoT, IEEE Trans. Fuzzy Syst. 30 (11) (2022) 4642–4656.

[98] F.Z. Coulibaly, Software Obfuscation for Security of COTS-Based Embedded Systems, University of Central Arkansas, 2021.

[99] F.-X. Standaert, Introduction to side-channel attacks, in: I.M. Verbauwhede (Ed.), Secure Integrated Circuits and Systems, Springer US, Boston, MA, 2010, pp. 27–42, http://dx.doi.org/10.1007/978-0-387-71829-3_2.

[100] N. Veyrat-Charvillon, B. Gérard, F.-X. Standaert, Soft analytical side-channel attacks, in: P. Sarkar, T. Iwata (Eds.), Advances in Cryptology, ASIACRYPT 2014, Springer Berlin Heidelberg, Berlin, Heidelberg, 2014, pp. 282–296.

[101] S.R. Shanmugham, S. Paramasivam, Survey on power analysis attacks and its impact on intelligent sensor networks, IET Wirel. Sens. Syst. 8 (6) (2018) 295–304, Available: https://ietresearch.onlinelibrary.wiley.com/doi/abs/10.1049/iet-wss.2018.5157.

[102] H.J. Mahanta, K. Nath, A.K. Roy, K. Kotecha, V. Varadaranjan, Using genetic algorithm in inner product to resist modular exponentiation from higher order DPA attacks, IEEE Access 10 (2022) 3238–3251.

[103] A. Ghosh, D.-H. Seo, D. Das, S. Ghosh, S. Sen, A digital cascoded signature attenuation countermeasure with intelligent malicious voltage drop attack detector for EM/Power SCA resilient parallel AES-256, in: 2022 IEEE Custom Integrated Circuits Conference, CICC, 2022, pp. 01–02.

[104] W. Shan, X. Fu, Z. Xu, A secure reconfigurable crypto IC with countermeasures against SPA, DPA, and EMA, IEEE Trans. Comput.-Aided Des. Integr. Circuits Syst. 34 (7) (2015) 1201–1205.

[105] I. Kabin, Z. Dyka, D. Klann, P. Langendoerfer, Horizontal DPA attacks against ECC: Impact of implemented field multiplication formula, in: 2019 14th International Conference on Design & Technology of Integrated Systems in Nanoscale Era, DTIS, 2019, pp. 1–6.

[106] O. Lo, W.J. Buchanan, D. Carson, Power analysis attacks on the AES-128 S-box using differential power analysis (DPA) and correlation power analysis (CPA), J. Cyber Secur. Technol. 1 (2) (2017) 88–107, http://dx.doi.org/10.1080/23742917.2016.1231523.

[107] C. Sharma, N.K. Gondhi, Communication protocol stack for constrained IoT systems, in: 2018 3rd International Conference on Internet of Things: Smart Innovation and Usages, IoT-SIU, 2018, pp. 1–6.

[108] S. Verma, Y. Kawamoto, N. Kato, A network-aware internet-wide scan for security maximization of IPv6-enabled WLAN IoT devices, IEEE Internet Things J. 8 (10) (2021) 8411–8422.

[109] M. Šarac, N. Pavlović, N. Bacanin, F. Al-Turjman, S. Adamović, Increasing privacy and security by integrating a blockchain secure interface into an IoT device security gateway architecture, Energy Rep. 7 (2021) 8075–8082, Available: https://www.sciencedirect.com/science/article/pii/S2352484721005448.

[110] M.M. Cherian, S.L. Varma, Mitigation of DDOS and MiTM attacks using belief based secure correlation approach in SDN-based IoT networks, Int. J. Comput. Netw. Inf. Secur. (IJCNIS) 14 (1) (2022) 52–68.

[111] G. Pabbisetty, H. Mori, A simple decentralized timeslot synchronization algorithm for large-scale wireless IoT networks, in: 2021 16th Annual Conference on Wireless on-Demand Network Systems and Services Conference, WONS, 2021, pp. 1–4.

[112] D. Minoli, B. Occhiogrosso, Blockchain mechanisms for IoT security, Internet Things 1–2 (2018) 1–13, Available: https://www.sciencedirect.com/science/article/pii/S2542660518300167.

[113] F. Meneghello, M. Calore, D. Zucchetto, M. Polese, A. Zanella, IoT: Internet of threats? A survey of practical security vulnerabilities in real IoT devices, IEEE Internet Things J. 6 (5) (2019) 8182–8201.

[114] G. Nebbione, M.C. Calzarossa, Security of IoT application layer protocols: Challenges and findings, Future Internet 12 (3) (2020) Available: https://www.mdpi.com/1999-5903/12/3/55.

[115] A. Raghuvanshi, U.K. Singh, C. Joshi, A review of various security and privacy innovations for IoT applications in healthcare, in: Advanced Healthcare Systems, John Wiley & Sons, Ltd, 2022, pp. 43–58, Available: https://onlinelibrary.wiley.com/doi/abs/10.1002/9781119769293.ch4.

[116] W. Jiang, B. Wu, Z. Jiang, S. Yang, Cloning vulnerability detection in driver layer of IoT devices, in: J. Zhou, X. Luo, Q. Shen, Z. Xu (Eds.), Information and Communications Security, Springer International Publishing, Cham, 2020, pp. 89–104.

[117] J. Kwon, M.G. Seok, D. Park, User insensible sliding firmware update technique for flash-area/time-cost reduction toward low-power embedded software replacement, in: 2020 IEEE Symposium in Low-Power and High-Speed Chips, COOL CHIPS, 2020, pp. 1–3.

[118] J.H. Anajemba, C. Iwendi, I. Razzak, J.A. Ansere, I.M. Okpalaoguchi, A counter-eavesdropping technique for optimized privacy of wireless industrial IoT communications, IEEE Trans. Ind. Inform. 18 (9) (2022) 6445–6454.

[119] A.A. Ashlam, A. Badii, F. Stahl, A novel approach exploiting machine learning to detect SQLi attacks, in: 2022 5th International Conference on Advanced Systems and Emergent Technologies, IC_ASET, 2022, pp. 513–517.

[120] C. Choi, J. Choi, Ontology-based security context reasoning for power IoT-cloud security service, IEEE Access 7 (2019) 110510–110517.

[121] R. Geetha, A.K. Suntheya, G.U. Srikanth, Cloud integrated IoT enabled sensor network security: Research issues and solutions, Wirel. Pers. Commun. 113 (2020) 747–771.

[122] D. Yu, L. Zhang, Y. Chen, Y. Ma, J. Chen, Large-scale IoT devices firmware identification based on weak password, IEEE Access 8 (2020) 7981–7992.

[123] M.M. Raikar, S.M. Meena, SSH brute force attack mitigation in Internet of Things (IoT) network : An edge device security measure, in: 2021 2nd International Conference on Secure Cyber Computing and Communications, ICSCCC, 2021, pp. 72–77.

[124] B. Vignau, R. Khoury, S. Hallé, 10 Years of IoT malware: A feature-based taxonomy, in: 2019 IEEE 19th International Conference on Software Quality, Reliability and Security Companion, QRS-C, 2019, pp. 458–465.

[125] S. Sarkar, J. Liu, E. Jovanov, A robust algorithm for sniffing BLE long-lived connections in real-time, in: 2019 IEEE Global Communications Conference, GLOBECOM, 2019, pp. 1–6.

[126] W.-C. Tsai, T.-H. Tsai, G.-H. Xiao, T.-J. Wang, Y.-R. Lian, S.-H. Huang, An automatic key-update mechanism for M2M communication and IoT security enhancement, in: 2020 IEEE International Conference on Smart Internet of Things, SmartIoT, 2020, pp. 354–355.

[127] R. Chatila, J.C. Havens, The IEEE global initiative on ethics of autonomous and intelligent systems, in: M.I. Aldinhas Ferreira, J.a. Silva Sequeira, G. Singh Virk, M.O. Tokhi, E. E. Kadar (Eds.), Robotics and Well-Being, Springer International Publishing, Cham, 2019, pp. 11–16, http://dx.doi.org/10.1007/978-3-030-12524-0_2.

[128] N.M. Karie, N.M. Sahri, W. Yang, C. Valli, V.R. Kebande, A review of security standards and frameworks for IoT-based smart environments, IEEE Access 9 (2021) 121975–121995.

[129] M.P. Barrett, Framework for improving critical infrastructure cybersecurity version 1.1, in: NIST Cybersecurity Framework, 2023, Available: https://www.nist.gov/cyberframework.

[130] M.K. Abiodun, J.B. Awotunde, R.O. Ogundokun, E.A. Adeniyi, M.O. Arowolo, Security and information assurance for IoT-based big data, in: S. Misra, A. Kumar Tyagi (Eds.), Artificial Intelligence for Cyber Security: Methods, Issues and Possible Horizons Or Opportunities, Springer International Publishing, Cham, 2021, pp. 189–211, http://dx.doi.org/10.1007/978-3-030-72236-4_8.

[131] A. Kendall, A. Das, B. Nagy, B. Johnson, A. Ghosh, Using hyperledger fabric blockchain to improve information assurance of IoT devices for AI model development, in: Y. Maleh, L. Tawalbeh, S. Motahhir, A.S. Hafid (Eds.), Advances in Blockchain Technology for Cyber Physical Systems, Springer International Publishing, Cham, 2022, pp. 233–259, http://dx.doi.org/10.1007/978-3-030-93646-4_11.

[132] J. Payton, X. Du, X. He, J. Wu, Envisioning an information assurance and performance infrastructure for the internet of things, in: 2018 IEEE 4th International Conference on Collaboration and Internet Computing, CIC, 2018, pp. 266–271.
[133] R. Ram, M. Kumar, S. Ramamoorthy, An efficient hybrid computing environment to develop a confidential and authenticated IoT service model, Wirel. Pers. Commun. 117 (2021) 2903–2927.
[134] R. Hodgson, Solving the security challenges of IoT with public key cryptography, Netw. Secur. 2019 (1) (2019) 17–19, http://dx.doi.org/10.1016/S1353-4858(19)30011-X.
[135] R. Togneri, G. Camponogara, J.-P. Soininen, C. Kamienski, Foundations of data quality assurance for IoT-based smart applications, in: 2019 IEEE Latin-American Conference on Communications, LATINCOM, 2019, pp. 1–6.
[136] H.A. Abdul-Ghani, D. Konstantas, M. Mahyoub, A comprehensive IoT attacks survey based on a building-blocked reference model, Int. J. Adv. Comput. Sci. Appl. 9 (3) (2018).
[137] E. Reilly, M. Maloney, M. Siegel, G. Falco, An IoT integrity-first communication protocol via an ethereum blockchain light client, in: 2019 IEEE/ACM 1st International Workshop on Software Engineering Research & Practices for the Internet of Things, SERP4IoT, 2019, pp. 53–56.
[138] A.K. Tyagi, M.M. Nair, Internet of everything (IoE) and Internet of Things (IoTs): Threat analyses, possible opportunities for future, J. Inf. Assur. Secur. 15 (5) (2020) 194–218.
[139] B. Cambou, P.G. Flikkema, J. Palmer, D. Telesca, C. Philabaum, Can ternary computing improve information assurance? Cryptography 2 (1) (2018) Available: https://www.mdpi.com/2410-387X/2/1/6.
[140] W. Fang, W. Chen, W. Zhang, Digital signature scheme for information non-repudiation in blockchain: a state of the art review, J. Wirel. Commun. Netw. 56 (2020).
[141] K. Tsiknas, D. Taketzis, K. Demertzis, C. Skianis, Cyber threats to industrial IoT: A survey on attacks and countermeasures, IoT 2 (1) (2021) 163–186, Available: https://www.mdpi.com/2624-831X/2/1/9.
[142] M. Al-Shaboti, I. Welch, A. Chen, M.A. Mahmood, Towards secure smart home IoT: Manufacturer and user network access control framework, in: 2018 IEEE 32nd International Conference on Advanced Information Networking and Applications, AINA, 2018, pp. 892–899.
[143] N. Jayashri, K. Kalaiselvi, Cloud cryptography for cloud data analytics in IoT, in: Machine Learning Approach for Cloud Data Analytics in IoT, John Wiley & Sons, Ltd, 2021, pp. 119–142, Available: https://onlinelibrary.wiley.com/doi/abs/10.1002/9781119785873.ch6.
[144] T. Dimitrakos, How to develop a security controls oriented reference architecture for cloud, IoT and SDN/NFV platforms, in: N. Gal-Oz, P.R. Lewis (Eds.), Trust Management XII, Springer International Publishing, Cham, 2018, pp. 1–14.
[145] J. Cryer, R. Zounlome, Cybersecurity: Bridging the gap between training and the effective knowledge base of employees in cyberthreat mitigation, IU South Bend Undergrad. Res. J. 18 (2018).
[146] K. Bálint, Modern, decentralized blockchain-based solutions for saving video footage, in: 2020 IEEE 18th International Symposium on Intelligent Systems and Informatics, SISY, 2020, pp. 11–14.
[147] V. Valentin, A. Mehaoua, F.A. Guenane, Security challenges and requirements for industrial IoT systems, in: Recent Advances in Security, Privacy, and Trust for Internet of Things (IoT) and Cyber-Physical Systems (CPS), first ed., 2020, p. 20.
[148] S.R. Alam, S. Jain, R. Doriya, Security threats and solutions to IoT using blockchain: A review, in: 2021 5th International Conference on Intelligent Computing and Control Systems, ICICCS, 2021, pp. 268–273.
[149] H. Taherdoost, Understanding cybersecurity frameworks and information security standards—A review and comprehensive overview, Electronics 11 (14) (2022) Available: https://www.mdpi.com/2079-9292/11/14/2181.
[150] B.K. Mohanta, D. Jena, U. Satapathy, S. Patnaik, Survey on IoT security: Challenges and solution using machine learning, artificial intelligence and blockchain technology, Internet Things 11 (2020) 100227, Available: https://www.sciencedirect.com/science/article/pii/S2542660520300603.
[151] D. Minoli, B. Occhiogrosso, Blockchain mechanisms for IoT security, Internet Things 1 (2018) 1–13.
[152] S. Singh, A.S.M.S. Hosen, B. Yoon, Blockchain security attacks, challenges, and solutions for the future distributed IoT network, IEEE Access 9 (2021) 13938–13959.