A Systematic Review of IoT Security: Research Potential, Challenges, and Future Directions

WEN FEI, Faculty of Computer Science, Dalhousie University, Canada
HIROYUKI OHNO, Faculty of Emerging Media Initiative, Kanazawa University, Japan
SRINIVAS SAMPALLI, Faculty of Computer Science, Dalhousie University, Canada

The Internet of Things (IoT) encompasses a network of physical objects embedded with sensors, software, and data processing technologies that can establish connections and exchange data with other devices and systems via the Internet. IoT devices are incorporated into various products, ranging from ordinary household items to complex industrial appliances. Despite the increasing demand for IoT, security concerns have impeded its development. This article systematically reviews IoT security research, focusing on vulnerabilities, challenges, technologies, and future directions. It surveys 171 recent publications in the field, providing a comprehensive discussion on the development status, challenges, and solutions in IoT. The article outlines IoT architecture patterns and typical features, evaluates existing limitations, and explores strategies for enhancing IoT security. Additionally, the article delves into known IoT attacks and discusses the security countermeasures and mechanisms to address these challenges. It explores the functional requirements of IoT security and explores related technologies and standards. Finally, the article discusses potential future research directions in IoT security.

CCS Concepts: • **Security and privacy** → *Formal methods and theory of security*; *Intrusion/anomaly detection and malware mitigation*; *Malware and its mitigation;* • **Networks**;

Additional Keywords and Phrases: Internet of Things (IoT), IoT architecture, IoT security, IoT security challenges, IoT security goals, IoT security technology, IoT vulnerabilities, Machine Learning (ML), Cloud Computing, Edge Computing, Blockchain

ACM Reference format:
Wen Fei, Hiroyuki Ohno, and Srinivas Sampalli. 2023. A Systematic Review of IoT Security: Research Potential, Challenges, and Future Directions. *ACM Comput. Surv.* 56, 5, Article 111 (November 2023), 40 pages.
https://doi.org/10.1145/3625094

The authors gratefully acknowledge the support of the Natural Sciences and Engineering Research Council (NSERC) of Canada through a research grant.

Authors' addresses: W. Fei and S. Sampalli (Corresponding author), Emerging Wireless Technologies Laboratory, Faculty of Computer Science, Dalhousie University, Halifax, NS B3H 1W5, Canada; e-mails: Wen.Fei@dal.ca, srini@cs.dal.ca; H. Ohno, Faculty of Emerging Media IniIaIve, Kanazawa University, Kanazawa, IshiKawa Prefecture, Japan; e-mail: hohno@staff.kanazawa-u.ac.jp.

0360-0300/2023/11-ART111 $15.00
https://doi.org/10.1145/3625094

1 INTRODUCTION

There has been phenomenal growth in wireless and mobile communication technologies in the past decade. In particular, one technology that is poised to revolutionize almost every application sector is the **Internet of Things (IoT)** [1–6].

With the popularization of the IoT, consumer networks, industrial networks, public networks, hybrid networks, and so on, jointly use the Internet to create a closed-loop network and link the IoT infrastructure with cloud computing technology. The closed loop has paved the way for the automation and effective communication of IoT devices, which in turn saves cost and time [7–12]. However, as the scale of the global IoT continues to expand, a large number of IoT applications have emerged in the consumer market, leading to frequent occurrences of IoT security incidents, which have a negative impact on the further large-scale development of IoT [3, 6, 13–15]. In addition, since most manufacturers believe that adding additional security measures will not increase the market value of the product but will increase its production cost, they do not provide users with patches and updates after the product is produced. Therefore, for a long time, there have been a large number of easy-to-use, high-risk vulnerabilities in existing IoT devices, such as default passwords and plaintext transmission of keys [6, 14, 16].

This survey article presents an overview of IoT architecture and infrastructure while introducing contemporary standard IoT wireless technologies. It conducts a comprehensive review of 171 peer-reviewed publications in this field and introduces a novel taxonomy for categorizing recent common IoT security attacks and corresponding mitigation efforts. Furthermore, it delves into the security challenges and strategies for protecting IoT systems. Finally, the article analyzes future research directions in IoT security, providing valuable insights for researchers in the field.

1.1 Contribution of the Survey

This survey provides researchers and organizations with a report that presents a detailed overview of the current state of IoT security research. The contributions of this article are as follows:

- —The survey covers a detailed review of IoT architecture, infrastructure, and wireless technology, aiming to allow readers from different backgrounds and new researchers in the field of IoT to understand the basic concepts of IoT quickly and easily.
- —It provides a detailed analysis of current IoT security vulnerabilities and the mitigation strategies provided by recent research.
- —It classifies different kinds of IoT security attacks and corresponding related work based on different layers.
- —It analyzes the protection strategies and mitigation techniques of IoT security challenges and conducts comparative studies on existing standards and solutions.
- —It discusses the future research directions of IoT security and provides a summary.

1.2 Article Organization

The rest of the article is organized as follows: Section 2 presents and compares the related work of IoT security. Section 3 introduces the details of the IoT architecture and infrastructure. Section 4 outlines the wireless technology in IoT. Section 5 provides a detailed analysis of IoT security vulnerabilities. Section 6 provides a novel classification of IoT security attacks based on IoT layers. Section 7 discusses the protection strategies against IoT security challenges and mitigation techniques. Section 8 outlines the future research directions of IoT security. Section 9 concludes this article.

Table 1. Comparison of This Article with Other Related Papers

Reference	This Article	[29]	[30]	[26]	[6]	[31]	[32]	[33]	[34]	[35]	[36]
IoT Architecture & Infrastructure	√	√	√	√	√	√	√	√	×	√	√
IoT Wireless Technologies	√	√	√	P	√	×	P	×	×	×	×
IoT Vulnerabilities	√	×	×	×	P	×	P	×	×	√	×
IoT Security Attacks	√	P	P	√	√	×	√	√	√	P	√
IoT Security Goals	√	×	×	×	×	×	×	×	P	×	√
Countermeasures against IoT Security Challenges	√	P	×	×	√	×	P	×	P	P	×
Countermeasures against IoT Security Mechanism	√	P	×	P	P	P	P	P	√	P	×
Future Research Direction	√	√	√	√	√	√	√	√	√	√	×
	√: Covered			P: Partially Covered				×: Not Covered			

2 RELATED WORK & IOT ARCHITECTURE

2.1 Related Work

This section describes related research on IoT security. Following a comprehensive evaluation of recently published papers regarding IoT security, Table 1 highlights the main contributions of each related paper and compares them with this article.

Mrabet et al. [17] propose a new five-layer IoT architecture and a new classification of security threats and attacks based on this new IoT architecture. The authors detail each architecture layer and the IoT security challenges each layer faces. In addition, they discuss future research directions in this area. Sobin [18] studies and classifies various architectures and protocols used in IoT systems. In addition, the author introduces and evaluates various IoT applications and discusses technical challenges and open issues of IoT. Mohanta et al. [15] introduce IoT infrastructure, protocols, and applications. In addition, the authors analyze IoT security attacks and systematically study the use of **machine learning (ML), artificial intelligence (AI)**, and blockchain to solve IoT security threats. Mohamad Noor and Hassan [6] analyze the latest research, trends and unanswered questions in IoT security. Patnaik et al. [19] systematically discuss the different levels and the corresponding vulnerabilities of IoT architecture. The authors also analyze IoT security issues, challenges, and possible solutions. Alaba et al. [20] describe IoT applications, architectures, and focus on state-of-the-art IoT security threats and vulnerabilities. Liang and Kim [21] introduce the three-layer architecture of IoT and give a detailed overview of IoT security attacks and current security solutions based on the three-layer architecture. Furthermore, the authors also discuss future research challenges. Hassija et al. [22] review security-related challenges and sources of threats in IoT applications in detail and discuss emerging and existing technologies in various IoT applications. Neshenko et al. [23] classify IoT security issues based on various vulnerabilities and concerns, such as IoT attack vectors, security impact, and countermeasures based on the proposed classification. Abbood et al. [24] introduce IoT and its components and discuss IoT security requirements in detail. In addition, IoT security challenges and threats are analyzed based on the IoT layers.

As seen from Table 1, much of the previous research is focused on IoT security attacks without considering IoT security vulnerabilities, which are important for researchers to monitor IoT

devices in all aspects of practical applications to prevent attacks against such devices. Furthermore, although countermeasures against IoT security mechanisms in the IoT security field demonstrate advanced progress, some of these methodologies leave room for further research. Therefore, this article provides researchers not only with a systematic analysis of the countermeasures against IoT security threats but also the security challenges, aiming to provide a more comprehensive strategy for IoT security protection.

2.2 IoT Architecture

This section provides a detailed overview of the IoT architecture. The core of IoT consists of sensors, actuators, gateways, protocols, cloud services, networks, and application servers [25, 26]. The IoT network needs to integrate all resources, hardware, software, and systems into a framework to form an integrated, reliable, and cost-effective solution [15, 25, 26]. Therefore, for different IoT application domains, each IoT architecture needs to be developed according to its function and implementation in different domains, that is, there is no single, standard-defined IoT architecture [25, 27]. Depending on different business tasks, the complexity and number of architectural layers will vary. In addition, the resulting efficiency and applicability of the system depend to a large extent on the quality of the infrastructure developed [15]. Nevertheless, the foundation of each IoT architecture and its general data processing flow is roughly the same [25].

In References [25, 26, 28, 29], the standard IoT layered protocol stack and architecture were observed. Iqbal et al. [25] outline the characteristics of IoT security and propose a general IoT architecture and IoT protocol stack. Swamy and Kota [26] summarize the architecture of IoT and its contemporary status and analyze the status of the communication standards and application layer protocols used in IoT. Bouaouad et al. [28] analyze IoT architectures and their layers in the cloud environment and determine the essential layers to define a complete and detailed architecture. Al-Fuqaha et al. [29] discuss the overall architecture of IoT and its security issues. Among these studies, the three-layer and five-layer architectures are the most prominently used. The three-layer architecture is a subset of the five layers. A brief description of each layer in the five-layer architecture is given below.

(1) **Perception Layer:** The perception layer, also called the sensor layer, is the physical layer of the IoT architecture [29]. It is responsible for using sensors and embedded systems to identify objects and collect data from them, which makes them popular targets for attackers, who can replace them with their sensors.
(2) **Network Layer:** The network layer carries and transmits the data collected by the sensors in a wired or wireless manner [26]. It also connects various smart objects, network devices, and servers. Security issues related to information authentication and integrity occur at this layer.
(3) **Middleware Layer:** The middleware or service management layer has features such as data storage, computation, processing, and analysis [29]. This layer makes decisions by processing the received data and provides appropriate services based on the device address and name.
(4) **Application Layer:** The application layer manages all application processes based on the information obtained from the middleware layer. This layer interfaces IoT devices and networks and interacts with users [29]. It provides users with high-quality application services to meet their requirements. Vertical markets such as smart homes, smart transportation, and industrial automation are included in the application layer [26, 29].
(5) **Business Layer:** The business layer manages the entire IoT system, which involves constructing flowcharts, graphs, analyzing results, and improving IoT devices [29]. It monitors

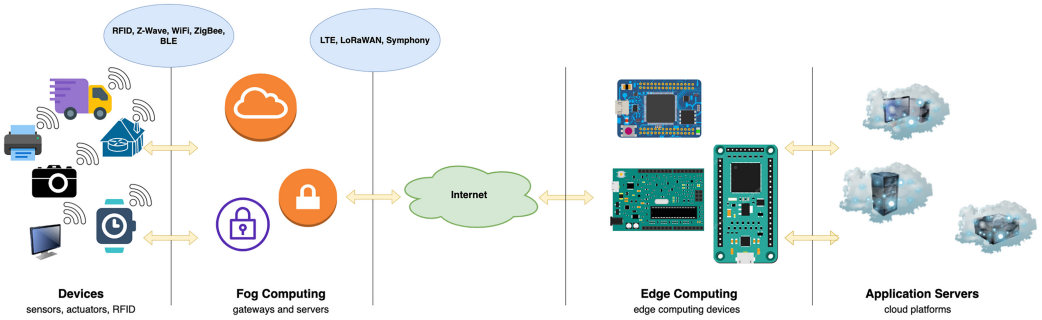

Fig. 1. Generic IoT architecture.

and manages the underlying four layers. It compares the output of each layer with the expected output to ensure data consistency and effectiveness, thereby improving services and maintaining user privacy.

Figure 1 shows the generic IoT architecture, which consists of a variety of sensor nodes that are further connected to the Internet through IoT gateways. Edge computing devices are accountable for further processing the data. At the cloud level, processing is done according to the needs of business applications, such as smart IoT applications [18, 25]. From left to right, sensors and actuators exist in the perception/physical layer. They can collect information by sensing the surrounding environment and passing it to IoT gateways. Energy utilization, security, and interoperability are some of the challenges that exist in this layer [25, 26, 29]. The second stage includes IoT data collection systems and gateways [26]. The sensor nodes are connected to the Internet through these gateways. This stage collects a large amount of unprocessed data, converts it into a digital stream, and then filters and preprocesses it for analysis. Network availability, scalability, power utilization, and security are some problems the network layer faces [25]. The fourth stage consists of edge devices responsible for further processing and enhancing data analysis [26, 28]. At this stage, visualization and machine learning can enable IoT systems to make intelligent and independent data analysis decisions [15]. In the final stage, data is transmitted to the cloud or locally installed data centers [40]. It is the stage of data storage, management, and in-depth analysis. This stage is in the application layer of the IoT architecture [26].

3 IOT WIRELESS TECHNOLOGIES

This section provides an overview of the most common types of wireless technologies used in IoT.

(A) **LPWANs: Low-Power Wide Area Networks** (LPWANs) provide the low-power, low-cost, long-range communications needed for large-scale IoT networks with transceivers optimized for power consumption and run on small, inexpensive batteries that can last for years [30, 31]. LPWAN technology provides connectivity for applications and devices such as IoT sensors that require infrequent data transfer, low speed, and low mobility. Allowing thousands of sensors over a wide area to communicate while maintaining low power consumption makes LPWAN very useful for IoT adoption. This family of technologies is purpose-built to support large-scale IoT networks across vast industrial and business parks, where applications include consumables monitoring, environmental monitoring, occupancy detection, and asset tracking. LPWANs contain different technologies and competing standards. Technologies operate in licensed (e.g., NB-IoT, LTE-M) and

unlicensed (e.g., MYTHINGS, LoRa, Sigfox) spectrums with varying performance degrees on key network factors [31]. For example, scalability and quality of service can be significant issues for unlicensed technologies and power consumption for licensed LPWANs.

(B) **Cellular (3G/4G/5G):** Cellular networks provide reliable broadband communications for the mobile consumer market, supporting a variety of voice calling and video streaming applications [31]. However, these wireless technologies have high power consumption and operating costs, making cellular connectivity ideal for applications without battery-powered sensor networks, such as traffic routing and fleet telematics. Instead, cellular connections act as an excellent backhaul, using LPWAN to connect to IoT devices and sensors, and then the cellular network connects to the cloud to provide IoT data, making them ideal for specific use cases such as connected cars or in transportation and logistics fleet management. Additionally, new cellular technologies such as NB-IoT and LTE-M are positioned to support different IoT applications by reducing power requirements and data costs per sensor. Furthermore, these NB-IoT-enabled devices will provide regular updates from remote locations while ensuring low power consumption.

(C) **Wi-Fi: Wireless Fidelity** (WiFi) provides the Internet connection for nearby devices within a specific range. Another way to use WiFi is to create a hotspot, where a phone or computer can share a wireless or wired Internet connection with other devices through the broadcast signals. WiFi uses radio waves to broadcast information on specific frequencies, and the range and speed of its Internet connection depends on the environment and the internal or external coverage it provides [30, 32]. A key difference from other wireless technologies is that Wi-Fi transmits at higher frequencies, which means it can carry more data. However, Wi-Fi has high power requirements and limited coverage. These issues and scalability limitations have made Wi-Fi less popular in the IoT space. In addition, due to high energy requirements, Wi-Fi is often not a viable solution for large networks of battery-powered IoT sensors, especially in industrial IoT and smart building scenarios. Instead, it is better for connecting devices easily connected to a power outlet, such as smart home gadgets and appliances, digital signage, or security cameras.

(D) **Zigbee and Other Mesh Protocols:** The ZigBee protocol adopts the 802.15.4 standard and is a low-power, high-reliability wireless network technology designed for short-term communication, usually deployed in mesh topologies by relaying sensor data over multiple sensor nodes [18, 30]. Compared to LPWAN, Zigbee offers higher data rates, but at the same time, it is much less energy-efficient due to the mesh configuration. Due to their physically short-range (< 100 m), Zigbee and similar mesh protocols (e.g., Z- Wave, Thread) are well suited for mid-range IoT applications that are evenly distributed near nodes. Therefore, Zigbee is an excellent choice for home automation applications such as HVAC control, smart lighting, smart meters, home energy, security monitoring, and smart thermostats. Additionally, Thread is designed for smart home products and features IPv6 connectivity that enables connected devices to communicate, access services in the cloud, or interact with users through the Thread mobile app.

(E) **Bluetooth and BLE:** Bluetooth is a technology that allows various electronic devices to be connected wirelessly and is an open standard described in the IEEE 802.15.1 specification [30]. To extend the application of Bluetooth to power-constrained devices such as wireless sensors, **Bluetooth Low Energy (BLE)**, with low power consumption, flexibility, and scalability, was introduced in 2010 [33, 34]. Classic Bluetooth is initially intended for point-to-point or point-to-multipoint data exchange between consumer devices. Bluetooth Low Energy is optimized for power consumption and has been later introduced to address small-scale consumer IoT applications. Unlike Wi-Fi, the BLE

protocol is a high-bandwidth, low-range wireless connectivity option designed with cost-effectiveness and reduced power consumption, requiring very little device power. This technology is often used in fitness and medical wearables (e.g., smart watches, blood glucose meters, pulse oximeters, etc.) and smart home devices (e.g., door locks), where data can be easily transferred to and stored on the smartphone. However, BLE may not be the most efficient solution when large amounts of data are frequently transmitted.

(F) **RFID: Radio Frequency Identification** (RFID) is a type of wireless communication that uses radio waves to identify and find objects [18, 35]. It includes an RFID tag, reader, antenna, and back-end database server. RFID reader converts radio waves into data form, which is then forwarded to the back-end server for users to access and analyze the data. RFID uses radio waves to transmit small amounts of data from an RFID tag to a reader within a short distance, providing a positioning solution for IoT applications. This IoT wireless technology works out of sight and is attached with labels that can be read within inches or even meters. The technology is mainly used in supply chain management and logistics. By linking RFID tags to various products and equipment, companies can track their inventory and assets in real-time, enabling better inventory and production planning and optimized supply chain management.

4 IOT SECURITY VULNERABILITIES

While enhancing users' quality of life, IoT technology presents inherent vulnerabilities that pose security risks and challenges. These weaknesses expose IoT to cyberattacks, disrupting industries and economies due to the absence of built-in security measures. The primary culprits are the constrained environments and limited computing power of IoT devices, which are typically low-power and incapable of accommodating robust security mechanisms and data protection. Moreover, IoT devices often employ diverse transport technologies, complicating the establishment of standardized protection methods and protocols. Additionally, vulnerabilities in critical components and insufficient user awareness further compromise IoT security, as detailed in this section.

4.1 Improper Encryption

The protection of IoT data at rest, in transit, or during processing is important to the reliability and integrity of IoT applications. Although many IoT vendors focus on secure storage, ensuring that data remains secure in transit is often overlooked. Encryption is an efficient mechanism for storing and transmitting data in a way that only authorized users can use. Lack of encryption in transit involves insecure communication between devices and the cloud, devices and gateways, devices and mobile applications, one device and another, and communications between the gateway and the cloud [6]. Since the strength of encryption algorithms can be affected by the resource limitations of IoT applications, attackers can exploit the vulnerabilities in encryption algorithms to leak sensitive information or control operations [23]. Strong encryption throughout the IoT data lifecycle will help protect IoT data from damage and destruction.

4.2 Inadequate Authentication

Due to limited energy and computing power constraints, it is not easy to implement complex authentication mechanisms on IoT devices. Protocols currently supporting IoT system authentication are **Message Queuing Telemetry Transport (MQTT), Data distribution service (DDS)**, Zigbee, and Zwave [6]. However, even if developers provide the authentication tools required for IoT communication, pairing, and messaging, there is still an opportunity for IoT device and network communication to be hijacked. For example, authentication keys risk being lost, destroyed, or damaged because they are not securely stored or transmitted. Li et al. [36] highlight the

issue of API authentication when IoT APP accesses IoT devices through API. They emphasize that unauthorized access threatens the security of cloud resources or control equipment.

4.3 Improper Patch Management Capabilities

It is important to keep IoT operating systems and embedded firmware/software updated and repaired [23]. Over time, security vulnerabilities will appear in the IoT device system, which will make IoT devices vulnerable. Therefore, IoT devices need to use the latest system without known vulnerabilities, and the system must have an update function to patch any known vulnerabilities after the device is deployed. In addition, network administrators should pay attention to the update mechanism.

In February 2021, a hacker used the outdated Windows 7 **operating system (OS)** to increase the amount of sodium hydroxide (lye) in Oldsmar's water treatment system [37]. While a worker noticed this and reduced the level back to its normal value, this incident demonstrates the importance of updating the OS of devices and using more complex passwords.

4.4 Insufficient Access Control

Access control is a set of permissions for connected IoT devices to specify which users are granted access permissions and the operations they are allowed to perform [21]. The access control attack refers to unauthorized users accessing the IoT network. Attackers can use vulnerabilities in the **access control list (ACL)** to access confidential information, exposing individuals and organizations to the risk of data leakage.

4.5 Insufficient Security Configurability

Since hard-coded credentials are often used in IoT devices, it causes insufficient security configurability. Weak passwords, default passwords, and hard-coded passwords are the easiest way for attackers to break into IoT devices and further launch large-scale botnets and other malware, resulting in hard-coded credentials that can be easily compromised [6]. Additionally, IoT devices come with default hardcoded settings. Thus, once those settings are compromised, attackers can steal hardcoded default passwords, hidden backdoors, and vulnerabilities in the device firmware.

4.6 Deficient Physical Security

Deficient physical security is a security vulnerability caused by hardware. Since IoT devices are deployed in distributed remote environments, attackers can access and tamper with the physical layer to gain sensitive information and disrupt services provided by IoT devices. Moreover, due to the simplicity of IoT devices such as sensors, it is not easy to build complete encryption algorithms on these IoT devices. However, it is possible to implement lightweight encryption in the IoT device to ensure user confidentiality and security.

4.7 Unnecessary Open Ports

When IoT devices run vulnerable services, some unnecessary ports are opened. Attackers can exploit these port vulnerabilities to access sensitive information in IoT devices.

4.8 Insufficient Energy Harvesting

Since IoT devices have limited energy, the attacker could potentially drain the energy stored by an IoT device by generating a flood of legitimate or corrupt messages, making the device unavailable to valid processes or users [23].

Table 2. Classification of the IoT Attacks

IoT Layers	Possible IoT Attacks	
Perception Layer	Malicious node attack	Side channel attack (SCA)
	False data injection attack	Eavesdropping
	Hardware malfunctioning	Battery drainage attack
	Unauthorized admittance to the device	
Network Layer	Distributed Denial of Service (DDoS)/ DoS attack	Eavesdropping
	Routing attack	Main in the Middle (MITM) attack
	Spoofing attack	Malicious node attack
	Access control attack	
Middleware Layer	SQL injection attack	MITM attack
	Flooding attack	Cloud malware injection
	Signature wrapping attack	
Application Layer	DDoS/DoS attack	Access control attack
	False data injection attack	Brute force/dictionary attack
	Sniffing attack	
Other (Gateway)	End-to-End encryption	Extra interfaces
	Firmware updates	

4.9 Insufficient Audit Mechanisms

Most IoT devices do not have complete logging procedures, resulting in malicious activity generated in the IoT devices or services being hidden [23].

5 IOT SECURITY ATTACKS CLASSIFICATION

The communication architecture of the IoT system consists of the perception, network, middleware, and application layers. The four layers play different roles in terms of functionality, and this section categorizes the various possible IoT attacks in these four layers. Table 2 shows the possible attacks against these four layers. Additionally, this section details these attacks and summarizes related literature research on each of the attacks.

5.1 Malicious Node Attack

The malicious node [38] is defined as a node that refuses to provide services to other nodes in the network, and its purpose is to attack other nodes in the network or the entire network. Malicious nodes will launch attacks based on tampering, retransmitting, and discarding [38].

Li et al. [38] propose a malicious node trust detection mechanism based on an online learning algorithm. This method calculates the credibility of each path in the network based on the collected data packets and then uses the online learning algorithm to model the obtained path based on the trust of nodes. Finally, the authors detect malicious nodes based on the trust level of each node and the clustering algorithm. The authors propose **original TG detection (OTGD), enhanced TG detection (ETGD), original OGD detection (OOGD)**, and **enhanced OGD detection (EOGD)** to verify the effectiveness of the mechanism. The results show that the detection mechanism can detect malicious nodes with high accuracy and stability. Khatun et al. [39] propose a malicious node detection method based on the **artificial neural network (ANN)**. The authors test the classification accuracy of the method for malicious nodes, and the results show that the success rate of the ANN classifier is 77.51%.

5.2 Side Channel Attack (SCA)

Side channel attacks (SCA) can be used to retrieve any sensitive information from a device. The leakage of sensitive information may be related to timing, power, electromagnetic signals, sound, light, and other factors. SCA is a non-intrusive and passive attack that is performed without removing the chip to gain direct access to a device's internal components or actively tamper with any of its operations. SCA is most commonly used against encrypted devices. SCA is not aimed at standard encryption algorithms but at their implementation on physical devices, recovering secret parameters by measuring and analyzing leaked information (such as power analysis, timing analysis, electromagnetic analysis, etc.).

By analyzing and comparing the countermeasures against SCA in low-power devices using 128-AES encryption, Ruminot-Ahumada et al. [40] find that algorithm-based countermeasures are more suitable for low-power devices. Therefore, the authors propose a countermeasure based on byte logic. The proposed countermeasure can provide a new method to hide the relationship between energy consumption and processing data. To build countermeasures tailored to these devices, the authors ran tests to understand the scope of **Correlation Power Analysis (CPA)** attacks. The results show that the proposed countermeasures have higher security than traditional countermeasures of the same type. However, almost all countermeasures against SCA are based on the equipment used. Therefore, global countermeasures to solve the SCA problem still need to be studied.

Khan and Chen [41] propose a **commercial off-the-shelf (COTS)**-based **Randomized Switched-Mode Voltage Regulation System (RSMVRS)** to prevent **power analysis-based side channel attacks (P-SCA)** on bare-metal IoT edge devices. RSMVRS supplies power to target devices by directing power to IoT edge devices and activating power stages with random time delays. Therefore, an attacker cannot perform SCA by measuring the power trace. The results show that by utilizing the COTS component, the random activation of power levels proposed by RSMVRS can effectively defend against insider attacks, and large samples cannot eliminate the entropy induced in the power trace.

5.3 False Data Injection Attack

Attackers can use captured nodes to inject erroneous data into IoT systems to compromise data integrity. This attack can cause the IoT system to crash or malfunction. Alternatively, attackers can also use this method to conduct DDoS attacks.

Since **state estimation (SE)**, the most important real-time function in modern **energy management systems (EMS)**, is vulnerable to **false data injection (FDI)** attacks, Živković and Sarić [42] develop an efficient method to detect such malicious attacks. The proposed method combines an **unscented Kalman filter (UKF)** with a **weighted least square (WLS)**-based SE algorithm to detect differences between SV estimates in real-time, identifying false data attacks. Furthermore, the solution can send alerts to operators when an attack is detected, so operators can take actions to prevent or minimize potential influences. The authors tested on benchmark IEEE 14-bus and 300-bus test systems. The results show that the proposed algorithm can successfully identify all FDI attacks with significant strength, achieving reasonable prediction quality. **Fake data injection attacks (FDIAs)** can tamper with meter measurements and influence the state estimation results, which seriously threatens the security of smart grids. Zhang et al. [43] summarize recent advancements in FDIAs for smart grid state estimation, offering a comprehensive introduction to background materials, construction methods, and strategies for detection and prevention. They also conduct an analysis of smart grid vulnerability to malicious attacks through an FDIA review, providing a valuable reference for fellow researchers. Khanna et al. [44] propose a defense

strategy to identify and protect the data integrity of SE from malicious actors. The proposed strategy selects the most critical measurements to protect the power system from false data injection attacks. Additionally, the proposed strategy considers normalized measurement Jacobian matrix and is verified using standard IEEE test cases. The results show that the proposed defense strategy can effectively mitigate the possibility of FDIA compared with existing methods.

5.4 Eavesdropping/Sniffing Attack

Eavesdropping [25], also known as sniffing attacks, uses insecure network traffic to access data sent or received by users. Since the network traffic seemed normal when the attack was carried out, it was difficult to detect. In addition, it usually occurs on unprotected or unencrypted networks, where attackers intercept data by installing network detection sniffers on the clients and servers. Eavesdropping can lead to the loss or interception of important private information of individuals or organizations, and there are risks of financial loss and identity theft.

Banerjee and Maity [45] propose a **Cognitive Radio network (CRN)** model, which aims to satisfy the sensing reliability of the **primary user (PU)**, the individual energy causality of each **secondary user (SU)**, and the friendly jammer, the interference of the PU receiver, the individual secondary and the sum secondary throughput of the network is maximized under the constraint of confidential outage probability. The results show that this model can solve the security threats of simulation attacks and eavesdropping in the CR system. Ahuja et al. [46] propose a framework for optimizing the efficiency of hybrid attackers, with eavesdropping and jamming capabilities, while considering potential energy consumption to maximize the **attacker's energy efficiency (AEE)** in the secure IoT. Shorubiga and Kartheeswaran [47] propose a model for protecting header information to mitigate passive eavesdropping. The authors use Speck (a lightweight encryption algorithm) to encrypt metadata such as the source and destination MAC addresses and select a **software-defined network (SDN)** as the central control for packet transmission to overcome the anonymity of the packet flow. In addition, the model has been simulated using the RYU controller and tested on the Mininet SDN simulation platform using four nodes, connected Ovsk switches, and the central controller. Finally, they used Wireshark to verify the model, and the results show that the model solved the data privacy problem of passive eavesdropping.

5.5 Hardware Malfunctioning

Since IoT devices are used in most IoT applications, such as smart homes, smart grids, smart medical, and so on, it is crucial to protect them from IoT attacks. Once these devices have a product failure or are subject to any form of cyber-attack, it will significantly impact the device system and the user's life. Hassija et al. [22] highlighted many IoT applications vulnerable to cyberattacks.

Existing Trojan detection self-referencing schemes have high computational complexity for larger circuits and may lead to false positive and false negative detections due to **process variation (PV)**. Therefore, Rajendranet al. [48] propose a reduction technique for Trojan detection and diagnosis of IoT hardware devices to eliminate the need for golden design by adopting a self-referencing scheme. The results show that this work can minimize the false positive cases caused by PV and reduce the time complexity by 54.6%, on average. Additionally, node reduction based on **transition probability (TP)** and SCOAP measurements improves detection accuracy with minimal power measurements.

Due to security gaps in IoT devices, Mohammed et al. [49] present a non-invasive approach to studying **Hardware Intrinsic Attack Detection in IoT (HIADIoT)** devices. The proposed method utilizes machine learning algorithms to detect covert channel and power depletion attacks through the power profiles of IoT devices in different operating modes. The results show that the

random forest algorithm can classify **Smart Home Appliances (SHAs)** devices between normal and attack modes and identify potential **Hardware Intrinsic (HI)** attacks with 95.5% accuracy.

Threats due to **hardware Trojans (HTs)** in **integrated circuits (Ics)** have become a severe problem, which affects **IoT edge devices (IoT-ED)**. Therefore, Mohammed et al. [50] discuss the possibility of IoT-ED with embedded HT and propose a technique to detect malicious activity in HAN using **power profiling (PP)** and **network traffic (NT)** data without interfering with IC design. The proposed technique can effectively prevent HT-based attacks during IC design and testing. The authors study IoT-ED behavior for five random attacks: covert channel, DoS, ARQ, power exhaustion, and simulated attacks. The results show that the proposed technique can detect each attack individually with up to 99% accuracy without design-time intervention. Moreover, the technology can detect all attacks simultaneously with 92% accuracy.

5.6 Battery Drainage Attack

Attackers drain the battery of resource-constrained IoT devices by continuously sending requests, which results in a denial of service for the nodes in the IoT application due to a dead battery. Besides, the attackers can drain the device's battery by using malicious code to run an infinite loop in the IoT device or artificially increase the IoT device's power consumption to prevent the device from going into sleep or power-saving mode.

To better understand battery-draining attacks against edge computing nodes in IoT networks, Smith et al. [51] simulated five significant attacks in the Cooja simulator that could drain the small batteries of devices. The authors looked at metrics such as CPU time, low power mode time, TX/RX time, and battery consumption and tested the stretch attack as an extreme scenario with three different batteries. The results show that version control attacks are the most severe in draining the network's power resources, followed by packet and HELLO flooding attacks. Since wireless networks in blockchain-enabled IoT frameworks are **Low Power and Lossy Networks (LLNs)**, Alsirhani et al. [52] propose a mitigation strategy called **DODAG Information Solicitation Spam Attack Mitigation (DISAM)**. The results show that the proposed DISAM can effectively detect and mitigate the impact of spam **DODAG Information Solicitation (DIS)** attacks on network performance. Ioulianou et al. [53] study the impact of battery-draining DoS attacks (i.e., "HELLO" flood and version number modification) on IoT devices using the Cooja simulator and propose a new **Intrusion Detection System (IDS)** for securing IoT networks and devices. The proposed IDS follows a hybrid placement approach to detect external and internal network intrusions. The results show that the proposed IDS requires no firmware modifications to IoT devices, and the detectors are wired to avoid jamming and other wireless attacks. In addition, the IDS supports general IDS modules and heterogeneous devices, which can effectively detect DoS attacks.

5.7 Unauthorized Admittance to the Device

Due to the growing number and variety of IoT devices, and producers using default passwords and built-in credentials, IoT devices are vulnerable to unattended attacks. Furthermore, developers intentionally leaving insecure APIs for remote access and ignoring regular system audits pose security threats to IoT devices [25].

Janes et al. [54] study the design of authentication and access control schemes and explore the challenges of propagating credential revocation and access control list modifications in a shared IoT ecosystem. The authors evaluated authentication and access control schemes for 19 popular security cameras and networked doorbells. The results show that 16 of the 19 devices had flaws that could lead to unauthorized access after credential modification or revocation. To detect unauthorized access to APIs, Li et al. [36] propose a framework named IoT-APIScanner, which aims to identify unauthorized access vulnerabilities in APIs. IoT-APIScanner extracts the interaction

information between the IoT application and the cloud by analyzing the code of the IoT application and using it to mutate API test cases. The authors extracted a total of five platform APIs for detection. The results show that IoT-APIScanner can effectively help cloud platforms check the security issues of APIs, and the proportion of APIs that are not authorized and verified reaches 13.3%. **Attribute-based encryption (ABE)** is an efficient access control tool. To address the limitations of ABE in the IoT environment, Hahn et al. [55] propose an efficient and secure cloud-based IoT data management scheme using ABE. The proposed scheme eliminates the storage side's dependence on the complexity of access control policies and ensures that most computationally intensive operations are safely outsourced to cloud servers. In addition, the scheme strictly prohibits unauthorized access to data through illegal key sharing. The results show that the proposed scheme can securely defend against unauthorized cloud storage access. Guerar et al. [56] propose an authentication scheme called CirclePIN to strengthen the authentication mechanism of smartwatches. The proposed scheme provides resilience against the most common attacks and availability in user tests. The results show that CirclePIN provides enhanced security against side-channel, shoulder-surfing, and single-record attacks while providing a level of availability lock comparable to standard authentication methods.

5.8 Distributed Denial of Service (DdoS)/DoS Attack

Denial of Service (DoS) attack [26, 57] floods the target host or network by sending multiple requests until the target fails to respond or crashes due to traffic overload, thus preventing legitimate users from accessing expected services or resources. Furthermore, it can slow down or disable services.

Distributed Denial of Service (DdoS) attack [21, 26] uses multiple computers or machines to flood a targeted resource. The essential difference between DdoS attacks and DoS attacks is that DdoS attack comes from multiple remote locations, while DoS attack comes from a single location. Attackers using DdoS attacks can control many devices by exploiting security vulnerabilities or device weaknesses. Due to the random distribution of the attack system, the attack location is difficult to detect. Thus, the attackers can carry out large-scale attacks without the device owner's knowledge.

Sinha et al. [58] introduce the impact of various DoS attacks on IoT systems and implement a type of DoS attack called selective forwarding attack based on the network layer. The authors use the Cooja simulator for simulation to analyze the impact of different scenarios and generate charts to observe this attack's severity through different network settings. This research work shows that it is easy to implement DoS attacks. Ghahramani et al. [59] study two lightweight authentication protocols and propose a solution called received signal strength, which is an energy-efficient approach to protect IoT service protocols from DoS attacks. The authors also study the impact of internal errors in IoT devices on location and proposed an effective and optimized computational intelligence algorithm to find the exact location of the attacker. Shurman et al. [60] propose a hybrid design of signature-based **Intrusion Prevention System (IPS)** and anomaly-based IDS to enhance the **intrusion detection and prevention system (IDPS)** by classifying network packets based on user behavior to detect any DoS attack at an early stage. This research proves that the DoS attack can be successfully detected in the early stage.

Munshi et al. [61] introduce the DdoS attack in detail and study its impact on IoT devices, aiming to understand the mechanism of DdoS attacks and the corresponding protection strategies. Huang et al. [62] propose a DdoS attack architecture suitable for attackers with limited resources. The proposed architecture has the advantages of zero management cost, good undetectability, and robustness and is based on a novel botnet growth model. In this architecture, the optimal design of the attack strategy is reduced to a variational problem, which is solved by using three different

types of DdoS defense strategies. Ravi and Shalinie [63] use the cloud and SDN paradigm to propose a new security mechanism called **learning-driven detection mitigation (LEDEM)** to mitigate DdoS attacks on IoT servers. LEDEM has a semi-supervised ML model for attack detection and two different mitigation strategies for **fixed IoT (fIoT)** and **mobile IoT (mIoT)**. In addition, the authors test the mechanism in the testbed and emulate topology. The results show that the accuracy of LEDEM in detecting DdoS attacks has increased to 92.28% in detecting DdoS attack. Hussain et al. [64] propose a method to convert non-image network traffic data into image form and train the most advanced **convolutional neural network (CNN)** model, i.e., ResNet, on the converted data to detect DoS and DDoS attacks. This method only normalizes the features without any coding scheme or transformation technique. The proposed method achieves 99.99% accuracy in detecting DoS and DdoS attacks. Furthermore, this method identifies 11 DoS and DdoS attack patterns, with an average accuracy rate of 87%, which is 9% higher than the state-of-the-art technology. Bhayo et al. [65] propose a framework based on **software-defined IoT (SD-IoT)** to provide security services for IoT networks, namely, **Counter-based DdoS Attack Detection (C-DAD)**. The C- DAD framework has been designed based on counter values of different network parameters, which can detect DdoS attacks within an affordable time. C-DAD comprises anSDNWISE controller, IoT controller **Sensor Open Flow Switch (SOPS)**, and IoT devices. It is a dynamic and programmable solution. The authors carry out in-depth tests under different network parameters, and the results show that the proposed framework can effectively detect attacks while minimizing the attack detection time and consuming less CPU and memory.

5.9 Routing Attack

Routing attack [15] refers to generating wrong routing to interfere with normal routing by sending forged routing information. There are two types of routing attacks. One is to generate incorrect routing table entries on legitimate nodes by forging legitimate routing control packets with incorrect routing information, which increases network transmission cost, destroys legitimate routing data, or directs a large amount of traffic to other nodes to consume energy quickly. Another attack is to forge packets with illegal header fields.

Agiollo et al. [66] develop an **intrusion detection system (IDS)** called **DETector of rOutiNg Attacks in Rpl (DETONAR)**, which is designed to detect routing attacks in RPL-based IoT. DETONAR relies on a packet sniffing approach, combining signatures and exception-based rules to identify any malicious behavior in the traffic. The design of DETONAR considers no RPL communication overhead, no RPL node overhead, attack resistance, and implementation flexibility. In addition, the authors propose the RADAR-Rpl routing attack dataset to test this approach, where the dataset contains 14 types of routing attacks against RPL in a network of 16 static nodes. The test results show that DETONAR has a detection rate of over 80% for 10 out of 14 attacks while maintaining the false positives rate close to zero without RPL communication overhead. To protect IoT-**Low Power and Lossy Network (LLN)** from routing attacks, Sahay et al. [67] propose a hierarchical model of IoT routing security based on blockchain to analyze different vulnerabilities related to various stages of the routing process. The **Blockchain Network (BCN)** acts as a data link between IoT-LLN and applications containing **security analysis (SA)** tools and is designed to improve the performance of routing attack detection based on the **eXtreme Gradient Boosting (XGBoost)** algorithm. The proposed blockchain framework includes a smart contract to generate real-time alerts to effectively identify nodes in IoT-LLN that are involved in tampering with LLN configuration information. Since participating nodes may deliberately announce false level or version number information to make the routing attack, the level and version number play an important role in the IoT-LLN topology.

5.10 Man in the Middle (MITM) Attack

The goal of the **Man-in-the-Middle (MITM)** attack [21, 26] is to capture and modify the communication between two separate systems and intercept the information of it. Since IoT devices share data in real time, MITM attacks can attack multiple IoT devices simultaneously and cause serious failures. Common types of MITM attacks include email hijacking, Wi-Fi eavesdropping, session hijacking, and **Domain Name System (DNS)** spoofing [68].

Wong et al. [69] design and propose a MITM attack scheme against IoT devices that use the MQTT protocol to communicate. The scheme includes an MQTT parser for analyzing and changing MQTT messages and a BERT-based confrontation model for generating malicious messages. The results show that the attack scheme can successfully evade logistic regression, random forest, K-nearest neighbors, and **support vector machine (SVM)**-based anomaly detection models. The authors demonstrate the vulnerabilities of typical security defense mechanisms through this attack scheme. Thomas et al. [70] analyze the MITM attack in LoRaWAN, which occurred during the communication between two peer-to-peer modules on the wireless network, and propose a mitigation technique as a countermeasure for the attack. This countermeasure is designed to protect encrypted communication between nodes from attacks and can mitigate the attacks carried out by the **Galois/Counter Mode (GCM)** [71] cryptographic algorithm. Kang et al. [72] propose a hybrid routing scheme for MITM attack detection in IoT networks. This solution uses an algorithm to enforce routing between IoT devices by specifying dedicated nodes and effectively detecting anomalies in **trusted time servers (TTS)**. The authors use **True Positive (TP), False Negative (FN), False Positive (FP), True Negative (TN), True Positive Rate (TP Rate), False Positive Rate (FP Rate), Overall Accuracy (OA)**, and **Receiver Operating Characteristics (ROC)** to evaluate the scheme in a heterogeneous network. They conclude that a thorough experimental analysis of the proposed model is still needed in future work.

5.11 Spoofing Attack

Spoofing attack [21, 26] is an attack method in which attackers disguise their identity and gain trust through authentication. Attackers use flaws in the authentication mechanism to disguise themselves as others and use various methods and techniques to steal sensitive information from victims. The spoofing attacks include email spoofing, DNS spoofing, IP spoofing, DdoS spoofing, and **Address Resolution Protocol (ARP)** spoofing.

Mohammadnia and Slimane [73] propose the IoT-NETZ security application running on the **Software-defined Wireless Network (SDWN)**, which aims to detect and mitigate spoofing attacks and outbound network traffic launched on large-scale IoT networks against cloud infrastructure and services. IoT-NETZ is designed auto-flow processing on the data planes to reduce the burden of network flooding when a large amount of incoming traffic occurs, and it is defined in the spoofing detection algorithm. Therefore, the proposed model can eliminate the network overhead of per-flow processing tasks of the controller application, source verification, and backtracking of generated network traffic. In addition, since the IoT-NETZ has environmental sustainability characteristics, it can save the power of IoT network devices. Aldabbas and Amin [74] propose a secure IOT architecture based on SDN. The proposed server acts as an intermediary between the SDN controller and the connected nodes and obtains network topology information from the **dynamic host configuration protocol (DHCP)** server on the controller and the proposed machine to detect and mitigate ARP spoofing attacks. The proposed server can receive queries related to address translation, and the authors have performed simulation tests on the Ubuntu VM. The authors use Mininet as a simulation tool and add a large number of SDN switches, hosts, and controllers for different scenario tests. The authors calculate different parameters such as attack

discovery time, CPU overhead, attack mitigation time, and system throughput and conduct different types of attacks to evaluate the performance of the proposed architecture. This architecture increases network throughput, and the attack detection and mitigation time has decreased by 35%. Galtier et al. [75] propose a new physical device fingerprint identification method to detect potential link layer spoofing attacks in the wireless IoT environment. The proposed method uses **power spectral density (PSD)** to capture the frequency distribution of the transmitter and is not affected by position or phase offset. This method compares the fingerprint of the transmission device with the fingerprint of the previously stored legal device, observes the corresponding PSD similarity, and applies the community detection algorithm for detection. The proposed method has been tested on various experimental settings and connected devices supporting wireless protocols such as BLE and Zigbee. The authors use LimeSDR Mini for signal acquisition, and the results show that the accuracy and recall rates obtained are always higher than 85%. This method has the advantages of low cost, high efficiency, and easy deployment. In addition, since the proposed method is flexible to unpredictable phenomena in transmission, it can not only be applied to static smart IoT environments such as smart industries but also can be easily adapted to dynamic environments.

5.12 Access Control Attack

Access control [21] is a set of permissions for connected IoT devices to specify which users are granted access permissions and the operations they are allowed to perform. The access control attack refers to unauthorized users can access the IoT network. Attackers can use vulnerabilities in the **access control list (ACL)** to access confidential information, exposing individuals and organizations to the risk of data leakage.

Chaudhry et al. [76] propose an improved solution of certificate-based **lightweight access control and key agreement scheme for IoT devices (LACKA-IoT)**, namely, iLACKA-IoT. The authors conducted a formal validation through the **Real-Or-Random (ROR)** model and discussed informal validation of attack resilience to prove the security of the proposed iLACKA-IoT. Das et al. [77] designed a new certificate-based lightweight access control and key agreement protocol in IoT environment called LACKA-IoT, which aims to achieve secure communication between two adjacent sensor devices in the IoT network. LACKA-IoT uses **elliptic curve cryptography (ECC)** and a unidirectional cryptographic hash function. It uses the ROR model for formal and informal security analysis. In addition, the authors used the **Automated Validation of Internet Security Protocols and Applications (AVISPA)**, a software verification tool, to perform the security analysis on the proposed protocol. Sun et al. [78] propose a blockchain-based access control system for IoT, which is a lightweight security system that integrates a permissioned blockchain (HLF), an **attribute-based access control (ABAC)**, and an **identity-based signature (IBS)**. The authors build channels to achieve cross-access control. They divide the IoT system into IoT domains with different functions and then establish a local blockchain ledger for each IoT domain. The ledger records the attributes of the IoT field, a summary of policy documents, and access decisions. Furthermore, they also design a **policy decision point (PDP)** selection algorithm that can select multiple IoT devices as blockchain nodes and implement real-time distributed policy decisions. Oktian and Lee [79] propose a blockchain-based IoT endpoint access control framework named BorderChain. BorderChain protocol includes gateway authentication, device authentication, endpoint authorization, and accessing endpoints. It allows many IoT entities to collaborate in a unified environment. The authors use the P2P platform as the Ethereum blockchain and implement the protocol in the Node JS application. In addition, they test the security of BorderChain using multiple Raspberry Pis and server-level computers.

5.13 SQL Injection Attack

With the rapid growth of SQL-driven IoT applications, the threat of **SQL injection attacks (SQLIA)** at the middleware layer has increased significantly. **SQL Injection (SQLi)** is a cyber-attack against databases that use SQL. The attack interferes with or manipulates the database and gains access to potentially valuable information by injecting malicious SQL statements into the application.

Latchoumi et al. [80] propose an efficient hashing method to detect and prevent SQLIA. The proposed method introduces the **support vector machine (SVM)** algorithm in machine learning and is empirically evaluated in the mixture matrix and ROC chart. The results show that this method can effectively detect SQLIA. M. and H. B. [81] propose a robust semantic query-featured ensemble learning model for SQLIA prediction. The proposed model is trained using latent semantic features from large SQL queries and a state-of-the-art, highly robust computing environment. Moreover, the model can classify each query as a normal or SQLIA query. The results show that the proposed model can serve predictions based on maximum voting ensembles and eliminate overfitting and convergence problems in previous studies. In addition, the model achieved 98% accuracy. Li et al. [82] propose a long short-term memory-based SQLIA detection method. The proposed method can automatically learn efficient data representations and has strong advantages in dealing with complex high-dimensional massive data. In addition, to solve the problem of overfitting caused by insufficient positive samples, this paper proposes an injection sample generation method based on the data transmission channel from the penetration perspective. This method can formally model SQLIA and generate valid positive samples. The results show that, compared with classical machine learning algorithms and commonly used deep learning algorithms, the proposed method improves the accuracy of SQLIA detection and reduces the false positive rate. Using natural language processing models and deep learning frameworks, Chen et al. [83] propose an SQLi detection method that does not rely on background rule bases. The proposed method enables machines to automatically learn language model features for SQLIA, reducing human intervention. The results show that the method can detect SQLIA efficiently and accurately and with a low false-positive rate.

5.14 Flooding Attack

Flooding attack [84] is one type of DoS attack that aims to send a series of packet requests to a specific device to flood the target server, thus consuming its resources and making it unable to process requests from legitimate users.

Srinivas and Manivannan [85] develop a novel robust model combining deep learning and improving Rider optimization algorithm to detect and prevent Hello flooding attacks in IoT. The proposed model uses cluster head selection, k-path generation, HELLO flooding attack detection and prevention, and optimal shortest path selection. After selecting the cluster head and generating k paths, the proposed model determines the route discovery time of each node and defines the route discovery frequency vector to detect HELLO flooding attacks. The proposed model considers objective constraints such as node trust, the distance between nodes, and transmission delay to select the optimal shortest path. The research results show that, compared with the traditional model, the proposed model is more effective in preventing HELLO flooding attacks and performs better in finding the shortest path. Ding et al. [86] propose an active **Link-flooding attack (LFA)** mitigation mechanism called Linkbait, which is an active and preventive defense measure designed to mitigate the LFA of the IoT. The authors design a link obfuscation algorithm in Linkbait, which selectively reroutes the detection process and misleads the opponent to recognize the decoy link as a targeted link by hiding the target link from the opponent. Moreover, the research proposes an

algorithm for detecting infected IoT devices. The proposed algorithm extracts the unique traffic characteristics of the IoT LFA from the link graph construction phase and the flooding phase and uses SVM to identify infected devices and legitimate IoT devices. The authors implement a prototype on a real SDN test platform and prove the feasibility and effectiveness of Linkbait through large-scale simulation experiment results. Gajbhiye et al. [87] propose detecting and preventing the **Detection and Prevention Low Power and Lossy Network (DPLPLN)** scheme to protect IoT communications. DPLPLN is designed to identify the flooding behavior or packet spam of attackers and apply **Intrusion Prevention System (IPS)** to the network to provide security. The proposed scheme can identify the malicious behavior of the attacker and prevent the malicious activity of the attacker in the network. The research results show that, compared with the performance of RMDD, DPLPLN provides better performance metrics such as overhead and throughput.

5.15 Cloud Malware Injection

Cloud malware injection attacks inject malicious code or **virtual machines (VM)** into the cloud. Attackers masquerade as valid services by attempting to create virtual machine instances or malicious service modules, and then they manage to gain access to service requests from victim services and capture sensitive data.

Devi et al. [88] take a holistic approach to the most common security vulnerabilities in cloud computing, then analyze specific attacks to address a granular level. In addition, this paper analyzes the intrusion methods of honeypot attacks. McDole et al. [89] analyze and compare seven **CNNs** for online malware detection in cloud **infrastructure-as-a-service (IaaS)**, and they use state-of-the-art DenseNets and ResNets to detect malware in online cloud systems effectively. Experiments are performed on the OpenStack testbed. The results show that DenseNet models have higher accuracy and precision, indicating that they are less likely to generate false positives, which is helpful in cloud IaaS environments where service availability is paramount. Therefore, the DenseNet model performs best with 93% accuracy. Panker and Nissim [90] propose a framework based on trusted machine learning. The proposed framework uses **machine learning (ML)** algorithms to detect unknown malware in a Linux VM cloud environment from nine different classes. Experimental results show that trusted detection of various malware of different classes and types is possible. Additionally, the proposed framework can accurately detect unknown malware on unknown virtual servers and fileless malware.

5.16 Signature Wrapping Attack

In a signature wrapping attack, the attacker acts or modifies the eavesdropping message by subverting the signature algorithm or exploiting a vulnerability in the **Simple Object Access Protocol (SOAP)**.

Modak et al. [91] comprehensively analyze the signature wrapping attack of XML data and the countermeasures to detect and defend against this Web security threat. It turned out that XML security specifications, including message flows, were inadequate, and validating and processing each SOAP account header was costly and time-consuming. Also, before accepting XML data, it is necessary to do proper validation on the server and client.

5.17 Brute Force/Dictionary Attack

Brute force attacks use trial-and-error to crack passwords, login credentials, and encryption keys, allowing unauthorized access to individual accounts and an organization's systems and networks. An attacker finds a user's login information by testing various usernames and passwords with a computer. Dictionary attacks are a basic form of brute force attack. Unlike the brute force attack, where an attacker amplifies a single user, a dictionary attack breaks the encryption of a password

database to gain access to the accounts of all service or network users. The attacker chooses a target and tests for possible passwords against that individual's username by running through a dictionary and modifying the words with specific characters or numbers.

Hossain et al. [92] study SSH and FTP brute force attack detection using the **long short-term memory (LSTM)** deep learning approach. The authors train the model on the labeled dataset CICIDS2017. The proposed model can predict abnormal network traffic behavior and identify malicious activities in network systems. The results show that the proposed LSTM model outperforms the ML algorithm with an accuracy of 99.88% and a low false-positive rate. Park et al. [93] propose a model to detect SSH brute force attacks from logs generated by routers over a year. The proposed model extracts and segments the specific data required to detect SSH brute force attacks from the collected packets of routers. The model multiplies the user access records in each packet by weight and adds them to a blacklist based on the resulting value calculated at the end. In addition, the method prevents unauthorized access to internal IPs and attack site IPs by creating a blacklist based on risk, thereby preventing the infection of other systems. However, this method is designed to prevent future attacks by analyzing attacks that have already occurred, so it cannot respond to attacks in real-time. Raikar and Meena [94] propose a system to detect and mitigate SSH brute force attacks in IoT. The proposed system can continuously monitor traffic and analyze attack pattern logs. The results show that the system saves 25% CPU, 40% power, and 10% memory regarding resource utilization.

5.18 Extra Interfaces

The attacker exploits the extra port of the IoT gateway for backdoor authentication, resulting in the disclosure of user information. Therefore, IoT gateway manufacturers should only implement the necessary interfaces and protocols and limit the services and functions used by end-users.

Šarac et al. [95] propose a secure gateway architecture for bringing basic interfaces to IoT devices and blockchain to provide decentralization and authentication. The proposed scheme adds much-needed anonymity and versatility to the currently lacking IoT infrastructure and enhances the reliability of data sent to remote services by applying compatible encryption algorithms before sending it. Furthermore, all requests should be authenticated through the blockchain interface and, if correct, pass. By implementing a simple interface as a security gateway, device manufacturers can add another layer of security to Internet communications. Pavlovicét al. [96] propose a way to add simple interfaces as a secure gateway architecture for IoT devices. This scheme improves the security of data sent by IoT devices to remote services through encryption algorithms compatible with the data before it is sent to the remote service. The results show that the scheme provides a secure interface for any cryptographic algorithm, using **Internet Protocol (IP)** mapping to prevent access to devices from unauthorized IP addresses behind the interface, providing strong protection against attacks and data manipulation.

5.19 End-to-End Encryption

Suresh and Priyadarsini [97] propose an enhanced modern symmetric encryption to protect data to ensure data security in IoT data transmission and storage in the cloud. The proposed **Enhanced Modern Symmetric Data Encryption (EMSDE)** is a block cipher encryption technique that uses a single key to encrypt and decrypt data, designed to protect data in cloud-based IoT environments. The results show that the proposed EMSDE requires less encryption and decryption time than other existing encryption techniques, and it is specifically tailored to protect data stored in the cloud from IoT devices. Khan et al. [98] propose an **edge security gateway (ESG)** based on a double ratchet algorithm providing communication and endpoint security. The proposed gateway ensures each message is encrypted with a different short-term key and

Table 3. IoT Attacks and Security Requirements Compromised

IoT Attacks	Security Requirements
Eavesdropping, Man-in-the-Middle (MITM), Worms attack	Confidentiality
Man-in-the-Middle (MITM), Worms attack	Integrity
Man-in-the-Middle (MITM), DoS/DdoS attack, Worms attack	Availability
Man-in-the-Middle (MITM), Worms attack	Non-Repudiation

provides localized firewall protection for individual devices. In addition, ESG is easy to customize and suitable for a wide range of industrial applications. This paper presents the design and verification of synchrophasor technology in smart grids. The results show that ESG successfully blocks port scanning and validates its effectiveness in detecting reconnaissance, manipulation, replay, and command injection attacks. Peng et al. [99] propose a secure IoT scheme based on a fine-grained multiple-receive encryption scheme for IoT gateway-based applications to achieve secure end-to-end transmission and data access control. Furthermore, the authors analyze the security and performance of the proposed scheme. The results show that the scheme can achieve the expected IND-CCA and EUF-CMA security with efficient computational performance, linearly with the number of messages and recipients.

5.20 Firmware Updates

Since most IoT devices are resource-constrained, they do not have a user interface or computing power to download and install firmware updates. However, the IoT gateway can be used to download and apply firmware updates. Therefore, make sure that the IoT gateway downloads the current and new versions of the firmware and checks the validity of the signature.

Pillai et al. [100] propose a blockchain-based solution for managing firmware updates in IoT. The proposed scheme aims to validate and securely distribute firmware binaries to IoT devices deployed by device vendors. The proposed method uses a hash chain to verify firmware updates, and after downloading the binary in the IoT gateway, the smart contract uses the hash chain information provided by the vendor for verification. In addition, the method uses a smart contract mechanism to link the latest version information with the previous version information, thereby maintaining the integrity of the firmware. Yohan and Lo [101] propose a secure and verifiable blockchain-based firmware update framework for IoT environments to provide a secure **peer-to-peer (P2P)** verification mechanism and guarantee distributed integrity of the firmware. The proposed framework can ensure the integrity of firmware during distribution over the Internet. Furthermore, the authors evaluate the performance and security strength of the proposed framework. The results show that the proposed framework supports mutual authentication and can defend against major network attacks. The authors propose a FUOTA-based framework designed to update IoT device firmware using the LoRa communication protocol securely. Anastasiou et al. [102] evaluate the firmware update process using network and firmware sizes. The results show that using multiple IoT gateways is recommended to improve the reliability and performance of the firmware update process through collaboration.

Table 3 summarizes the prominent attacks and how they are interrelated in terms of security requirements.

6 CURRENT IOT SECURITY COUNTERMEASURES

This section categorizes current IoT security solutions for IoT security challenges and mechanisms.

Table 4. Types and Characteristics of Cryptography for IoT

Cryptography	Symmetric Key Cryptography	Asymmetric Key Cryptography	Hash Functions
Number of Keys	1	2	0
NIST Recommended Key Length	128 or 256 bits	RSA key size is 2,048 bits or higher	256 bits
Speed	Fast	Relatively slow	Fast
Complexity	Medium	High	Medium
Usage	Used to transmit big data	Used to transmit small data	The size of the input data can be varied, but the output value always remains the same size.
Security of the Key	The secret key is shared, which has chances of key being compromised.	The private key is not shared, which is more secure than symmetric key cryptography.	N/A
Examples	AES, DES, 3DES, RC4, Twofish, Blowfish	RSA, DSA, ECC, Diffie-Hellman	SHA-1, SHA-2 family (includes SHA-224, SHA-256, SHA-384, SHA-512), MD5

6.1 Security Countermeasures against IoT Security Challenges

The popularity of IoT devices has increased demand for the IoT market. Although IoT devices have proven to bring production advantages to enterprises, connecting IoT devices to the network poses security challenges. This subsection lists the common security challenges of IoT and related research work.

6.1.1 Data-related Security. Due to the continuous increase of IoT devices, a large amount of data is generated, including confidential data such as personal information, which will cause security issues such as loss of sensitive data. Therefore, IoT devices and services need to process sensitive data correctly and securely while ensuring the confidentiality and authenticity of the transmitted data. Cryptography [103] is an effective way to solve this challenge. Data encryption and decryption ensure that data privacy and confidentiality can be protected and minimize the risk of data theft. Table 4 shows the classification and related characteristics of cryptography [104, 105].

Symmetric key cryptography is also known as secret key cryptography, in which the sender and receiver of the message use the same key to encrypt and decrypt the message [106]. It is a simple form of encryption, but the problem is that the sender and receiver must securely exchange keys to avoid the key being compromised [106].

Asymmetric key cryptography, also known as public key cryptography, uses a pair of keys (public key and private key) to encrypt and decrypt messages [107]. The public key is used for encryption, and the private key is used for decryption. Unlike symmetric key cryptography, even if the public key is used for encryption, there is no way to decrypt the message with it, and only the private key can be used to decrypt the message [107]. Moreover, the private key cannot be derived from the public key, but the public key can be derived from the private key [107, 108]. The private key should not be distributed but only be reserved for the owner. The public key can be shared across the network so a message can be transmitted through public keys [108].

A hash function is an irreversible one-way function, and the algorithm does not use any key [109]. It converts a given string into a fixed-length string, making the plaintext content unrecoverable [109, 110]. It is secure, since the only way to crack the hash is to try all possible inputs until the attacker gets the same hash.

Kumar et al. [111] propose a hybrid cryptosystem that provides better security for cloud data storage. The authors implement the proposed algorithm in JAVA and test on a sample plain text. The results prove that the proposed method can provide better security for data. Sittampalam and Ratnarajah [112] propose a novel **Random Secret Key (RSK)** technique to provide simple and effective key-based security for symmetric **Lightweight Cryptography (LWC)** algorithms for IoT applications. The research uses RSK to share a random matrix among IoT devices, and the devices generate RSK from the random matrix to encrypt and transmit ciphertext. In addition, the proposed method is successfully implemented in a smart greenhouse environment, proving that it can provide enhanced and effective protection for the symmetric LWC algorithm in any IoT system.

6.1.2 Authentication and Access Control. Authentication and access control of IoT devices is one of the security challenges of IoT [113]. If IoT devices connect to the IoT network without proper authentication, then they may become targets of attackers, thereby compromising the system. Therefore, IoT devices should strictly regulate remote and direct server access to prevent unauthorized access. To enable authorized users to access information securely, Aftab et al. [114] propose a **hybrid access control (HAC)** model, which implements the dynamic **conflict of interest (COI)** in it at the role level. To modify the RBAC model, the authors insert new attributes into **role-based access control (RBAC)** entities. Compared with the previously proposed model, the HAC model effectively handles COI at the role level and is suitable for protecting the localization systems.

6.1.3 Weak Password. Weak passwords can lead to security attacks on IoT devices [115]. Vulnerable passwords include default passwords frequently used by humans, which seem to improve the security of the IoT, but there are still hidden security risks [116]. Therefore, a reliable password management mechanism is needed to mitigate the security risks caused by weak passwords. One solution is to set the password to a mixture of case-sensitive characters, and individuals should avoid using the same password on different devices. In addition, the passwords on important devices need to be changed frequently. Since **Textual-Based Passwords (TBPs)** are vulnerable to brute force cracking, dictionary attacks, and social engineering attacks, Alfard et al. [116] propose a new **Graphical-Based Password (GBP)** scheme called IoTGazePass, which solves the memorability and ease of use of the traditional GBP schemes and satisfies authentication requirements in IoT security. The proposed scheme uses grid diagrams and eye gaze to infer text passwords without touching the user interface. Compared with the traditional GBPs scheme, the proposed scheme has the advantages of being easy to remember, difficult to be cracked, minimal resource consumption, randomness, and changeability.

6.1.4 Lack of Secure Update Mechanism. It is important to keep IoT devices updated and repaired. Over time, security vulnerabilities will appear in the IoT device system, which will make IoT devices vulnerable. It requires IoT devices to use the latest system without any known vulnerabilities, and the system must have an update function to patch any known vulnerabilities after the device is deployed. In addition, network administrators should pay attention to the update mechanism.

Zandberg et al. [117] design a secure IoT firmware update prototype based on open standards and open-source libraries. The proposed prototype is a universal, secure, and standards-compliant firmware update solution that can serve constrained IoT devices with no more than 32 kB RAM and 128 kB flash memory. To ensure the security of firmware updates on IoT devices, Mtetwa et al. [118] use blockchain to provide a mechanism for nodes to verify the authenticity and integrity of the firmware and ensure its high availability before updating the software. The prototype has been tested to enable secure IoT firmware updates using smart contracts.

Table 5. IoT Malware Removal and Protection Software

Software	Norton	Bitdefender	McAfee	Malwarebytes	TotalAV	Avira
Free Version	No	Yes	No	Yes	Yes	Yes
Malware Scanner with ML	Yes	Yes	Yes	Yes	No	No
Cloud-based Scanning Option	No	Yes	Yes	No	Yes	Yes
Parental Control	Yes	Yes	Yes	No	No	No
Virtual Private Network (VPN)	Yes	Yes	Yes	Yes (additional purchase)	Yes	Yes (500 MB monthly limit)
Network Firewall	Yes	Yes	Yes	No	No	No
Identity Theft Protection	Yes (US only)	No	Yes (US only)	No	Yes (Canada, US, Western Europe)	No

6.1.5 Lack of Secure Devices Mechanism. The security challenges of IoT devices include constrained devices, unauthorized devices, and the use of unsupported old OS. The combination of old legacy systems and connected devices such as patient monitors, ventilators, infusion pumps, and thermostats has very poor security features and is particularly vulnerable to attacks. Constrained devices are small devices with limited CPU, memory, and power resources. They can form a network in which they are called constrained nodes. Typically, these constrained nodes communicate through low-power wireless protocols such as BLE. Aborujiah et al. [119] propose an **IoT-based Paradigm for Medical Equipment Management Systems (IoT MEMS)** to manage medical equipment in ICU effectively. The proposed IoT MEMS aims to strengthen the information flow between the medical device management system and the ICU to ensure the highest transparency and fairness in redistributing medical devices. The information quality of the proposed paradigm has a positive impact and can effectively mitigate the impact of COVID-19 on medical equipment.

6.1.6 Malware and Ransomware. Hackers can launch ransomware attacks by discovering vulnerabilities in IoT networks and combining them with malware or ransomware [120, 121]. In ransomware attacks, hackers control the system or encrypt valuable information and then ask for a ransom from the victim [120]. Malware and ransomware can cause operational disruption, information loss, and financial losses. Table 5 shows some common malware removal and protection software and their features. Lee et al. [122] propose a cross-platform IoT malware classification method based on printable strings. The authors collect **executable and linkable format (ELF)** files of IoT malware and extract printable strings from them. They obtain useful features through different feature selection methods and then use a set of ML algorithms to classify malware. The test results achieve 98% accuracy in the training set. Jeon et al. [123] propose a **dynamic analysis for IoT malware detection (DAIMD)** based on the CNN model, which aims to mitigate the damage of malware to IoT devices. DAIMD dynamically analyzes IoT malware in a nested cloud environment and uses debugging, feature extraction, feature preprocessing, feature selection, and classification to train, validate, and test to create recommended models. The results show that the proposed model can accurately detect new and variant IoT malware with various intelligent attack technologies.

6.2 Security Countermeasures against IoT Security Mechanisms

6.2.1 Machine Learning (ML) in IoT Security. By using complex algorithms to analyze large amounts of data, ML can build models and predict the future behavior of research objects. ML architectures are generally divided into three types, namely, supervised learning, unsupervised learning, and reinforcement learning. There has been a surge of research interest in the application of ML to IoT security.

Jiang et al. [124] use various ML algorithms to detect anomalies in the IoT network intrusion dataset. The research results show that an accuracy of 99%–100% can be achieved by using the ML approach. Abdelmoumin et al. [125] study the use of optimization techniques such as PCA and **One-class Support Vector Machine (1-SVM) Anomaly-based machine learning-enabled intrusion detection systems (AML-IDS)** model to improve the performance of single-learner AML-IDS, aiming to build efficient, scalable, and distributed intelligent IDS to detect intrusions in IoT network. Yahyaoui et al. [126] design an ML-based architecture for the real-time network IDS for IoT streaming applications. The proposed architecture uses two leading stream processing frameworks (Apache Flink and Apache Spark Streaming) for development, deployment, and testing. The authors use two different public datasets and different ML algorithms to test the proposed architecture, and the results show that the architecture has high accuracy and throughput. Ioannou and Vassiliou [127] use supervised learning for local intrusion detection in IoT networks. The authors test the approach based on SVM and use IoT test platform data to train and evaluate the detection model for selective forward and blackhole attacks. The results show that the study achieves 99.8% accuracy rates and 100% recall values. Joshi and Abdelfattah [128] study the efficiency of four ML algorithms for multivariate classification of IoT botnet attacks. The authors use the N_BaIoT dataset to detect abnormal traffic. The results show that when all algorithms are used to train and test anomalies in the same device, all classifiers perform well. However, when training on a particular device and testing for anomalies on completely unrelated devices, the performance of the random forest classifier is better than all other classifiers. Liu et al. [129] propose a malware detection method based on ML from health sensor data. The authors use XGBoost, LightGBM, and random forest to analyze the code from health sensor data. The results show that when a model detects a malicious program, it will broadcast its pattern to other models, which can effectively prevent malware program intrusion. Makkar et al. [130] use ML to detect spam in IoT to protect IoT devices. The authors use the REFIT smart home dataset to verify the proposed technology. The results show that the proposed technology can effectively detect spam. Nadia et al. [131] propose an ML-based IoT user authentication system that uses human body impedance as a user identifier and uses ML to create an identification machine to determine the pattern similarity between the input and the existing model. In addition, the proposed system is easy to use and has a high accuracy rate. Chen et al. [132] propose an ML-based IoT DdoS attack detection system to prevent attacks in IoT gateways. The proposed system is a multi-layer DdoS detection system, including IoT devices, gateways, SDN switches, and cloud servers. The authors extract the characteristics of four DdoS attacks and launch DdoS attacks from eight smart poles. The research results show that the proposed system can detect DdoS attacks and block malicious devices. Aboelwafa et al. [133] propose an ML-based **false data injection (FDI)** attack detection method for the Industrial IoT. The proposed method uses an **automatic encoder (AE)** and the correlation of sensor data in time and space to identify fake data. In addition, the proposed method also uses **denoising Aes (DAEs)** to clean up fake data. Compared with other SVM-based methods, the proposed method can detect FDI attacks more effectively. Hoang et al. [134] use **one-class support vector machines (OC-SVM)** and K-means clustering to build a predictive model to detect eavesdropping attacks in UAV-aided wireless systems. The authors propose two frameworks for generating datasets; one is used to create relevant test data from wireless signals, and the other is used to generate training

data. The results show that OC-SVM is better than K- means in terms of stability, and K-means clustering is better when the eavesdropper uses high power in the transmission.

Rey et al. [135] propose a privacy-preserving framework for IoT malware detection that utilizes **Federated Learning (FL)** to train and evaluate supervised and unsupervised models without sharing sensitive data. The framework is designed to be deployed on network nodes to provide access to IoT devices in WiFi, 5G, or **Beyond (B5G)** networks, thereby reducing the computational burden on IoT devices. Furthermore, the authors use the N-BaIoT dataset to demonstrate the feasibility of the proposed framework in real-world IoT scenarios. The results show that using more diverse and larger data positively impacts model performance. Furthermore, the federated model shows results similar to the centralized model while preserving the privacy of the participants. Mehedi et al. [136] propose a deep transfer learning-based reliable IDS model called P-ResNet that outperforms several existing methods. The proposed model is best suited for identifying normal and attack scenarios with little labeled data, designing reliable deep transfer learning-based ResNet models and considering real-world data for evaluation. After a comprehensive experimental performance evaluation, the results show that the overall accuracy of the proposed detection model is 87%, ensuring reliability and low time complexity. In addition, the model significantly improves the precision score of 88%, the recall score of 86%, and the F1-score of 86%, which is higher than the baseline model. Therefore, the P-ResNet model is robust, more efficient, performs better, and ensures reliability. Lin et al. [137] propose a **Data Fusion and transfer learning empowered granular Trust Evaluation mechanism (DFTE)** enabled by data fusion and transfer learning to defend against IoT security threats and ensure the reliability of the data sources of collected data. Two trust evaluation models are established using data fusion-based **deep reinforcement learning (DRL)** methods, which are constructed using the deep **deterministic policy gradient algorithm (DDPG)** and the coarse-grained trust evaluation model based on **Deep Q-learning Network (DQN)** to establish a spatiotemporal-enabled fine/coarse-grained trust evaluation model to achieve trust evaluation at different granularities. Additionally, **transfer learning (TL)** is applied to unified trust evaluation to reduce model training time. The results show that the proposed DFTE achieves high-precision trust evaluation under different granularity requirements through effective data fusion and performs well regarding participation rate and data reliability. Xue, Zhao, and Yao [138] propose a **heterogeneous transfer learning (HTL)**-based intrusion detection method to improve intrusion detection performance with a small amount of unlabeled data in heterogeneous IoT environments. The proposed method includes an autoencoder architecture for aligning heterogeneous features and a lightweight CNN for unsupervised domain adaptation. The performance of the proposed method is evaluated by classifying three **Network Intrusion Detection (NID)** data samples into normal or attack categories. The results show that the proposed method greatly improves the overall performance of the cross-domain network intrusion detection task compared to the baseline method without domain adaptation and achieves better performance than other deep data analytic methods.

Malibari et al. [139] propose a novel metaheuristic intrusion detection system with deep learning for secure, intelligent environments, called the MDLIDS-SSE technique, aimed at identifying the presence or absence of intrusions in secure, intelligent environments. The MDLIDS-SSE technique employs a Z-score normalization method as a data preprocessing step. In addition, MDLIDS-SSE technology supports the **Improved Arithmetic Optimization Algorithm-based Feature Selection (IAOA-FS)** technique to select the best subset of features. MDLIDS-SSE technology also includes classification based on **Deep Wavelet Neural Network (DWNN)** and parameter optimization based on **Particle Swarm Optimization (QPSO)**. Simulations and comparison studies illustrate the enhanced intrusion detection results of the MDLIDS-SSE technique over other recent approaches. Since the development of intelligent analysis tools that require data prepro-

cessing and machine learning algorithm performance enhancement requires a **feature selection (FS)** method, Kareem et al. [140] propose a new FS method through boosting the performance of **Gorilla Troops Optimizer (GTO)** based on the **algorithm for bird swarms (BSA)**. This BSA was used to improve the performance of GTO in the newly developed GTO-BSA. The performance of GTO-BSA is evaluated using various performance metrics on four IoT-IDS datasets: NSL-KDD, CICIDS-2017, UNSW-NB15, and BoT-IoT. Compared with the original GTO, BSA, and other state-of-the-art results, the results show that GTO-BSA has better convergence speed and higher-quality solutions. Seif et al. [141] propose a **Hybrid Intelligent Intrusion Detection System (HIIDS)** based on machine learning and metaheuristic algorithms aimed at applying it to IoT-based healthcare systems. The authors use meta-heuristic algorithms such as **Particle Swarm Optimization (PSO), Genetic Algorithm (GA)**, and **Differential Evaluation (DE)** for optimal feature selection and supervised learning algorithms to reduce computational cost. Furthermore, they propose a hybrid approach for feature selection and classification. The authors evaluate the performance of the proposed HIIDS using the popular NSL-kDD dataset containing 41 features and 125,973 samples. The results show that the proposed model can accurately classify attack and normal traffic in a shorter time and has relatively low CPU and memory usage, making it suitable for resource-constrained IoT-based smart healthcare applied in the system. To protect private information and communications, Otoum, Yadlapalli, and Nayak built an IDS model by combining federated learning and transfer learning. The proposed model is designed to secure IoT networks with less training time and enhanced performance while ensuring user data privacy. The authors use **deep neural network (DNN)** and CNN to evaluate the performance of the proposed model on the benchmark dataset CSE-CIC-IDS2018. Moreover, they also show the feasibility of adopting **Federated Transfer Learning (FTL)** in terms of performance metrics as well as training and fine-tuning times. The results show that the proposed model is more efficient and reduces training time more than traditional machine learning techniques [142]. Otoum, Liu, and Nayak [143] propose a novel **deep learning-based intrusion detection system (DL-IDS)** to detect security threats in IoT environments by combining the **spider monkey optimization (SMO)** algorithm and **stacked deep polynomial network (SDPN)**. The proposed model utilizes SMO to select the best features in the dataset and SDPN to classify the data as normal or abnormal. So far, the model can detect DoS, **user-to-root (U2R)** attacks, probe attacks, and **remote-to-local (R2L)** attacks. The analysis shows that the proposed DL-IDS performs better in accuracy, precision, recall, and F-score.

ML can solve the IoT security issues such as malware detection, DdoS attack, eavesdropping, authentication, false data injection, spam detection, malware detection, anomaly detection, and IDS.

6.2.2 Edge Computing in IoT Security. Edge computing uses the cloud concept, placing the edge servers between the end-user and the cloud server, computing at or near the data source, instead of relying on the cloud to complete all the work [21]. Figure 2 shows the general edge computing architecture [26]. Edge computing solves the cloud computing problems such as latency and communication speed. Near instant computing and analytics at the edge reduce latency, thus greatly improving performance, and edge computing can process large amounts of data, which no longer requires the costly bandwidth, thus reducing load and cost on cloud services [21]. In addition, edge computing can analyze sensitive IoT data in the private network to protect these data [21].

Kuo and Wang [144] propose a system scheme that can balance the power consumption between computation and communication. The authors use edge computing to analyze and calculate the power consumption of transmission, aiming to find a way to minimize the total energy consumption of IoT mobile devices. The actual measurement results show that the proposed scheme can find the most energy-efficient option in different situations and save the battery of the device.

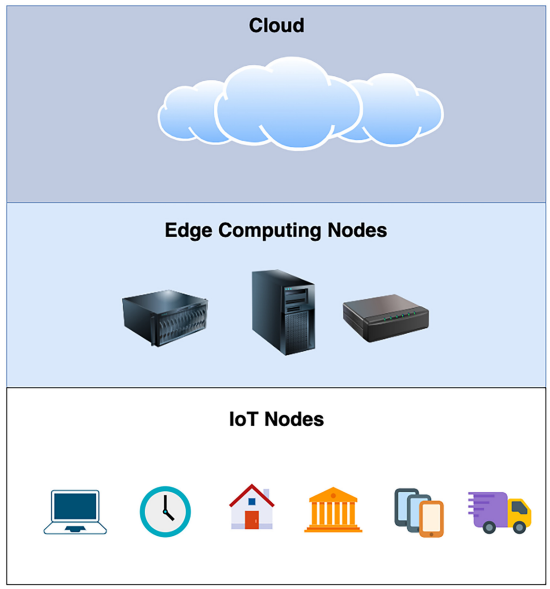

Fig. 2. General edge computing architecture.

Amin et al. [145] propose a mechanism based on edge computing to detect and mitigate spoofing attacks and network intrusion attacks automatically. In addition, the authors use a graph computation-based method to identify the location of the attackers and immediately block their communication port. Nie et al. [146] propose a secure social IoT intrusion detection based on collaborative edge computing. The authors use a feature selection module to process collaborative edge network traffic and design an intrusion detection system for a single attack based on a **generative adversarial network (GAN)**. It has been verified that the proposed method can effectively perform intrusion detection. J. Li et al. [147] design an SDN-based edge computing security framework in the IoT healthcare system. In the proposed framework, the edge server uses a lightweight authentication scheme to authenticate IoT devices. The verified device sends the collected data from patients to the edge server for storage, processing, and analysis, where the edge server is connected to the SDN controller. The research results show that the proposed framework effectively improves network performance and efficiently uses resources.

Edge computing can solve the IoT security issues such as IDS, network performance, power consumption, spoofing attack, network intrusion, and authentication.

6.2.3 Cloud Computing in IoT Security. Cloud computing is an application-based software infrastructure that can transmit and store data to the cloud data center over the Internet [148, 149]. Cloud computing is an on-demand computing service that allows users to easily access data and programs from the centralized cloud system [149]. Cloud computing architecture includes two basic components, namely, front-end and back-end. Figure 3 shows the cloud computing architecture. The front-end works as a client in cloud computing architecture and communicates with the back-end via the Internet. The service provider uses the back-end to manage all resources required for cloud computing services, including large-capacity data storage devices, security mechanisms, virtual machines, servers, flow control mechanisms, and so on [26]. Cloud computing can be divided into three models, which are **Infrastructure as a Service (IaaS), Platform as a Service (PaaS)**, and **Software as a Service (SaaS)** [150].

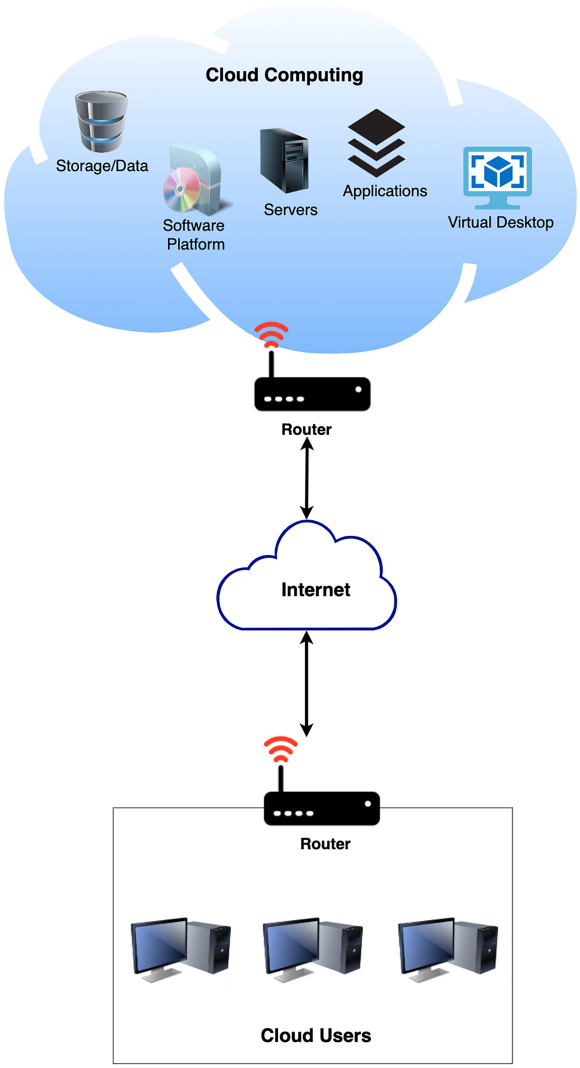

Fig. 3. Cloud computing architecture.

Cloud computing is an important part of IoT, which aggregates servers, analyzes information obtained from sensors, increases processing power, and provides good storage capacity [12]. Cloud computing provides users with powerful security measures. The cloud computing system can manage and verify user access to prevent data leakage. In addition, cloud computing can implement data encryption and authentication procedures to prevent unauthorized users from accessing IoT devices or networks [151].

Xiong et al. [152] propose an efficient and secure access control system SEM-ACSIT for IoT applications. The proposed system can guarantee forward and backward security when user attributes are revoked. In addition, the proposed system utilizes encryption outsourcing, simplified key structure, and the **attribute authority management (AAM)** module, which significantly reduces the storage overhead of the system. Moreover, the proposed system builds a **user access control list (UACL)** in the cloud server, which can support authorization for specific users to

access shared data. Compared with other existing solutions, the proposed system is more flexible, has lower storage costs, and has high security. Riad et al. [153] propose a **multi-dimensional access control (MD-AC)** scheme to dynamically authorize and revoke users in the cloud with multiple permissions. Compared with existing schemes, the proposed scheme evaluates access requests within a reasonable and acceptable processing time, and unauthorized attackers cannot recover the original data. To solve the unauthorized access to IoT medical data in the healthcare system, Rashid et al. [154] propose an **Enhanced Role Based Access Control (ERBAC)** model to protect the storage of IoT medical data on the public cloud system. The proposed model adds a function to restrict roles and users in **Role Based Access Control (RBAC)** to ensure the security of medical data stored on the cloud system. In addition, the proposed model uses two authentication and encryption technologies to protect data on the cloud system. Ding et al. [155] propose an IoT security information transmission algorithm based on cloud computing to reduce errors in resource management and improve security and accuracy in the process. The proposed algorithm uses information security transmission technology to collect and extract all resources in the heterogeneous integrated network and establish a resource management model. The research results show that the effectiveness, security, and accuracy of the resource management algorithm are verified. In addition, to prevent information leakage and theft, the authors introduce the main data encryption technologies to improve network communication security. Anuradha et al. [156] designed an IoT-enabled cancer prediction system and used cloud computing to enhance authentication and security. The authors use IoT to collect and process the medical data of cancer patients and use the AES algorithm to encrypt the patient's data, which requires doctors or nurses to provide security authentication when processing sensitive medical data. In addition, the authors use CloudSim as an adaptable simulation structure and store the encrypted medical information of the patients in the cloud. Wang and Zhang [157] propose an optimized data storage algorithm for IoT based on cloud computing in a distributed system to improve data processing efficiency and fault tolerance and provide advanced technical support for the storage and management of data access. This research uses HDFS to optimize cloud computing data access storage algorithms. The authors conduct simulation experiments in OPNET Modeler. The experimental results show that the IoT data optimized by the algorithm is better than the original state in terms of transmission speed, system resource occupation, and response time. Furthermore, the IoT data processing efficiency of the optimized transmission can reach up to 99%, and the maximum fault tolerance rate of the optimized algorithm can reach 96.12%. SaiSindhuTheja and Shyam [158] propose an efficient meta-heuristic OCSA algorithm based on feature selection and **Recurrent Neural Network (RNN)** for DoS attack detection in the cloud computing environment. The proposed algorithm combines **opposition-based learning (OBL)** and **crow search algorithm (CSA)**, selects the feature, and then uses RNN to classify the selected features. The authors use the KDD Cup 99 datasets to conduct experiments. The experimental results show that the proposed algorithm is better than existing algorithms in terms of Precision, Recall, F-Measure, and Accuracy. Using a collaborative cloud computing approach, Saxena and Dey [159] propose a data packet tracing approach based on a **third-party auditor (TPA)** to prevent DDoS attacks. The authors use the Weibull distribution to analyze the source of DDoS attacks and obtain the availability, reliability, and median lifetime of DDoS defense in a cloud environment. Moreover, the proposed approach also solves the problem of IP spoofing. The authors use an application based on the Hadoop and MapReduce frameworks to test this approach. Compared with existing approaches, the proposed approach can effectively mitigate and prevent DDoS attacks. In addition, the proposed approach reduces the overhead of cloud users.

Cloud computing can solve IoT security issues such as DoS attack, access control, spoofing attack, DDoS attack, data integrity, authentication and authorization, and secure storage.

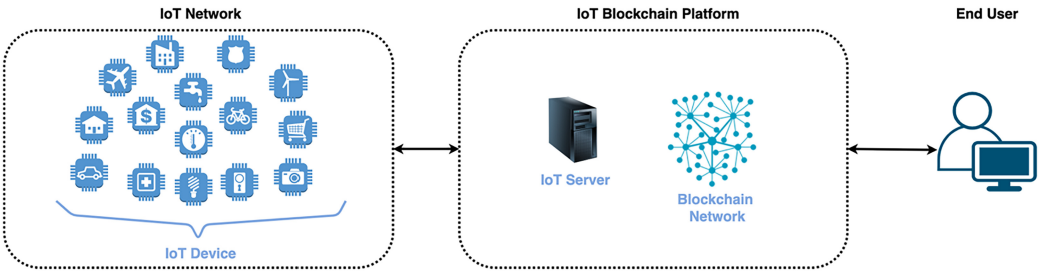

Fig. 4. Conceptual framework of the integrated IoT blockchain platform.

6.2.4 Blockchain in IoT Security. Blockchain is a combination of computers linked to each other instead of a central server, meaning the entire network is decentralized [160, 161]. The core of the blockchain system is composed of a distributed digital ledger shared by system participants, which resides on the Internet [15, 160]. The verified transactions or events are recorded in the ledger and cannot be modified or deleted. Furthermore, blockchain allows the user community to record and share information [15]. Blockchain provides strong data-tampering protection, locks access to IoT devices, and allows the shutdown of damaged devices in the IoT network [21]. Figure 4 shows the conceptual framework of the integrated IoT blockchain platform [160, 161].

Al-Madani and Gaikwad [162] propose a blockchain-based IoT data security model, **service-centric networking (SCN)**. SCN provides communication through service names instead of addresses and a decentralized network that allows network users to communicate quickly with reliable and secure data. In addition, the proposed model encrypts the user's identity on the device supported by the **InterPlanetary File System (IPFS)** and provides storage data in the user's device. Bhandary et al. [163] introduce IOTA, a blockchain solution based on **Directed Acyclic Graph (DAG)**, a new distributed ledger technology for IoT data security. To ensure data confidentiality and authentication, the authors use the **Masked Authenticated Messaging (MAM)** of IOTA. The results show that the proposed scheme can guarantee the tamper-proof and secure transmission of IoT sensor data. In addition, IOTA is resilient to quantum computer attacks. Xu et al. [164] propose a **blockchain-based secure data-sharing platform with fine-grained access control (BSDS-FA)**. Since the **hierarchical attribute-based encryption algorithm (HABE)** can ensure the security of user data and provide users with fine-grained access control, the authors apply the HABE algorithm combined with smart contract technology to BSDS-FA so BSDS-FA can not only prevent illegal users from accessing shared data but also reduce the user's decryption overhead. The authors test the security of BDSS-FA, and the experimental results show that BDSS-FA can provide users with more secure and reliable data-sharing services while providing fine-grained access control without affecting download performance. Wei et al. [165] propose a blockchain data integrity protection mechanism, which aims to realize the security protection and integrity verification of cloud data. The proposed mechanism uses mobile agent technology to deploy a distributed **virtual machine (VM)** agent model in the cloud to ensure multiple tenants can collaborate and verify data trust. Zhao et al. [166] propose a blockchain-based remote data integrity check scheme for the privacy protection of IoT information systems without **trusted third parties (TTP)**. The proposed scheme utilizes the Lifted EC-ElGamal cryptosystem, bilinear pairing, and blockchain to support efficient public batch signature verification and ensure the security, privacy, and dynamics of IoT data. In addition, the proposed scheme can resist data privacy breaches caused by TTP. Liu et al. [167] propose an IoT access control system called fabric-IoT, which is based on the Hyperledger Fabric blockchain framework and **attribute-based access control (ABAC)**. The proposed system consists of three types of smart contracts, which are **Device Contract (DC),**

Table 6. Comparison between the Protection Strategies

Comparison	Machine Learning	Edge Computing	Cloud Computing	Blockchain
Security	Secure	Secure	Less Secure	Secure
Architecture	Distributed Centralized Decentralized	Distributed	Centralized	Distributed Decentralized
Latency	Less	Less	High	High
Data Analysis	Real Time	Real Time	N/A	Real Time
Easy Target	Medium	Less	High	High
Energy Consumption	High	Less	High	High
Computing Devices Used	Smart phones, Smart Sensors	Routers, Smart Sensors, Server Systems, Edge Gateways, Smart Phones	Databases, Servers, Data Storages	Smart Sensors, Server Systems
Applications	Smart Home, Smart Agriculture, Smart Transportation, Smart Environment, Smart Grid, Smart City, Smart Retail, Industrial Automation	Smart Home, Smart Agriculture, Smart Transportation, Smart Environment	Smart Home, Smart City, Smart Grid, Banking	Smart Home, Banking
Research Papers in This Area	[139–157]	[157–160]	[165–172]	[175–181]

Policy Contract (PC), and **Access Contract (AC)**. It adopts a distributed architecture to provide fine-grained dynamic access control management for physical networks. The authors design simulation experiments to verify the performance of the proposed system. The results show that the proposed system can maintain high throughput and ensure data consistency. Cui et al. [168] propose a blockchain-based IoT multi-WSN identity authentication scheme. The proposed scheme combines the decentralization of the blockchain and the distributed structure of IoT nodes to build a local blockchain between the cluster heads of a single WSN and add all WSN base stations to the public chain to form a hybrid blockchain model. In this model, node identity authentication is implemented in various communication scenarios. The security and performance analysis shows that the scheme has good security and efficiency.

Blockchain can solve IoT security issues such as data integrity, privacy preservation, secure communication, data confidentiality, secure storage, authentication, and access control. Table 6 compares the protection strategies provided in this survey article. Cloud computing is a standard of computing and can be accessed through a set of services provided by a service provider through the Internet so the risk of data breaches and cyber-attacks can occur when data is transmitted over long distances or across multiple networks [26]. Furthermore, transmitting data over the network can lead to sensitive data leakage. Therefore, cloud computing is less secure than other computing paradigms used by IoT.

7 FUTURE RESEARCH DIRECTIONS

This survey presented a comprehensive study of IoT security in the previous sections. This section introduces some future research directions for IoT security.

—IoT devices are connected to the Internet through gateways [169], but due to the lack of a comprehensive security mechanism inside the network management, such as lack of authentication certification, more security measures need to be implemented on these gateways to improve the overall security of the IoT system.

—Due to a large number of connected IoT devices, system throughput and consensus algorithm issues need to be considered. Otherwise, the system processing efficiency will be reduced, which will result in the failure of IoT devices. Machine learning and Blockchain technology can be explored to solve these issues.
—To meet the resource constraints of IoT devices, the lightweight encryption scheme should be designed for security protocols, and the scalability of the IoT should be considered.
—Lightweight authentication is also one of the future security research directions [26]. It is important, since authenticating user identity can avoid sensitive data breaches and improve IoT network performance.
—Biometric security is an authentication mechanism that uses human physiological or behavioral characteristics to verify an individual's identity [170, 171]. Future research needs to consider the cost-effectiveness of using biometrics to authenticate users and the stability of biometrics.
—Create an IoT ecosystem to promote IoT security technology standards and compliance. In addition, researchers need to consider improving the computing speed of security algorithms for IoT applications, as well as considering authorization and access control [26].
—Another future research direction is to protect the security of IoT data storage. Using cloud computing and blockchain-based solutions is one of the ways to solve this problem. Since transactions in the blockchain are public, personal privacy issues need to be considered in future research. In addition, it is necessary to consider the cost of using cloud computing.
—Using edge computing can mitigate spoofing attacks, but the limited power capacity of edge IoT devices needs to be considered in future research, because attackers can perform a large number of operations on the CPU to reduce battery life.

8 CONCLUSION

This survey article provides a detailed introduction to IoT, which analyzes the IoT architecture, infrastructure, and wireless technology. In addition, this article introduces current security vulnerabilities and mitigation strategies. Further, the article analyzes the common IoT security attacks against different layers and studies current solutions to these attacks. To solve IoT security issues, this article introduces the security goals of IoT, and the existing solutions are categorized based on challenges and mechanisms. This article presents the detailed architecture of these solutions, how they solve IoT security challenges, and compares these solutions. Finally, the future research directions for improving IoT security are discussed in detail, which helps with further research in IoT security and lays a foundation for individuals and organizations to propose new technologies and solutions.

REFERENCES

[1] S. Narang, T. Nalwa, T. Choudhury, and N. Kashyap. 2019. An efficient method for security measurement in internet of things. In *International Conference on Communication, Computing and Internet of Things*. 319–323. DOI: https://doi.org/10.1109/IC3IoT.2018.8668159

[2] K. Shafique, B. A. Khawaja, F. Sabir, S. Qazi, and M. Mustaqim. 2020. Internet of things (IoT) for next-generation smart systems: A review of current challenges, future trends and prospects for emerging 5G-IoT scenarios. *IEEE Access* 8 (2020), 23022–23040. DOI: https://doi.org/10.1109/ACCESS.2020.2970118

[3] C. Wheelus and X. Zhu. 2020. IoT network security: Threats, risks, and a data-driven defense framework. *Internet Things* 1, 2 (2020), 259–285. DOI: https://doi.org/10.3390/IOT1020016

[4] Somayya Madakam, R. Ramaswamy, and Siddharth Tripathi. 2015. Internet of things (IoT): A literature review. *J. Comput. Commun.* 03, 05 (2015), 164–173. DOI: https://doi.org/10.4236/JCC.2015.35021

[5] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami. 2013. Internet of things (IoT): A vision, architectural elements, and future directions. *Fut. Gen. Comput. Syst.* 29, 7 (2013), 1645–1660. DOI: https://doi.org/10.1016/J.FUTURE.2013.01.010

[6] M. binti Mohamad Noor and W. H. Hassan. 2019. Current research on internet of things (IoT) security: A survey. *Comput. Netw.* 148 (2019), 283–294. DOI: https://doi.org/10.1016/J.COMNET.2018.11.025

[7] M. M. Sadeeq, N. M. Abdulkareem, S. R. M. Zeebaree, D. M. Ahmed, A. S. Sami, and R. R. Zebari. 2021. IoT and cloud computing issues, challenges and opportunities: A review. *Qubahan Acad. J.* 1, 2 (2021), 1–7. DOI: https://doi.org/10.48161/QAJ.V1N2A36

[8] L. Yao, X. Wang, Q. Z. Sheng, S. Dustdar, and S. Zhang. 2019. Recommendations on the internet of things: Requirements, challenges, and directions. *IEEE Internet Comput.* 23, 3 (2019), 46–54. DOI: https://doi.org/10.1109/MIC.2019.2909607

[9] A. A. A. Sen and M. Yamin. 2020. Advantages of using fog in IoT applications. *Int. J. Inf. Technol.* 13, 3 (2020), 829–837. DOI: https://doi.org/10.1007/S41870-020-00514-9

[10] A. Tiwary, M. Mahato, A. Chidar, M. Kumar Chandrol, M. Shrivastava, and M. Tripathi. 2018. View of internet of things (IoT): Research, architectures and applications. *Int. J. Fut. Revolut. Comput. Sci. Commun. Eng.* 4, 3 (2018), 23–27.

[11] J. Xu and W. Lu. Smart construction from head to toe: A closed-loop lifecycle management system based on IoT. Construction Research Congress 2018. DOI: https://doi.org/10.1061/97807844812640.16

[12] F. Firouzi and B. Farahani. 2020. Architecting IoT cloud. *Intell. Internet Things* (2020), 173–241. DOI: https://doi.org/10.1007/978-3-030-30367-9_4

[13] M. A. Obaidat, S. Obeidat, J. Holst, A. Al Hayajneh, and J. Brown. 2020. A comprehensive and systematic survey on the internet of things: Security and privacy challenges, security frameworks, enabling technologies, threats, vulnerabilities and countermeasures. *Comput.* 9, 2 (2020), 44. DOI: https://doi.org/10.3390/COMPUTERS9020044

[14] H. Wu, H. Han, X. Wang, and S. Sun. 2020. Research on artificial intelligence enhancing internet of things security: A survey. *IEEE Access* 8 (2020), 153826–153848. DOI: https://doi.org/10.1109/ACCESS.2020.3018170

[15] B. K. Mohanta, D. Jena, U. Satapathy, and S. Patnaik. 2020. Survey on IoT security: Challenges and solution using machine learning, artificial intelligence and blockchain technology. *Internet Things* 11 (2020), 100227. DOI: https://doi.org/10.1016/J.IOT.2020.100227

[16] T. Alladi, V. Chamola, B. Sikdar, and K. K. R. Choo. 2020. Consumer IoT: Security vulnerability case studies and solutions. *IEEE Consum. Electron. Mag.* 9, 2 (2020), 17–25. DOI: https://doi.org/10.1109/MCE.2019.2953740

[17] H. Mrabet, S. Belguith, A. Alhomoud, and A. Jemai. 2020. A survey of IoT security based on a layered architecture of sensing and data analysis. *Sensors* 20, 13 (2020), 3625. DOI: https://doi.org/10.3390/S20133625

[18] C. C. Sobin. 2020. A survey on architecture, protocols and challenges in IoT. *Wirel. Pers. Commun.* 112, 3 (2020), 1383–1429. DOI: https://doi.org/10.1007/S11277-020-07108-5

[19] R. Patnaik, N. Padhy, and K. Srujan Raju. 2021. A systematic survey on IoT security issues, vulnerability and open challenges. *Adv. Intell. Syst. Comput.* 1171 (2021), 723–730. DOI: https://doi.org/10.1007/978-981-15-5400-1_68

[20] F. A. Alaba, M. Othman, I. A. T. Hashem, and F. Alotaibi. 2017. Internet of things security: A survey. *J. Netw. Comput. Appl.* 88 (2017), 10–28. DOI: https://doi.org/10.1016/J.JNCA.2017.04.002

[21] X. Liang and Y. Kim. 2021. A survey on security attacks and solutions in the IoT network. In *IEEE 11th Annual Computing and Communications Workshop and Conference.* 853–859. DOI: https://doi.org/10.1109/CCWC51732.2021.9376174

[22] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar. 2019. A survey on IoT security: Application areas, security threats, and solution architectures. *IEEE Access* 7 (2019), 82721–82743. DOI: https://doi.org/10.1109/ACCESS.2019.2924045

[23] N. Neshenko, E. Bou-Harb, J. Crichigno, G. Kaddoum, and N. Ghani. 2019. 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. DOI: https://doi.org/10.1109/COMST.2019.2910750

[24] A. A. Abbood, Q. M. Shallal, and M. A. Fadhel. 2020. Internet of things (IoT): A technology review, security issues, threats, and open challenges. *Indones. J. Electr. Eng. Comput. Sci.* 20, 3 (2020), 1685–1692. DOI: https://doi.org/10.11591/ijeecs

[25] W. Iqbal, H. Abbas, M. Daneshmand, B. Rauf, and Y. Abbas. 2020. An in-depth analysis of IoT security requirements, challenges and their countermeasures via software defined security. *IEEE Internet Things J.* 1–1. DOI: https://doi.org/10.1109/jiot.2020.2997651

[26] S. N. Swamy and S. R. Kota. 2020. An empirical study on system level aspects of internet of things (IoT). *IEEE Access* 8 (2020), 188082–188134. DOI: https://doi.org/10.1109/ACCESS.2020.3029847

[27] L. Boyanov, V. Kisimov, and Y. Christov. 2020. Evaluating IoT reference architecture. In *2020 International Conference Automatics and Informatics (ICAI).* DOI: https://doi.org/10.1109/ICAI50593.2020.9311357

[28] A. E. Bouaouad, A. Cherradi, S. Assoul, and N. Souissi. 2020. The key layers of IoT architecture. In *2020 5th International Conference on Cloud Computing and Artificial Intelligence: Technologies and Applications (CloudTech).* DOI: https://doi.org/10.1109/CLOUDTECH49835.2020.9365919

[29] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash. 2015. Internet of things: A survey on enabling technologies, protocols, and applications. *IEEE Commun. Surv. Tutor.* 17, 4 (2015), 2347–2376. DOI: https://doi.org/10.1109/COMST.2015.2444095

[30] M. Lombardi, F. Pascale, and D. Santaniello. 2021. Internet of things: A general overview between architectures, protocols and applications. *Inf. 2021* 12, 2 (2021), 87. DOI: https://doi.org/10.3390/INFO12020087

[31] S. Al-Sarawi, M. Anbar, K. Alieyan, and M. Alzubaidi. 2017. Internet of things (IoT) communication protocols: Review. In *2017 8th International Conference on Information Technology (ICIT).* 685–690. DOI: https://doi.org/10.1109/ICITECH.2017.8079928

[32] R. Gunasagaran, L. M. Kamarudin, and A. Zakaria. 2018. Embedded device free passive (EDfP) system: Effect of WiFi protocols. In *2018 IEEE Student Conference on Research and Development (SCOReD).* DOI: https://doi.org/10.1109/SCORED.2018.8710806

[33] K. H. Chang. 2014. Bluetooth: A viable solution for IoT?. *IEEE Wirel. Commun* 21, 6 (2014), 6–7. DOI: https://doi.org/10.1109/MWC.2014.7000963

[34] A. Triantafyllou, P. Sarigiannidis, and T. D. Lagkas. 2018. Network protocols, schemes, and mechanisms for internet of things (IoT): Features, open challenges, and trends. *Wirel. Commun. Mob. Comput* (2018). DOI: https://doi.org/10.1155/2018/5349894

[35] X. Jia, Q. Feng, T. Fan, and Q. Lei. 2012. RFID technology and its applications in Internet of Things (IoT). In *2012 2nd International Conference on Consumer Electronics, Communications and Networks (CECNet).* 1282–1285. DOI: https://doi.org/10.1109/CECNET.2012.6201508

[36] Y. Li, Y. Yang, X. Yu, T. Yang, L. Dong, and W. Wang. 2020. IoT-APIScanner: Detecting API unauthorized access vulnerabilities of IoT platform. In *2020 29th International Conference on Computer Communications and Networks (ICCCN).* DOI: https://doi.org/10.1109/ICCCN49398.2020.9209626

[37] "Hacker tries to poison water supply of Florida city - BBC News.". Retrieved from: https://www.bbc.com/news/world-us-canada-55989843

[38] B. Li, R. Ye, G. Gu, R. Liang, W. Liu, and K. Cai. 2020. A detection mechanism on malicious nodes in IoT. *Comput. Commun* 151 (2020), 51–59. DOI: https://doi.org/10.1016/J.COMCOM.2019.12.037

[39] M. A. Khatun, N. Chowdhury, and M. N. Uddin. 2019. Malicious nodes detection based on artificial neural network in IoT environments. In *2019 22nd International Conference on Computer and Information Technology (ICCIT).* DOI: https://doi.org/10.1109/ICCIT48885.2019.9038563

[40] N. Ruminot-Ahumada, C. Valencia-Cordero, and R. Abarzua-Ortiz. 2021. Side channel attack countermeasure for low power devices with AES encryption. In *2021 IEEE International Conference on Automation/XXIV Congress of the Chilean Association of Automatic Control (ICA-ACCA).* DOI: https://doi.org/10.1109/ICAACCA51523.2021.9465337

[41] M. Khan and Y. Chen. 2021. A randomized switched-mode voltage regulation system for IoT edge devices to defend against power analysis based side channel attacks; A randomized switched-mode voltage regulation system for IoT edge devices to defend against power analysis based side channel attacks. In *2021 IEEE Intl Conf on Parallel & Distributed Processing with Applications, Big Data & Cloud Computing, Sustainable Computing & Communications, Social Computing & Networking (ISPA/BDCloud/SocialCom/SustainCom)* DOI: https://doi.org/10.1109/ISPA-BDCloud-SocialCom-SustainCom52081.2021.00238

[42] N. Živković and A. T. Sarić. 2018. Detection of false data injection attacks using unscented Kalman filter. *J. Mod. Power Syst. Clean Energy* 6, 5 (2018), 847–859. DOI: https://doi.org/10.1007/S40565-018-0413-5/FIGURES/9

[43] Meng Zhang, Chao Shen, Ning He, SiCong Han, Qi Li, Qian Wang, and XiaoHong Guan. 2019. False data injection attacks against smart gird state estimation: Construction, detection and defense. *Sci. China Technol. Sci* 62, 12 (2019), 2077–2087. DOI: https://doi.org/10.1007/S11431-019-9544-7

[44] K. Khanna, B. K. Panigrahi, and A. Joshi. 2020. Priority-based protection against the malicious data injection attacks on state estimation. *IEEE Syst. J.* 14, 2 (2020), 1945–1952. DOI: https://doi.org/10.1109/JSYST.2019.2933023

[45] A. Banerjee and S. P. Maity. 2020. Cognitive radio networks with energy harvesting and eavesdropping-emulation resilience. In *2020 International Conference on COMmunication Systems & NETworkS (COMSNETS).* 873–875. DOI: https://doi.org/10.1109/COMSNETS48256.2020.9027337

[46] B. Ahuja, D. Mishra, and R. Bose. 2020. Optimal green hybrid attacks in secure IoT. *IEEE Wirel. Commun. Lett* 9, 4 (2020), 457–460. DOI: https://doi.org/10.1109/LWC.2019.2958910

[47] P. Shorubiga and T. Kartheeswaran. 2020. Model for mitigating passive eavesdropping attack in IoT. University of Jaffna.

[48] S. R. Rajendran, N. Devi, and M. Jayakumar. 2022. A node reduction technique for trojan detection and diagnosis in IoT hardware devices. *Internet Things* 43–64. DOI: https://doi.org/10.1201/9781003219620-3

[49] H. Mohammed, T. A. Odetola, S. R. Hasan, S. Stissi, I. Garlin, and F. Awwad. 2019. (HIADIoT): Hardware intrinsic attack detection in internet of things; Leveraging power profiling. In *2019 IEEE 62nd International Midwest Symposium on Circuits and Systems (MWSCAS).* 852–855. DOI: https://doi.org/10.1109/MWSCAS.2019.8885183

[50] H. Mohammed, S. R. Hasan, and F. Awwad. 2020. Fusion-on-field security and privacy preservation for IoT edge devices: Concurrent defense against multiple types of hardware trojan attacks. *IEEE Access* 8 (2020), 36847–36862. DOI: https://doi.org/10.1109/ACCESS.2020.2975016

[51] R. Smith, D. Palin, P. P. Ioulianou, V. G. Vassilakis, and S. F. Shahandashti. 2020. Battery draining attacks against edge computing nodes in IoT networks. Taylor & Francisin Cyber-Physical Systems, 96–116. DOI: https://doi.org/10.1080/23335777.2020.1716268

[52] Amjad Alsirhani, Muhammad Ali Khan, Abdullah Alomari, Sauda Maryam, Aiman Younas, Muddesar Iqbal, Muhammad Hameed Siqqidi, and Amjad Ali. 2021. Securing low-power blockchain-enabled IoT devices against energy depletion attack. *ACM Trans. Internet Technol.* 23, 3 (2021). DOI: https://doi.org/10.1145/3511903

[53] P. P. Ioulianou, V. G. Vassilakis, and M. D. Logothetis. 2019. Battery drain denial-of-service attacks and defenses in the internet of things. *J. Telecommun. Inf. Technol.* 2 (2019), 37–45. DOI: https://doi.org/10.26636/JTIT.2019.131919

[54] B. Janes, H. Crawford, and T. J. Oconnor. 2020. Never ending story: Authentication and access control design flaws in shared IoT devices. In *2020 IEEE Security and Privacy Workshops (SPW)*. 104–109. DOI: https://doi.org/10.1109/SPW50608.2020.00033

[55] C. Hahn, J. Kim, H. Kwon, and J. Hur. 2020. Efficient IoT management with resilience to unauthorized access to cloud storage. *IEEE Trans. Cloud Comput.* 10, 2 (2020), 1–1. DOI: https://doi.org/10.1109/TCC.2020.2985046

[56] M. Guerar, L. Verderame, A. Merlo, F. Palmieri, M. Migliardi, and L. Vallerini. 2020. CirclePIN. *ACM Trans. Cyber-phys. Syst.* 4, 3 (2020). DOI: https://doi.org/10.1145/3365995

[57] Z. A. Baig, S. Sanguanpong, S. N. Firdous, V. N. Vo, T. G. Nguyen, and C. So-In. 2020. Averaged dependence estimators for DoS attack detection in IoT networks. *Fut. Gen. Comput. Syst.* 102 (2020), 198–209. DOI: https://doi.org/10.1016/J.FUTURE.2019.08.007

[58] S. Sinha and S. B. 2021. Impact of DoS attack in IoT system and identifying the attacker location for interference attacks. In *2021 6th International Conference on Communication and Electronics Systems (ICCES)*. 657–662. DOI: https://doi.org/10.1109/ICCES51350.2021.9489041

[59] M. Ghahramani, R. Javidan, M. Shojafar, R. Taheri, M. Alazab, and R. Tafazolli. 2021. RSS: An energy-efficient approach for securing IoT service protocols against the DoS attack. *IEEE Internet Things J.* 8, 5 (2021), 3619–3635. DOI: https://doi.org/10.1109/JIOT.2020.3023102

[60] M. M. Shurman, R. M. Khrais, and A. A. Yateem. 2019. IoT denial-of-service attack detection and prevention using hybrid IDS. In *2019 International Arab Conference on Information Technology (ACIT)*. 252–254. DOI: https://doi.org/10.1109/ACIT47987.2019.8991097

[61] A. Munshi, N. A. Alqarni, and N. Abdullah Almalki. 2020. DDOS attack on IOT devices. In *2020 3rd International Conference on Computer Applications & Information Security (ICCAIS)*. DOI: https://doi.org/10.1109/ICCAIS48893.2020.9096818

[62] K. Huang, L. X. Yang, X. Yang, Y. Xiang, and Y. Y. Tang. 2020. A low-cost distributed denial-of-service attack architecture. *IEEE Access* 8 (2020), 42111–42119. DOI: https://doi.org/10.1109/ACCESS.2020.2977112

[63] N. Ravi and S. M. Shalinie. 2020. Learning-driven detection and mitigation of DDoS attack in IoT via SDN-cloud architecture. *IEEE Internet Things J.* 7, 4 (2020), 3559–3570. DOI: https://doi.org/10.1109/JIOT.2020.2973176

[64] F. Hussain, S. G. Abbas, M. Husnain, U. U. Fayyaz, F. Shahzad, and G. A. Shah. 2020. IoT DoS and DDoS attack detection using ResNet. In *2020 IEEE 23rd International Multitopic Conference (INMIC)*. DOI: https://doi.org/10.1109/INMIC50486.2020.9318216

[65] J. Bhayo, S. Hameed, and S. A. Shah. 2020. An efficient counter-based DDoS attack detection framework leveraging software defined IoT (SD-IoT). *IEEE Access* 8 (2020). DOI: https://doi.org/10.1109/ACCESS.2020.3043082

[66] A. Agiollo, M. Conti, P. Kaliyar, T. N. Lin, and L. Pajola. 2021. DETONAR: Detection of routing attacks in RPL-based IoT. *IEEE Trans. Netw. Serv. Manag* 18, 2 (2021), 1178–1190. DOI: https://doi.org/10.1109/TNSM.2021.3075496

[67] R. Sahay, G. Geethakumari, and B. Mitra. 2020. A novel blockchain based framework to secure IoT-LLNs against routing attacks. *Comput* 102, 11 (2020), 2445–2470. DOI: https://doi.org/10.1007/S00607-020-00823-8

[68] Anca Jurcut, Tiberiu Niculcea, Pasika Ranaweera, and Nhien-An Le-Khac. 2020. Security considerations for internet of things: A survey. Springer Nature. DOI: https://doi.org/10.1007/s42979-020-00201-3

[69] H. Wong, T. T. Luo, and T. Luo. 2020. Man-in-the-middle attacks on MQTT-based IoT using BERT based adversarial message generation mobile edge computing view project mobile crowdsensing and crowdsourcing view project man-in-the-middle attacks on MQTT-based IoT using BERT based adversarial mess. In *3rd International Workshop on Artificial Intelligence of Things (AIoT'20)*.

[70] J. Thomas, S. Cherian, S. Chandran, and V. Pavithran. 2020. Man in the middle attack mitigation in LoRaWAN. In *2020 International Conference on Inventive Computation Technologies (ICICT)*. 353–358. DOI: https://doi.org/10.1109/ICICT48043.2020.9112391

[71] D. A. McGrew and J. Viega. 2004. The security and performance of the Galois/counter mode (GCM) of operation. *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)* 3348, 343–355. DOI: https://doi.org/10.1007/978-3-540-30556-9_27

[72] J. J. Kang, K. Fahd, S. Venkatraman, R. Trujillo-Rasua, and P. Haskell-Dowland. 2019. Hybrid routing for man-in-the-middle (MITM) attack detection in IoT networks. In *2019 29th International Telecommunication Networks and Applications Conference (ITNAC)*. DOI: https://doi.org/10.1109/ITNAC46935.2019.9077977

[73] H. Mohammadnia and S. Ben Slimane. 2020. IoT-NETZ: Practical spoofing attack mitigation approach in SDWN network. In *2020 7th International Conference on SoZware Defined Systems (SDS)*. 5–13. DOI: https://doi.org/10.1109/SDS49854.2020.9143903

[74] H. Aldabbas and R. Amin. 2021. A novel mechanism to handle address spoofing attacks in SDN based IoT. *Clust. Comput.* 24, 4 (2021), 1–16. DOI: https://doi.org/10.1007/S10586-021-03309-0

[75] F. Galtier, R. Cayre, G. Auriol, M. Kaaniche, and V. Nicomette. 2020. A PSD-based fingerprinting approach to detect IoT device spoofing. In *2020 IEEE 25th Pacific Rim International Symposium on Dependable Computing (PRDC)*. 40–49. DOI: https://doi.org/10.1109/PRDC50213.2020.00015

[76] S. A. Chaudhry, K. Yahya, F. Al-Turjman, and M. H. Yang. 2020. A secure and reliable device access control scheme for IoT based sensor cloud systems. *IEEE Access* 8 (2020), 139244–139254. DOI: https://doi.org/10.1109/ACCESS.2020.3012121

[77] A. K. Das, M. Wazid, A. R. Yannam, J. J. P. C. Rodrigues, and Y. Park. 2019. Provably secure ECC-based device access control and key agreement protocol for IoT environment. *IEEE Access* 7 (2019), 55382–55397. DOI: https://doi.org/10.1109/ACCESS.2019.2912998

[78] S. Sun, R. Du, S. Chen, and W. Li. 2021. Blockchain-based IoT access control system: Towards security, lightweight, and cross-domain. *IEEE Access* 9 (2021), 36868–36878. DOI: https://doi.org/10.1109/ACCESS.2021.3059863

[79] Y. E. Oktian and S. G. Lee. 2021. BorderChain: Blockchain-based access control framework for the internet of things endpoint. *IEEE Access* 9 (2021), 3592–3615. DOI: https://doi.org/10.1109/ACCESS.2020.3047413

[80] T. P. Latchoumi, M. S. Reddy, and K. Balamurugan. 2020. Applied machine learning predictive analytics to SQL injection attack detection and prevention. *Eur. J. Mol. Clin. Med.* 7, 2 (2020), 3543–3553.

[81] G. M. and P. H. B. 2021. Semantic query-featured ensemble learning model for SQL-injection attack detection in IoT-ecosystems. *IEEE Trans. Reliab.* 71, 2 (2021). DOI: https://doi.org/10.1109/TR.2021.3124331

[82] Q. Li, F. Wang, J. Wang, and W. Li. 2019. LSTM-based SQL injection detection method for intelligent transportation system. *IEEE Trans. Veh. Technol.* 68, 5 (2019), 4182–4191. DOI: https://doi.org/10.1109/TVT.2019.2893675

[83] D. Chen, Q. Yan, C. Wu, and J. Zhao. 2021. SQL injection attack detection and prevention techniques using deep learning. *J. Phys. Conf. Ser.* 1757, 1 (2021), 012055. DOI: https://doi.org/10.1088/1742-6596/1757/1/012055

[84] J. Tournier, F. Lesueur, F. Le Mouël, L. Guyon, and H. Ben-Hassine. 2020. A survey of IoT protocols and their security issues through the lens of a generic IoT stack. *Internet of Things*. 16 (2020), 100264. DOI: https://doi.org/10.1016/J.IOT.2020.100264.

[85] T. Aditya Sai Srinivas and S. S. Manivannan. 2020. Prevention of hello flood attack in IoT using combination of deep learning with improved rider optimization algorithm. *Comput. Commun.* 163 (2020), 162–175. DOI: https://doi.org/10.1016/J.COMCOM.2020.03.031.

[86] X. Ding, F. Xiao, M. Zhou, and Z. Wang. 2020. Active link obfuscation to thwart link-flooding attacks for internet of things. In *2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*. 217–224. DOI: https://doi.org/10.1109/TRUSTCOM50675.2020.00040

[87] A. Gajbhiye, D. Sen, A. Bhatt, and G. Soni. 2020. DPLPLN: Detection and prevention from flooding attack in IoT. In *2020 International Conference on Smart Electronics and Communication (ICOSEC)*. 704–709. DOI: https://doi.org/10.1109/ICOSEC49089.2020.9215381

[88] B. T. Devi, S. Shitharth, and M. A. Jabbar. 2020. An appraisal over intrusion detection systems in cloud computing security attacks. In *2020 2nd International Conference on Innovative Mechanisms for Industry Applications (ICIMIA)*. 722–727. DOI: https://doi.org/10.1109/ICIMIA48430.2020.9074924

[89] A. McDole, M. Abdelsalam, M. Gupta, and S. Mittal. 2020. Analyzing CNN based behavioural malware detection techniques on cloud IaaS. *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 12403 LNCS 64–79. DOI: https://doi.org/10.1007/978-3-030-59635-4_5/FIGURES/10

[90] T. Panker and N. Nissim. 2021. Leveraging malicious behavior traces from volatile memory using machine learning methods for trusted unknown malware detection in Linux cloud environments. *Knowl.-based Syst.* 226 (2021), 107095. DOI: https://doi.org/10.1016/J.KNOSYS.2021.107095

[91] S. Modak, K. Majumder, and D. De. 2021. Vulnerability of cloud: Analysis of XML signature wrapping attack and countermeasures. *Adv. Intell. Syst. Comput* 1255 (2021), 755–765. DOI: https://doi.org/10.1007/978-981-15-7834-2_70/TABLES/1

[92] M. D. Hossain, H. Ochiai, F. Doudou, and Y. Kadobayashi. 2020. SSH and FTP brute-force attacks detection in computer networks: LSTM and machine learning approaches. In *2020 5th International Conference on Computer and Communication Systems (ICCCS)*. 491–497. DOI: https://doi.org/10.1109/ICCCS49078.2020.9118459

[93] J. Park, J. Kim, B. B. Gupta, and N. Park. Network log-based SSH brute-force attack detection model. Computers, Materials & Continua. DOI: https://doi.org/10.32604/cmc.2021.015172

[94] M. M. Raikar and S. M. Meena. 2021. 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)*. 72–77. DOI: https://doi.org/10.1109/ICSCCC51823.2021.9478131

[95] M. Šarac, N. Pavlović, N. Bacanin, F. Al-Turjman, and S. Adamović. 2021. Increasing privacy and security by integrating a blockchain secure interface into an IoT device security gateway architecture. *Energy Rep.* 7 (2021), 8075–8082. DOI: https://doi.org/10.1016/J.EGYR.2021.07.078

[96] Nikola Pavlović, Marko Šarac, Saša Adamović, Muzafer Saračević, Khaleel Ahmad, Nemanja Maček, and Deepak Kumar Sharma. 2021. An approach to adding simple interface as security gateway architecture for IoT device. *Multimed. Tools Appl.* 81, 26 (2021), 1–16. DOI: https://doi.org/10.1007/S11042-021-11389-8/FIGURES/5

[97] S. A. Suresh and R. J. Priyadarsini. 2022. Design of maintaining data security on IoT data transferred through IoT gateway system to cloud storage. *Int. J. Comput. Netw. Appl.* 9, 1 (2022), 135–149. DOI: https://doi.org/10.22247/ijcna/2022/211632

[98] R. Khan, K. McLaughlin, B. Kang, D. Laverty, and S. Sezer. 2021. A novel edge security gateway for end-to-end protection in industrial internet of things. In *2021 IEEE Power & Energy Society General Meeting (PESGM)*. DOI: https://doi.org/10.1109/PESGM46819.2021.9638002

[99] C. Peng, J. Chen, P. Vijayakumar, N. Kumar, and D. He. 2021. Efficient distributed decryption scheme for IoT gateway-based applications. *ACM Trans. Internet Technol.* 21, 1 (2021). DOI: https://doi.org/10.1145/3414475

[100] A. Pillai, M. Sindhu, and K. V. Lakshmy. 2019. Securing firmware in internet of things using blockchain. In *2019 5th International Conference on Advanced Computing & Communication Systems (ICACCS)*. 329–334. DOI: https://doi.org/10.1109/ICACCS.2019.8728389

[101] A. Yohan and N. W. Lo. 2020. FOTB: A secure blockchain-based firmware update framework for IoT environment. *Int. J. Inf. Secur* 19, 3 (2020), 257–278. DOI: https://doi.org/10.1007/S10207-019-00467-6/TABLES/5

[102] A. Anastasiou, P. Christodoulou, K. Christodoulou, V. Vassiliou, and Z. Zinonos. 2020. IoT device firmware update over LoRa: The blockchain solution. In *2020 16th International Conference on Distributed Computing in Sensor Systems (DCOSS)*. 404–411. DOI: https://doi.org/10.1109/DCOSS49796.2020.00070

[103] M. Khari, A. K. Garg, A. H. Gandomi, R. Gupta, R. Patan, and B. Balusamy. 2020. Securing data in internet of things (IoT) using cryptography and steganography techniques. *IEEE Trans. Syst. Man, Cybern. Syst.* 50, 1 (2020), 73–80. DOI: https://doi.org/10.1109/TSMC.2019.2903785

[104] S. Sivagowry and M. Durairaj. 2014. PSO – An intellectual technique for feature reduction in heart malady anticipation data. *Int. J. Adv. Res. Comput. Sci. Softw. Eng.* 4, 9 (2014), 735–742. DOI: https://doi.org/10.23956/IJARCSSE

[105] S. Chandra, S. Paira, S. S. Alam, and G. Sanyal. 2014. A comparative survey of symmetric and asymmetric key cryptography. In *2014 International Conference on Electronics, Communication and Computational Engineering (ICECCE)*. 83–93. DOI: https://doi.org/10.1109/ICECCE.2014.7086640

[106] S. Sangeeta and E. A. Kaur. 2017. A review on symmetric key cryptography algorithms. *Int. J. Adv. Res. Comput. Sci.* 8, 4 (2017). DOI: https://doi.org/10.26483/IJARCS.V8I4.3777

[107] M. B. Yassein, S. Aljawarneh, E. Qawasmeh, W. Mardini, and Y. Khamayseh. 2018. Comprehensive study of symmetric key and asymmetric key encryption algorithms. In *2017 International Conference on Engineering and Technology (ICET)*. 1–7. DOI: https://doi.org/10.1109/ICENGTECHNOL.2017.8308215

[108] S. Rani and H. Kaur. 2017. Technical review on symmetric and asymmetric cryptography algorithms. *Int. J. Adv. Res. Comput. Sci.* 8, 4 (2017). DOI: https://doi.org/10.26483/IJARCS.V8I4.3728

[109] I. E. Salem, A. M. Salman, and M. M. Mijwil. 2019. A survey: Cryptographic hash functions for digital stamping. *J. Southw. Jiaotong Univ.* 54, 6 (2019). DOI: https://doi.org/10.35741/ISSN.0258-2724.54.6.2

[110] D. Wang, Y. Jiang, H. Song, F. He, M. Gu, and J. Sun. 2017. Verification of implementations of cryptographic hash functions. *IEEE Access* 5 (2017), 7816–7825. DOI: https://doi.org/10.1109/ACCESS.2017.2697918

[111] A. Kumar, V. Jain, and A. Yadav. 2020. A new approach for security in cloud data storage for IOT applications using hybrid cryptography technique. In *2020 International Conference on Power Electronics & IoT Applications in Renewable Energy and its Control (PARC)*. 514–517. DOI: https://doi.org/10.1109/PARC49193.2020.236666.

[112] G. Sittampalam and N. Ratnarajah. 2020. Enhanced symmetric cryptography for IoT using novel random secret key approach. In *2020 2nd International Conference on Advancements in Computing (ICAC)*. 398–403. DOI: https://doi.org/10.1109/ICAC51239.2020.9357316

[113] J. Qiu, Z. Tian, C. Du, Q. Zuo, S. Su, and B. Fang. 2020. A survey on access control in the age of internet of things. *IEEE Internet Things J.* 7, 6 (2020), 4682–4696. DOI: https://doi.org/10.1109/JIOT.2020.2969326

[114] Muhammad Umar AZab, Yasir Munir, Ariyo Oluwasanmi, Zhiguang Qin, Muhammad Haris Aziz, Zakria, Ngo Tung Son, and Van Dinh Tran. 2020. A hybrid access control model with dynamic COI for secure localization of satellite and IoT-based vehicles. *IEEE Access* 8 (2020), 24196–24208. DOI: https://doi.org/10.1109/ACCESS.2020.2969715

[115] D. Yu, L. Zhang, Y. Chen, Y. Ma, and J. Chen. 2020. Large-scale IoT devices firmware identification based on weak password. *IEEE Access* 8 (2020), 7981–7992. DOI: https://doi.org/10.1109/ACCESS.2020.2964646

[116] F. M. Alfard, A. Ali Keshlaf, and O. M. Bouzid. 2021. IoTGazePass: A new password scheme for IoT applications. IEEE, 299–304. DOI: https://doi.org/10.1109/MI-STA52233.2021.9464390.

[117] K. Zandberg, K. Schleiser, F. Acosta, H. Tschofenig, and E. Baccelli. 2019. Secure firmware updates for constrained IoT devices using open standards: A reality check. *IEEE Access* 7 (2019), 71907–71920. DOI: https://doi.org/10.1109/ACCESS.2019.2919760

[118] N. Mtetwa, P. Tarwireyi, and M. Adigun. 2019. Secure the internet of things software updates with Ethereum blockchain. In *2019 International Multidisciplinary Information Technology and Engineering Conference (IMITEC)*. DOI: https://doi.org/10.1109/IMITEC45504.2019.9015865

[119] A. Aborujiah, A. E. F. M. Elsebaie, and S. A. Mokhtar. 2021. IoT MEMS: IoT based paradigm for medical equipment management systems of ICUs in light of COVID-19 outbreak. *IEEE Access*. 9 (2021). DOI: https://doi.org/10.1109/ACCESS.2021.3069255

[120] Ibrahim Bello, Haruna Chiroma, Usman A. Abdullahi, Abdulsalam Ya'u Gital, Fatsuma Jauro, Abdullah Khan, Julius O. Okesola, and Shafi'i M. Abdulhamid. 2020. Detecting ransomware attacks using intelligent algorithms: Recent development and next direction from deep learning and big data perspectives. *J. Amb. Intell. Hum. Comput.* 12, 9 (2020), 8699–8717. DOI: https://doi.org/10.1007/S12652-020-02630-7

[121] M. Humayun, N. Z. Jhanjhi, A. Alsayat, and V. Ponnusamy. 2021. Internet of things and ransomware: Evolution, mitigation and prevention. *Egypt. Inform. J.* 22, 1 (2021), 105–117. DOI: https://doi.org/10.1016/J.EIJ.2020.05.003

[122] Y. T. Lee et al. 2020. Cross platform IoT- malware family classification based on printable strings. In *2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*. 775–784. DOI: https://doi.org/10.1109/TRUSTCOM50675.2020.00106

[123] J. Jeon, J. H. Park, and Y. S. Jeong. 2020. Dynamic analysis for IoT malware detection with convolution neural network model. *IEEE Access* 8 (2020), 96899–96911. DOI: https://doi.org/10.1109/ACCESS.2020.2995887

[124] C. Jiang, J. Kuang, and S. Wang. 2019. Home IoT intrusion prevention strategy based on edge computing. In *2019 IEEE 2nd International Conference on Electronics and Communication Engineering (ICECE)*. 94–98. DOI: https://doi.org/10.1109/ICECE48499.2019.9058536

[125] G. Abdelmoumin, D. B. Rawat, and A. Rahman. 2021. On the performance of machine learning models for anomaly-based intelligent intrusion detection systems for the internet of things. *IEEE Internet Things J.* 9, 6 (2021), 1–1. DOI: https://doi.org/10.1109/JIOT.2021.3103829

[126] A. Yahyaoui, H. Lakhdhar, T. Abdellatif, and R. Attia. 2021. Machine learning based network intrusion detection for data streaming IoT applications. In *2021 21st ACIS International Winter Conference on SoZware Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD-Winter)*. 51–56. DOI: https://doi.org/10.1109/SNPDWINTER52325.2021.00019

[127] C. Ioannou and V. Vassiliou. 2020. Experimentation with local intrusion detection in IoT networks using supervised learning. In *2020 16th International Conference on Distributed Computing in Sensor Systems (DCOSS)*. 423–428. DOI: https://doi.org/10.1109/DCOSS49796.2020.00073

[128] S. Joshi and E. Abdelfattah. 2020. Efficiency of different machine learning algorithms on the multivariate classification of IoT botnet attacks. In *2020 11th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)*. 0517–0521. DOI: https://doi.org/10.1109/UEMCON51285.2020.9298095

[129] Hanwen Liu, Xiaohan Helu, Chengjie Jin, Hui Lu, Zhihong Tian, Xiaojiang Du, and Khalid Abualsaud. 2020. A malware detection method for health sensor data based on machine learning. In *2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT)*. 277–282. DOI: https://doi.org/10.1109/ICIOT48696.2020.9089478

[130] A. Makkar, S. Garg, N. Kumar, M. S. Hossain, A. Ghoneim, and M. Alrashoud. 2021. An efficient spam detection technique for IoT devices using machine learning. *IEEE Trans. Industr.. Inform.* 17, 2 (2021), 903–912. DOI: https://doi.org/10.1109/TII.2020.2968927

[131] R. Nadia, B. A. Tama, and J. S. Song. 2020. Seamless human impedance-based IoT authentication with machine learning techniques. In *2020 International Conference on Information and Communication Technology Convergence (ICTC)*. 339–343. DOI: https://doi.org/10.1109/ICTC49870.2020.9289323

[132] Y. W. Chen, J. P. Sheu, Y. C. Kuo, and N. Van Cuong. 2020. Design and implementation of IoT DDoS attacks detection system based on machine learning. In *2020 European Conference on Networks and Communications (EuCNC)*. 122–127. DOI: https://doi.org/10.1109/EUCNC48522.2020.9200909

[133] M. M. N. Aboelwafa, K. G. Seddik, M. H. Eldefrawy, Y. Gadallah, and M. Gidlund. 2020. A machine-learning-based technique for false data injection attacks detection in industrial IoT. *IEEE Internet Things J.* 7, 9 (2020), 8462–8471. DOI: https://doi.org/10.1109/JIOT.2020.2991693

[134] T. M. Hoang, N. M. Nguyen, and T. Q. Duong. 2020. Detection of eavesdropping attack in UAV-aided wireless systems: Unsupervised learning with one-class SVM and k-means clustering. *IEEE Wirel. Commun. Lett.* 9, 2 (2020), 139–142. DOI: https://doi.org/10.1109/LWC.2019.2945022

[135] V. Rey, P. M. Sánchez Sánchez, A. Huertas Celdrán, and G. Bovet. 2022. Federated learning for malware detection in IoT devices. *Comput. Netw.* 204 (2022), 108693. DOI: https://doi.org/10.1016/J.COMNET.2021.108693

[136] S. T. Mehedi, A. Anwar, Z. Rahman, K. Ahmed, and R. Islam. 2023. Dependable intrusion detection system for IoT: A deep transfer learning based approach. *IEEE Trans. Ind. Inform.* 19, 1 (2023), 1006–1017. DOI: https://doi.org/10.1109/TII.2022.3164770

[137] H. Lin, S. Garg, J. Hu, X. Wang, M. J. Piran, and M. S. Hossain. 2022. Data fusion and transfer learning empowered granular trust evaluation for internet of things. *Inf. Fusion* 78 (2022), 149–157. DOI: https://doi.org/10.1016/J.INFFUS.2021.09.001

[138] B. Xue, H. Zhao, and W. Yao. 2022. Deep transfer learning for IoT intrusion detection. In *2022 3rd International Conference on Computing, Networks and Internet of Things (CNIOT)*. 88–94. DOI: https://doi.org/10.1109/CNIOT55862.2022.00023

[139] Areej A. Malibari, Saud S. Alotaibi, Reem Alshahrani, Sami Dhahbi, Rana Alabdan, Fahd N. Al-wesabi, and Anwer Mustafa Hilal. 2022. A novel metaheuristics with deep learning enabled intrusion detection system for secured smart environment. *Sustain. Energy Technol. Assessments* 52 (2022), 102312. DOI: https://doi.org/10.1016/J.SETA.2022.102312

[140] S. S. Kareem, R. R. Mostafa, F. A. Hashim, and H. M. El-Bakry. 2022. An effective feature selection model using hybrid metaheuristic algorithms for IoT intrusion detection. *Sensors* 22, 4 (2022), 1396. DOI: https://doi.org/10.3390/S22041396

[141] S. Saif, P. Das, S. Biswas, M. Khari, and V. Shanmuganathan. 2022. HIIDS: Hybrid intelligent intrusion detection system empowered with machine learning and metaheuristic algorithms for application in IoT based healthcare. *Microprocess. Microsyst.* 104622. DOI: https://doi.org/10.1016/J.MICPRO.2022.104622

[142] Y. Otoum, S. K. Yadlapalli, and A. Nayak. 2022. FTLIoT: A federated transfer learning framework for securing IoT. In *GLOBECOM 2022 - 2022 IEEE Global Communications Conference*. 1146–1151. DOI: https://doi.org/10.1109/GLOBECOM48099.2022.10001461

[143] Y. Otoum, D. Liu, and A. Nayak. 2022. DL-IDS: A deep learning–based intrusion detection framework for securing IoT. *Trans. Emerg. Telecommun. Technol* 33, 3 (2022), e3803. DOI: https://doi.org/10.1002/ETT.3803

[144] W. H. Kuo and Y. C. Wang. 2019. An energy-saving edge computing and transmission scheme for IoT mobile devices. In *2019 IEEE 8th Global Conference on Consumer Electronics (GCCE)*. 443–444. DOI: https://doi.org/10.1109/GCCE46687.2019.9015228

[145] R. Amin, M. Hussain, S. Mohsan Raza, M. Alhameed, F. Jeribi, and A. Tahir. 2020. Edge-computing with graph computation: A novel mechanism to handle network intrusion and address spoofing in SDN hybrid SDN view project efficient handling of network policy change in SDN view project edge-computing with graph computation: A novel mechanism to handle network intrusion and address spoofing in SDN. *C. C.* 65, 3 (2020), 1869–1890. DOI: https://doi.org/10.32604/cmc.2020.011758

[146] Laisen Nie, Yixuan Wu, Xiaojie Wang, Lei Guo, Guoyin Wang, Xinbo Gao, and Shengtao Li. 2021. Intrusion detection for secure social internet of things based on collaborative edge computing: A generative adversarial network-based approach. *IEEE Trans. Comput. Soc. Syst.* 9, 1 (2021). DOI: https://doi.org/10.1109/TCSS.2021.3063538

[147] Junxia Li, Jinjin Cai, Fazlullah Khan, Ateeq Ur Rehman, Venki Balasubramaniam, Jiangfeng Sun, and P. Venu. 2020. A secured framework for SDN-based edge computing in IoT-enabled healthcare system. *IEEE Access* 8 (2020), 135479–135490. DOI: https://doi.org/10.1109/ACCESS.2020.3011503

[148] W. Ahmed, S. M. Hizam, I. Sentosa, J. Ali, and T. Ali. 2020. Structural equation modeling for acceptance of cloud computing. In *2019 International Conference on Advances in the Emerging Computing Technologies (AECT)*. DOI: https://doi.org/10.1109/AECT47998.2020.9194206

[149] A. A. A. Alkhatib, T. Sawalha, and S. Alzu'Bi. 2020. Load balancing techniques in software-defined cloud computing: An overview. In *2020 Seventh International Conference on SoZware Defined Systems (SDS)*. 240–244. DOI: https://doi.org/10.1109/SDS49854.2020.9143874

[150] A. Markandey, P. Dhamdhere, and Y. Gajmal. 2019. Data access security in cloud computing: A review. In *2018 International Conference on Computing, Power and Communication Technologies (GUCON)*. 633–636. DOI: https://doi.org/10.1109/GUCON.2018.8675033

[151] P. Yang, N. Xiong, and J. Ren. 2020. Data security and privacy protection for cloud storage: A survey. *IEEE Access* 8 (2020), 131723–131740. DOI: https://doi.org/10.1109/ACCESS.2020.3009876

[152] S. Xiong, Q. Ni, L. Wang, and Q. Wang. 2020. SEM-ACSIT: Secure and efficient multiauthority access control for IoT cloud storage. *IEEE Internet Things J.* 7, 4 (2020), 2914–2927. DOI: https://doi.org/10.1109/JIOT.2020.2963899

[153] K. Riad, T. Huang, and L. Ke. 2020. A dynamic and hierarchical access control for IoT in multi-authority cloud storage. *J. Netw. Comput. Appl.* 160, 102633. DOI: https://doi.org/10.1016/J.JNCA.2020.102633

[154] M. Rashid, S. A. Parah, A. R. Wani, and S. K. Gupta. 2020. Securing e-health IoT data on cloud systems using novel extended role based access control model. *Internet Things Concepts Appl.* 473–489. DOI: https://doi.org/10.1007/978-3-030-37468-6_25

[155] L. Ding, Z. Wang, X. Wang, and D. Wu. 2020. Security information transmission algorithms for IoT based on cloud computing. *Comput. Commun* 155 (2020), 32–39. DOI: https://doi.org/10.1016/J.COMCOM.2020.03.010

[156] M. Anuradha, T. Jayasankar, N. B. Prakash, Mohamed Yacin Sikkandar, G. R. Hemalakshmi, C. Bharatiraja, and A. Sagai Francis Britto. 2021. IoT enabled cancer prediction system to enhance the authentication and security using cloud computing. *Microprocess. Microsyst.* 80 (2021), 103301. DOI: https://doi.org/10.1016/J.MICPRO.2020.103301

[157] M. Wang and Q. Zhang. 2020. Optimized data storage algorithm of IoT based on cloud computing in distributed system. *Comput. Commun.* 157 (2020), 124–131. DOI: https://doi.org/10.1016/J.COMCOM.2020.04.023

[158] R. SaiSindhuTheja and G. K. Shyam. 2021. An efficient metaheuristic algorithm based feature selection and recurrent neural network for DoS attack detection in cloud computing environment. *Appl. Soft Comput.* 100 (2021), 106997. DOI: https://doi.org/10.1016/J.ASOC.2020.106997

[159] R. Saxena and S. Dey. 2019. DDoS attack prevention using collaborative approach for cloud computing. *Clust. Comput.* 23, 2 (2019), 1329–1344. DOI: https://doi.org/10.1007/S10586-019-02994-2

[160] H. H. Pajooh, M. Rashid, F. Alam, and S. Demidenko. 2021. Hyperledger fabric blockchain for securing the edge internet of things. *Sensors* 21, 2 (2021), 359. DOI: https://doi.org/10.3390/S21020359

[161] L. Hang and D.-H. Kim. 2019. Design and implementation of an integrated IoT blockchain platform for sensing data integrity. *Sensors* 19, 10 (2019), 2228. DOI: https://doi.org/10.3390/S19102228

[162] A. M. Al-Madani and A. T. Gaikwad. 2020. IoT data security via blockchain technology and service-centric networking. In *2020 International Conference on Inventive Computation Technologies (ICICT).* 17–21. DOI: https://doi.org/10.1109/ICICT48043.2020.9112521

[163] M. Bhandary, M. Parmar, and D. Ambawade. 2020. A blockchain solution based on directed acyclic graph for IoT data security using IoTA tangle. IEEE, 827–832. DOI: https://doi.org/10.1109/ICCES48766.2020.9137858

[164] H. Xu, Q. He, X. Li, B. Jiang, and K. Qin. 2020. BDSS-FA: A blockchain-based data security sharing platform with fine-grained access control. *IEEE Access* 8 (2020), 87552–87561. DOI: https://doi.org/10.1109/ACCESS.2020.2992649

[165] P. C. Wei, D. Wang, Y. Zhao, S. K. S. Tyagi, and N. Kumar. 2020. Blockchain data-based cloud data integrity protection mechanism. *Fut. Gen. Comput. Syst.* 102 (2020), 902–911. DOI: https://doi.org/10.1016/J.FUTURE.2019.09.028

[166] Q. Zhao, S. Chen, Z. Liu, T. Baker, and Y. Zhang. 2020. Blockchain-based privacy-preserving remote data integrity checking scheme for IoT information systems. *Inf. Process. Manag.* 57, 6 (2020), 102355. DOI: https://doi.org/10.1016/J.IPM.2020.102355

[167] H. Liu, D. Han, and D. Li. 2020. Fabric-IoT: A blockchain-based access control system in IoT. *IEEE Access* 8 (2020), 18207–18218. DOI: https://doi.org/10.1109/ACCESS.2020.2968492

[168] Zhihua Cui, Fei Xue, Shiqiang Zhang, Xingjuan Cai, Yang Cao, Wensheng Zhang, and Jinjun Chen. 2020. A hybrid blockchain-based identity authentication scheme for multi-WSN. *IEEE Trans. Serv. Comput.* 13, 2 (2020), 241–251. DOI: https://doi.org/10.1109/TSC.2020.2964537

[169] F. A. A. Lins and M. Vieira. 2021. Security requirements and solutions for IoT gateways: A comprehensive study. *IEEE Internet Things J.* 8, 11 (2021), 8667–8679. DOI: https://doi.org/10.1109/JIOT.2020.3041049

[170] B. L. Tait. 2021. Aspects of biometric security in internet of things devices. *Adv. Sci. Technol. Secur. Appl.* 169–186. DOI: https://doi.org/10.1007/978-3-030-60425-7_7

[171] Xinyu Jiang, Xiangyu Liu, Jiahao Fan, Xinming Ye, Chenyun Dai, Edward A. Clancy, Dario Farina, and Wei Chen. 2021. Enhancing IoT security via cancelable HD-sEMG-based biometric authentication password, encoded by gesture. *IEEE Internet Things J.* 8, 22 (2021). DOI: https://doi.org/10.1109/JIOT.2021.3074952

Received 15 June 2022; revised 28 April 2023; accepted 21 August 2023