Hindawi
Security and Communication Networks
Volume 2021, Article ID 1723535, 21 pages
https://doi.org/10.1155/2021/1723535

Review Article

Home Automation and RFID-Based Internet of Things Security: Challenges and Issues

Haram Fatima,[1] Habib Ullah Khan,[2] and Shahzad Akbar[1]

[1]*Department of Computing, Riphah International University, Faisalabad Campus, Faisalabad, Punjab 38000, Pakistan*
[2]*Department of Accounting and Information Systems, College of Business and Economics, Qatar University, Doha, Qatar*

Correspondence should be addressed to Shahzad Akbar; shahzadakbarbzu@gmail.com

Received 12 July 2021; Revised 6 September 2021; Accepted 28 September 2021; Published 28 November 2021

Academic Editor: Shehzad Ashraf Chaudhry

Internet of Things (IoT) protection refers to the software field related to securing the Internet of Things and associated linked devices and systems. The IoT is a system of interconnected computers, sensors, actuators, or people on the World Wide Web (WWW). All these different devices have a unique identity in the IoT and must convey data across the network automatically. If computers are not adequately secured, allowing them to connect to the Internet exposes them to a range of serious vulnerabilities. Because the consequences of IoT failures are severe, it is necessary to observe and analyze security issues related to IoT. The prime goal of IoT security is to protect personal safety, while also guaranteeing and ensuring accessibility. In the context of IoT technology, the present study conducts a systematic literature review that analyzes the security problems associated with commercial and educational applications of home automation and details the technical possibilities of IoT with respect to the network layer. In this systematic review, we discuss how current contexts result in the inability of designers of IoT devices to enhance their cyber-security initiatives. Typically, application developers are responsible for training themselves to understand recent security advancements. As a result, active participation on the ridge scale with passive improvement can be achieved. A comparative analysis of the literature was conducted. The main objective of this research is to provide an overview of current IoT security research in home automation, particularly those using authentication methods in different devices, and related technologies in radio frequency identification (RFID) on network layers. IoT security issues are addressed, and various security problems in each layer are analyzed. We describe cross-layer heterogeneous integration as a domain of IoT and demonstrate how it can provide some promising solutions.

1. Introduction

In recent years, the Internet of Things (IoT) has expanded rapidly as network technology device access and related analytical systems have improved. IoT protection refers to techniques and systems designed to protect IoT infrastructure and networks [1]. Defense against threats is still not always handled because the networking systems are viewed as accountable for the threats. The IoT is an advanced protection model that allows for interactions between a diverse range of devices via routing protocols. It typically refers to engines, network devices, and other objects that are all digitally integrated; these items are interlinked with different sensor technologies to provide improved accessibility on a given platform. Based on this interconnectedness, it is possible to collect and share data and information among these machines [2]. There are several research fields in which IoT devices could be deployed to provide performance, infrastructure, and support improvements. For example, applications pertaining to climatic conditions, living space accommodations, and advanced education can all benefit from IoT implementation [3]. Generally, IoT gadget usability requires the system to detect devices and conduct observations and simulations to make the necessary changes to improve the gadget's performance.

One example of a field for which the use of IoT devices is important is in clinical healthcare settings. Clinicians' welfare plays a vital role in the success of these healthcare systems. In these settings, IoT devices can be used to measure and control pulses, heart rate, and other body functions.

Advanced medical equipment assists with the practice of medicine in the event of a disaster, allowing doctors to quickly assess medical symptoms and provide early diagnosis therapy for patients [4]. The IoT also affects profitability for its users, by allowing for innovative products to be designed, capable of operating in unique environments and improving functionality over existing methods. IoT methods have been created based on a wide range of previous technologies. Ultimately, structures based on a three-layer framework that incorporates awareness, systems, and software [5] in the application layer of the IoT are based on a variety of technologies [6].

Previous researchers have developed competing perspectives regarding privacy and protection at all levels of IoT systems and how to handle vulnerability in the form of security threats [5, 6]. The existing resources for IoT sensor node optimization and replication are the devices often used to develop rapid advancements in academic IoT security research [7]. Previous research has provided a systematic list of prototypes used in the current research [8]. The most commonly used emulator for IoT information security is NS 3, because many new security procedures develop their own security protocol and the assessor method provided by NS 3 is required, such as for the Automated Validation of Internet Security Protocols and Applications (AVISPA) [5]. The current paper surveys the current state of IoT security issues and research from 2016 to 2021. In particular, emphasis is placed on protection and privacy issues in IoT, as well as on the effects of malicious attackers, which have the ability to damage and crash IoT systems. Our goal is that future research will incorporate the simulation models and the improved IoT security divisions outlined here. The previous research regarding IoT security [6] was collected and evaluated using the credible Network of Information and Google searches.

The main contribution of this paper is its comprehensive comparison of topics such as IoT, security strategies, and process simulations, including the results from the most recently published research. Principally, it addresses the importance and necessity of applications spanning from hospital administrators, commercial facilities, agile cities, and home automation. This study focuses on different design architectures and IoT applications that attempt to solve problems in these varied contexts. This is particularly important, because the IoT infrastructure is vulnerable at each level from previous failed security protections, for which there are known exploits. This results in a number of security issues, for which suitable solutions are necessary. A systematic overview of vulnerabilities and associated issues is described here. We highlight the value of and need for extending and adopting IoT methods for retrieving data by highlighting current problems and questions that arise in this field. In addition, we address commercial, corporate, and industry requirement issues and user-related security issues and their prevention. The roles of the network layers and authentication systems are also defined here. In IoT, there exist different network layer perspectives. By gathering and screening and data routing from unrelated IoT systems, the network gateways act as an intermediary for sending and receiving data from different sensors. This method involves identifying IP addresses within the network and granting permissions to authentic users.

The IoT ecosystem that addresses these issues [9] is shown in Figure 1. Table 1 presents the main contributions of this study.

The rest of the paper is organized as follows: Section 2 discusses the related work in IoT. In Section 3, the research selection and assessment method are presented to classify IoT security issues. Section 4 presents IoT challenges and their security issues. The current research on IoT security issues, research techniques, and comparisons between them are presented in Section 5. The weaknesses of IoT authentication methods are discussed in Section 6. General IoT security issues are presented in Section 7. Section 8 presents systematic literature review (SLR) questions and discussion and questions related to IoT. Section 9 elaborates on the conclusion and future directions.

2. Related Work

Previous researchers [1] have examined many aspects of IoT systems, as well as innovations related to them. The IoT is a platform that is required to help IoT-connected networks and devices. The potential to design IoT devices based on adaptability considerations and their effectiveness and accuracy has been the subject of investigation. For example, the authors of [2] presented an organizing IoT ecosystem. Similarly, security video deformations with decreased IoT access have been proposed [3, 11], in an attempt to improve the privacy of transactional devices. Yet other work on IoT [4, 12] focused on security issues when cloud and edge services mix, wherein encryption is a form of the cloud. The aim, characteristics, and structural problems of IoT devices have been reviewed in the previous literature [7, 9, 13].

Other comparable methods of utilization based on different input data have been evaluated, and the results suggest that improving transit maintenance could produce positive economic effects [5, 9]. The IoT additionally assists farming by allowing them to deploy embedded sensors to track their food, monitor their crops, and control the thermal properties of their soil [10, 14]. In one previous study [15], the authors identified security challenges and design associated with IoT. From a more general perspective, IoT, its features, and its various method designs have been the subject of multiple reviews [16, 17]. The structure of the IoT and the considerable difficulties resulting from IoT issues have also been discussed deeply [18]. Researchers [19, 20] have also examined the middleware structure and provided a comprehensive review of its methodologies, strategies, and problems.

Service-oriented architecture (SOA) refers to a method of design that focuses on delivering resources. Intended to connect additional functionalities, it is also referred to as the network units of a system via its terminals and mechanisms [21, 22]. In this article, we will examine some of the most significant data protection challenges in the world of security and IoT applications [23, 24]. Because the layers of the proposed ecosystem are vulnerable to cyber-attacks, the

Figure 1: IoT ecosystem.

attacker does not have access to confidential information. IoT devices are resistant to several security risks; however, assaults can lead to a shortage of electrical energy, memory, and processing capability of the IoT devices [25, 26]. In addition, the insertion of malicious software, denial-of-service threats [27, 28], privilege escalation, and harmful infections [29] all are examples of attacks that can compromise IoT security if a hacker exploits access to the database [30]. This method of attack, which uses a code encryption algorithm, should be implemented into IoT to prevent against assault [31, 32].

We discuss the IoT security issues, privacy challenges, challenges of authentication on cloud computing and other systems, malware attacks on network layers of home automation, and RFID models. These systems and applications can provide information regarding why the attacker hacked the authentication system. The IoT structure, generally, envisions a 3-layer system that consists of a perspective tier, a channel layer, and a runtime environment layer.

Elements that comprise IoT systems are hardware devices, communication messaging protocols, and interface services [33]. These technologies are the most crucial aspects of IoT, especially embedded systems. For these systems, at the hardware level, the thickness of the microcontroller is based on the ARM, MIPS, or X86 chip design [34–36]. Protection technology, such as an encrypted code converter or a safety chip, can be included during the planning process [37, 38]. IoT applications are used commonly in Automatic Identification Systems (AIS). IoT applications use the operating system, which itself contains a hardware abstraction layer, physical layer surface, connectivity drivers, and features like program separation, secure installations, and software environment. There are desktop applications for the application software layer's cryptographic protocols, third-party libraries, and drivers.

Hardware design is also essential for protecting connected devices, implementing IoT identification abilities, and edge traffic protection [39]. The need for a private bootloading procedure, how to implement data encryption during the oriented method, and how to achieve accessible transactions are all difficulties associated with IoT devices [40]. The essential part of an IoT system is to define how the protocols for transmission and communication through messaging are handled [41]. However, in the past, many IoT systems have lacked adequate security [42]. A network of handheld devices can communicate directly with cloud computing through connections such as Amazon Kinesis [43]. IoT involves combining wireless sensor networks for all communication modalities governed by concepts [44].

The previous weaknesses of IoT security design have been suggested by existing review papers. A systematic literature survey is necessary to remedy the following deficiencies [45]:

Table 1: Main contributions of this study.

Existing method	Working methodology	Weaknesses with solution	Future work with improvements
Wei et al.	Authentication at cloud computing performed in [1].	Password authentication is used here for quick devices. Form registration methods are used on the login page. Then, the attacker hacks personal data, such as passwords or user identification codes. In the design solution, a person must protect their data through different verification steps and update their data via nonidentical screening methods. Because of the deterministic function of a strong password, it is necessary to regularly reset the password to maintain security.	In the future, we will use secure apps for digital encryption tools. Experienced users can use different verification apps. For future improvements, security will be tightened using different network IoT algorithms in the actual IoT devices.
Gupta et al.	IoT issues in different network layers performed in [4].	The applications or network layers do not perform their intended function. When the user attaches the IoT device to a different network, it gives the appropriate solution. The user enhances the readability and organization of the device.	In the future, they plan to train different phone apps and VPN secure methods and test them at different levels. Only people who are familiar with a device will know how to use it; it will possess login passwords for their items. Facial verification and other pattern systems can also accomplish several levels of security objectives.
Hageman et al.	IoT privacy and protection challenges used in [8].	Cloud and edge services can be combined in encryption systems. However, attackers are able to hack in and change the key. Previous researchers provided short encryption key methods only for professionals who used the services and each trained application. Alternatively, they provided information at a level that hackers could not access in their existing solutions.	In high-resolution or pattern-based procedures, we should secure our application authentication methods to higher Internet models. Using this process, 60% of tools are safe from attackers and 40% of apps and layers are destroyed because of the incorrect combination of layers with different methods.
Meshveliani et al.	Lightweight cryptography IoT techniques [7].	When using the most inexpensive cryptography methods for security, researchers used a hashing function with a one-way technique. When users encrypt their data, it generates errors at different modes. In our version of this method, we encrypted the data and only used the short keys that attackers could not easily reach.	Use monitoring or tracking devices. This allows professionals to handle the security and privacy of a device by providing its effectiveness and impact factors.
Haji pour et al. (2020)	Challenges associated with different IoT application methods [8].	When a user creates an application, it compromises the data integrity and can reveal the user's identity. In their solution, the authors supply a verification application that uses various security techniques and has a large storage capacity. However, they do not destroy validated personal data.	Use validated apps in the home appliance for security using pattern methods.
Lohiya et al.	IoT architecture and its security with different issues and its solution [10].	When the architecture is created, it harms the network layer in the solution (ARM and MIPS, X86) encrypted code. Hardware levels protect this system from attackers and increase the storage capacity.	The lack of confidential information in systems is an advantage for malware structure design and testing implementation. We recover the damaged data with service-oriented architecture. The software security environment is helpful to maintain connectivity for driver installation. The architecture and its confidentiality are important for future work.

(i) The current research lacks an empirical evaluation and overarching set of terminology for IoT system techniques [46]

(ii) The structure of most proposed research does not have a systematic layout, and the paper selection technique is not evident [47]

(iii) Some prior studies do not examine the prime assessment aspects of IoT applications [44]

3. Research Selection Method

This section provides a systematic review based on the SLR method, classifying the most challenging IoT security issue results [46], as shown in Figure 2.

A complete solution to the following analytical questions (AQ) pertaining to the study objective defines this systematic literature review:

(i) AQ1: how can we preserve the confidentiality, privacy, and security of services using the IoT ecosystem?

(ii) AQ2: there are severe security failures that exist in IoT: how do we resolve the IoT security issues?

(iii) AQ3: what are the current research trends in IoT security?

(iv) AQ4: what security problems can occur on IoT layers and their solutions?

(v) AQ5: how do we minimize IoT issues, and what is the role of IoT development in this context?

4. Introduction to IoT Security

Along with the variety of platforms and networking devices used in IoT systems, there are multiple protocols and functions that have been supplied to IoT network solutions. However, many view the current regulatory procedures in the United States as ineffective [48]. The Open Web Application Security Project (OWASP) focused on the three levels of an IoT device: technology, data communications, and communication protocols [49]. As a result, as shown in Figure 1, the authors concluded that the deployment of Internet security countermeasures must include security infrastructure at all IoT layers [50]. Radio frequency identification (RFID) and wireless sensor network (WSN) are both defined as part of the IoT network [51]. The ramifications of a possible attack on the layers of these two systems are shown in Table 2.

4.1. IoT Architecture. Every level in the network performs specific tasks. In the IoT, there are various perspectives on the number of layers necessary [48]. According to numerous studies [48], the IoT primarily operates on three tiers: observation, connection, and access layers. Each layer of the IoT has its own set of security concerns based on the equipment and devices that assist each layer [50]:

(i) Perception layer

In the IoT, it is called the sensing device layer. The goal of this layer is to obtain data from the server. A wearable sensor can be used to monitor and control the environment. This layer identifies, gathers, and analyzes data before transmitting it. It processes onto the network layer. This layer is also responsible for the cloud server [51].

(ii) Network layer

The IoT protocol is used for network communication and data transfer to various IoT ports and sensors via the Internet. At this level, there are many virtualization systems available on the World Wide Web. Access points and transit devices, among other devices, work by combining some of the most cutting-edge technologies, including Android, Ethernet, 3G, GSM, and other wireless technologies. By gathering, screening, and routing data across multiple IoT systems, network gateways act as an intermediary for sending and receiving data from various sensors [52].

(iii) Application layer

The validity, safety, and privacy of the data are all ensured by the application layer. The objective of IoT at these tiers is to establish a network grid [44], as shown in Figure 3.

4.2. IoT Security and Privacy Challenges. IoT provides users with significant advantages; nevertheless, it also presents certain drawbacks. The main concern of scholars and legal experts regarding IoT devices has been issues related to cyber-security and privacy threats. Several companies and corporations have struggled to deal with the problems of IoT, and these dangers have been highlighted by recent high-profile cyber-security breaches. In addition, problems associated with anonymity and dishonesty on the Internet represent difficulties in using IoT devices [53].

None of the aforementioned problems have a greater impact on IoT acceptance than security and privacy. However, unfortunately, consumers often do not have an essential understanding of the security consequences until after they encounter a compromise that results in losses. As a consequence of this lack of user education, consumer willingness to deploy weak security is too common [54, 55]. In a recent examination of privacy and security, IoT devices performed well, but there still exist numerous flaws in the computer systems [56]. Thus, the popularity of IoT is determined by how effectively it can respect people's privacy preferences. Concerns about privacy and other threats associated with IoT have been critical in delaying IoT's complete implementation. Full implementation requires an understanding of the needs of clients, an ability to protect their personal information, and security of their privacy terms.

There has been significant research on the IoT that reframes security concerns, such as the escalation of monitoring recording [57]. The integration of unique information from objects can be used to create a survey

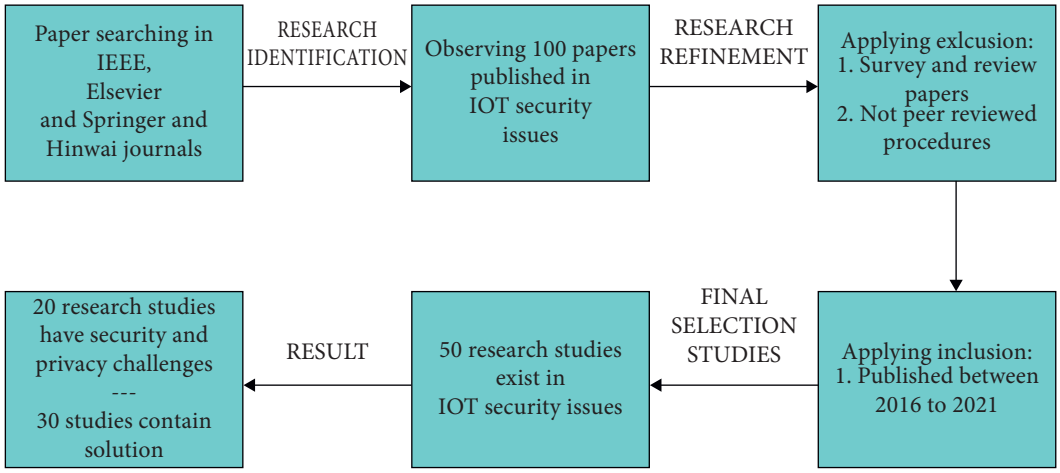

Figure 2: A criteria for selecting the literature to be reviewed in this study.

Table 2: Comparison of network layers based on RFID/WSN systems and existing attacks.

References	Layers	RFID	WSN	Protection from these attacks
Yadav et al. [51]	Physical/link layer	Replay attacks, blackmail, the precision of the results, and synchronization assaults are all examples of detectors.	Sybil, passive distraction, aggressive programming of temporarily disconnecting the device, replay attacks, and RFID readers are all used.	Tag (disable, removal, destruction) and all commands are rewritten and created error-free. When attacks accrue, we can build different prevention walls by updating and deletion processes. We can use a wireless sensor to detect higher radio frequencies at all stages of the attack. We can use short keys and digital signature keys in this situation for communication without sharing descriptions with anyone.
Rahaman et al. [52]	Network/ transport layer	Eavesdropping, quick injustice, bogus routing, introduction, and session overflow all are discussed here.	Attacks on network protocol are replication and spoofing and are two types of label attacks. Attacks against readers include deception and spying.	Tag (spoofing and cloning) attacks are removed by professionals. Routing protocols, eavesdropping, and impersonations are defined here. We can create the network protocols authentically. This method puts privacy rules in bank cards, changes pins, and only sees that person who held these cards or knew the pins from different privacy methods.
Zhu et al. [53]	Application layer	Memory spills and infusion are introduced here.	Infusion, memory leaks, illegal label scanning, and tag alteration are all potential threats.	Illegal people hack personal data and know the application codes or information about the victim. We can use legal tags symmetric and asymmetric processes for personal info and save the application layers, such as the name, password, and passport PINs, for legal malware injection. Memory was lacking in this approach.

Table 2: Continued.

References	Layers	RFID	WSN	Protection from these attacks
Mohammadzadeh et al. [54]	Multilayer	Replay attacks, policy enforcement, and cryptography attacks are all examples of malicious activities.	Active attacks, data aggregation, and encryption attacks are all examples of spear phishing.	All attacks exist in these layers. We only prevent our data from attackers by deleting unused memory storage, changing passwords, and hiding encryption keys and modem wires.

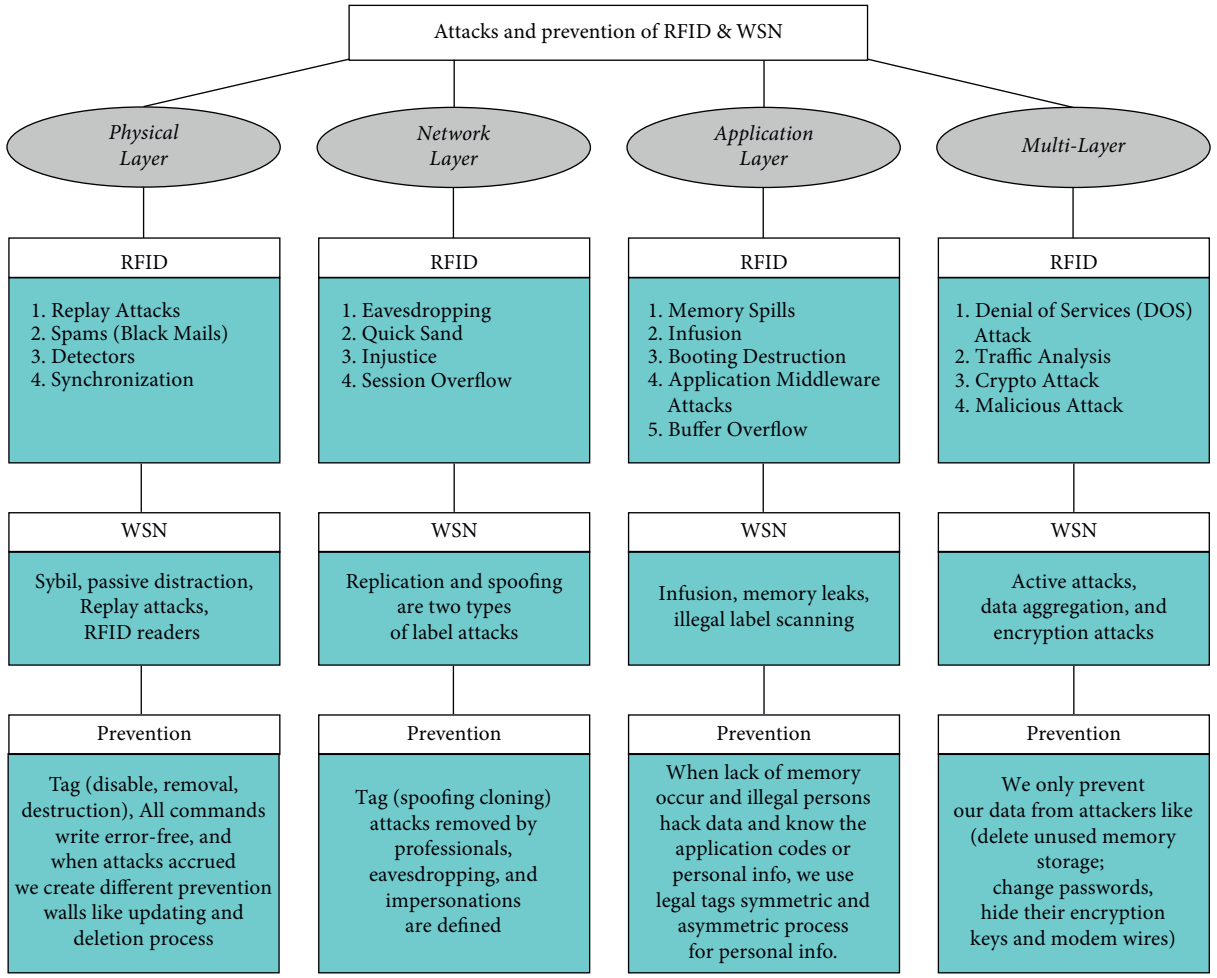

Figure 3: RFID used in IOT architecture and the attacks on network layers and their associated prevention methods [51].

strategy and implement global communication in the IoT. The ability to connect with the Internet is also an aspect that aids in identifying these issues, because these distinct processes would be difficult to solve in isolation [58]. Accessing personal information from anywhere in the world is convenient; however, there still exist some privacy challenges [59]:

(i) Interoperability

Risks to the system should be restricted or limited. Customer benefits are hampered by a heterogeneous ecosystem of unique IoT digital transformations. Although complete interoperability between goods and services is not always possible, the user may dislike purchasing specific IoT-related goods. For example, improperly designed IoT devices may hurt the environment. They are expensive with respect to networking resources [60]. Another feature that has been employed for many years to provide security is cryptography, which addresses security flaws in crowded and complex scenarios [61]. Infections can be mitigated by establishing powerful security features and incorporating them into IoT goods. This has tangible benefits when customers purchase items that already have adequate security protections to safeguard against flaws. Some of the precautions implemented include cyber-security guidelines to guarantee the

protection of IoT devices [62]. Different requirements and problems can have an impact on the ability of devices and their protections.

(ii) Periodic updates

The manufacturers of IoT devices generally update the software every quarter. Furthermore, operating system platforms and security fixes are maintained on a more semifrequent basis [61]. As a result, attackers have sufficient time to break the security systems and capture data.

(iii) Embedded passwords

Sensor nodes keep integrated passwords, which makes support easier. Professionals can remotely fix operating system issues or deploy essential updates on their devices. However, hackers can subvert these features to break data encryption [62].

(iv) Automation

In IoT applications, system application developers use different features to collect data and streamline business processes. Artificially intelligent methods can access these features if the dangers are not specified through proper integration, which can allow dangers to compromise the system [62].

(v) Remote access

IoT systems use different hosts for different protocols for remote access, such as area networks, Lurton, Bluetooth, and Z-Wave, although typically explicit limits are not indicated. As a result, hackers and cybercriminals might positively identify links between users and their data using these methods for wireless monitoring [63].

(vi) A diverse set of third-party programs

There are many technological websites on the Internet that companies can use to perform different tasks. However, it can be difficult to determine the legitimacy of these sites. If terminals and staff download or access software from illegitimate sites, malicious hackers can immediately enter the system using these applications and damage the user's system, particularly if the database is integrated [64].

(vii) Inadequate device identification

Most IoT systems do not use strong passwords to protect the user's data. As a result, gaining access through conventional entrances using stolen passwords can pose a threat to privacy [65].

(viii) Weak device monitoring

To control and identify objects, most IoT vendors set unique device identifiers. Alternatively, some companies do not adhere to such strict security protocols. As a result, tracing suspects based on their Internet activity becomes difficult. Some related challenges and their possible solutions are shown in Table 3.

5. Current Research

The primary objective of current strategic preventions is to track the user's confidentiality and integrity and to maintain the protection of IoT devices, platforms, information, and applications. Thus, the reliability of the IoT facilities offered by an IoT environment depends on its availability. Prevention and interventions are necessary for frequently used applications to prevent traditional potential attacks. Figure 3 depicts the current state of the market [67].

For data from 2016 to 2021, we used the following strategies and procedures. We found that authentication was a difficult task used for security strategy; however, the confidence-based system has gained popularity due to its ability to detect and prevent harmful devices [68]. Alternatively, research on encryption and decryption has attained lightweight and low-cost encryption and constrained devices, as shown in Figure 4.

6. Authentication

Authentication refers to the method that involves identifying the IP addresses of a network and providing permissions to authentic people. This approach is used to protect IoT systems from assaults, such as response attacks, replay attacks, so-called man-in-the-middle attacks, and imitation onslaughts. Authentication is still the most commonly used protection method, as shown in Figure 4. Approximately 60% of systems use this approach to provide access to the application layer, whereas 40% use it to grant access to users at the data layer.

6.1. Importance of User Authentication. Illegal activities can be prevented from accessing confidential material via user authentication. For example, if User A has access only to information necessary for them, this secures the data of User B. However, if the authentication process is not protected, hackers can obtain access to the system and extract passwords. Companies like Microsoft, Experian, and Yahoo have experienced data breaches due to their failure to secure verification. Hackers hacked into Yahoo user profiles between 2012 and 2016 and extracted data pertaining to contacts, calendars, and personal conversations. In 2017, the Equifax cyber-attack compromised the credit card information of over 147 million people. Any firm can be put at risk if they do not have a safe authentication mechanism [69], as shown in Figure 5.

For transmission encryption and decryption, Internet protocol security uses transport layer security (TLS) access in this system. TLS offers two authentication methods for limited devices: TLS-PSK, which utilizes preshared keys, and TLS-DHE-RSA, which uses RSA and Diffie–Hellman (DH) information distributions. Both use public keys and encryption algorithms. The two objects performing secure communication in this technique must first verify their identity by providing confidential info (i.e., exchange protocol keys) because the verification process using this method is just a cryptographic hash function. The second technique works well with restricted devices, like sensors. There are three varieties of authentication protocols

Table 3: Comparison of challenges that exist in previous studies.

References	How existing methods work	Weaknesses in the existing method	Solution of weaknesses	Future work
Zhao et al.	In IoT technology, using a secure routing method to detect on-off attacks means that malicious attacks work as node captures [53].	It detects the damaged nodes based on the misbehavior history of each node in the network.	The occurrence and misconduct records exist as a dependable factor that should impact the estimation of a nonblocking source node.	For the future, one could build high encryption and decryption algorithms to detect only those nodes that already know about the laws of on-off attacks and malicious attacks.
Cavada et al.	Ubiquitous technologies for tourists working in this approach function as wearable devices that can be enjoyed at any time [59].	This method does not communicate directly without portable devices. They lack fast communication with systems in public places due user authentication problems. In remote areas, people do not communicate using these technologies.	One can improve the design of user interfaces for these technologies. One can create changes to the wearable device for communication, and the customer should understand all of its procedures.	Security login pages must be included in these technologies. When attackers target user identification and steal user information, one should destroy the profiles.
Khalique et al.	Interoperability enables safer communication from one device to another using a cryptographic algorithm [62].	This method affects the algorithm work and device connectivity because they are limited in time or use encryption only.	Fast working devices function with large data type key algorithms for better communication, resulting in unrestricted or unlimited running devices.	Low-power-wide area networks (LPWANs) and IoT provide a solution to convey large amounts of data with low energy consumption, enable effective communication across many devices, and increase tolerance levels. As a result, the method can be applied to many sectors, including monitoring, navigation systems, and security.
Elwy et al.	Periodic updates are collected to perform specific actions on devices, such as in a washing machine. When the machine is switched on, it runs and washes clothes for a specific period and stops when the switch is off [63].	This method provides updates at every level of the OS process, which creates many problems for users as they run or close apps that are connected with these devices.	Poor wide area networks (WANs) allow devices interconnected with IoT to operate according to our requirements.	As a result, attackers have ample time to break the security systems and capture data. However, this is the incorrect way to update the devices at the network level if the attacker hacks all identities of the devices.
Talal et al.	Embedded passwords in automation systems enable professionals to embed their passwords with their devices for authentication from unauthorized people [64].	The most recent communication systems, such as international mobile telecommunications service (IMTS) and long-term evolution (LTE), do not provide simultaneous connections to a significant number of computers.	Face patterns or fingerprints allow for authentication that avoids hackers and detection devices.	This study examines security issues that are addressed by integrating the Internet, monitoring networks, intrusion detection, and image processing. It aids in the elimination of duplication, allowing for quicker detection and avoidance of assaults. This innovation assists in the early detection of acts of terrorism, alarm systems, and intelligent traffic systems, all of which will improve the performance and adaptability of current communication networks.

Table 3: Continued.

References	How existing methods work	Weaknesses in the existing method	Solution of weaknesses	Future work
Halder et al.	For remote access, IoT systems use a host of different protocols such as area network, Lurton, and Bluetooth [65].	This method is used to prevent certain types of attacks. As a result, hackers might positively identify a link using these methods for wireless monitoring.	Limits must be included in this system to prevent attacks.	The technology decreases emissions while also contributing to sustainable development by saving energy, increasing reach, and creating a more secure system. Its application across several sectors, other than wireless operators, would improve its effectiveness and help in infrastructure projects.
Sikder et al.	Weak device monitoring is used to control and identify objects. Most IoT vendors set unique device identifiers, although some do not adhere to security protocols.	From this, tracing suspects based on Internet activity becomes difficult [66].	The LTE-A is an evolution of the D2D model. The LTE-An authentication protocol minimizes cellular network interactions by combining Internet circumstances and Internet protocol access.	This research concentrates on employing a dark basement system for effective Internet connectivity to provide faster connections, which are relatively inexpensive and efficient.

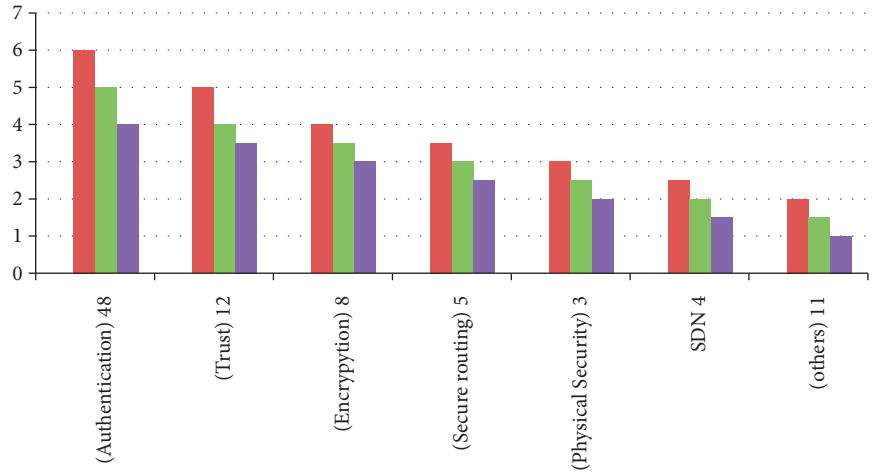

Figure 4: Publications pertaining to IoT security from 2016 to 2021.

currently available for IoT: convergent-based protocols, asymmetric cryptosystem-based protocols, and hybrid protocols [38, 70]. There is a two-way connection between humans and machines. In the IoT system, there is a consensual interaction between the smartphone and the workstations. The system sends information to the server and obtains control data emitted by the console. The authentication process is essential in an IoT platform to verify the authenticity of both the browser and the network. Previously, there has been a significant shortage of lightweight authentication and encryption methods. More recently, there has been an increase in the employment of lightweight authentication and encryption. The goal is to provide an inexpensive authentication process for network access, with encrypted communications that are authenticated with many factors [69]. There are various methods to improve IoT authentication's function, such as employing bio-hashing and enhanced privacy to all recommendations. Figure 6 presents the status of IoT authentication methods [69] from 2016 to 2021.

Figure 6 shows the current IoT research trends applied for authentication using different methods: lightweight, multifactor, and multiauthentication. Lightweight authentication constitutes 65% of the authentication methods and is used for secure and better communication in IoT and for securing devices. Multifactor comprised 15% and is used to achieve authentication goals, and multiauthentication comprised 20% and is used for access control.

6.2. Common Authentication Types. Hackers constantly refine their cyber-attacks. As a result, security professionals must deal with many varied security issues. As a result, businesses are beginning to deploy more

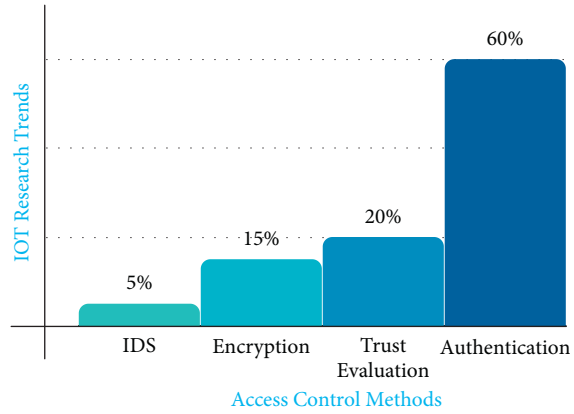

Figure 5: Current IoT research trend in access control methods.

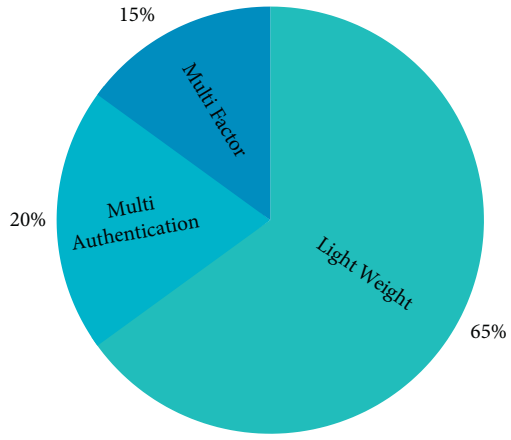

Figure 6: Current authentication trend.

comprehensive disaster recovery plans that include authentication [71]. The following is a list of the most frequent authentication mechanisms used to protect information technologies.

6.2.1. Password-Based Authentication. The most frequent method of protection is passwords. A combination of characters, figures, and punctuation marks can all be used for a password. Users must develop secure passwords that incorporate a mixture of all feasible alternatives to secure themselves. However, passwords are vulnerable to spoofing assaults, which reduces their usefulness. Only 54% of people use unique passwords throughout their profiles for all websites, and the average adult has roughly 25 different Internet financial records. As a result, many people prefer comfort to protection and use basic password patterns instead of complex passwords, because they are easier to remember. Attackers can quickly guess a username and password by trying all conceivable permutations (i.e., using "brute force") until they discover one that fits if the user has used a simple password. Biometrics is an alternate strategy that may be adequate for securing Internet data, although it has numerous flaws.

6.2.2. Multifactor Authentication. Multifactor authentication (MFA) is a verification strategy that integrates recognition using two different methods. Barcodes produced by smartphone applications, scrambler challenges, fingerprints, and facial recognition are examples of this approach. By providing new security features, MFA concepts and approaches improve user satisfaction. MFA is secure against other profile breaches, but it has some negatives associated with its use. Individuals may misplace their phones or SIM cards, rendering them unable to produce a code for authentication, locking them out of their devices [72].

6.2.3. Certificate-Based Authentication. Cryptographic keys for social security card authentication are applied and provide solutions to target individual devices and types of equipment in networks. A digital certificate is a form of semiconductor identification that is similar to an officer's learner permit. A cryptographic key and accreditation agency cryptographic certificate represent the voltage profile of a user's online signature. A certification authority can produce authentication to show the marketing authorization holder. When a tenant moves to a website, they must supply their cryptographic keys. The server checks the authenticity of the password diploma committee's validity. The website

only verifies the visitor, who has the secret key to attach to the license in the system as a password.

6.2.4. Biometric Authentication. Biometric identification is a type of security that relies on a person's unique biological traits. The following are some of the primary benefits of adopting access control technologies: Authorized features are maintained in a directory and can be quickly associated with the bio-data parameters. When mounted on gateways and entrances, bio-data information regulates direct access. Biometrics can be included in multifactor user authentication. Individual authorities and commercial companies employ biometric security systems at runways, army assets, and political boundaries. The most popular identification techniques were as follows:

(1) Face Recognition. Many facial traits of a person can be used as biometric information. However, face recognition may be unreliable when comparing features of a person from different angles or when comparing people who look similar, such as family members. These vulnerabilities have prevented face input validation innovation [73].

(2) Fingerprint Scanners. These devices match the distinctive patterns on an individual's palms. People's fingers can be evaluated by some new touch screens that focus on the circulatory system. Despite their frequent mistakes, biometric authentications using fingerprints are still the most used screening method for businesses and individuals, largely owing to the popularity of smartphones.

(3) Voice Recognition. This method refers to the task of evaluating an interviewer's speaking style for the development of appropriate forms and sounds. Speech devices such as pins are regularly used as predefined terms to authenticate individuals.

(4) Eye Scanner. Computer vision systems and scanners are examples of eye scanners. Optical scanners shine a beam at the user's eyes and look for distinct patterns in the colorful ring surrounding the pupil. However, if the user is wearing glasses, eye-based identification may be inaccurate.

6.2.5. Token-Based Authentication. Using this method, people submit their identities once and obtain a unique protected stream of random letters in return using gesture visualization. Instead of typing passwords repeatedly, users can utilize the token to access protected systems. The biometric certificate verifies that the user has the granted access. REST-APIs (representational state transfer-application program interfaces) take the theoretical representations of employees as examples of token-based authentication use cases [74].

7. Weakness of IoT Authentication Methods

All of the suggested passwords are one-time procedures, and using a digital signature for lightweight verification is not an appropriate security option because such an identifier can be hacked [75]. The following are the weaknesses of heterogeneous IoT authentication solutions, as described in previous research [76]:

(i) Attacks on cloned validators and numerous stored users with the same username and password
(ii) Router assaults takeover and deception
(iii) Stealing microchips and IoT devices reproduction accused
(iv) Disabling portal networks and faking detector's key
(v) Impersonation, attack assuming, and off-site identification
(vi) Speculations and smart card thefts are examples of off-line attacks
(vii) IoT device authentication is still the standard security technique for attacks, deception of a user, and imitation
(viii) IoT applications have flaws and limitations and thus may not represent a comprehensive solution for IoT security reduction

However, several existing cryptographic algorithms proposed from 2016 to 2021 are worth investigating, as shown in Table 3. We have defined the devices used in home automation. The current research is presented in Table 4, with a different perspective of authentication on layers of applications.

7.1. Encryption. Reduced and limited devices can only integrate industrial control systems (ICs) [80] because of their low requirement for system resources and limited standby time, compactness, constrained storage, minimal power supply, and conventional encryption primitives for handheld devices. Cheap security may be a good option for all these systems. The purpose of IoT cryptography is to promote effective edge connectivity [81]. Weak compact cryptography in the physical and network layers has remained the main focus of this research. Alternatively, there have been proposals for an innate quality-decoding method to existing customer repudiation. The current research on this topic is defined in Table 5.

7.2. IoT Security Issues. In this section, we present the seven most significant IoT-related security problems, ranging from theft of IoT devices to prospective burglaries to the perils of uncontrolled devices [88].

7.2.1. Malware and IoT Device Piracy. Ransomware is a type of software that encodes and denies access to people's data, potentially by exploiting IoT devices with inadequate security protocols. The actual problem starts when a hacker infiltrates a gadget with spyware. The hacker then requests extortion money in exchange for the suspect's files. However, hidden hackers have become more common in the world. Smart watches, medical monitors, and smart homes

Table 4: Comparison of network layers with simulation on authentication.

References	Layers	Security objective	Advantages/security issues	Simulators/computation analysis tools
Racine et al. [77]	Network	Secure communication	Overhead reduced. Lacked privacy.	Coosa/generic
Ometov et al. [72]	Application	Access control	Multifactor identity provides the cheapest biometric privacy and security key.	AVISPA
Zadeh et al. [54]	Network	Secure communication	Secure for mobile and other wireless devices but lacking an authentication process.	MATLAB, but not available all time that users can deploy it
Rahaman et al. [52]	Application	Access control	RFID verification protocol is lightweight. However, they exist in pattern codes that lack info when using fingerprints for the login page.	C++; no other linked tools or technologies
Qian et al. [78]	Network	Identification	Use NFC and handheld devices, like in mobile environments.	When patients' records enter the systems, they depend on the medical field or NBS; however, they have privacy issues and lack layers to exchange the data over the Internet
Hageman et al. [6]	Application	Access control generic	Software as a service virtualization solution. A parallel matching method is used but destroys data due to the effectiveness of web pages.	Prototype available in generic form
Tanka et al. [69]	Network	Access control	Bio-hashing in encryption systems is used but only in data exchanging. It is not secure because it can be key hacked by attackers.	AVISPA/bed net
Hussein et al. [79]	Application	Secure communication	The digital signature used for encryption or decryption methods. It is a one-way algorithm and lacks in key encryption due to size limitations.	WSP/networking protocol
Mary et al. [26]	Network	Access control	Verification at handheld devices and smart cards. However, there are issues created at the time of pin exchanging.	Bed net/networking protocol

Table 5: Encryption on network layers with simulation.

References	Domain/ network layers	Security objective	Advantage	Simulator/security issues
Batra et al. [82]	Generic/ network layer	Role in maintaining of data confidentiality	Low cost	Not available and lacking in privacy.
Setiawan et al. [83]	Industrial/ physical layer	Secure in interconnection systems	Detect multiple instruments, such as counterfeit and proximity attacks	Depends on prototype testing. It is not secure during login authentication.
Yuga et al. [84]	Generic/ application layer	Secure communication	Decryption shows improved classification with application installation	Layers like MICA. In the reverse of encryption, when entering, the hierarchy of keys is too complex.
Panda et al. [85]	Middle/ network layer	Helps to avoid loss of energy	The attacker's exact location is known by the layer	In experiments (test-bed), the attacker hacks all data and wastes their time and energy because the key is stolen in this layer.
Hossein et al. [79]	Generic/ application layer	Authentication system	Security and privacy are much better than other systems	WSN, when the user sends emails, spam emails appeared.
Naira et al. [86]	Not Generic/ physical layer	Security in designing transformations	Reduce computation at top layers	COMS and UMCE are two types of the protocol system.
Hosen et al. [79]	Generic/ application layer	Ordered data protection	Lightweight with high-speed resolution	Cheap in memory but also suffers when data are encrypted.
Aruna et al. [87]	Industrial/ physical layer	Access control insurance	Algorithm for the asymmetrical circular track	Real-time embedded; when a key is large, then replay attacks can accrue.

are all at risk concerning this security issue. Cyber-attacks block clients from their IoT systems and connected networks, destroy machines, and grant unauthorized access. Because of the exponential increase in IoT users, this specific IoT risk is inherently uncertain owing to the large number of possible configurations [89]. The best approach in IoT data is to virtualize the infection so that it may not have any sensitive information to lock. However, most IoT system providers fail to offer critical security fixes and tests.

7.2.2. Inadequate Testing and a Shortage of Improvements. Another security issue concerning connected systems is that manufacturers frequently provide inadequate testing and security [90] and do not always undertake all necessary precautions to prevent safety problems. With the rapid expansion of the IoT sector, many companies are now building and selling devices without testing. In addition, sometimes, security improvements are only available for a short period. Devices are being produced at an accelerated rate, and thus, designers may forego these upgrades in favor of promoting the next generation of equipment and encouraging users to upgrade. Sensor nodes running application technology could be vulnerable to a variety of viruses and criminal threats, as well as other security flaws. In addition, when a machine uploads its information to the server during an update, there may be downtime. Software files are exposed during this period if the connection is not secured, allowing hackers to access files and posing a security risk.

7.2.3. Home Invasions. Home invasions or burglaries are perhaps the most frightening example of IoT security risks because they erode the boundaries between the physical and virtual world and put users in significant danger. The concept of "home automation" was born as the IoT sensors became a part of an increasing number of houses. This AI poses a significant risk because rogue devices with weak protection measures may expose users to threats. Attackers may be able to find the location of the data owner using search engine queries. The potential for harm is obvious, and it can even lead to the user's information entering illegal contacts [91]. Communicating using proxies and encrypting your account information are two ways to avoid this type of IoT security problem.

7.2.4. Monetary Corruption Fueled by IoT. Tax evasion and counterfeit identity fraud can increase for money transfer companies that use the Internet. Some of these organizations are exploring cognitive computing, whereas others may see the value of incorporating information across several levels of the industry [92]. Artificial intelligence can be used to discover malicious activities and provide prompt indications of threatening activity. All investment banks, for example, will face difficulties in introducing these new models. Prototype maintenance and risk management procedures account for the growing threat of cyber-attacks.

7.2.5. Smart Car Access from Abroad. In the IoT of smart vehicles, theft has become more common on highways. Defective IoT systems introduce significant dangers regarding the remote monitoring of smart cars.

Security threats related to IoT may endanger the independent features of their devices, such as personality and motion detection [93]. These hostile hacks pose a significant risk to the community's security and can even result in death. Remote monitoring connectivity is also vulnerable to malware, as an attacker may expect payment in exchange for unlocking the vehicle or activating its motors. IoT item vendors are currently attempting to develop methods to address these security flaws. Microsoft and General Motors cooperated on an instrument cluster that is sensitive to these assaults. Fortunately, because these attacks usually occurred before the mainstream use of communication systems, the engineers had sufficient time to respond effectively. Figure 7 shows the chain of devices protected by passwords and some issues that affect the IoT devices at the top level.

7.2.6. Fake and Malicious Smart Devices. Covering the firewall and controlling all the individual pieces of equipment is an IoT security issue. The rapid surge in mobile and volume flexibility of IoT devices has created a problem within residential networks [14]. Hackers deploy rogue and counterfeit IoT devices in secured networks with unauthorized permission. These machines can restore the source material and connect to the Internet to capture sensitive information, effectively breaching the network firewall. These devices come in the form of malicious wireless networks, surveillance cameras, radiators, and other devices that steal network information without the user's awareness.

7.2.7. Lack of User Knowledge about the Privacy of the IoT. Many users think that they already understand the risks and features of the IoT. However, fraud, worms, and spyware risks on laptops and personal computers and cyber-identity theft are examples of situations wherein users' sense of security have been exploited by threats. Users feel secure when they have figured out how to protect their Wi-Fi hotspots and safeguard their PayPal. However, in the literature, when it comes to IoT security vulnerabilities, researchers attribute fault to the vendor and the consumer's lack of understanding and negligence. The IoT devices that data breach are likely due to user illiteracy and lack of knowledge. When attacking individuals through the IoT, media manipulation assaults take advantage of the human tendency to avoid these problems [95].

The deadly 2010 attack on an Iranian nuclear site was an example of such misuse of human psychology. The targeted device was an Internet technology known as a microcontroller, which required one employee to attach a Micro-SD card through one of the internal computers to break the private platform's separation from the public network, exposing it to attack:

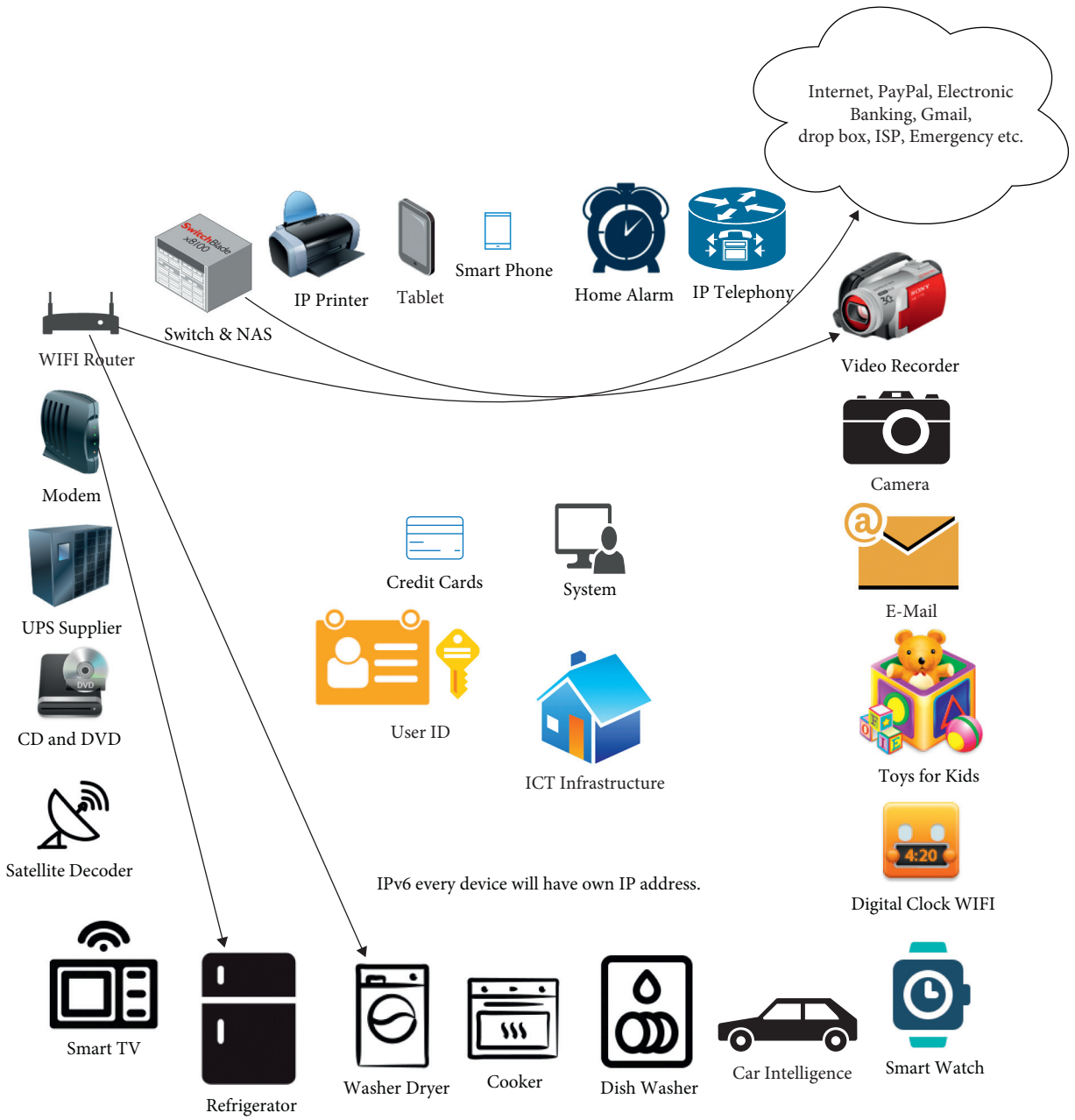

Figure 7: Remote monitoring of autonomous sensors is a serious IoT security risk [94].

7.3. Ways to Identify IoT Security Vulnerability and Methods to Secure IoT Systems. The IoT potential threat is in consideration with the last subscriber, and we will now discuss some practical strategies for IoT consumers to avoid data breaches [75]:

(i) Users must frequently create efficient forms of authentication.

(ii)Updating accounts of online activities, desktops, and applications have frequently been the standard in recent years. These practices should also be standard for IoT devices.

(iii) Users must constantly stay updated on best practices of security and ensure the following:

(a) Each IoT gadget has its password.
(b) Users must check their credit report a minimum of once per year.
(c) Passwords are widespread, and duplication is avoided.
(d) Credentials must be extremely difficult to guess. Users can use encryption software to memorize passwords for them or write them down on a piece of paper.

7.3.1. Do Not Depend on Cloud Computing. Mobile computing is efficient, but it is also highly susceptible to attack. Every gadget acquired from an IoT vendor comes with

Internet power consumption. Although it may be tempting to get an inexpensive one, it is important to remember the appropriate guidelines [96]:

(i) To utilize documents and programs encrypted form, you must have an active Internet connection

(ii) Obtain a complete review of the security settings that come with your Wi-Fi network

(iii) Furthermore, ensure that the system is protected and the user can save their information and folders privately, away from the reach of malicious agents

7.3.2. Avoid the Use of Global Connector Capabilities. A large proportion of IoT devices offer an international connect and play functionality that allows various wireless modems to communicate with each other. This suggests that users do not have to activate each alternative available. Although there is a clear benefit to the IoT environment in your home or office, users should be aware of the following:

(i) International socket and forget methods connect to network devices.

(ii) These systems can be connected to outside threats and exploited.

(iii) If the assault is successful, it might harm all of the connected systems by allowing hackers to inject themselves directly from one to another. In this case, switching off the connect and forget mode on IoT technology devices will provide some security.

7.3.3. Make Use of the Sensor Node. Wi-Fi customers regularly construct numerous networks that are only available for themselves and their dependents. The method of creating a second network is used with connected systems because it aids in data collection:

(i) Protect your confidential files from illegal disclosure

(ii) Disable any efforts to take control of IoT devices and the installation of malicious software

(iii) Put the IoT sensor above the range of any external entity to secure its confidential messages

7.3.4. Update Your IOT Devices Daily. Notifications must be available onsite to monitor for authoritative updates by the software vendor. We described in this section a lack of innovation as one of the IoT security concerns. Therefore, downloading all software updates improves your interface and prevents attackers from infiltrating your devices in novel ways [97].

7.3.5. Standard IoT New Features Provide the Following Benefits

(i) Understanding that your networks are updated with the most up-to-current protective measures that avoid the most recent types of assault gives you some security.

(ii) It is a better level of protection for your house or office.

8. Discussion

AQ1: how to preserve the confidentiality, privacy, and security of users and guarantee the services by the IoT ecosystem?

The goal of implementing the safety reduction is to protect anonymity and secrecy. The integrity of remote devices is facilitated, as are the communications and sensors that maintain the reliability of systems. As a result, prevention responses are implemented for the following traditional potential attacks. Identification is still a prevalent security mechanism, but intrusion detection is gaining popularity because of its potential to suppress or identify bad networks. According to a cryptography study, the other extreme concentrates on ultralights and limited encoding for reduced and restricted devices [98].

8.1. Authentication. The method for devices on the network connection to access systems, people, and pseudo-objects is known as verification. The reply assault, imitation assault, and Sybil assault are all examples of threats to IoT networks [99].

8.2. Encryption. The process of achieving end-to-end security in systems is known as encryption. Furthermore, IoT devices are versatile networks that can incorporate particular computer chips. Moderate and restrictive devices can only integrate implementation ICs [80]. As a result of their low computation power, restricted battery performance, portability, limited storage, and constrained supply voltage, conventional authentication is not suited for relatively low power digital sensors. Thus, inexpensive security may be a good option for some of these devices. The purpose of IoT cryptography is to facilitate the final transmission while utilizing fewer components and ultralight techniques to satisfy this goal. Securing the routing protocol at the network layer and implementing trust- and reputation-based malicious node detection results in an end-to-end delay, communication overhead, and a high false-positive rate [100]. The findings from this study demonstrate that authentication alone may not be sufficient for IoT security. Instead, current trends of IoT security mechanisms should work on lightweight, mutual, and multifactor authentication, especially at the network and application layers. Lightweight and low-cost encryption are proposed for the physical layer to mitigate security issues.

AQ2: there are severe security failures of IoT: how can we resolve IoT security issues?

Safety prevention and the IoT security infrastructure are embedded in three layers of the core technology stack: observation, communication, and application (even though most existing solutions are in the network layer). From this, it can be inferred that successful IoT security mitigation benefits from accurate IoT threat modeling.

AQ3: what are the current research trends in IoT security?

We presented an SDN-based cloud for data transmission safety and QoS, Ge. We also use SDN to alter the attack surface of this type. We identified the quality improvement necessary for our technologies and services to achieve adequate quality enhancement and network performance. Evaluation functions on home automation using different authentication processes were performed. We also analyzed the RFID-based network layers that function in homes and businesses using algorithms and discussed the weaknesses and challenges associated with their promising solutions. This paper can also assist network enthusiasts in better understanding, investigating, and improving the authentication process in all places and solve their issues held in IoT devices.

AQ4: what security problems can occur on IoT layers and what are their solution?

The Internet of things infrastructure has three layers: an interpretation layer, a channel layer, and a user-interface layer. Electronics, information sharing technologies, and communication protocols all are parts of IoT devices. Other crucial aspects of the IoT are the equipment, such as embedded systems, the underlying hardware, and most semiconductor fibs based on the Risk, MIPS, or X86 platforms. Protection devices as an encrypted code encoder or a security microchip are included in the design process. Sensor nodes often employ a Network Operating Standard (NOS) only for the computer user interface and contain a hardware abstraction layer, a physical layer top, connectivity adapters, and features like program separation, booting, and software isolation.

Personalized software, encryption methods, and the third-party component controllers compose the programming interface. Device configuration is also necessary to protect IoT devices. Identification features, edge traffic cryptography, a private switch method, the verification of digital signatures throughout oriented models, and accessible operations are all problems with IoT devices. Identification and cryptography may be viable options for addressing IoT security concerns. In the development of integrated methods, encryption that is reduced for physically embedded networks and cognitive methods are still in their immaturity. They do not ensure the safety of hostile devices in the system, including damaged machines or desktop computers. In addition, advertisers usually use encoded identities or usernames for simplicity, which results in a substantial verification problem. According to the results of this survey, current access control studies have primarily concentrated on developing compact data encryption for limited devices.

AQ5: how can IoT issues be minimized and what is the role of IoT development in this context?

The primary goal of security reduction is to protect anonymity and security. The security of IoT users, facilities, information, and sensors and maintaining the accessibility provided for these systems are paramount. As a result, detection and intervention methods are implemented to detect the traditional security threats. Identification is the most common encryption technique for access control and is gaining popularity because of its potential to suppress or identify bad networks. The study of cryptography has focused on compact and minimal cryptography for reduced and restricted devices. Cryptocurrency's foundation is blockchain. Stable and reliable interactions, along with the independence of interactions and procedures, will provide all benefits for IoT systems. Recently, the riskiest strategy has proven to be a great success. The features of distributed ledger technology for IoT include scalable and safe transactions.

9. Conclusion and Future Work

The IoT is an extremely powerful modern technology. The applications spanning home automation and hospital administrators, smart cities, and commercial facilities are discussed in this section. In addition, IoT provides a plethora of benefits to drawbacks and data protection is specific [101]. This study concentrated on IoT applications and various designs and architectures that solve associated difficulties. The IoT infrastructure is vulnerable to multiple assaults at each level, resulting in a slew of security issues and requirements to address these problems. All stages of the proposed ecosystem are susceptible to threats. For example, a method with surveillance techniques intends to ensure that confidential information is not exposed [102].

This paper provides an overview of the numerous issues and vulnerabilities that exist in the sophisticated realm of IoT. It highlighted the need and value of adopting and extending methods and procedures for retrieving and conserving information by highlighting current problems and open questions in this research domain. It also emphasized the importance of the strategic relevance of different proposals to risks that will likely continue to expand at an unprecedented rate. This research addresses major economic, production, corporate, and commercial requirement issues. The success of IoT also relies on the lucrative contract that every IoT approach has for regulatory affairs [103]. IoT security issues must provide solutions for user's protection from attackers as well as all unauthorized people. Further development of the IoT ecosystem will focus on privacy concerns.

The IoT technology has shown security problems in the commercial domain, and a part of the education that is necessary must acknowledge and analyze the possibilities of these technologies [104]. By 2021, most organizations will understand the potential of IoT, with economic activity related to IoT accounting for more than 80% of all providers. This means that an inability to provide adequate designs to suppliers will result in a need to further strengthen their cyber-security initiatives. Application developers will have to play a role by training themselves and staying put on existing security advancements and their significance [105]. The US parliament sponsored counter-terrorism legislation in March 2019, intending to ensure that IoT devices purchased by the government have certain minimum basic security features.

Integrated protection has already been available in some IoT devices from some vendors. In addition, potential clients are enhancing electromagnetic information exchange analysis, such as [106] the following:

(i) Linear machining
(ii) Heuristic techniques
(iii) Computer-assisted education
(iv) Neural network-based AI
(v) Evolvement of algorithms
(vi) AI mixtures and other adaptive control

Researchers can indeed anticipate the emergence of manufacturing domains of IoT software testing that will specialize as they progress [107]:

(i) Patterns of data integrity from beginning to end
(ii) In the IoT, reliable virtualization is essential
(iii) Challenges of confidentiality and protection in IoT formulation and construction
(iv) Deep learning threat prevention and vulnerability scanning for IoT systems
(v) Design of protected IoT systems
(vi) Privacy concerns and IoT platform security strategies

Conflicts of Interest

The authors declare no conflicts of interest.

Acknowledgments

The authors acknowledge the support provided by Riphah Artificial Intelligence Research (RAIR) Lab, Riphah International University, Faisalabad Campus, Pakistan. This work was supported by Qatar University High Impact Grant (QUHI-CBE-21/22-1).

References

[1] K. Sha, W. Wei, T. Andrew Yang, Z. Wang, and W. Shi, "On security challenges and open issues in Internet of Things," *Future Generation Computer Systems*, vol. 83, pp. 326–337, 2018.
[2] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, "A survey on security and privacy issues in internet-of-things," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1250–1258, 2017.
[3] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, "A survey on Internet of Things: architecture, enabling technologies, security and privacy, and applications," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1125–1142, 2017.
[4] A. Tewari and B. B. Gupta, "Security, privacy and trust of different layers in internet-of-things (IoTs) framework," *Future Generation Computer Systems*, vol. 108, pp. 909–920, 2020.
[5] G. Mei, N. Xu, J. Qin, B. Wang, and P. Qi, "A survey of Internet of Things (IoT) for geohazard prevention: applications, technologies, and challenges," *IEEE Internet of Things Journal*, vol. 7, pp. 4371–4386, 2019.
[6] R. Hagemann, J. Huddleston Skees, and A. Thierer, "Soft law for hard problems: the governance of emerging technologies in an uncertain future," *Colorado Technology Law Journal*, vol. 17, p. 37, 2018.
[7] L. Mirtskhulava, N. Gulua, and N. Meshveliani, "IoT security analysis using neural key exchange protocol," *Computer Science and Telecommunications*, vol. 57, 2019.
[8] M. Tavana, V. Hajipour, and S. Oveisi, "IoT-based enterprise resource planning: challenges, open issues, applications, architecture, and future research directions," *Internet of Things*, vol. 11, Article ID 100262, 2020.
[9] D. E. Kouicem, A. Bouabdallah, and H. Lakhlef, "Internet of Things security: a top-down survey," *Computer Networks*, vol. 141, pp. 199–221, 2018.
[10] A. Thakkar and R. Lohiya, "A review on machine learning and deep learning perspectives of IDS for IoT: recent updates, security issues, and challenges," *Archives of Computational Methods in Engineering*, vol. 28, no. 4, pp. 3211–3243, 2021.
[11] A. Riahi Sfar, E. Natalizio, Y. Challal, and Z. Chtourou, "A roadmap for security challenges in the Internet of Things," *Digital Communications and Networks*, vol. 4, no. 2, pp. 118–137, 2018.
[12] F. A. Alaba, M. Othman, I. A. T. Hashem, and F. Alotaibi, "Internet of Things security: a survey," *Journal of Network and Computer Applications*, vol. 88, pp. 10–28, 2017.
[13] W. H. Hassan, "Current research on the Internet of Things (IoT) security: a survey," *Computer Networks*, vol. 148, pp. 283–294, 2019.
[14] B. K. Mohanta, D. Jena, U. Satapathy, and S. Patnaik, "Survey on IoT security: challenges and solution using machine learning, artificial intelligence and blockchain technology," *Internet of Things*, vol. 11, Article ID 100227, 2020.
[15] M. Bures, T. Cerny, and B. S. Ahmed, "Internet of Things: current challenges in the quality assurance and testing methods," in *Proceedings of the International Conference on Information Science and Applications*, pp. 625–634, Macau, China, March 2018.
[16] M. Marjani, F. Nasaruddin, A. Gani et al., "Big IoT data analytics: architecture, opportunities, and open research challenges," *IEEE Access*, vol. 5, pp. 5247–5261, 2017.
[17] Q. Jing, A. V. Vasilakos, J. Wan, J. Lu, and D. Qiu, "Security of the Internet of Things: perspectives and challenges," *Wireless Networks*, vol. 20, no. 8, pp. 2481–2501, 2014.
[18] M. Safkhani and N. Bagheri, "Passive secret disclosure attack on an ultralightweight authentication protocol for Internet of Things," *The Journal of Supercomputing*, vol. 73, no. 8, pp. 3579–3585, 2017.
[19] P. K. Dhillon and S. Kalra, "A lightweight biometrics based remote user authentication scheme for IoT services," *Journal of Information Security and Applications*, vol. 34, pp. 255–270, 2017.
[20] C. Wang, G. Xu, and J. Sun, "An enhanced three-factor user authentication scheme using elliptic curve cryptosystem for wireless sensor networks," *Sensors*, vol. 17, no. 12, p. 2946, 2017.
[21] A. Adavoudi-Jolfaei, M. Ashouri-Talouki, and S. F. Aghili, "Lightweight and anonymous three-factor authentication and access control scheme for real-time applications in wireless sensor networks," *Peer-to-Peer Networking and Applications*, vol. 12, no. 1, pp. 43–59, 2019.
[22] Y. Lu, G. Xu, L. Li, and Y. Yang, "Anonymous three-factor authenticated key agreement for wireless sensor networks," *Wireless Networks*, vol. 25, no. 4, pp. 1461–1475, 2019.

[23] S. K. Vishwakarma, P. Upadhyaya, B. Kumari, and A. K. Mishra, "Smart energy-efficient home automation system using IoT," in *Proceedings of the 2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU)*, pp. 1–4, Ghaziabad, India, April 2019.

[24] H. Singh, V. Pallagani, V. Khandelwal, and U. Venkanna, "IoT based smart home automation system using sensor node," in *Proceedings of the 2018 4th International Conference on Recent Advances in Information Technology (RAIT)*, pp. 1–5, Dhanbad, India, March 2018.

[25] I. Froiz-Míguez, T. M. Fernández-Caramés, P. Fraga-Lamas, and L. Castedo, "Design, implementation and practical evaluation of an IoT home automation system for fog computing applications based on MQTT and ZigBee-WiFi sensor nodes," *Sensors*, vol. 18, p. 2660, 2018.

[26] S. S. Harsha, S. C. Reddy, and S. P. Mary, "Enhanced home automation system using Internet of Things," in *Proceedings of the 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics, and Cloud)(I-SMAC)*, pp. 89–93, Palladam, India, February 2017.

[27] J. Zhang, R. S. Blum, and H. V. Poor, "Approaches to secure inference in the Internet of Things: performance bounds, algorithms, and effective attacks on IoT sensor networks," *IEEE Signal Processing Magazine*, vol. 35, no. 5, pp. 50–63, 2018.

[28] H. Damghani, L. Damghani, H. Hosseinian, and R. Sharifi, "Classification of attacks on IoT," in *Proceedings of the 4th International Conference on Combinatorics, Cryptography*, Tehran, Iran, November 2019.

[29] S.-C. Lin, C.-Y. Wen, and W. A. Sethares, "Two-tier device-based authentication protocol against PUEA attacks for IoT applications," *IEEE Transactions on Signal and Information Processing over Networks*, vol. 4, pp. 33–47, 2017.

[30] A. Aldaej, "Enhancing cyber security in modern Internet of Things (IoT) using intrusion prevention algorithm for IoT (Spain)," *IEEE Access*, 2019.

[31] A. Hameed and A. Alomary, "Security issues in IoT: a survey," in *Proceedings of the 2019 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT)*, pp. 1–5, Sakhier, Bahrain, September 2019.

[32] Y. N. Soe, Y. Feng, P. I. Santosa, R. Hartanto, and K. Sakurai, "Rule generation for signature-based detection systems of cyber-attacks in IoT environments," *Bulletin of Networking, Computing, Systems, and Software*, vol. 8, pp. 93–97, 2019.

[33] M. Frustaci, P. Pace, G. Aloi, and G. Fortino, "Evaluating critical security issues of the IoT world: present and future challenges," *IEEE Internet of Things Journal*, vol. 5, pp. 2483–2495, 2017.

[34] S. Mondal and S. Patkar, "Hardware-Software co-implementation of a high performance and light-weight scalable Systolic-Montgomery based modified RSA for portable IoT devices," in *Proceedings of the 2021 International Conference on Emerging Smart Computing and Informatics (ESCI)*, pp. 439–443, Pune, India, March 2021.

[35] S. Madni, M. Shafiq, and H. U. Rashid, "ARMINTEL: a heterogeneous microprocessor architecture enabling intel applications on ARM," in *Proceedings of the 2020 17th International Bhurban Conference on Applied Sciences and Technology (IBCAST)*, pp. 370–377, Islamabad, Pakistan, January 2020.

[36] A. A. Abudaqa, T. M. Al-Kharoubi, M. F. Mudawar, and A. Kobilica, "Simulation of ARM and x86 microprocessors using in-order and out-of-order CPU models with Gem5 simulator," in *Proceedings of the 2018 5th International Conference on Electrical and Electronic Engineering (ICEEE)*, pp. 317–322, Istanbul, Turkey, May 2018.

[37] B. Afzal, M. Umair, G. Asadullah Shah, and E. Ahmed, "Enabling IoT platforms for social IoT applications: vision, feature mapping, and challenges," *Future Generation Computer Systems*, vol. 92, pp. 718–731, 2019.

[38] W. Zhou, Y. Jia, A. Peng, Y. Zhang, and P. Liu, "The effect of IoT new features on security and privacy: new threats, existing solutions, and challenges yet to be solved," *IEEE Internet of Things Journal*, vol. 6, pp. 1606–1616, 2018.

[39] A. Castiglione, M. Nappi, F. Narducci, and C. Pero, "Fostering secure cross-layer collaborative communications by means of covert channels in MEC environments," *Computer Communications*, vol. 169, pp. 211–219, 2021.

[40] A. Sangwan, "Cloud communication," *Design and Analysis of Security Protocol for Communication*, pp. 317–343, 2020.

[41] S. Jaloudi, "Communication protocols of an industrial Internet of Things environment: a comparative study," *Future Internet*, vol. 11, no. 3, p. 66, 2019.

[42] W. Anani, A. Ouda, and A. Hamou, "A survey of wireless communications for IoT echo-systems," in *Proceedings of the 2019 IEEE Canadian Conference of Electrical and Computer Engineering (CCECE)*, pp. 1–6, Edmonton, Canada, May 2019.

[43] M. Ammar, G. Russello, and B. Crispo, "Internet of Things: a survey on the security of IoT frameworks," *Journal of Information Security and Applications*, vol. 38, pp. 8–27, 2018.

[44] Y. Xiong, Y. Sun, L. Xing, and Y. Huang, "Extend cloud to edge with kubeedge," in *Proceedings of the 2018 IEEE/ACM Symposium on Edge Computing (SEC)*, pp. 373–377, Seattle, WA, USA, October 2018.

[45] L. Calderoni, A. Magnani, and D. Maio, "IoT manager: an open-source IoT framework for smart cities," *Journal of Systems Architecture*, vol. 98, pp. 413–423, 2019.

[46] N. Neshenko, E. Bou-Harb, J. Crichigno, G. Kaddoum, and N. Ghani, "Demystifying IoT security: an exhaustive survey on IoT vulnerabilities and a first empirical look on internet-scale IoT exploitations," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 3, pp. 2702–2733, 2019.

[47] F. A. Bukhsh, Z. A. Bukhsh, and M. Daneva, "A systematic literature review on requirement prioritization techniques and their empirical evaluation," *Computer Standards & Interfaces*, vol. 69, Article ID 103389, 2020.

[48] N. N. Thilakarathne, "Security and privacy issues in IoT environment," *International Journal of Engineering and Management Research*, vol. 10, 2020.

[49] Y. Ding, M. Jin, S. Li, and D. Feng, "Smart logistics based on the Internet of Things technology: an overview," *International Journal of Logistics Research and Applications*, vol. 24, no. 4, pp. 323–345, 2021.

[50] A. Salam, "Internet of Things for sustainability: perspectives in privacy, cybersecurity, and future trends," in *The Internet of Things For Sustainable Community Development*, pp. 299–327, Springer, Berlin, Germany, 2020.

[51] O. P. Yadav, "Internet of Things (IoT) security issue in wireless sensor network (WSN) with radio frequency identification (RFID)," vol. 2020.

[52] I. Rahaman, M. F. Reza, M. H. H. Hasib, M. I. Hossain, S. A. Hossain, and P. K. Sarkar, "A low-cost intelligent multi wireless sensor network perspective on real-time traffic surveillance," in *Proceedings of the 2019 International Conference on Computer, Communication, Chemical,*

Materials, and Electronic Engineering (IC4ME2), pp. 1–4, Rajshahi, Bangladesh, July 2019.

[53] J. Chen and Q. Zhu, "Interdependent strategic security risk management with bounded rationality in the Internet of Things," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 11, pp. 2958–2971, 2019.

[54] A. K. Mohammadzadeh, S. Ghafoori, A. Mohammadian, R. Mohammadkazemi, B. Mahbanooei, and R. Ghasemi, "A Fuzzy Analytic Network Process (FANP) approach for prioritizing Internet of Things challenges in Iran," *Technology in Society*, vol. 53, pp. 124–134, 2018.

[55] P. Malhotra, Y. Singh, P. Anand, D. K. Bangotra, P. K. Singh, and W.-C. Hong, "Internet of Things: evolution, concerns and security challenges," *Sensors*, vol. 21, no. 5, Article ID 1809, 2021.

[56] R. Zhang and Q. Zhu, "FlipIn: a game-theoretic cyber insurance framework for incentive-compatible cyber risk management of Internet of Things," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 2026–2041, 2019.

[57] S. Milivojevic, *Crime and Punishment in the Future Internet: Digital Frontier Technologies and Criminology in the Twenty-First Century*, Routledge, London, UK, 2021.

[58] B. Y. Lee, R. Cooper, D. Hands, and P. Coulton, "Exploring design implications for IoT products and services through comprehensive case studies," in *Proceedings of the 28th IPDMC: Innovation and Product Development Management Conference*, June 2021.

[59] E. Not, D. Cavada, and A. Venturini, "Internet of Things and ubiquitous computing in the tourism domain," *Handbook of e-Tourism*, Springer Nature, Switzerland, 2020.

[60] G. Fortino, C. Savaglio, C. E. Palau et al., "Towards multilayer interoperability of heterogeneous IoT platforms: the INTER-IoT approach," in *Integration, Interconnection, and Interoperability of IoT Systems*Springer, Berlin, Germany, 2018.

[61] V. R. Konduru and M. R. Bharamagoudra, "Challenges and solutions of interoperability on IoT: how far have we come in resolving the IoT interoperability issues," in *Proceedings of the 2017 International Conference on Smart Technologies for Smart Nation (SmartTechCon)*, pp. 572–576, Bengaluru, India, August 2017.

[62] A. Khalique, M. A. Alam, M. M. Khan, and I. Hussain, "A security paradigm of WSN, IoT, and CPS: challenges and solutions," *Integration of WSNs into the Internet of Things*, CRC Press, pp. 201–220, Boca Raton, FL, USA.

[63] H. ElSawy, "Characterizing IoT networks with asynchronous time-sensitive periodic traffic," *IEEE Wireless Communications Letters*, vol. 9, no. 10, pp. 1696–1700, 2020.

[64] M. Talal, A. A. Zaidan, B. B. Zaidan et al., "Smart home-based IoT for real-time and secure remote health monitoring of triage and priority system using body sensors: multi-driven systematic review," *Journal of Medical Systems*, vol. 43, no. 3, p. 42, 2019.

[65] S. Halder, A. Ghosal, and M. Conti, "Secure OTA software updates in connected vehicles: a survey," 2019, https://arxiv.org/abs/1904.00685.

[66] A. K. Sikder, G. Petracca, H. Aksu, T. Jaeger, and A. S. Uluagac, "A survey on sensor-based threats to internet-of-things (IoT) devices and applications," 2018, https://arxiv.org/abs/1802.02041.

[67] J. Y. Lee and J. Lee, "Current research trends in IoT security: a systematic mapping study," *Mobile Information Systems*, vol. 2021, Article ID 8847099, 25 pages, 2021.

[68] M. Mehta and K. Patel, "A review for IOT authentication–current research trends and open challenges," *Materials Today: Proceedings*, vol. 2018, 2020.

[69] M. Trnka, T. Cerny, and N. Stickney, "Survey of authentication and authorization for the Internet of Things," *Security and Communication Networks*, vol. 2018, Article ID 4351603, 17 pages, 2018.

[70] R. An, H. Feng, Q. Liu, and L. Li in *Proceedings of the International Conference on Broadband and Wireless Computing*, pp. 857–878, Communication and Applications, Asan, Korea, November 2016.

[71] J. Zhang, C. Shen, H. Su, M. T. Arafin, and G. Qu, "Voltage over-scaling-based lightweight authentication for IoT security," *IEEE Transactions on Computers*, vol. 2018, 2021.

[72] A. Ometov, V. Petrov, S. Bezzateev, S. Andreev, Y. Koucheryavy, and M. Gerla, "Challenges of multi-factor authentication for securing advanced IoT applications," *IEEE Network*, vol. 33, no. 2, pp. 82–88, 2019.

[73] Y. Liang, S. Samtani, B. Guo, and Z. Yu, "Behavioral biometrics for continuous authentication in the internet-of-things era: an artificial intelligence perspective," *IEEE Internet of Things Journal*, vol. 7, no. 9, pp. 9128–9143, 2020.

[74] M. Zhaofeng, M. Jialin, W. Jihui, and S. Zhiguang, "Blockchain-based decentralized authentication modeling scheme in edge and IoT environment," *IEEE Internet of Things Journal*, vol. 8, 2020.

[75] T. Alladi, V. Chamola, B. Sikdar, and K.-K. R. Choo, "Consumer IoT: security vulnerability case studies and solutions," *IEEE Consumer Electronics Magazine*, vol. 9, no. 2, pp. 17–25, 2020.

[76] B. I. Mohideen and B. Assiri, "Internet of Things (IoT): classification, secured architecture based on data sensitivity, security issues and their countermeasures," *Journal of Information and Knowledge Management*, vol. 20, no. 1, Article ID 2140001, 2021.

[77] A. S. Rachini and R. Khatoun, "Distributed key management authentication algorithm in the Internet of Things (IoT)," in *Proceedings of the 2020 Sixth International Conference on Mobile And Secure Services (MobiSecServ))*, pp. 1–5, Miami Beach, FL, USA, February 2020.

[78] Y. Qian, Y. Jiang, J. Chen et al., "Towards decentralized IoT security enhancement: a blockchain approach," *Computers and Electrical Engineering*, vol. 72, pp. 266–273, 2018.

[79] M. S. Hossein, T. Tabassum, M. A. Islam, R. Karim, L. S. Rumi, and A. A. Kobita, "Digital signature authentication using asymmetric key cryptography with different byte number," in *Evolutionary Computing and Mobile Sustainable Networks*Springer, Berlin, Germany, 2021.

[80] A. Acar, H. Fereidooni, T. Abera et al., "Peek-a-Boo: I see your smart home activities, even encrypted," in *Proceedings of the 13th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, pp. 207–218, Linz, Austria, July 2020.

[81] W. Iqbal, H. Abbas, B. Rauf, Y. Abbas, F. Amjad, and A. Hemani, "PCSS: privacy-preserving communication scheme for SDN enabled smart homes," *IEEE Sensors Journal*, 2021.

[82] I. Batra, S. Verma, M. Kavita, and M. Alazab, "A lightweight IoT-based security framework for inventory automation using wireless sensor network," *International Journal of Communication Systems*, vol. 33, no. 4, Article ID e4228, 2020.

[83] R. Setiawan, R. R. Ganga, P. Velayutham et al., "Encrypted network traffic classification and resource allocation with

deep learning in a software-defined network," *Wireless Personal Communications*, pp. 1–17, 2021.

[84] R. Yugha and S. Chithra, "A survey on technologies and security protocols: reference for future generation IoT," *Journal of Network and Computer Applications*, vol. 169, Article ID 102763, 2020.

[85] D. K. Panda and S. Das, "Smart grid architecture model for control, optimization and data analytics of future power networks with more renewable energy," *Journal of Cleaner Production*, vol. 301, Article ID 126877, 2021.

[86] L. A. Neira Lagos, *Desarrollo de un módulo "off-line" que permita el funcionamiento de un dispositivo de aprendizaje del alfabeto braille*, Universidad del Rosario, Bogotá, Colombia, 2021.

[87] S. Aruna, G. Usha, P. Madhavan, and M. V. R. Kumar, "Lightweight cryptography algorithms for IoT resource-starving devices," *Role of Edge Analytics in Sustainable Smart City Development*, pp. 139–169, 2020.

[88] M. Chakraborty and M. Singh, "Introduction to network security technologies," in *The "Essence" of Network Security: An End-To-End Panorama*, pp. 3–28, Springer, Berlin, Germany, 2021.

[89] A. M. Abuagoub, "IoT security evolution: challenges and countermeasures review," *International Journal of Communication Networks and Information Security*, vol. 11, pp. 342–351, 2019.

[90] L. Gutiérrez-Madroñal, A. García-Domínguez, and I. Medina-Bulo, "Evolutionary mutation testing for IoT with recorded and generated events," *Software: Practice and Experience*, vol. 49, pp. 640–672, 2019.

[91] I. Ha, "Security and usability improvement on a digital door lock system based on Internet of Things," *International Journal of security and its applications*, vol. 9, no. 8, pp. 45–54, 2015.

[92] S. Singh, P. K. Sharma, B. Yoon, M. Shojafar, G. H. Cho, and I.-H. Ra, "Convergence of blockchain and artificial intelligence in IoT network for the sustainable smart city," *Sustainable Cities and Society*, vol. 63, Article ID 102364, 2020.

[93] J. H. Jo, P. K. Sharma, J. C. S. Sicato, and J. H. Park, "Emerging technologies for sustainable smart city network security: issues, challenges, and countermeasures," *Journal of Information Processing Systems*, vol. 15, pp. 765–784, 2019.

[94] M. B. Janjua, A. E. Duranay, and H. Arslan, "Role of wireless communication in healthcare system to cater disaster situations under 6G vision," *Frontiers in Communications and Networks*, vol. 1, no. 6, 2020.

[95] T. Lei, Z. Qin, Z. Wang, Q. Li, and D. Ye, "EveDroid: event-aware Android malware detection against model degrading for IoT devices," *IEEE Internet of Things Journal*, vol. 6, no. 4, pp. 6668–6680, 2019.

[96] I. B. Ida, A. Jemai, and A. Loukil, "A survey on security of IoT in the context of eHealth and clouds," in *Proceedings of the 2016 11th International Design and Test Symposium (IDT)*, pp. 25–30, Hammamet, Tunisia, December 2016.

[97] F. Meneghello, M. Calore, D. Zucchetto, M. Polese, and A. Zanella, "IoT: internet of threats? a survey of practical security vulnerabilities in real IoT devices," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8182–8201, 2019.

[98] Z. Vahdati, S. Yasin, A. Ghasempour, and M. Salehi, "Comparison of ECC and RSA algorithms in IoT devices," *Journal of Theoretical and Applied Information Technology*, vol. 97, 2019.

[99] B. Mbarek, M. Ge, and T. Pitner, "An efficient mutual authentication scheme for Internet of Things," *Internet of Things*, vol. 9, Article ID 100160, 2020.

[100] H. Golpîra, S. A. R. Khan, and S. Safaeipour, "A review of logistics internet-of-things: current trends and scope for future research," *Journal of Industrial Information Integration*, Article ID 100194, 2021.

[101] C. G. Schmidt and S. M. Wagner, "Blockchain and supply chain relations: a transaction cost theory perspective," *Journal of Purchasing and Supply Management*, vol. 25, no. 4, Article ID 100552, 2019.

[102] Z. E. Mrabet, N. Kaabouch, H. E. Ghazi, and H. E. Ghazi, "Cyber-security in smart grid: survey and challenges," *Computers & Electrical Engineering*, vol. 67, pp. 469–482, 2018.

[103] C. J. D'Orazio, R. Lu, K.-K. R. Choo, and A. V. Vasilakos, "A Markov adversary model to detect vulnerable iOS devices and vulnerabilities in iOS apps," *Applied Mathematics and Computation*, vol. 293, pp. 523–544, 2017.

[104] M. Abomhara and G. M. Køien, "Cyber security and the Internet of Things: vulnerabilities, threats, intruders and attacks," *Journal of Cyber Security and Mobility*, vol. 4, no. 1, pp. 65–88, 2015.

[105] P. Goyal, A. K. Sahoo, T. K. Sharma, and P. K. Singh, "Internet of Things: applications, security and privacy: a survey," *Materials Today: Proceedings*, vol. 34, pp. 752–759, 2021.

[106] S. A. Al-Qaseemi, H. A. Almulhim, M. F. Almulhim, and S. R. Chaudhry, "IoT architecture challenges and issues: lack of standardization," in *Proceedings of the 2016 Future Technologies Conference (FTC)*, pp. 731–738, San Francisco, CA, USA, December 2016.

[107] D. Saba, Y. Sahli, R. Maouedj, and A. Hadidi, "Energy management based on Internet of Things," *Recent Advances in Technology Acceptance Models and Theories*, Springer International Publishing, Berlin, Germany, pp. 349–372, 2021.