Hindawi
Journal of Sensors
Volume 2022, Article ID 5724168, 20 pages
https://doi.org/10.1155/2022/5724168

Review Article

A Review of Security and Privacy Concerns in the Internet of Things (IoT)

Muhammad Aqeel,[1] Fahad Ali,[2] Muhammad Waseem Iqbal,[1] Toqir A. Rana,[3,4] Muhammad Arif,[5] and Md. Rabiul Auwul[6]

[1]*Department of Software Engineering, The Superior University, Lahore, Pakistan*
[2]*Department of Information Technology, The Superior University, Lahore, Pakistan*
[3]*Department of Computer Science and IT, The University of Lahore, Lahore, Pakistan*
[4]*School of Computer Sciences, Universiti Sains Malaysia, Penang, Malaysia*
[5]*Department of Computer Science, The Superior University, Lahore, Pakistan*
[6]*Faculty of Science and Technology, Department of Mathematics, American International University-Bangladesh, Dhaka, Bangladesh*

Correspondence should be addressed to Md. Rabiul Auwul; rabiulauwul@gmail.com

Received 29 July 2022; Revised 26 August 2022; Accepted 8 September 2022; Published 29 September 2022

Academic Editor: Sweta Bhattacharya

The recent two decades have witnessed tremendous growth in Internet of things (IoT) applications. There are more than 50 billion devices connected globally. IoT applications' connectivity with the Internet persistently victimized them with a divergent range of traditional threats, including viruses, worms, malware, spyware, Trojans, malicious code injections, and backdoor attacks. Traditional threats provide essential services such as authentication, authorization, and accountability. Authentication and authorization are the process of verifying that a subject is bound to an object. Traditional authentication and authorization mechanisms use three different factors to identity a subject to verify if the subject has the right capability to access the object. Further, it is defined that a computer virus is a type of malware. Malware includes computer viruses, worms, Trojan horses, spyware, and ransomware. There is a high probability that IoT systems can get infected with a more sophisticated form of malware and high-frequency electromagnetic waves. Purpose oriented with distinct nature IoT devices is developed to work in a constrained environment. So there is a dire need to address these security issues because relying on existing traditional techniques is not good. Manufacturers and researchers must think about resolving these security and privacy issues. Most importantly, this study identifies the knowledge and research gap in this area. The primary objective of this systematic literature review is to discuss the divergent types of threats that target IoT systems. Most importantly, the goal is to understand the mode of action of these threats and develop the recovery mechanism to cover the damage. In this study, more than 170 research articles are systematically studied to understand security and privacy issues. Further, security threats and attacks are categorized on a single platform and provide an analysis to explain how and to what extent they damage the targeted IoT systems. This review paper encapsulates IoT security threats and categorizes and analyses them by implementing a comparative study. Moreover, the research work concludes to expand advanced technologies, e.g., blockchain, machine learning, and artificial intelligence, to guarantee security, privacy, and IoT systems.

1. Introduction

Current trends of technology "connect the unconnected," which means every object that can be connected will be connected in the upcoming years. The IoT is the network of physical objects containing sensors and processing powers embedded in devices to connect the end-users to wide-area networks for transmission [1]. It can be seen everywhere around us, including automobiles, public lights, domestic appliances, health-care systems, and personal digital assistants like Google Home. For example, IoT gateways allow fast and easy access to the IoT world, and they are

compatible with IoT servers (Microsoft Azure, Amazon AWS, IBM Cloud, Google Cloud, etc.) and customized servers that support MQTT. Globally, IoT devices are attached to the Internet and communicate information through embedded sensors and software [2]. These devices minimize the human effort to create easiness in life and maximize resource utilization. These devices help humans to make better decisions for upgrading the standard of a user's life [3]. The idea of connecting the unconnected devices is almost 188 years old. It was introduced in 1832 when the first electromagnetic telegraph was invented. At that time, the idea was translated into the terms "Embedded Internet" or "Pervasive Computing," and the first-ever connected device was Coca-Cola vending machine [4].

Today's term "The Internet of Things (IoT)" was first introduced by Kelvin Ashton in 1999 to advance communication and facilitate human interaction in a virtual environment. According to a survey, the number of connected devices touches the figure of 50 billion by the end of 2020 and will grow to 14.7 billion by 2023 [5]. Nowadays, IoT technology is primarily seen in industries and commercial sectors. The interconnected divergent kinds of intelligent gadgets vary from simple wearable and household devices to large machines. These objects contain chips that are used to inspect and pursue the facts. It is predicted that the IoT market will touch the figure of 5.8 billion by the end of 2020, which is 21% higher than in 2019. This technology is used in intelligent projects, i.e., smart cities, smart farming, smart homes, and health-care systems. According to Grand View Research, the small patient market generates around $1.8 billion by the end of 2026 [6].

The significance and contribution of this research on IoT security and privacy are the well-being of humanity according to people's likes, needs, wishes, and desires without any explicit instruction to IoT devices. These devices also serve the community by aiding in surgery, weather forecasting, animal identification, and automobile tracking.

The rapid growth of intelligent devices made IoT a growing technology, so it is essential to understand the privacy and security challenges. It is necessary to understand and address these issues for human sake. Humans can get benefit to handle these security and privacy threats in IoT. This systematic literature review (SLR) provides significant guidelines for IoT security and privacy issues. In this study, 170 research articles have been used as a reference to conduct the survey for security and privacy issues in IoT.

2. Literature Review

Tremendous work and effort have been made recently to cope with safety and confidential problems in IoT. Many reports and surveys are published to address IoT security-related issues and challenges. Yang et al.'s survey presents the safety and personal issues with solutions directly related to low-end systems [7]. Different authors briefly discuss the IoT security-based issues and challenges for networks, devices, and systems [2]. Weber and Gopi and Rao's surveys discuss the challenges and issues concerned with security in four steps such as (1) limitations of IoT devices like battery life extension, (2) lightweight computation, (3) classification of security attacks, and (4) control access mechanisms and architecture [8, 9]. The discussion is also available on different IoT architecture layers (presentation, network, transport, and application).

Weber's survey discusses security and privacy challenges, and researchers also present a security framework for IoT-based devices [8]. The IoT devices are getting fame globally that involve other innovating technologies widely used in the whole world to transport goods from region to region. This technology is visibly becoming familiar. The low-ended devices contain different sensing gadgets and also have the capacity to interconnect with other similar gadgets and can transmit facts or information. The main challenge of IoT devices is related to privacy and security. The administration of that extensive data to process reliably and securely in machines is a real problem. These IoT also present challenges for individuals' protection, safety, and confidentiality. In this research article, the authors discuss the growing requirement of this technology for appropriate regulatory and technicalities to heal the gap between automated surveillance by IoT-based devices and the official rights of people unaware of their safety and confidentiality risk. Aleisa and Renaud identify the issues and challenges related to IoT privacy, its principles, threats, and proposed solutions [10].

Tewari and Gupta presented another survey for security-related problems in IoT devices. This article analyzes IoT devices' layered architecture and highlights new security issues. They discussed the crosslayer heterogeneous integration problems and provided tools and techniques for research in IoT [11]. The comparison of different studies in various aspects (simulation tools, mechanisms, IoT devices security, and privacy) was made by Noor and Hassan in 2019. It explores the current IoT security mechanisms such as authentication, security encryption, trust management, and emerging technologies to secure IoT devices [12].

Further, a study is presented on personal and safety-related problems identified by the experts in IoT devices and highlights how privacy is different from the other fields. It contains facts belonging to IoT specialists who tried to perceive safety and confidential problems and proposed new security protocols for efficient security and privacy mechanisms (SPMs) [13]. Most all connected devices have high risks and threats and can be hacked.

The objective behind this malicious act may differ depending upon the intruder's intention. There are mainly two types of threats, i.e., natural threats and human threats. The data can be protected from natural hazards, but devices may be physically damaged and not be restored. Moreover, many researchers have made tremendous efforts to protect IoT devices from human-generated threats and attacks. Table 1 shows the comparison of different types of attacks in IoT.

Cybersecurity threats can be categorized into two main types based on their objectives. The intruder intends to knock out the targeted device in the first type completely. In the second type, the attacker aims to get the privileges of admin or unauthorized access privileges to targeted devices. Divergent methods are utilized to gain unauthorized access, i.e., malware, denial of service, SQL injection, and cybercriminal. With the advancement of technologies, these

Table 1: Comparison of security and privacy attacks in IoT.

Reference paper	Attack type	Citation	Year	Objectives
Sybil attacks and their defenses in the IoT [14].	Sybil attacks	131	2014	Sybil attacks and defenses scheme research issues for Sybil defense in IoT.
Deceptive attack and defense game in honeypot-enabled networks for the IoT [15].	Deceptive attack	38	2016	Designed and extended a game-theoretic model.
Secure Location of Things (SLOT): mitigating, localization, and spoofing attacks in the IoT [16].	Spoofing	04	2017	The maximum likelihood estimator (MLE) for the tag's location is essential to protect IoT devices from malicious attacks.
Securing the SDN infrastructure of IoT-fog networks from MitM attacks [17].	Man in the middle attack	12	2017	The security issues of open flow channels like MitM attacks.
A security design for detecting buffer overflow attacks in IoT devices [18].	Buffer overflow attack	02	2018	They suggest lightweight design methodologies and architectural techniques to solve IoT devices' security problems.
Side-channel security analysis of our signature for cloud-based IoT [19].	Side-channel security	04	2018	Proposed an algorithm to secure UOV and related signatures from side-channel attacks.
IoT application protection against power analysis attack [20].	Power analysis attack	11	2018	Different attack scenarios of SPA introduced a branchless countermeasure approach.
Security in fog computing: a novel technique to tackle an impersonation attack [21].	Impersonation attack	12	2018	Q-learning algorithm detects the impersonation attack more accurately in fog computing-based networks.
Routing attacks and mitigation methods for RPL-based IoT [22].	Routing attacks	18	2018	Discussed RPL comprehensively. Study and present the RPL standard, mitigation methods, and published attacks in detail.
DDoS attack detection and mitigation with software-defined IoT framework [23].	Distributed DoS	44	2018	Introduced a framework for software-defined Internet of Things (SD-IoT).
Extensive validation of a SIR epidemic model to study the propagation of jamming attacks against IoT wireless networks [24].	Jamming attacks	01	2019	Proposed the SIR epidemiological model for jamming attacks in physical and MAC layers in IoT wireless networks.
A mobile code-driven trust mechanism for detecting internal attacks in sensor node-powered IoT [25].	Internal attacks	03	2019	Introduced the energy-efficient mobile code-driven trust mechanism (MCTM) to identify and handle malicious forwarding attacks, like a black and grey hole.
Analytical model for Sybil attack phases in the IoT [26].	Sybil attacks	03	2019	Sybil attacks from the IoT perspective comprehensively. Introduced and implemented an algorithm based on K-means clustering.
RAV: relay aided vectorised secure transmission in physical layer security for the IoT under active attacks [27].	Active attacks	05	2019	Introduced a transmission scheme for IoT networks to secure downlink communication.
An efficient collision power attack on AES encryption in edge computing [28].	Power analysis attack	04	2019	Discussed three AES implementations in edge computing. Introduced a new type of collision attack for masked linear layers and masked S-boxes.
IoT-FBAC: function-based access control scheme using identity-based encryption in IoT [29].	Access control	06	2019	They have proposed a new scheme to control access to IoT devices. They named it the function-based access control scheme.
A real-time intrusion detection system for wormhole attacks in the RPL-based IoT [30].	Wormhole attack	09	2019	Proposed a system to detect wormhole attacks. This intrusion detection system runs on Contiki OS and Cooja simulator.
Detection of multiple-mix-attack malicious nodes using perceptron-based trust in IoT networks [31].	Malicious node	03	2019	We mainly discussed three attacks: replay, tamper, and drop. Suggest an approach of perceptron detection (PD) to identify malicious nodes.
Averaged dependence estimators for DoS attack detection in IoT networks [32].	DoS attacks	06	2020	They have proposed a framework for DoS detection. Experimentally tested this framework with an actual IoT attack.
Deep recurrent neural network for IoT intrusion detection system [33].	Intrusion detection System	03	2020	Proposed an automatic intrusion detection system to implement fog computing security against cyberattacks.

cyberattacks are also getting advanced. Cyberattacks pull the attention of researchers [2, 7, 9, 13, 18, 30] to address these issues, but still, these issues are needed to be addressed.

With the growth of connected devices, problems and challenges are also increasing rigorously. Many new and emerging technologies are integrated with IoT to overcome these issues, i.e., fog computing, artificial intelligence, and blockchain. These advanced technologies are also used in collaboration with IoT to solve security and privacy issues. These technologies, especially blockchain, are gaining the attention of researchers and playing the role of a trusted third party. The blockchain can protect IoT devices, security, and safety-critical data. Integrating blockchain with IoT technology can provide an effective solution for security- and privacy-related issues and the challenges of IoT gadgets. Many researchers [3, 8, 15, 20, 28, 34, 37, 39, 43] also address the collaboration of these technologies and provide a robust solution. Table 2 presents some work done by researchers in recent years to address IoT security threats and attacks.

IoT applications are used globally to facilitate users, but there are still issues with security and privacy. Many researchers have discussed significant guidelines and solutions to cater to these issues. Table 3 shows the comparison of cyberattacks in IoT applications.

Another study is conducted by Sengupta et al. about the industrial IoT issues. It classifies the security and privacy attacks on their destructibility that explains to provide a blockchain-based solution [74]. Further, Wang et al. and Weber have discussed blockchain technology and explored some features such as access management, decentralization, asymmetric encryption, and smart contracts [75, 76]. Khan and Salah discussed the layered architecture networking, management, and communication protocols [77]. Another study conducted by Qian et al. explores layer-based architecture security and privacy problems for IoT [78]. The proposed security mechanisms eliminate the need for a third party to protect IoT terminal devices [79]. The security mechanism using blockchain technology's decentralization feature in two conditions has been discussed in the remote cloud, network terminal, and devices [80, 81]. Bitcoin currency is a modern and visibly growing blockchain-based technology [82, 83]. IoT devices are progressively inclined to assault and cannot ensure themselves [84]. Besides that, it cannot be handled after the execution of the blockchain [85]. The solution for blockchain to eliminate safety is to use confidential transmission of the facts and figures [86–88].

Table 2: IoT security threats and attacks.

Focus area	References
Insecure nearest node discovery	[22, 34, 35]
Replay attack	[6, 36, 37]
Sleep deprivation attack	[38–40]
Buffer overflow attack	[6]
Jamming attacks	[41–43]
DoS attacks	[6, 44]
Spoofing attacks	[45–47]
Insecure initialization and configuration	[41–43, 45, 48]
Routing attack	[49–51]
Sinkhole and wormhole attacks	[52–54]
Sybil attacks	[14, 55–57]
Authentication and secure communication	[52, 53, 56–60]
End-to-end security	[61, 62]
Session hijacking	[63–65]
Deprivation attack	[66, 67]
Insecure interfaces	[68]

3. Review Methodology

The study is grounded in an SLR on IoT security and privacy issues by analyzing a significant data stream of substantial literature. There are three classified phases: planning, conducting, and reporting the review. Figure 1 describes the classified phases for this study.

3.1. Phase 1: Planning the Review. To conduct SLR on security and privacy issues in IoT, we followed the methodology proposed by Kitchenham [89]. The main work is divided into three steps: planning, conducting, and reporting the reviews.

3.1.1. Study Selection. This step describes the criteria to select material by studying the abstract, introduction, and conclusion sections of different research papers. Only those research articles are selected that fulfill the following requirements:

(i) Written in the English language

(ii) Describe the security challenges of IoT devices

(iii) Discuss the emerging technology-based solutions to IoT devices' security and privacy issues

(iv) Provide information about IoT devices

(v) Provide information about IoT threats

(vi) Present techniques to solve the problems of IoT devices

(vii) Published between 2003 and March 2021

Further, some absolute principles are excluded:

(i) Papers are not written in the English language

(ii) Papers related to IoT devices and applications were issued before 2003

(iii) Papers do not relate to IoT devices

(iv) Papers with less than four pages

(v) Papers that do not report any empirical study and solution

(vi) Papers without significant opinions and viewpoints

(vii) Irrelevant theses

Table 3: Comparison of cyberattacks in IoT applications.

Reference paper	Cited by	Year	Objectives
Cyberentity security in the IoT [69].	111	2013	The cyberentity domains in the U2IoT. Cybersecurity requirements, security attacks, and system vulnerabilities in the context of the cyberentities in the U2IoT.
Cybersecurity and the IoT: vulnerabilities, threats, intruders, and attacks [70].	221	2015	Cybersecurity attacks. Identification and vulnerabilities of threats. Malicious attacks.
Defense against black holes and selective forwarding attacks for medical WSNs in the IoT [71].	43	2016	Issues in wireless routing. Cyberattacks on IoT devices, especially black holes, and selective forwarding (SF) attacks.
Intrusion detection system to detect sinkhole attack on RPL protocol in the IoT [72].	76	2017	Identify the sinkhole attack in the network. Introduced an intrusion detection system (IDS) based on RPL as a routing protocol.
Cybersecurity threats to IoT applications and service domains [73].	30	2017	Discussed IoT applications and also presented significant cybersecurity challenges and issues.

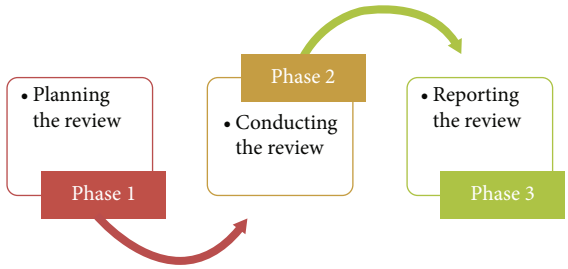

Figure 1: Systematic literature review (SLR) planning phases.

3.1.2. Data Extraction and Quality Assessment. To perform the quality assessment of this article, both qualitative and quantitative methods are used. There is no restriction in terms of experimental design. A quality assessment study checklist ensures the data extraction fulfills the quality criteria. Table 4 shows a list of general questions to measure the quality of selected papers by using two scales for the quality assessment checklist: yes = 1 and no = 0.

3.1.3. Identification of the Need for Review. The main objective of this study is to closely analyze the existing literature on IoT security, privacy, and threats to IoT systems. The study highlights significant research findings in the field of IoT security. The other purpose of this study is to emphasize utilizing emerging technologies for better solutions.

3.1.4. Inclusion/Exclusion Criteria. The criteria of inclusion and exclusion of papers are decided based on the significance of the literature. Initially, 500 papers were downloaded in IoT security and privacy. After the slight screening, 345 articles were filtered according to their duplication and irrelevance. The best 245 articles were identified in the next round by carefully reading their titles, abstracts, and introductions. Finally, we read full papers to further categorize them according to work needs, and 176 were selected to answer the questions related to our research problem. Figure 2 shows the inclusion and exclusion criteria for the selection of papers.

3.1.5. Specifying the Research Questions. The research questions are made based on the existing research studies. The significant articles and in-depth knowledge motivate us to create questions.

The research questions for this study are described below.

RQ1: How has IoT evolved drastically in the modern era?

RQ2: What types of challenges and issues of IoT systems are essential to be addressed?

RQ3: Why do IoT security and privacy challenges need to be reported?

RQ4: How the security and privacy challenges are classified?

RQ5: How do emergent technologies can resolve these issues in IoT applications?

3.1.6. Bibliographic Database. We use some digital libraries to search for the required material: Academia, Science Direct, Google Scholar, Google Search, Springer, IEEE Xplore, and Research Gate to conduct this survey. These automated libraries comprise literature linked to the discipline of security and IoT. In this research article, the studies are limited to research journals and conference papers published between 2003 and 2021. Figure 3 describes the detailed information of the digital libraries used for this article.

We classified the papers based on the discussed attacks. Only 1% of the articles addressed access-level attacks, 16% described cryptanalysis attacks, and 10% discussed network-based security issues. The percentage of other attacks is presented in Figure 4.

3.2. Phase 2: Conducting the Review. Figure 5 shows the three subphases for the review: (i) study selection, (ii) data extraction and quality assessment, and (iii) data extraction and synthesis.

The umbrella terms such as security, privacy, low-ended devices, and small automatic and fully automated devices are identified to determine the search engine. In the end, the Boolean operators "OR" and "AND" combine the various keywords and create different combinations for searching terms related to research questions. Some examples of keywords and operators to extract data are given:

(i) Security "OR" privacy issues "OR" security "OR" privacy challenges "OR" problems

Table 4: Quality assessment of the survey.

No	Item	Yes	No
Q1	Are the aims and objectives of the research clearly stated?	1	
Q2	Does the author review previous studies?	1	
Q3	Is current and relevant research used?	1	
Q4	Does work seem helpful for this research?	1	
Q5	Does the author appear to have any biases (gender, race, class, or politics)?		0
Q6	Is the writing clear and easy to follow?		0
Q7	Are visuals such as tables, charts, maps, and figures helpful?	1	
Q8	Are visuals such as tables, charts, maps, and figures confusing or hard to read?		0
Q9	Is there any need to conduct more research on this subject?	1	
Q10	Is the article relevant to this domain of research?	1	
Q11	Have the researcher(s) adequately carried out the data collection process?	1	
Q12	Have the researcher(s) used enough data to support their results and analysis?		0
Q13	Is there a detailed comparison of other techniques in the experiment?		0

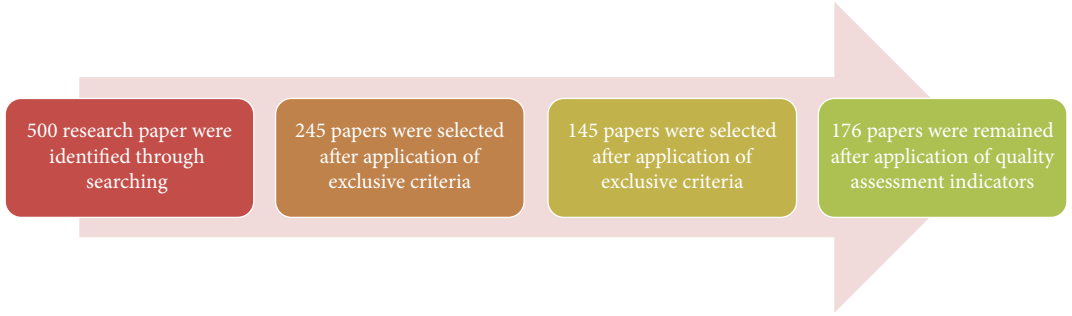

Figure 2: Flow diagram for the inclusion and exclusion criteria.

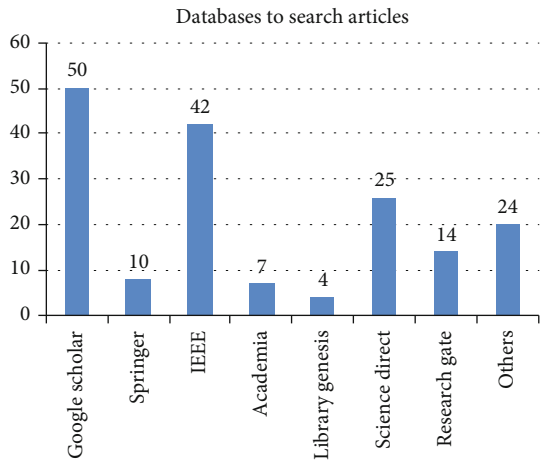

Figure 3: Databases used to search research papers.

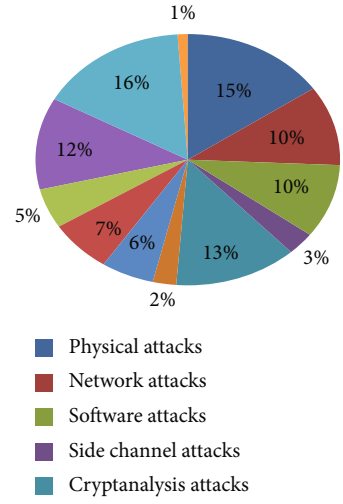

Figure 4: Databases used to search research papers.

(ii) IoT "OR" low ended "OR" small "OR" handheld "OR" consumer connected "OR" smart "OR" automated "OR" mobile devices

(iii) Security "OR" privacy issues "OR" challenges in IoT devices "And" security problems in smart devices "AND" security challenges in mobile devices

3.3. Phase 3: Reporting the Review. In this phase, the discussed research questions are answered by keeping in mind the significance of the study.

3.3.1. RQ1: How Has IoT evolved Drastically in the Modern Era? IoT technology is growing faster day by day and dominating globally. According to a survey conducted in 2019 by

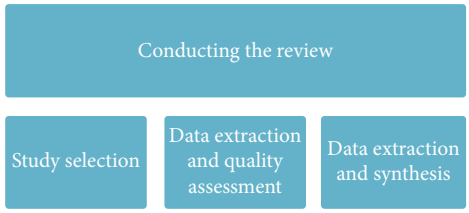

Figure 5: Phases for conducting the review.

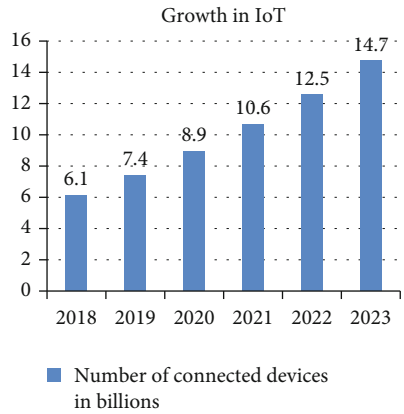

Figure 6: Growth in IoT devices during 2018-2023 [6].

Gartner, it is predicted that the IoT market will touch the figure of 5.8 billion by the end of 2020, which is 21% higher than in 2019 [6]. According to a current report for the year 2018-2023 that Cisco IBSG conducts, the number of connected devices was 6.1 billion in 2018 and will grow to 14.7 billion by 2023. The growth of IoT devices is shown in Figure 6.

3.3.2. RQ2: What Types of Challenges and Issues of IoT Systems Are Essential to be Addressed? Nowadays, the rapid growth of intelligent devices made IoT a growing technology. It is essential to understand all challenges and deal with issues related to these devices; the advancement and maintainability of IoT devices make these systems complex to manage. The system cannot prevail due to these IoT issues such as outdated software and hardware, compatibility issues, security issues, cloud attacks, modifications, difficulties related to passwords, low-ended worms, facts related to security, and confidential provocations. Further, IoT discrepancies may also occur due to untrustworthy communication, problem finding the device's effectiveness, automation systems for data management, limited IoT device management, low power network support, IoT operating systems, and processor-related issues [77, 90].

3.3.3. RQ3: Why Do IoT Security and Privacy Challenges Need to Be Reported? Advancements in technology can be seen in recent years, introducing variant types of IoT devices. These devices are connected to many networks and each other, making them vulnerable and easy to attack. To mitigate the vulnerabilities of the devices that share sensitive information/data, it is essential to identify all possible attacks to make countermeasures or defense strategies. Figure 7 shows the different issues and challenges in IoT devices.

3.3.4. RQ4: How the Security and Privacy Challenges Are Classified? The security threats in IoT are classified into various types like physical attacks, network attacks, software-based attacks, data attacks, side-channel attacks, cryptanalysis attacks, access-level attacks, and strategy-level attacks. Figure 8 shows the classification of IoT security attacks.

(1) Physical Attack. In physical attacks, direct physical access to the devices is required. Physical attacks utilize the hardware components of IoT devices [70, 91]. Based on interaction with the targeted systems, the physical attack is classified into three categories, i.e., invasive attacks, noninvasive attacks, and semi-invasive attacks [92, 93].

Invasive attacks: the category of attacks in which the attacker needs to approach the chips or detach the targeted devices physically is known as invasive attacks. High skills and specialized tools are required to launch invasive physical attacks depending on what type of attack is to be established and IoT device [92].

Noninvasive attacks: in this category of physical attacks, the attacker approaches the targeted devices using the device's input interface. These attacks harm the targeted IoT devices without physical damage.

Semi-invasive attacks: in this category of physical attacks, the attacker approaches the targeted IoT devices without interacting with internal structures and wires.

Jamming attacks: these attacks are designed to block IoT network wireless communication channels by employing malicious nodes that generate noise signals [94]. Other categories known as reactive jamming attacks generate the interfering signals only when the transmission channels communicate [95].

Object replication: this type of attack intruder injects a duplicate node into the IoT network to alter its function. The objective of object replication attacks is to steal the information and authentication credentials by introducing a replicated malicious node [96, 97].

Malicious node injection attacks: in malicious node injection attacks, attackers physically inject a malicious node between two or additional existing nodes of an IoT network. The term "man in the middle attacks" can also be referred to as "malicious node injection attacks" [91, 98].

Sleep denial attack: these attacks affect the sleep mode and keep the device awake to increase the battery consumption and affect IoT devices. In some cases, these attacks transfer unauthenticated packets; the decoding of these transmitted packets causes wastage of battery. The intruder observes the IoT networks to determine when to reseal the packet [99, 100].

Tampering attacks: the main objective behind node tampering attacks is to access the IoT device to alter other communication layers' functions or steal the data like cryptographic keys [101, 102].

Permanent denial of service (PDoS): permanent denial-of-service attacks (PDoS), also known as plashing, is an attack that damages the device so severely that it requires replacement or reinstallation of hardware. BrickerBot, coded to exploit hard-coded passwords in IoT devices and cause a permanent denial of service, is one such example of malware

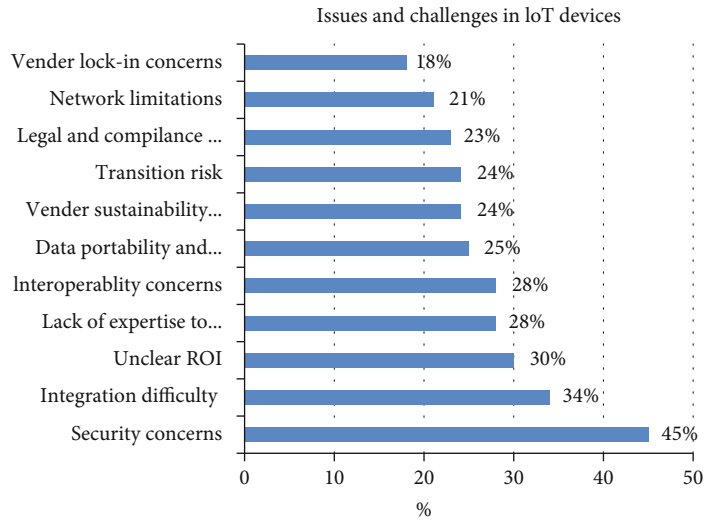

Figure 7: Comparison of issues and challenges of IoT [6, 9].

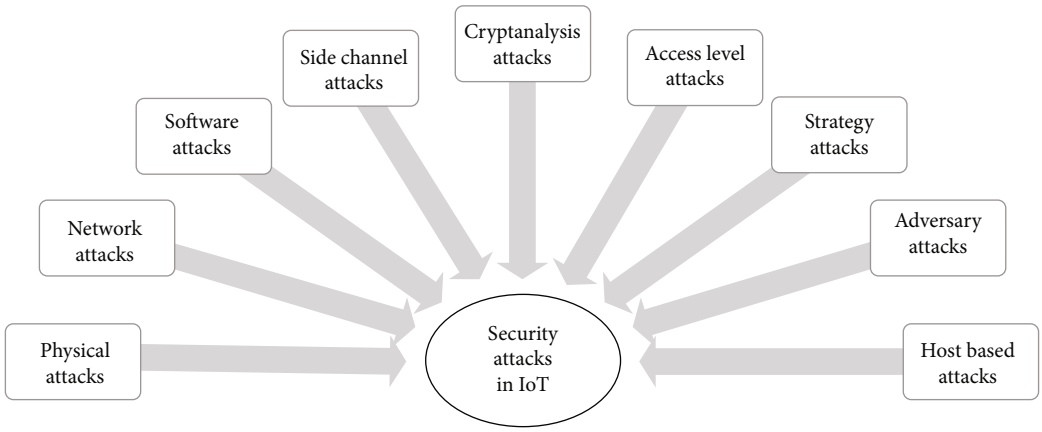

Figure 8: Classification of IoT security attacks.

that could be used to disable critical equipment on a factory floor wastewater treatment plant or an electrical substation [103].

Fake node injection: fake node injection attacks are one of the most damaging attacks for IoT devices in which attackers insert a malicious node or generate a false identity with the help of a fake node to access the IoT network and flow the incorrect information hits all the nodes in the network [104]. These attacks also lead to poor performance by consuming whole IoT system resources. In worse cases, false node injection attacks can destroy the entire IoT network or help the attacker take complete control of the IoT network [105].

Hardware Trojan: in HT, attackers physically insert a malicious circuit or modify an existing circuit in IoT devices to alter the circuit's operation. The primary purpose behind Trojan attacks is to bypass the authentication and access control mechanisms, steal information, or seriously damage the chips [106]. In HT, attackers physically insert a malicious circuit or modify an existing circuit in IoT devices to alter the circuit's operation [107].

Outage attack: outage attacks prevent remote IoT devices from completing their routine task. In worse cases, these attacks turn off IoT devices. Outage attacks may launch a sleep denial attack and drain the battery to shut down the remote IoT device [108]. An example of these attacks is Stuxnet, inserted in Iran's nuclear process control program. Due to the Stuxnet attack, the system cannot detect emergency conditions. Therefore, it does not turn off [109].

Tag cloning: the tag cloning attacks scan the RFID tags from the targeted device into the attacker's defined RFID tag, providing access to confidential information about individuals. The tag cloning attacks can cause financial loss and damage the manufacturer's image in the market [110]. Tag cloning attacks are launched to access highly confidential data such as information account bank accounts [111].

Radio frequency interference attacks: in RF interference attacks, powerful radio frequency signals are utilized to disrupt RFID communication between IoT devices. Attackers use radio frequency signals to generate solid interfering signals, known as radio jamming attacks [96, 112].

Table 5: Comparison of physical attacks in IoT.

Sr. #	Security issue	Reference	Affected layer	IoT level	Category	Attack type
1	Jamming	[28, 95]	Physical layer	Low level	Physical attack	Active
2	Object replication	[97, 104]	Network layer	Low level	Physical attack	Active
3	Malicious node injection	[91, 98]	Network layer, perception layer	High level	Physical attack	Active
4	Sleep denial attack	[99, 100]	MAC layer, physical layer	Low level	Physical attack	Active
5	Tampering	[101, 102]	Physical layer	Low level	Physical attack	Active
6	Permanent denial of service (PDoS)	[6]	MAC layer	High level	Physical attack	Active
7	Fake node injection	[36, 105]	Network layer	High level	Physical attack	Active
8	Hardware Trojan	[39, 108]	Application layer	Low level	Physical attack	Active
9	Outage attack	[109]	Network layer	Low level	Physical attack	Passive
10	Tag cloning	[111]	Perception layer	Intermediate level	Physical attack	Active, internal
11	Radio frequency interference attacks	[96, 112]	Application layer, physical layer	Intermediate level	Physical attack	Active

A detailed comparison of physical attacks in IoT devices has been summarized in Table 5.

(2) Network Attacks. The network attacks are classified into the following subtypes.

Sinkhole attack: to launch sinkhole attacks, intruders inject a malicious node that presents itself to other IoT network nodes as the best shortest channel for communication. This malicious node collects and "sinks" all of the information packets which flow on the targeted IoT network. Therefore, this malicious node is called a "sinkhole," and these attacks are named "sinkhole attacks" [113]. These attacks reduce the performance of targeted networks because the whole traffic of the IoT network flows towards the sinkhole. Still, this malicious node does not drop even a single message packet; they also harm the other performance-related attributes like efficiency and reliability of communication and disrupt the network protocols, especially the RPL protocol of IoT networks [114, 115].

Wormhole attack: in wormhole attacks, the attackers generate private channels between two or more nodes of an IoT network by controlling these nodes or injecting malicious code into the network to alter the transmission path, and attackers receive the transmitted information and send only the selective packet to the destination. Wormhole attacks are launched to damage network topologies and disturb network traffic [116–118].

Sybil attack: in Sybil attacks, attackers generate multiple fake identities by injecting a malicious node that pretends as multiple ordinary users. They are single user or attacker who launches divergent identities by utilizing a single platform. Fake profiles on social media sites like Twitter, Facebook, or Instagram also fall into Sybil attacks [119]. They also can be launched to attack routing algorithms [14].

Selective forwarding: in selective forwarding attacks, the attacker launches a malicious node placed on the route between the source and a destination node, which acts like a black hole that receives all the message packets flowing on the IoT network, but in this case of selective forwarding, the malicious node sends only the particular message packets to the destination and drops the remaining message packets. Selective forwarding attacks can filter all types of traffic [120, 121].

Traffic analysis attack: in traffic analysis attacks, the attackers launch a malicious node to notify the daily traffic routines to collect the routing information. The encryption of message packets is not enough to protect the IoT network from traffic analysis attacks. The distance from the root node and the less information is collected [122].

Man in the middle attack: man in the middle attacks attackers launch a malicious node between two nodes to intercept the two nodes' communication without their permission. The concept of man in the middle attacks is similar to the middle person who intercepts the communication between two persons by opening the letters before handing them over to the original recipient. IoT devices can launch these attacks by implementing various SSS hijacking, session hijackings, DSN spoofing, or side jacking [111, 123].

Routing information attack: routing information attacks are launched to redirect, spoof, misdirect, and drop the information packets. These attacks are projected to alter the way of message routing [104]. The altering attacks also fall in this category, launched to modify the routing information. Network partitioning, routing loop, rushing, and replay routing information are also subtypes of routing information attacks [120].

RFID spoofing: in RFID unauthorized access, attackers read the information of RFID tags without user permission. RFID systems do not have robust mechanisms to protect IoT devices because RFID tags are readable to everyone [124].

RFID unauthorized access: in RFID unauthorized access, attackers read the information of RFID tags without user permission. RFID systems do not have robust mechanisms to protect IoT devices because RFID tags are readable to everyone [124].

Table 6: Comparison of network attacks in IoT.

Sr. #	Security issue	Reference	Affected layer	IoT level	Category	Attack type
1	Sinkhole	[114, 115]	Network layer	Intermediate level	Network attacks	Active
2	Wormhole	[116, 117]	Network layer	Intermediate level	Network attacks	Active
3	Sybil	[14]	Network layer	Intermediate level	Network attacks	Active, internal
4	Selective forwarding	[120, 121]	Network layer	Low to intermediate	Routing attacks	Active, internal
5	Traffic analysis attack	[122]	Network layer	Low level	Network attacks	Passive
6	Man in the middle attack	[111, 123]	Network layer	Low to intermediate level	Network attacks	Active
7	Routing information attack	[120]	IPv6Network layer	Intermediate level	Network attacks	Active
8	RFID spoofing	[127–129]	Physical layer, network layer	Low level	Network attacks	Active
9	Unauthorized access	[124]	Perception layer	Intermediate level	Network attacks	Active
10	Replay attack	[126]	6LoWPAN adaptation layer and network layer	Intermediate level	Network attacks	Active
11	DoS/DDoS attack	[104]	Perceptions layer, network layer	High level	Network attacks	Active

Replay attack: in replay attacks, an attacker receives, stores, intercepts the message packet, replays or resends it, and presents it as its packet. Intruders gain the trust of the targeted IoT node by sending a message packet. Once attackers develop confidence, they access specific information such as packets received by the sensors or message packets sent to a cloud-based server [125]. The replay attacks are deceptive attacks that decrease network performance because they utilize network resources like bandwidth and are launched against protocols used for authentication [126].

DoS/DDoS attack: DoS attacks also affect network communication. DoS attacks are launched to affect data transmission between nodes by jamming the radio signals or injecting the fake malicious node on the IoT network [104].

A detailed comparison of network attacks in IoT devices has been summarized in Table 6.

(3) Software Attacks. Software attacks are malicious programs or codes that are put down purposefully to damage, harm, or gain unauthorized access to someone's device.

Operating system attacks: operating systems have to run many services and many open ports; by using these open ports, attackers installed malicious programs to alter the functions and steal the data or information.

Viruses: it is a computer program that can make copies by replicating itself and can infect other devices by transmitting via transferring infected files through wire or wireless networks, USBs, or different such types of portable devices. Due to limited memory and storage space and lack of update mechanisms, it is challenging to secure IoT gadgets from viruses, so they quickly become victims of attackers. Mirai, SILEX, Stuxnet, and BrickerBot are some types of viruses created to attack IoT devices [112]. CIH is a virus that attacks BIOS, and due to the CIH Virus attack, IoT devices are unable to boot [130].

Worms: a worm is a virus that can replicate itself but cannot alter the system's files or functions. Worms continuously repeat themselves to create copies and fill the entire disk and memory space, so worms slow down or crash IoT devices. UbootKit is a worm that infects divergent types of IoT devices and affects the bootloader of IoT gadgets. This worm can transfer from one device to another and fully control these devices [130]. Linux bricking worm can disable the infected IoT device [131]. Silex is another worm that overwrites IoT devices' storage disks [132]. BrickerBot is a worm that destroys or bricks the infected IoT devices [133].

Trojan horse: Trojans are malicious programs that seem harmless to the user and are downloaded and installed into the device by tricking them. After activation, it harms the user's devices by stealing data, deleting user files, or spreading viruses, worms, or other malicious applications. Hackers can control IoT devices through Trojan attacks or capture username, passwords, screenshots, bank details, and account information [134]. Hackers use Zeus Game over Trojan to attack IoT devices to access bank account details [135].

Phishing attacks: in phishing attacks, the malicious program is usually intruded on by a fraud communication that appears to come from reliable sources. Phishing attacks' objective is to steal information like the device's password or username or activate a malicious application into an IoT device [91, 136].

Backdoor attacks: back door is a malicious and complex code that can bypass authentication processes to remotely access system resources. The operating systems for IoT devices like RTOS or Contiki have back doors that can be used to gain unauthorized access [137]. This type of attack has been designed to hack an IoT system by breaking its security mechanisms such as cryptography and authentication using different techniques.

Brute force search attacks: brute force search attacks are programs that use divergent techniques to hack and break IoT applications' security mechanisms [138].

A detailed comparison of operating system attacks in IoT devices has been summarized in Table 7.

(4) Web Attacks. IoT web applications have numerous weaknesses due to poor coding. Hackers use these weaknesses to

Table 7: Comparison of operating system attacks in IoT.

Sr. #	Security issue	Reference	Affected layer	IoT level	Category	Attack type
1	Viruses	[2, 130]	Application layer	Intermediate level	Software attacks	Active
2	Worms	[5, 130, 133]	Application layer	Intermediate level	Software attacks	Active
3	Trojan horse	[7, 135]	Application layer	Intermediate level	Software attacks	Active
4	Phishing attacks	[91, 136]	Application layer	Low level	Software attacks	Passive
5	Backdoor attacks	[137]	Data processing layer	Low level	Software attacks	Active
6	Brute force search attacks	[12]	Transport layer, network layer	Low level	Software attacks	Active

access these IoT web applications' databases or servers containing sensitive personal or finical information. In some cases, the IoT web applications are linked with other infected applications, due to which these software applications become vulnerable to divergent attacks [112]. The standard web applications attacks are the following.

DDoS attacks: in DDoS attacks, hackers block the system or network resources. A most common example of a DDoS attack in IoT is access denial to a resource by flooding it with too many requests [23, 139].

Explication of a misconfiguration: security misconfiguration is improper configuration settings or mistakes in the configuration which cause misuse of data, privileges, and passwords. The poorly configured IoT applications lead to security- and privacy-related issues. In many IoT devices, the poor configuration, default settings, or technical issues of databases, operating systems, and other such components arise many security problems.

Malicious code injection: malicious code injection is when attackers attempt to control IoT devices or IoT networks by physically introducing malicious code into the device or IoT network nodes. The main goal of injecting this code is to steal data and bypass the access controls [91, 112, 140].

SQL injection attacks: SQL injection attacks are the subcategory of injection attacks. In these SQL injection attacks, attackers inject malicious SQL queries to access a database server to retrieve the information inaccessible to attackers [141].

Path-based DoS attacks: in these types, attackers attack multiple hop paths end-to-end communication by flooding data packets. The path-based DoS attacks can quickly have launched and affect or destroy a very large portion of IoT networks, usually wireless sensor-based networks. The path-based DoS attacks harm the IoT networks by sending too many legitimate packets and engaging the whole network resources to the desired device [142, 143].

Malware is an abbreviation of malicious software intentionally designed to damage computers and IoT devices to steal personal data, bypass access controls, and harm computers and IoT devices without the user's permission. IoT malware such as Aidra, Mirai, and Bashlite are IoT malware families that scan the machine to look for open ports to gain access [144].

Spyware: malicious hackers attack IoT devices by using spyware. Spywares are malicious software applications that collect information about users' activities without their knowledge instead of physically damaging IoT devices. Some IoT Spywares like Duqu are designed to monitor users' web bowering habits [145]. IoT spyware can record videos and send them to intruders through emails. sKy Wiper is another example of spyware. This spyware can record microphone signals or communication and send them to intruders through a Bluetooth connection [134].

Reprogram attack: in reprogramming attacks, intruders attack the IoT devices by using weakly protected programming codes; attackers modify or reprogram the code to control IoT devices or in some cases; they hijack the code to contain the entire IoT network. IoT devices can easily be reprogrammed remotely by modifying network programming systems [146].

A detailed comparison of web application attacks in IoT devices has been summarized in Table 8.

(5) Firmware Attacks. New vulnerabilities are designed to attack the Internet every day, so installing new security patches and updating the firmware in IoT devices are very important. The diverse variety of IoT devices cannot update their systems regularly.

Control hijacking: in this type of attack, intruders made modifications in coding to hijack the IoT systems' control and affect the control flow. These attacks are format string vulnerability, buffer overflow attacks, and integer overflow attacks [147].

Reverse engineering: in reverse engineering attacks, intruders damaged the embedded IoT devices and generated serious issues by analyzing IoT software applications such as firmwares. Attackers look for input parsing errors in the program's code, and then, the attacker advertised his skills to resolve the issue and get access to the device's sensitive data [148, 149].

Eavesdropping: eavesdropping attacks are passive attacks in which attackers take advantage of poorly secured network transmission and steal information during transmission from IoT devices. We can say that intruders hear or read the victim's conversation secretly. The eavesdropping attacks are hardly detected because they do not affect the IoT network's normal working [70, 150].

A detailed comparison of firmware attacks in IoT devices has been summarized in Table 9.

(6) Side-Channel Attacks. The side-channel attacks are the most hardware-based severe IoT attacks. IoT devices are more vulnerable to these attacks due to limited resources like battery power, storage and processing power, open doors for

Table 8: Comparison of web application attacks in IoT.

Sr. #	Security issue	Reference	Affected layer	IoT level	Category	Attack type
1	DDoS attacks	[23, 139]	Application layer, network layer	High level	Software attacks	Active
2	Explication of a misconfiguration	[112]	Network layer, application layer	Low level	Routing	Active
3	Malicious code injection	[91, 112, 140]	Application layer	High level	Software attacks	Active, external
4	SQL injection attacks	[141]	Application layer	Low level	Software attacks	Active
5	Path-based DoS attacks	[142, 143]	Application layer	High level	Software attacks	Active
6	Malware	[144]	Application layer, data processing layer	Low level	Software attacks	Passive
7	Spyware	[134, 145]	Application layer	Low level	Software attacks	Passive
8	Reprogram attack	[146]	Application layer	Low level	Software attacks	Active

Table 9: Comparison of firmware attacks in IoT.

Sr. #	Security issue	Reference	Affected layer	IoT level	Category	Attack type
1	Control hijacking	[147]	Transport layer	Low level	Software attacks	Active
2	Reverse engineering	[148, 149]	Application layer	Intermediate level	Software attacks	Active
3	Eavesdropping	[70, 150]	Physical layer	Low level to intermediate level	Software attacks	Passive
4	Malware	[144]	Data processing layer	Low level	Software attacks	Passive

side-channel attacks, and the problematic detection of these malicious programs [151, 152].

Timing attacks: timing attacks are launched by implementing timing variations such as overclocking, which is frequently utilized to inject malicious nodes or other IoT gadgets' faults to leak sensitive information [107]. These attacks can measure the time an application takes to finish specific tasks and then utilize it to steal sensitive data like bank account numbers, PIN codes, passwords, and cryptographic keys. The purpose behind side-channel timing attacks is to extract the key of encryption algorithms [93, 153].

Power analysis attacks: in power analysis, attackers closely measure the power consumed by various cryptographic hardware components of IoT devices and then analyze electric current change to extract the confidential information stored in devices. The power analysis attacks are further classified into three subcategories, i.e., simple power analysis attacks (SPA), differential power analysis attacks (DPA), and correlation power analysis attacks (CPA), which are described below [20, 93, 107, 154].

Fault analysis attacks: in fault analysis attacks, the attacker introduced a crypto node with fault and then analyzed the difference between correct and faulty text to extract the cryptographic key value. To launch this attack, intruder required special knowledge about the design of hardware devices. To inject the fault, attackers use various techniques like voltage glitching, tampering with clock pin, EM disturbances, and laser glitching [65, 154, 155].

Electromagnetic attacks: attackers capture and analyze electromagnetic radiations to extract sensitive personal information from IoT devices' hardware components like display screens. In some cases, attackers place a microantenna closer to the integrated circuit (IC) to capture electromagnetic signals. These electromagnetic attacks are used in military operations [93, 107, 156].

Cryptanalysis attacks: the ciphertext-only attacks are launched to access encrypted information or ciphertext only; these attacks cannot let the attacker get the corresponding plaintext. The main challenge in these attacks is to convert the ciphertext into plaintext which determines these attacks' success in IoT systems [157].

Known-plaintext attacks: in known plaintext attacks, the attacker's main challenge is to extract the plaintext from the crypto text with some known plaintext, which is a small portion of this crypto text. To guess the remaining part of the crypto text, attackers may implement various methods like detecting the encryption key, or divergent shortcut techniques can also be applied [157].

Chosen-plaintext: in chosen-plaintext attacks, attackers access the encryption devices to extract the algorithm that encrypted the plaintext. The attacker then utilized this encryption algorithm to determine the encryption key by converting various time-divergent chosen-plaintext into crypto text and then analyzing and comparing the resultant crypto text through which the attacker generates the encryption key of an IoT-based cryptosystem [157, 158].

Chosen-ciphertext attacks: in chosen-ciphertext attacks, attackers attempt to get temporary access to the decryption mechanisms by converting the chosen-ciphertext into plaintext and then this plaintext to descript the subsequent ciphertext. Chosen-ciphertext attacks are related to decryption mechanisms in IoT systems [158].

(7) Access-Level Attacks. The IoT system contains limited resources and infrastructure, making them more vulnerable

to various attacks. In IoT systems based on access level, the security attacks are categorized into two types.

Active attacks: in active attacks, attackers read and attempt to modify the IoT-based system's message packets or hardware. The vigorous attacks affect the working of IoT networks. They can disrupt routing protocols by altering routing information [159]. The primary purpose is to insert errors or noise signals in message transmission [113, 160].

Masquerade attacks: in masquerade attacks, the attacker presents itself as another authenticated or real user and transmits data on the IoT network by using this fake identity [159].

Modification of message: in modification attacks, attackers tamper the message packets; they modify data, change the sequence of message packets, or cause delays in the delivery of the targeted message packets [159].

Repudiation: in repudiation attacks, attackers successfully send or, in some cases, receive the message, and after sending or receiving, he denies that he has received or sent any such type of message [159].

Replay: in replay attacks, intruders read, modify, and send it to the original recipient without their knowledge [126].

Denial of service attacks: in denial of service attacks, attackers made too many requests for resources to decrease IoT networks' performance [104].

(8) Passive Attacks. In passive attacks, the attacker accesses the message or steals the information stored in an IoT system and utilizes this data, but he does not modify the steeled content. These attacks do not damage the targeted IoT systems but affect confidentiality. The main objective behind passive attacks is to steal secret sensitive information like bank account numbers, PIN codes, and passwords. In passive attacks, intruders observe circumstances and can switch from passive to active attacks [113, 160, 161].

Traffic analysis attacks: in a traffic analysis, the attacker secretly observes and stores the information about the IoT network. They record the various transmitted message packets like length, size, or sequence of message packets, which may help the attacker guess the conversation's nature [122].

Privacy attacks: in this type of attack, the intruder observes and records confidential, sensitive information and publically leaks this information later. These attacks are known as the "release of message content" [162].

(9) Strategy Attacks. To target IoT devices, attackers utilize divergent techniques that extract confidential information for an attacker. These techniques implement various strategies to inject malicious code, malicious nodes, or errors in IoT devices. Some systems require physical interaction and damage the hardware devices, while others can implement remotely.

Logical attacks: in logical attacks, attackers remotely access the IoT devices to launch the bug without physically damaging the device. In other words, the attacks in which attackers logically access the IoT devices by utilizing communication channels are named "logical attacks" [163].

Physical attacks: to launch physical attacks, attackers need to physically approach the targeted IoT device. These attacks also severely damage and modify the settings and configuration of the target IoT device. Tempering attacks and malicious node injection are examples of physical attacks [164, 165].

(10) Adversary-/Location-Based Attacks. An attacker can be an insider who understands the targeted IoT system or reside inside the boundary of the targeted IoT network, or it can be an outsider without any knowledge about the system or launch the attack from anywhere; therefore, based on adversary location, IoT attacks are classified into two main types, i.e., internal attacks or external attacks.

Internal attacks: an insider who has access to the device injects the malicious code or nodes in the IoT network. In these attacks, attackers belong to the same IoT network; they have deep knowledge about the implemented software technology, hardware devices, and complete IoT infrastructure [166]. These attacks are divided into four categories, i.e., unintentional actors, technology perception actors, compromised actors, and emotional attackers. These attacks affect the network layer and physical layer [167].

External attacks: an outsider remotely accesses the IoT network to inject an error or bug in external attacks. Attackers launch these attacks from anywhere or can utilize any other public network. Attackers have almost zero or very little knowledge about implemented technology and architecture of the targeted IoT system [168, 169].

(11) Host-Based Attacks. In host-based attacks, attackers target IoT devices' operating systems to extract cryptographic keys and other confidential information. Host-based attacks are launched by attacking host systems of IoT devices. These attacks are classified into three types, i.e., user-compromised attacks, software-compromised attacks, and hardware-compromised attacks.

User-compromised attacks: user-compromised attacks are launched to extract confidential data from IoT devices such as passwords, keys, and bank account details. In some cases, attackers launch these attacks to read or even hear their conversation [119].

Software-compromised attacks: software-compromised attacks are launched to exhaust IoT systems by overflowing the resource buffers. One example of software-compromised attacks suddenly runs out of the battery of IoT battery-operated devices [168].

Hardware-compromised attacks: IoT systems' attacker tamper hardware devices to steal data or inject bugs and malicious nodes in hardware-compromised attacks. To launch these attacks, attackers need to physically access the IoT devices [119].

3.3.5. RQ5: How the Advanced Technologies Resolve These Security and Privacy Issues? Undoubtedly, putting all the things on IoT gives us many intelligent devices to enhance digitalization. But still, there are many security and privacy

issues in the IoT that can be solved by integrating some advanced technologies to become more secure.

The blockchain technique can ensure the security of IoT that got compromised. A blockchain is a decentralized approach that makes an immutable database. The following features make it more trustworthy while discussing security. The miners do timestamp a chain of blocks and perform validation. Blockchain uses a powerful hashing technique, SHA-256, to authentic and integrate data. Digital signatures were implemented for the verification. All the changes are made by verifying other blocks, i.e., having the valid node address. Putting in or retrieving data from a partnership does not involve any third that gains global trust. The connectivity of IoT with so many other devices makes it easy to attack. Blockchain is considered to get IoT out of vulnerability.

Especially in IoT, it becomes difficult to detect any countermeasures with the growing threats and their complexity level when numerous devices are attached [170]. Artificial intelligence (AI) could play a valuable role here, and the concept works as a system/machine is trained by giving some data. The given data makes a cognitive memory, and the system becomes artificial intelligence for the desired scenarios [171].

Artificial intelligence is followed by machine learning and deep learning algorithms that make machines artificially intelligent and efficient to make intelligent decisions [172, 173]. While discussing the IoT, an artificially intelligent system that uses an algorithm and machine/deep learning for processing the data can be trained to detect any threat and perform specific actions [174, 175].

3.4. Future Research Directions. Future directions provide the door for researchers to continue research in this significant area.

(1) There is a need to develop a standard platform to share IoT-based research datasets

(2) Keeping in mind the limited resources of IoT devices is the cost-efficient way to resolve IoT systems' security issues

(3) There is a need to develop a cost-efficient blockchain-based solution to resolve IoT systems' security issues

(4) There is a need to develop the most efficient artificial intelligence-based solution to resolve IoT systems' security issues

(5) Secure the data stored in a remotely located publically accessible IoT system under the control of attackers

(6) Implementing emerging technologies can resolve maximum security issues of IoT systems

4. Conclusion

This study emphasizes IoT systems' major security concerns to let the users know about the risks associated with these gadgets. To better understand, the classification of IoT threats into divergent categories has been made. Further, a detailed comparison of each class is provided.

The attacks launched by injecting malicious nodes to steal information packets and reduce the network's performance are classified as network attacks. To target both security and privacy simultaneously, attackers float side-channel attacks. In cryptanalysis attacks, the attacker accesses the decryption key to convert cipher text into plaintext. In access-level attacks, attackers take advantage of the limited resources to steal or alter the information. In active attacks, attackers read and modify the message packets, while in passive attacks, attackers can read the message but do not make any modifications. In strategy-level attacks, attackers implement various strategies to inject malicious code into the IoT devices. Some attacks require physical interaction and damage the hardware devices, so they are called physical attacks, while others can implement them remotely; therefore, they are called logical attacks. An attacker can be an insider who understands the targeted IoT system or can be an outsider without any knowledge about the system; therefore, IoT attacks are classified into internal or external attacks based on adversary location. In hardware-compromised attacks, the attacker tampers hardware to steal data. Software attacks are the injection of malicious programs purposefully to gain unauthorized access to the device. Due to poor coding, hackers access these IoT web applications, databases, or servers. Attacks launched due to a lack of firmware updates are called firmware attacks.

Further, we have classified these categories into subcategories. More than 75 IoT security threats are discussed in this systematic literature review to help manufacturers to secure IoT systems. In this modern era, new emerging technologies like blockchain, artificial intelligence, machine learning, and other advanced technologies (fog and cloud computing) are integrated with IoT technology to resolve security and privacy challenges. These emerging technologies, especially blockchain technology, can provide a better and more cost-efficient solution for IoT security issues. In the end, we sum up this review paper by suggesting some future research ideas in IoT security, which still need researchers' attention.

Data Availability

The data used in this research will be available upon request from the corresponding author.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

The authors would like to thank the support of all coauthors.

References

[1] N. C. Winget, A. R. Sadeghi, and Y. Jin, "Invited: can IoT be secured: emerging challenges in connecting the unconnected," in *Proceedings of the 53rd Annual Design Automation Conference*, pp. 1–6, New York, USA, 2016.

[2] G. S. Hukkeri and R. H. Goudar, "IoT: issues, challenges, tools, security, solutions and best practices," *International Journal of Pure and Applied Mathematics*, vol. 120, no. 6, pp. 12099–12109, 2019.

[3] S. G. H. Soumyalatha, "Study of IoT: understanding IoT architecture, applications, issues and challenges," *International Journal of Advanced Networking & Applications*, vol. 478, 2016.

[4] A. S. Genadiarto, A. Noertjahyana, and V. Kabzar, "Introduction of Internet of Thing technology based on prototype," *Jurnal Informatika*, vol. 14, no. 1, pp. 47–52, 2018.

[5] N. Sharma, M. Shamkuwar, and I. Singh, "The history, present and future with IoT," in *Internet of Things and Big Data Analytics for Smart Generation*, pp. 27–51, Springer, 2019.

[6] K. Hamid, M. W. Iqbal, A. U. R. Virk et al., "K-Banhatti Sombor invariants of certain computer networks," *Computers Materials & Continua*, vol. 73, no. 1, pp. 15–31, 2022.

[7] 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.

[8] R. H. Weber, "Internet of things: privacy issues revisited," *Computer Law and Security Review*, vol. 31, no. 5, pp. 618–627, 2015.

[9] A. Gopi and M. K. Rao, "Survey of privacy and security issues in IoT," *International Journal of Engineering & Technology*, vol. 7, no. 2.7, p. 293, 2018.

[10] N. Aleisa and K. Renaud, "Privacy of the Internet of Things: a systematic literature review," in *Proceedings of the 50th Hawaii International Conference on System Sciences*, pp. 1–10, Hilton Waikoloa Village, Hawaii, 2017.

[11] 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.

[12] M. B. M. Noor and W. H. Hassan, "Current research on Internet of Things (IoT) security: a survey," *Computer Networks*, vol. 148, pp. 283–294, 2019.

[13] O. O. Bamasag and K. Youcef-Toumi, "Towards continuous authentication in Internet of Things based on secret sharing scheme," in *Proceedings of the WESS'15: Workshop on Embedded Systems Security*, pp. 1–8, Amsterdam, Netherlands, 2015.

[14] K. Zhang, X. Liang, R. Lu, and X. Shen, "Sybil attacks and their defenses in the Internet of Things," *IEEE Internet of Things Journal*, vol. 1, no. 5, pp. 372–383, 2014.

[15] Q. D. La, T. Q. S. Quek, J. Lee, S. Jin, and H. Zhu, "Deceptive attack and defense game in honeypot-enabled networks for the Internet of Things," *IEEE Internet of Things Journal*, vol. 3, no. 6, pp. 1025–1035, 2016.

[16] P. Zhang, S. G. Nagarajan, and I. Nevat, "Secure Location of Things (SLOT): mitigating localization spoofing attacks in the Internet of Things," *IEEE Internet of Things Journal*, vol. 4, no. 6, pp. 2199–2206, 2017.

[17] C. Li, Z. Qin, E. Novak, and Q. Li, "Securing SDN infrastructure of IoT–fog networks from MitM attacks," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1156–1164, 2017.

[18] B. Xu, W. Wang, Q. Hao et al., "A security design for the detecting of buffer overflow attacks in IoT device," *IEEE Access*, vol. 6, pp. 72862–72869, 2018.

[19] H. Yi and Z. Nie, "Side-channel security analysis of UOV signature for cloud-based Internet of Things," *Future Generation Computer Systems*, vol. 86, pp. 704–708, 2018.

[20] J. Moon, I. Y. Jung, and J. H. Park, "IoT application protection against power analysis attack," *Computers and Electrical Engineering*, vol. 67, pp. 566–578, 2018.

[21] S. Tu, M. Waqas, S. U. Rehman et al., "Security in fog computing: a novel technique to tackle an impersonation attack," *IEEE Access*, vol. 6, pp. 74993–75001, 2018.

[22] A. Raoof, A. Matrawy, and C.-H. Lung, "Routing attacks and mitigation methods for RPL-based Internet of Things," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1582–1606, 2019.

[23] D. Yin, L. Zhang, and K. Yang, "A DDoS attack detection and mitigation with software-defined Internet of Things framework," *IEEE Access*, vol. 6, pp. 24694–24705, 2018.

[24] M. López, A. Peinado, and A. Ortiz, "An extensive validation of a SIR epidemic model to study the propagation of jamming attacks against IoT wireless networks," *Computer Networks*, vol. 165, article 106945, 2019.

[25] N. Tariq, M. Asim, Z. Maamar, M. Z. Farooqi, N. Faci, and T. Baker, "A mobile code-driven trust mechanism for detecting internal attacks in sensor node-powered IoT," *Journal of Parallel and Distributed Computing*, vol. 134, pp. 198–206, 2019.

[26] A. K. Mishra, A. K. Tripathy, D. Puthal, and L. T. Yang, "Analytical model for sybil attack phases in Internet of Things," *IEEE Internet of Things Journal*, vol. 6, no. 1, pp. 379–387, 2019.

[27] N. Zhang, R. Wu, S. Yuan, C. Yuan, and D. Chen, "RAV: relay aided vectorized secure transmission in physical layer security for Internet of Things under active attacks," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8496–8506, 2019.

[28] Y. Niu, J. Zhang, A. Wang, and C. Chen, "An efficient collision power attack on AES encryption in edge computing," *IEEE Access*, vol. 7, pp. 18734–18748, 2019.

[29] H. Yan, Y. Wang, C. Jia, J. Li, Y. Xiang, and W. Pedrycz, "IoT-FBAC: function-based access control scheme using identity-based encryption in IoT," *Future Generation Computer Systems*, vol. 95, pp. 344–353, 2019.

[30] S. Deshmukh-Bhosale and S. S. Sonavane, "A real-time intrusion detection system for wormhole attack in the RPL based Internet of Things," *Procedia Manufacturing*, vol. 32, pp. 840–847, 2019.

[31] L. Liu, Z. Ma, and W. Meng, "Detection of multiple-mix-attack malicious nodes using perceptron-based trust in IoT networks," *Future Generation Computer Systems*, vol. 101, pp. 865–879, 2019.

[32] Z. A. Baig, S. Sanguanpong, S. N. Firdous, V. N. Vo, T. G. Nguyen, and C. So-In, "Averaged dependence estimators for DoS attack detection in IoT networks," *Future Generation Computer Systems*, vol. 102, pp. 198–209, 2020.

[33] M. Almiani, A. Abu Ghazleh, A. Al-Rahayfeh, S. Atiewi, and A. Razaque, "Deep recurrent neural network for IoT intrusion detection system," *Simulation Modelling Practice and Theory*, vol. 101, article 102031, 2020.

[34] M. Malik, Kamaldeep, and M. Dutta, "Defending DDoS in the insecure Internet of Things: a survey," in *Advances in Intelligent Systems and Computing*, pp. 223–233, Springer, Singapore, 2018.

[35] R. Doshi, N. Apthorpe, and N. Feamster, "Machine learning DDoS detection for consumer Internet of Things devices," in *2018 IEEE Security and Privacy Workshops*, pp. 29–35, San Francisco, CA, USA, 2018.

[36] J. Pacheco, S. Hariri, and S. Hariri, "Anomaly behavior analysis for IoT sensors," *Transactions on Emerging Telecommunications Technologies*, vol. 29, no. 4, article e3188, 2018.

[37] P. Gope, R. Amin, S. K. Hafizul Islam, N. Kumar, and V. K. Bhalla, "Lightweight and privacy-preserving RFID authentication scheme for distributed IoT infrastructure with secure localization services for smart city environment," *Future Generation Computer Systems*, vol. 83, pp. 629–637, 2018.

[38] J. Sherry, C. Lan, R. A. Popa, and S. Ratnasamy, "Blind box: deep packet inspection over encrypted traffic," in *Proceedings of the 2015 ACM Conference on Special Interest Group on Data Communication*, pp. 213–226, London, UK, 2015.

[39] M. R. Naqvi, M. W. Iqbal, S. K. Shahzad et al., "A concurrence study on interoperability issues in IoT and decision making based model on data and services being used during interoperability," *Lahore Garrison University Research Journal of Computer Science and Information Technology*, vol. 4, no. 4, pp. 73–85, 2020.

[40] O. Brun, Y. Yin, E. Gelenbe, Y. M. Kadioglu, J. Augusto-Gonzalez, and M. Ramos, "Deep learning with dense random neural networks for detecting attacks against IoT-connected home environments," in *International ISCIS Security Workshop*, pp. 79–89, Springer, London, UK, 2018.

[41] Y. Li, L. Shi, P. Cheng, J. Chen, and D. E. Quevedo, "Jamming attacks on remote state estimation in cyber-physical systems: a game-theoretic approach," *IEEE Transactions on Automatic Control*, vol. 60, no. 10, pp. 2831–2836, 2015.

[42] S. Vadlamani, B. Eksioglu, H. Medal, and A. Nandi, "Jamming attacks on wireless networks: a taxonomic survey," *International Journal of Production Economics*, vol. 172, pp. 76–94, 2016.

[43] Y. Guan and X. Ge, "Distributed attack detection and secure estimation of networked cyber-physical systems against false data injection attacks and jamming attacks," *IEEE Transactions on Signal and Information Processing Over Networks*, vol. 4, no. 1, pp. 48–59, 2018.

[44] B. Park, "Threats and security analysis for enhanced secure neighbor discovery protocol (SEND) of IPv6 NDP security," *International Journal of Control and Automation*, vol. 4, no. 4, 2011.

[45] Y. W. P. Hong, P. C. Lan, and C. C. J. Kuo, "Enhancing physical-layer secrecy in multiantenna wireless systems: an overview of signal processing approaches," *IEEE Signal Processing Magazine*, vol. 30, no. 5, pp. 29–40, 2013.

[46] L. Xiao, L. J. Greenstein, N. B. Mandayam, and W. Trappe, "Channel-based detection of sybil attacks in wireless networks," *IEEE Transactions on Information Forensics and Security*, vol. 4, no. 3, pp. 492–503, 2009.

[47] B. Cheng, D. Zhu, S. Zhao, and J. Chen, "Situation-aware IoT service coordination using the event-driven SOA paradigm," *IEEE Transactions on Network and Service Management*, vol. 13, no. 2, pp. 349–361, 2016.

[48] S. H. Chae, W. Choi, J. H. Lee, and T. Q. S. Quek, "Enhanced secrecy in stochastic wireless networks: artificial noise with secrecy protected zone," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 10, pp. 1617–1628, 2014.

[49] A. Dvir and L. Buttyan, "VeRA-version number and rank authentication in RPL," in *2011 IEEE Eighth International Conference on Mobile Ad-Hoc and Sensor Systems*, pp. 709–714, Valencia, Spain, 2011.

[50] C. Pu and S. Hajjar, "Mitigating forwarding misbehaviors in RPL-based low power and lossy networks," in *2018 15th IEEE Annual Consumer Communications & Networking Conference*, pp. 1–6, Las Vegas, NV, USA, 2018.

[51] A. Le, J. Loo, A. Lasebae, A. Vinel, Y. Chen, and M. Chai, "The impact of rank attack on network topology of routing protocol for low-power and lossy networks," *IEEE Sensors Journal*, vol. 13, no. 10, pp. 3685–3692, 2013.

[52] K. Weekly and K. Pister, "Evaluating sinkhole defense techniques in RPL networks," in *2012 20th IEEE International Conference on Network Protocols*, pp. 1–6, Austin, TX, USA, 2012.

[53] F. Ahmed and Y. Ko, "Mitigation of black hole attacks in routing protocol for low power and lossy networks," *Security and Communication Networks*, vol. 9, no. 18, pp. 5143–5154, 2016.

[54] H. H. Pajouh, R. Javidan, R. Khayami, A. Dehghantanha, and K.-K. R. Choo, "A two-layer dimension reduction and two-tier classification model for anomaly-based intrusion detection in IoT backbone networks," *IEEE Transactions on Emerging Topics in Computing*, vol. 7, no. 2, pp. 314–323, 2019.

[55] S. Sivaraju and G. Umamaheswari, "Detection of sinkhole attack in wireless sensor networks using message digest algorithms," in *2011 International Conference on Process Automation, Control and Computing*, pp. 1–6, Coimbatore, India, 2011.

[56] Q. Cao and X. Yang, "Sybil fence: improving social-graph-based sybil defenses with user negative feedback," http://arxiv.org/abs/1304.3819.

[57] N. Maheshwari and H. Dagale, "Secure communication and firewall architecture for IoT applications," in *2018 10th International Conference on Communication Systems Networks*, pp. 328–335, Bengaluru, India, 2018.

[58] L. Alvisi, A. Clement, A. Epasto, S. Lattanzi, and A. Panconesi, "SoK: the evolution of sybil defense via social networks," in *2013 IEEE Symposium on Security and Privacy*, pp. 382–396, Berkeley, CA, USA, 2013.

[59] A. Mohaisen, N. Hopper, and Y. Kim, "Keep your friends close: incorporating trust into social network-based Sybil defenses," in *2011 Proceedings IEEE INFOCOM*, pp. 1943–1951, Shanghai, China, 2011.

[60] M. Wazid, A. K. Das, S. Kumari, and M. K. Khan, "Design of sinkhole node detection mechanism for hierarchical wireless sensor networks - Wazid -2016- Security and Communication Networks," *Security and Communication Networks*, vol. 9, 4614 pages, 2016.

[61] S. Raza, T. Chung, S. Duquennoy, D. Yazar, T. Voigt, and U. Roedig, *Securing Internet of Things with lightweight ipsec*, Swedish Institute of Computer Science, Kista, Sweden, 2010.

[62] S. Raza, S. Duquennoy, J. Höglund, U. Roedig, and T. Voigt, "Secure communication for the Internet of Things—a comparison of link-layer security and IPsec for 6LoWPAN," *Security and Communication Networks*, vol. 7, 2668 pages, 2014.

[63] J. Granjal, E. Monteiro, and J. S. Silva, "Application-layer security for the wot: extending coap to support end-to-end message security for Internet-integrated sensing applications," in *Wired/Wireless Internet Communication*, pp. 140–153, Springer, Berlin, Heidelberg, 2013.

[64] L. Barreto, A. Celesti, M. Villari, M. Fazio, and A. Puliafito, "An authentication model for IoT clouds," in *2015 IEEE/*

ACM International Conference on Advances in Social Networks Analysis and Mining, pp. 1032–1035, Paris, France, 2015.

[65] M. H. Ibrahim, "Octopus: an edge-fog mutual authentication scheme," *IJ Network Security*, vol. 18, no. 6, pp. 1089–1101, 2016.

[66] H. Xie, Z. Yan, Z. Yao, and M. Atiquzzaman, "Data collection for security measurement in wireless sensor networks: a survey," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 2205–2224, 2019.

[67] O. A. Osanaiye, A. S. Alfa, and G. P. Hancke, "Denial of service defence for resource availability in wireless sensor networks," *IEEE Access*, vol. 6, pp. 6975–7004, 2018.

[68] L. A. Tawalbeh, F. Muheidat, M. Tawalbeh, and M. Quwaider, "IoT privacy and security: challenges and solutions," *Applied Sciences*, vol. 10, no. 12, p. 4102, 2020.

[69] H. Ning, H. Liu, and L. T. Yang, "Cyberentity security in the Internet of Things," *Computer*, vol. 46, no. 4, pp. 46–53, 2013.

[70] M. Abomhara and G. M. K. Ien, "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.

[71] A. Mathur, T. Newe, and M. Rao, "Defence against black hole and selective forwarding attacks for medical WSNs in the IoT," *Sensors*, vol. 16, no. 1, 2016.

[72] R. Stephen and D. L. Arockiam, "Intrusion detection system to detect sinkhole attack on rpl protocol in Internet of Things," *International Journal of Electrical Electronics and Computer Science*, vol. 4, no. 4, 2016.

[73] K. Skouby, R. Tadayoni, and S. Tweneboah-Koduah, "Cyber security threats to IoT applications and service domains," *Wireless Personal Communications*, vol. 95, no. 1, pp. 169–185, 2017.

[74] J. Sengupta, S. Ruj, and S. Das Bit, "A comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT," *Journal of Network and Computer Applications*, vol. 149, article 102481, 2020.

[75] Q. Wang, X. Zhu, Y. Ni, L. Gu, and H. Zhu, "Blockchain for the IoT and industrial IoT: a review," *Internet of Things*, vol. 10, article 100081, 2019.

[76] R. H. Weber, "Internet of Things – new security and privacy challenges," *Computer Law & Security Review*, vol. 26, no. 1, pp. 23–30, 2010.

[77] M. A. Khan and K. Salah, "IoT security: review, blockchain solutions, and open challenges," *Future Generation Computer Systems*, vol. 82, pp. 395–411, 2018.

[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] A. Sultan, M. A. Mushtaq, and M. Abubakar, "IOT security issues via blockchain: a review paper," in *Proceedings of the 2019 International Conference on Blockchain Technology*, pp. 60–65, Espoo, Finland, 2019.

[80] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for IoT security and privacy: the case study of a smart home," in *2017 IEEE International Conference on Pervasive Computing and Communications Workshops*, pp. 618–623, Kona, HI, USA, 2017.

[81] M. R. Naqvi, M. W. Iqbal, M. U. Ashraf et al., "Ontology driven testing strategies for IoT applications," *Materials & Continua*, vol. 70, no. 3, pp. 5855–5869, 2022.

[82] M. I. Sarwar, M. W. Iqbal, T. Alyas et al., "Data vaults for blockchain-empowered accounting information systems," *IEEE Access*, vol. 9, no. 2021, pp. 117306–117324, 2021.

[83] M. Akram, M. W. Iqbal, S. A. Ali, M. U. Ashraf, K. Alsubhi, and H. M. Aljahdali, "Triple key security algorithm against single key attack on multiple rounds," *Materials & Continua*, vol. 72, no. 3, pp. 6061–6077, 2022.

[84] D. Minoli and B. Occhiogrosso, "Blockchain mechanisms for IoT security," *Internet of Things*, vol. 1-2, pp. 1–13, 2018.

[85] F. K. Gondal, S. K. Shahzad, M. W. Iqbal, M. Aqeel, and M. R. Naqvi, "Business process model for IoT based systems operations," *LGU, Research Journal for Computer Science and IT*, vol. 5, no. 4, pp. 1–10, 2021.

[86] K. M. Sadique, R. Rahmani, and P. Johannesson, "Towards security on Internet of Things: applications and challenges in technology," *Procedia Computer Science*, vol. 141, pp. 199–206, 2018.

[87] S. K. Shahzad, M. W. Iqbal, and N. Ahmad, "Privacy agents for IoT cloud communication," in *IoTBDS-2nd International Conference on Internet of Things, Big Data and Security*, pp. 239–245, Prague , Czech Republic, 2017.

[88] K. Fan, S. Wang, Y. Ren et al., "Blockchain-based secure time protection scheme in IoT," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 4671–4679, 2019.

[89] B. Kitchenham, *Procedures for Performing Systematic Reviews*, Keele University, Keele, UK, 2004.

[90] T. Xu, J. B. Wendt, and M. Potkonjak, "Security of IoT systems: design challenges and opportunities," in *2014 IEEE/ACM International Conference on Computer-Aided Design*, pp. 417–423, San Jose, CA, USA, 2014.

[91] J. Deogirikar and A. Vidhate, "Security attacks in IoT: a survey," in *2017 International Conference on I-SMAC*, pp. 32–37, Palladam, India, 2017.

[92] S. Bhunia and M. Tehranipoor, Eds., "Physical Attacks and Countermeasures," in *Hardware Security*, pp. 245–290, Morgan Kaufmann, 2019.

[93] M. Hutle and M. Kammerstetter, "Resilience against physical attacks," in *Smart Grid Security*, pp. 79–112, Syngress, Boston, USA, 2015.

[94] A. Fadele, M. Othman, I. Hashem, I. Yaqoob, M. Imran, and M. Shoaib, "A novel countermeasure technique for reactive jamming attack in Internet of Things," *Multimedia Tools and Applications*, vol. 78, 2019.

[95] A. Mpitziopoulos, D. Gavalas, C. Konstantopoulos, and G. Pantziou, "A survey on jamming attacks and countermeasures in WSNs," *IEEE Communications Surveys & Tutorials*, vol. 11, no. 4, pp. 42–56, 2009.

[96] H. Li, Y. Chen, and Z. He, "The survey of RFID attacks and defenses," in *2012 8th International Conference on Wireless Communications, Networking and Mobile Computing*, pp. 1–4, Shanghai, China, 2012.

[97] S. Hameed, F. I. Khan, and B. Hameed, "Understanding security requirements and challenges in Internet of Things (IoT): a review," *Journal of Computer Networks and Communications*, vol. 2019, Article ID 9629381, 14 pages, 2019.

[98] F. Kandah, Y. Singh, W. Zhang, and C. Wang, "Mitigating colluding injected attack using monitoring verification in mobile ad-hoc networks," *Security and Communication Networks*, vol. 6, no. 4, pp. 539–547, 2013.

[99] M. Pirretti, S. Zhu, N. Vijaykrishnan, P. McDaniel, M. Kandemir, and R. Brooks, "The sleep deprivation attack

in sensor networks: analysis and methods of defense," *International Journal of Distributed Sensor Networks*, vol. 2, 287 pages, 2006.

[100] A. Gallais, T.-H. Hedli, V. Loscri, and N. Mitton, "Denial-of-sleep attacks against IoT networks," in *2019 6th International Conference on Control, Decision and Information Technologies*, pp. 1025–1030, Paris, France, 2019.

[101] S. Alam and D. De, "Analysis of security threats in wireless sensor network," *International Journal of Wireless & Mobile Networks*, vol. 6, no. 2, pp. 35–46, 2014.

[102] M.-L. Messai, *Classification of Attacks in Wireless Sensor Networks*, 2014, arXiv:1406.4516.

[103] C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas, "DDoS in the IoT: Mirai and other botnets," *Computer*, vol. 50, no. 7, pp. 80–84, 2017.

[104] M. El-hajj, A. Fadlallah, M. Chamoun, and A. Serhrouchni, "A survey of Internet of Things (IoT) authentication schemes," *Sensors*, vol. 19, no. 5, 2019.

[105] P. Ganapathi and D. Shanmugapriya, "A survey of attacks, security mechanisms and challenges in wireless sensor networks," *International Journal of Computer Science and Information Security*, vol. 4, 2009.

[106] S. Bhunia, M. S. Hsiao, M. Banga, and S. Narasimhan, "Hardware trojan attacks: threat analysis and countermeasures," *Proceedings of the IEEE*, vol. 102, no. 8, pp. 1229–1247, 2014.

[107] S. Sidhu, B. J. Mohd, and T. Hayajneh, "Hardware security in IoT devices with emphasis on hardware trojans," *Journal of Sensor and Actuator Networks*, vol. 8, no. 3, 2019.

[108] M. Tehranipoor and F. Koushanfar, "A survey of hardware trojan taxonomy and detection," *IEEE Design & Test Of Computers*, vol. 27, no. 1, pp. 10–25, 2010.

[109] A. Matrosov, E. Rodionov, D. Harley, and J. Malcho, "Stuxnet under the microscope," *ESET LLC*, 2010.

[110] M. Lehtonen, D. Ostojic, A. Ilic, and F. Michahelles, "Securing RFID systems by detecting tag cloning," in *Lecture Notes in Computer Science*, vol. 5538, pp. 291–308, Springer, Berlin, Heidelberg, 2009.

[111] M. Obaidat, S. Obeidat, J. Holst, A. al Hayajneh, and J. Brown, "A comprehensive and systematic survey on the Internet of Things: security and privacy challenges, security frameworks, enabling technologies, threats, vulnerabilities and countermeasures," *Computers*, vol. 9, p. 44, 2020.

[112] H. Akram, D. Konstantas, and M. Mahyoub, "A comprehensive IoT attacks survey based on a building-blocked reference model," *International Journal of Advanced Computer Science and Applications*, vol. 9, no. 3, 2018.

[113] I. Butun, P. Österberg, and H. Song, "Security of the Internet of Things: vulnerabilities, attacks, and countermeasures," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 1, pp. 616–644, 2020.

[114] S. Pundir, M. Wazid, D. P. Singh, A. K. Das, J. J. P. C. Rodrigues, and Y. Park, "Designing efficient sinkhole attack detection mechanism in edge-based IoT deployment," *Sensors*, vol. 20, no. 5, 2020.

[115] S. Tahir, S. T. Bakhsh, and R. A. Alsemmeari, "An intrusion detection system for the prevention of an active sinkhole routing attack in Internet of Things," *International Journal of Distributed Sensor Networks*, vol. 15, Article ID 155014771988990, 2019.

[116] Y.-C. Hu, A. Perrig, and D. B. Johnson, "Packet leashes: a defense against wormhole attacks in wireless networks," in *IEEE INFOCOM 2003. Twenty-second Annual Joint Conference of the IEEE Computer and Communications Societies*, pp. 1976–1986, San Francisco, CA, USA, 2003.

[117] A. Mosenia and N. K. Jha, "A comprehensive study of security of Internet-of-Things," *IEEE Transactions on Emerging Topics in Computing*, vol. 5, no. 4, pp. 586–602, 2017.

[118] B. Mustafa, M. W. Iqbal, M. Saeed, A. R. Shafqat, H. Sajjad, and M. R. Naqvi, "IOT based low-cost smart home automation system," in *2021 3rd International Congress on Human-Computer Interaction, Optimization and Robotic Applications*, pp. 1–6, Ankara, Turkey, 2021.

[119] M. Nawir, A. Amir, N. Yaakob, and O. B. Lynn, "Internet of Things (IoT): taxonomy of security attacks," in *2016 3rd international conference on electronic design*, pp. 321–326, Phuket, Thailand, 2016.

[120] D. Sisodia, *On the State of Internet of Things Security: Vulnerabilities, Attacks, and Recent Countermeasures*, University of Oregon, 2020.

[121] L. Bysani and A. Turuk, "A survey on selective forwarding attack in wireless sensor networks," in *2011 International Conference on Devices and Communications*, pp. 1–5, Mesra, India, 2011.

[122] A. Mayzaud, R. Badonnel, and I. Chrisment, "A taxonomy of attacks in RPL-based Internet of Things," *International Journal Of Network Security*, vol. 18, no. 3, pp. 459–473, 2016.

[123] Z. Cekerevac, Z. Dvorak, L. Prigoda, and P. Cekerevac, "Internet of things and the man-in-the-middle attacks–security and economic risks," *MEST Journal*, vol. 5, no. 2, pp. 15–25, 2017.

[124] M. M. Ahemd, M. A. Shah, and A. Wahid, "IoT security: a layered approach for attacks defenses," in *2017 International Conference on Communication Technologies*, pp. 104–110, Rawalpindi, Pakistan, 2017.

[125] K. Zhao and L. Ge, "A survey on the Internet of Things security," in *2013 Ninth International Conference on Computational Intelligence and Security*, pp. 663–667, Emeishan, China, 2013.

[126] D. He, S. Chan, and M. Guizani, "Security in the Internet of Things supported by mobile edge computing," *IEEE Communications Magazine*, vol. 56, no. 8, pp. 56–61, 2018.

[127] I. Andrea, C. Chrysostomou, and G. Hadjichristofi, "Internet of Things: security vulnerabilities and challenges," in *2015 IEEE Symposium on Computers and Communication*, pp. 180–187, Larnaca, Cyprus, 2015.

[128] A. Kamble and S. Bhutad, "Survey on Internet of Things (IoT) security issues solutions," in *2018 2nd International Conference on Inventive Systems and Control*, pp. 307–312, Coimbatore, India, 2018.

[129] A. Mitrokotsa, M. R. Rieback, and A. S. Tanenbaum, "Classifying RFID attacks and defenses," *Information Systems Frontiers*, vol. 12, no. 5, pp. 491–505, 2010.

[130] E. Ronen, A. Shamir, A. O. Weingarten, and C. O'Flynn, "IoT goes nuclear: creating a zig bee chain reaction," in *2017 IEEE symposium on security and privacy*, pp. 195–212, San Jose, CA, USA, 2017.

[131] E. Bertino and N. Islam, "Botnets and Internet of Things security," *Computer*, vol. 50, no. 2, pp. 76–79, 2017.

[132] S. Edwards and I. Profetis, "Hajime: analysis of a decentralized Internet worm for IoT devices," *Rapidity Networks*, vol. 16, pp. 1–18, 2016.

[133] H. Takase, R. Kobayashi, M. Kato, and R. Ohmura, "A prototype implementation and evaluation of the malware detection

mechanism for IoT devices using the processor information," *International Journal of Information Security*, vol. 19, no. 1, pp. 71–81, 2020.

[134] M. M. Ogonji, G. Okeyo, and J. M. Wafula, "A survey on privacy and security of Internet of Things," *Computer Science Review*, vol. 38, article 100312, 2020.

[135] C. Dong, G. He, X. Liu, Y. Yang, and W. Guo, "A multi-layer hardware trojan protection framework for IoT chips," *IEEE Access*, vol. 7, pp. 23628–23639, 2019.

[136] A. Tsow, "Phishing with consumer electronics-malicious home routers," *MTW*, vol. 190, 2006.

[137] L. Sha, F. Xiao, W. Chen, and J. Sun, "IIoT-SIDefender: detecting and defense against the sensitive information leakage in industry IoT," *World Wide Web*, vol. 21, no. 1, pp. 59–88, 2018.

[138] S. Boddy and J. Shattuck, *The Hunt for IoT: The Rise of Thingbots*, F5 Labs, Seattle WA, USA, 2017.

[139] J. Mirkovic and P. Reiher, "A taxonomy of DDoS attack and DDoS defense mechanisms," *ACM SIGCOMM Computer Communication Review*, vol. 34, no. 2, pp. 39–53, 2004.

[140] M. Farooq, M. Waseem, A. Khairi, and P. Mazhar, "A critical analysis on the security concerns of Internet of Things (IoT)," *International Journal of Computers and Applications*, vol. 111, no. 7, pp. 1–6, 2015.

[141] L. Qian, Z. Zhu, J. Hu, and S. Liu, "Research of SQL injection attack and prevention technology," in *2015 International Conference on Estimation, Detection and Information Fusion*, pp. 303–306, Harbin, China, 2015.

[142] D. Martins and H. Guyennet, "Wireless sensor network attacks and security mechanisms: a short survey," in *2010 13th international conference on network-based information systems*, pp. 313–320, Takayama, Japan, 2010.

[143] M. L. Mahajan, D. Verma, and Acropolis technical Campus Indore, "Review of prevention techniques for denial of service attacks in wireless sensor network," *International Journal of Engineering Research*, vol. V4, no. 5, article IJERT-V4IS051191, 2015.

[144] Q. D. Ngo, H. T. Nguyen, V. H. Le, and D. H. Nguyen, "A survey of IoT malware and detection methods based on static features," *ICT Express*, vol. 6, no. 4, pp. 280–286, 2020.

[145] B. Bencsáth, G. Pék, L. Buttyán, and M. Félegyházi, *Duqu: analysis, detection, and lessons learned*, ACM European Workshop on System Security, Bern, Switzerland, 2012.

[146] U. Sabeel and S. Maqbool, "Categorized security threats in the wireless sensor networks: countermeasures and security management schemes," *International Journal of Computers and Applications*, vol. 64, no. 16, pp. 19–28, 2013.

[147] A. Mohanty, I. Obaidat, F. Yilmaz, and M. Sridhar, "Control-hijacking vulnerabilities in IoT firmware: a brief survey," in *Proceedings of the 1st International Workshop on Security and Privacy for the Internet-of-Things (IoTSec), and attack taxonomy*, New York, USA, 2015.

[148] M. R. Naqvi, M. Aslam, M. W. Iqbal, S. K. Shahzad, M. Malik, and M. U. Tahir, "Study of block chain and its impact on Internet of Health Things (IoHT): challenges and opportunities," in *2020 international congress on human-computer interaction, optimization and robotic applications*, pp. 1–6, Ankara, Turkey, 2020.

[149] M. Ghasemi, M. Saadaat, and O. Ghollasi, "Threats of social engineering attacks against security of Internet of Things (IoT): the selected papers of the first international conference on fundamental research in electrical engineering," in *Lecture Notes in Electrical Engineering*, pp. 957–968, Springer, Singapore, 2019.

[150] I. Naumann and G. Hogben, "Privacy features of European eID card specifications," *Network Security*, vol. 2008, no. 8, pp. 9–13, 2008.

[151] H. D. Tsague and B. Twala, "Practical techniques for securing the Internet of Things (IoT) against side channel attacks," in *Internet of things and big data analytics toward next-generation intelligence*, pp. 439–481, Springer, 2018.

[152] H. Y. Ghafoor, A. Jaffar, R. Jahangir, M. W. Iqbal, and M. Z. Abbas, "Fake news identification on social media using machine learning techniques," in *Lecture Notes in Networks and Systems*, pp. 87–98, Springer, Singapore, 2022.

[153] A. A. Pammu, K.-S. Chong, W.-G. Ho, and B.-H. Gwee, "Interceptive side channel attack on AES-128 wireless communications for IoT applications," in *2016 IEEE Asia Pacific Conference on Circuits and Systems*, pp. 650–653, Jeju, Korea, 2016.

[154] S. Bhunia and M. Tehranipoor, Eds., "Side-channel attacks," in *Hardware Security*, pp. 193–218, Morgan Kaufmann, 2019.

[155] F. K. Gondal, S. K. Shahzad, A. Jaffar, and M. W. Iqbal, "A process oriented integration model for smart health services," *Intelligent Automation & Soft Computing*, vol. 35, no. 2, pp. 1369–1386, 2023.

[156] A. Sayakkara, N. A. Le-Khac, and M. Scanlon, "Leveraging electromagnetic side-channel analysis for the investigation of IoT devices," *Digital Investigation*, vol. 29, pp. S94–S103, 2019.

[157] D. Shree and S. Ahlawat, "A review on cryptography, attacks and cyber security," *International Journal of Advanced Research in Computer Science*, vol. 8, no. 5, 2017.

[158] S. S. Kulkarni, H. M. Rai, and S. Singla, "Design of an effective substitution cipher algorithm for information security using fuzzy logic," *International Journal of Innovations in Engineering and Technology*, vol. 1, no. 2, 2012.

[159] R. Datta and N. Marchang, "Chapter 7-security for mobile ad hoc networks," in *Handbook on Securing Cyber-Physical Critical Infrastructure*, pp. 147–190, Morgan Kaufmann, Boston, USA, 2012.

[160] C. Li, "Security of wireless sensor networks: current status and key issues," *Smart Wireless Sensor Networks*, vol. 14, pp. 299–313, 2010.

[161] J. Grover and S. Sharma, "Security issues in wireless sensor network — a review," in *2016 5th International Conference on Reliability, Infocom Technologies and Optimization*, pp. 397–404, Noida, India, 2016.

[162] K. Somasundaram and K. Selvam, "IOT – attacks and challenges," *International Journal of Engineering and Technical Research*, vol. 8, no. 9, 2018.

[163] I. Stellios, P. Kotzanikolaou, M. Psarakis, C. Alcaraz, and J. Lopez, "A survey of IoT-enabled cyberattacks: assessing attack paths to critical infrastructures and services," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 4, pp. 3453–3495, 2018.

[164] M. N. Aman, K. C. Chua, and B. Sikdar, "Mutual authentication in IoT systems using physical unclonable functions," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1327–1340, 2017.

[165] S. Babar, A. Stango, N. Prasad, J. Sen, and R. Prasad, "Proposed embedded security framework for Internet of Things

(IoT)," in *2011 2nd International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace Electronic Systems Technology*, pp. 1–5, Chennai, India, 2011.

[166] D. Stiawan, M. Y. Idris, R. F. Malik, S. Nurmaini, N. Alsharif, and R. Budiarto, "Investigating brute force attack patterns in IoT network," *Journal of Electrical and Computer Engineering*, vol. 2019, Article ID 4568368, 13 pages, 2019.

[167] T. Wang, G. Zhang, A. Liu, M. Z. A. Bhuiyan, and Q. Jin, "A secure IoT service architecture with an efficient balance dynamics based on cloud and edge computing," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 4831–4843, 2019.

[168] M. D. M. Hossain, M. Fotouhi, and R. Hasan, "Towards an analysis of security issues, challenges, and open problems in the Internet of Things," in *2015 IEEE World Congress on Services*, pp. 21–28, New York, NY, USA, 2015.

[169] S. Alanazi, J. Al-Muhtadi, A. Derhab et al., "On resilience of wireless mesh routing protocol against DoS attacks in IoT-based ambient assisted living applications," in *2015 17th International Conference on E-health Networking, Application Services*, pp. 205–210, Boston, MA, USA, 2015.

[170] P. Kumar, G. P. Gupta, and R. Tripathi, "Toward design of an intelligent cyber attack detection system using hybrid feature reduced approach for IoT networks," *Arabian Journal for Science and Engineering*, vol. 46, pp. 1–30, 2021.

[171] S. Lee, A. Abdullah, N. Jhanjhi, and S. Kok, "Classification of botnet attacks in IoT smart factory using honeypot combined with machine learning," *Peer J Computer Science*, vol. 7, article e350, 2021.

[172] S. B. Gopal, C. Poongodi, D. Nanthiya, R. S. Priya, G. Saran, and M. S. Priya, "Mitigating DoS attacks in IoT using supervised and unsupervised algorithms–a survey," *IOP Conference Series: Materials Science and Engineering*, vol. 1055, no. 1, article 012072, 2021.

[173] J. Manhas and S. Kotwal, "Implementation of intrusion detection system for Internet of Things using machine learning techniques," in *Multimedia Security*, pp. 217–237, Springer, Singapore, 2021.

[174] A. Churcher, R. Ullah, J. Ahmad et al., "An experimental analysis of attack classification using machine learning in IoT networks," *Sensors*, vol. 21, no. 2, p. 446, 2021.

[175] S. Sahmim and H. Gharsellaoui, "Privacy and security in Internet-based computing: cloud computing, Internet of Things, cloud of things: a review," *Procedia Computer Science*, vol. 112, pp. 1516–1522, 2017.