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 Auwul6

1Department of Software Engineering, The Superior University, Lahore, Pakistan
2Department of Information Technology, The Superior University, Lahore, Pakistan
3Department of Computer Science and IT, The University of Lahore, Lahore, Pakistan
4School of Computer Sciences, Universiti Sains Malaysia, Penang, Malaysia
5Department of Computer Science, The Superior University, Lahore, Pakistan
6Faculty 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

Copyright © 2022 Muhammad Aqeel et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

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

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

Table 4: Quality assessment of the survey.

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

500 research paper were identified through searching

245 papers were selected after application of exclusive criteria

145 papers were selected after application of exclusive criteria

176 papers were remained after application of quality assessment indicators

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
3.3.4. 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 duplicated 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 reseat 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.
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].
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 “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].
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. 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.

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.

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. CIH is a virus that attacks BIOS, and due to the CIH virus attack, IoT devices are unable to boot. 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. Linux bricking worm can disable the infected IoT device. Silex is another worm that overwrites IoT devices’ storage disks. BrickerBot is a worm that destroys or bricks the infected IoT devices.

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 the device’s password or username, passwords, screenshots, bank details, and account information. Hackers use Zeus Game over Trojan to attack IoT devices to access bank account details.

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.

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. 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.

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...
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 browsing 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 7: Comparison of operating system attacks in IoT.**

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

### Table 8: Comparison of web application attacks in IoT.

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

### Table 9: Comparison of firmware attacks in IoT.

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

(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 steered 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


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


