Journal of Theoretical and Applied Information Technology
15th May 2022. Vol.100. No 9

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

ASSESSING AND REVIEWING OF CYBER-SECURITY THREATS, ATTACKS, MITIGATION TECHNIQUES IN IOT ENVIRONMENT

AZZAM M. ALBALAWI[1], MOHAMMED AMIN ALMAIAH[1*]

1 Department of Computer Networks and Communications, College of Computer Sciences and Information Technology, King Faisal University, Al-Ahsa 31982, Saudi Arabia

E-mail: Corresponding author: *malmaiah@kfu.edu.sa

ABSTRACT

Despite Internet of Things (IoT) technology has a great potential to connect devices and sensors through communication media, such as Wi-Fi, to the internet and customized applications. However, it is vulnerable to cyber security attacks. Thus, integrating IoT technology requires attention to the increased cybersecurity threats. Based on above, this study has several objectives: (1) to review the common types of cybersecurity threats and attacks on IoT and (2) to review the suitable mitigation techniques for IOT threats and attacks. A systematic review has been conducted on 35 recent paper which have published in top ranking journal like IEEE, Elsevier and Springer. Based on our findings, which indicates that Jamming attack is the most common threats on the perception layer or sensors layer, and DoS/DDoS attacks are the most common method at the Network and Application layer. In addition, the results indicate that the most suitable mitigation technique for addressing the IOT attacks is the authentication technique. In addition, some of studies have been employed the AI methods to reduce IoT threats to reduce risks that cannot be addressed with traditional mitigation techniques. Finally, few of IOT studies used the blockchain technology for mitigating the cybersecurity threats and attacks in IOT environment.

Keywords: *Internet of things(IoT), Cybersecurity, Threats, Attacks, Mitigation Techniques, Countermeasures*

1. INTRODUCTION

The terms of IOT cybersecurity threats and cybercrime are many improperly confined to the definition of illegal activeness, in which a system is an integral portion of the cybercrime and are often in use to describe typical crimes, as much as crime, robbery, influence, crime, in which the system are involved [1-4]. IOT cyberyber attacks have more relevant to the use of smart devices, mobile devices and sensors have increased. IOT cybersecurity attacks can be generally definite as cybercriminal activity related to infrastructure of IOT and can be done in one of IOT layers such as perception layer, network layer and application layer [5-8]. IOT cyber attacks problems especially those related to hackers, infractions have become higher visibility. In addition, when sensitive information is lost or intercepted, legitimately or otherwise, there are also privacy concerns. IOT attacks is an act performed by an attacker by accessing IOT devices without any permission. IOT hackers (hacking individuals) are computer programmers, who have an advanced understanding of computers and for devious purposes often exploit this expertise [9-11]. In one specific software program or language, they are usually technology buffs who have expert-level capabilities [12].

Internet of Things (IoT) is made of wired and wireless networks, geographically distributed, and connected over the Internet. It connects many diversified devices and provides end-users with a variety of applications to enhance their quality of life [13-17]. IoT devices usually contain an IP address and sensors though using a communications medium such as Wi-Fi and Bluetooth [18-22] to an application. IoT could be anything from client products to industrial devices. The software programs communicate with each sensor to automate expected actions without human interaction [22-26]. Nowadays, IoT technology is striving to be part of our life where new terms started to arise, such as smart home (e.g., smart bulb, learning thermostat), smart city (e.g., smart parking, smart lighting), medical and health care (e.g., real-time health monitoring system), smart farm, and connected vehicle [27-30]. Nevertheless, due to the massive amount of data transmitted over IoT, cybercriminals exploit the infrastructure of

IoT. For Instance, a hacker could exploit a vulnerability in the camera systems at a victim's house and record what happens, in an exchange for ransom from the victim, or manipulate the cooling system in a data center to increase the temperature of the data hall and cause damage to the hardware [31-34].

Statistics depict IoT applications have rapidly increased over the last few years and picked a good momentum during the COVID-19 pandemic where more people spent more time at home and interacting with devices [35]. Nevertheless, IoT encounters a considerable amount of challenges mainly related to cybersecurity concerns, this paper address such a concern and reflects some recommended solutions [36-39]. Several researchers investigated the security and privacy issues of IoT, such as security and privacy through analyzing the security threats, challenges, and the corresponding countermeasures [40-43]. The motivation of this paper is to provide a comprehensive review of the most recent cybersecurity threats and attacks on IoT system and sensors and determine mitigation techniques and countermeasures to have a safe IoT environment where our privacy should be secured. This study aims to answer the following:

(Q1) To review what are the common types of cybersecurity threats and attacks in IoT environment?

(Q2) To review what are the suitable cybersecurity mitigation techniques for IOT threats and attacks?

The rest of the paper is organized as follows: section 2 presents the background of the study. Section 3 includes the research methodology. Section 4 presents the related works on IOT. Section five discusses the results of the analysis. Finally, section 6 contains the discussion and conclusion.

2. BACKGROUND OF THE STUDY

IoT delivers a better life quality, but it also faces many challenges. For instance, the authors in [44] list multiple challenges that must be taken into consideration, including but not limited to: Poor Management, Big Data, Storage, Authentication and Authorization, and secure networks. For instance, there are many attack techniques on the network layer such as Denial of Service (DoS) and Man-in-the-Middle (MITM) Attacks. Others in [45] believe that lack of guidelines and standards in IoT that may drive many problems at the application layer.

Internet of things applications have increased dramatically in recent years and the amount of information that is sent from one device to another has increased. This increase of data volume and exchange led to cyber risks exponentially. For example, a security incident that happened on October 21, 2016, in the application layer called Mirai (IoT specialized malware) Botnet, it can gain access to IoT devices by SSH account or using the default password of the telnet. After gaining access and elevating privileges, the hacker started deleting some files by installing malware on the system. The infected devices that were under Mirai control halted and initiated DDoS attack. The attackers initiated the attack against one of the biggest computer companies in the United State and attacked DYN (Dyn Managed DNS) and made many websites to be unavailable for 10 hours, which impacted companies as BBC, Amazon, Twitter, Netflix, PayPal, and many others. The attack utilized Mirai malware to strike a DDoS attack [22], [31], [32]. Few attacks such as IoT Reaper, Hajime, BrickerBot, and Mirai exploit the vulnerabilities of IoT devices [32]. Authors in [36] demonstrated that it is feasible to hack a smart car to cause a crash or turn the engine off while the target driving at a high speed.

Data breaches in IOT environment continue to increase at many critical infrastructures such as the healthcare sector due to mis-configured databases, Phishing attacks, malware attacks, ransom-ware attacks, and errors caused by third-parties vendors and employees [32]. Therefore, this paper aims to specify and prioritize threats and identify the most suitable mitigation techniques to counter them.\

3. RESEARCH METHODOLOGY

A systematic literature review methodology is used in this paper to provide a detailed investigation of previous papers and studies in IoT security. In the first stage, the following search string was used to find the relative paper to this paper subject:

(IoT or Internet of Things) AND Risk AND (Assessment OR Analysis OR Management OR Mitigation).

The search was conducted in Google Scholar and Saudi Digital Library using the following criteria: Academic journal or conference paper that represents threats to IoT; papers

published between January 2017 to April 2022. The exclusion criteria were as followed: Papers not related to IoT security and not written in English.

During Identification phase, 36,295 papers were found, after removing the duplicated papers 18,497 papers remained. In the Screening abstract and title, 18,445 papers were excluded, and 52 papers remained for the next phase. After full-text assessment in the eligibility phase, 17 papers were excluded, and 35 papers were included in this literature review as depicted at Figure 1.

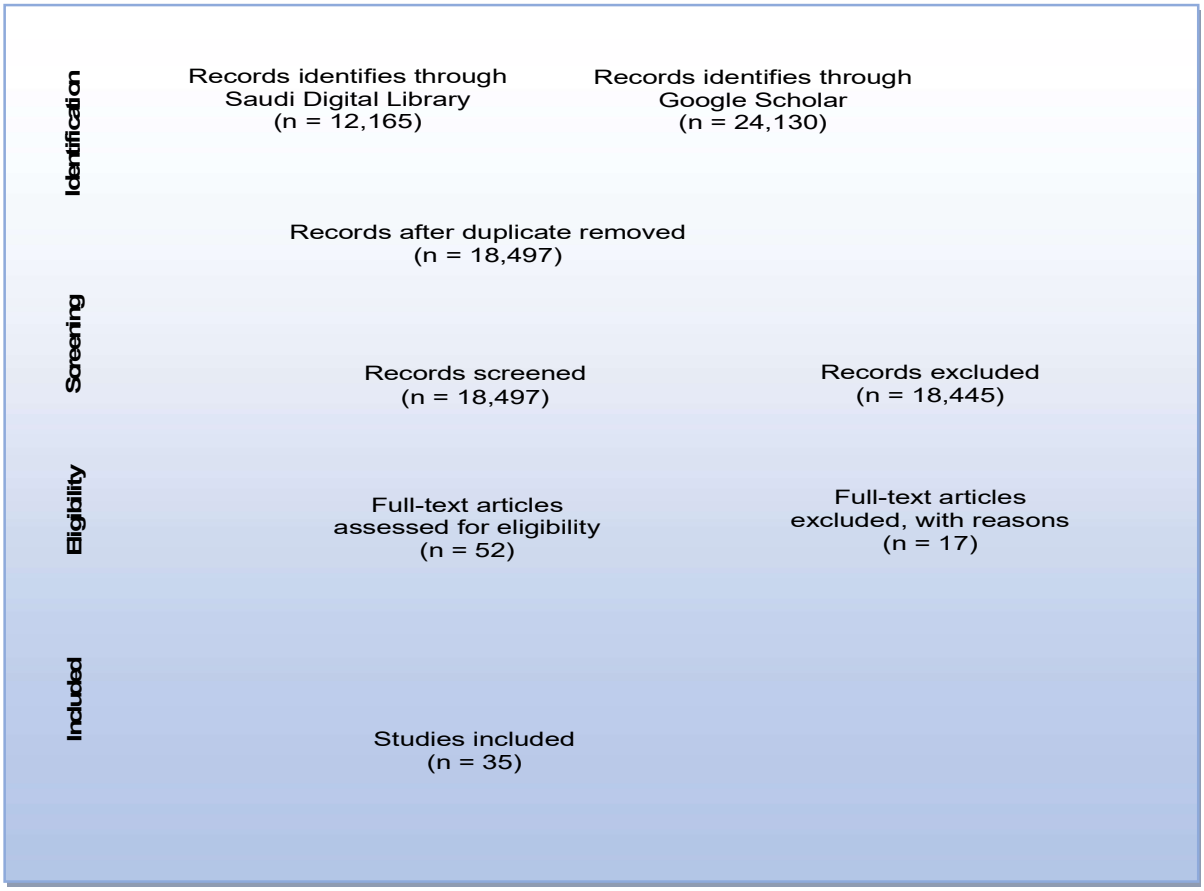

Figure 1: illustrates the process of inclusion and exclusion criteria to choose the relevant papers and articles.

Table 1: Inclusion and Exclusion Criteria.

No.	Inclusion Criteria	Exclusion Criteria
1	Journals, Conferences, Preprints, Chapter	Doesn't address IoT security
2	Published between 2016-2022	Not written in English
3	Presents challenges of IoT security	Electronically inaccessible
4	Cybersecurity attacks, threats on IOT environment	None

Figure 2 shows the distribution of the chosen studies by year. We noticed that more than 75% of the studies have been published between the years (2018-2021).

Journal of Theoretical and Applied Information Technology
15th May 2022. Vol.100. No 9

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

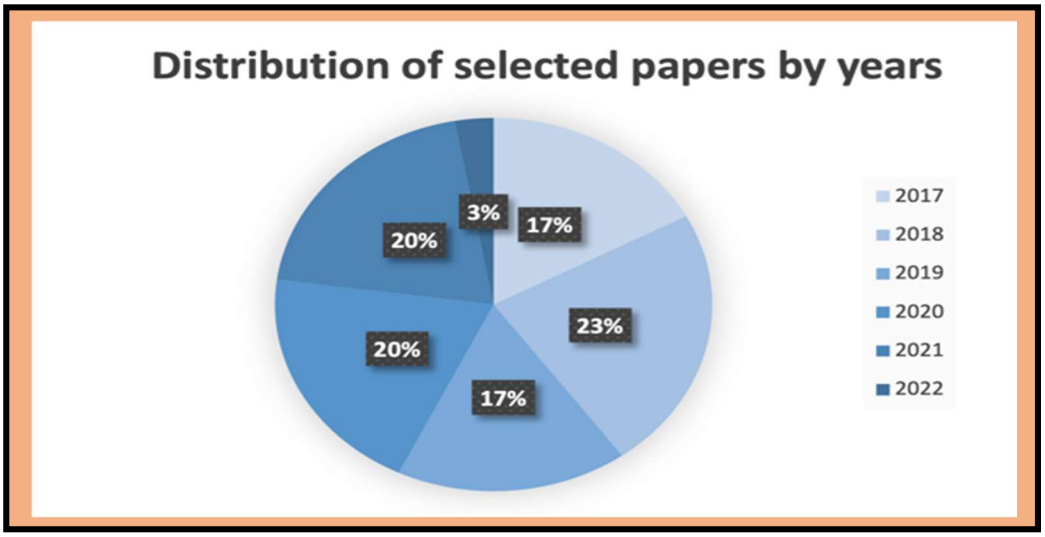

Figure 2: Distribution of selected papers by years.

4. RELATED WORKS ON IOT THREATS ANS ATTACKS

In this section, we have reviewed and summarized all the 36 selected studies that have been conducted by other researchers to answer the research questions for this study. For example, T. Thalawattha, P. Rodrigo, D. Dissanayake, K. Jayasinghe and R. Kathriarachchi [4] preformed a review on a defence against an IoT attacks based on current vulnerabilities. This paper discusses the security requirements in sensor layer, network layer, service layer, and application layer. It discusses the challenges in healthcare and education field. Finally, it discusses the current security techniques and challenges. A. Assiri and H. Almagwashi [2] present a review of the security issues and challenges of IoT. The authors provide an overview of three main layers in IoT: the perception layer, the network layer, and the application layer. Then discuss the challenges each layer faces. and what are the potential attacks? They discuss the security requirements in IoT such as confidentiality, authorization, authenticity, integrity, and availability, and how to achieve these requirements. Finally, the authors show a list of the IoT challenges such as (Date Volume, Constraints in resources, Protection, Scalability, and Autonomic control).

In addition, M. Obaidat, J. Brown, S. Obeidat, J. Holst, A. Hayajneh [3] performed a survey on IoT security and privacy challenges, threats, vulnerabilities, and countermeasures. The growth of IoT in our daily lives has increased so it created an Internet of Vulnerabilities (IoV). This paper provides an overview of IoT, its applications, limitations as well as and security issues related to each domain. Moreover, the paper discusses cybersecurity attacks, threats, and vulnerabilities and provides a classification of them based on the violation of Confidentiality, Integrity, and Availability (CIA), and approaches to the mitigation and countermeasures to these security concerns. In the same way, Azam, R. Munir, M. Ahmed, M. Ayub, A, Sajid, and Z. Abbasi [4] review the security issues in different IoT layers and discuss the potential solutions to overcome those security issues. This paper discusses the attacks that can happen in the sensing layer, network layer, middleware layer, and application layer, and propose a different solution for each layer. D. Alferidah and N. Jhanjhi [5] review the security issues, privacy issues, and challenges on the Internet of Things (IoT). The paper's contents are supported by a literature review to provide a detailed overview of previous studies and papers in IoT security. This paper discusses and analysis two kinds of attacks which are attack taxonomy and layer-wise attacks. E. Ezema, A. Abdullah, N. Sani [6] conducted a survey on IoT security challenges. This paper presents an overview of IoT architecture (application layer, network layer, and physical layer), and it reviews the previous studies related to IoT.

O. Abiodun, E. Abiodun, M. Alawida1, R. Alkhawaldeh, and H. Arshad [7] performed a review of the different security issues and challenges in IoT and provide potential solutions to

address the security challenges. IoT inter-connectivity does not require computer-to-machine connection and that brings different types of security challenges. This paper discusses some threats and vulnerabilities such as data leaks, it conducts a security assessment from different sources such as data at rest, data in use, data in flight, and it discusses the security requirement in IoT such as availability, confidentiality, Authentication, Authorization, and access control. It proposes solutions to the security challenges. Finally, they show me research gaps in IoT and future directions. M. Burhanuddin, A. Mohammed, R. Ismail, M. Hameed, A. Kareem, and H. Basiron [8] preformed a review on security challenges in wireless sensor networks (WSN) within the perspective of the Internet of Things. Conducted a classification of available attacks and threats against WSN requirements. W. Zhou, Y. Zhang, and Peng Liu [9] performed a survey on IoT threats and challenges. This paper proposes to discuss the concept of "IoT features" and discuss each feature with its threats, challenges, and solutions. IoT features are Interdependence, Diversity, Constrained, Myriad, Unattended, and Mobile. Finally, it discusses the challenges to be solved.

A recent study conducted by A. Bashir, S. Sholla, and A. Nazir [10] performed a survey on IoT threats and challenges. This paper proposes to discuss the concept of "IoT features" and discuss each feature with its threats, challenges, and solutions. IoT features are Interdependence, Diversity, Constrained, Myriad, Unattended, and Mobile. Finally, it discusses the challenges to be solved. F. Ullah, H. Naeem, S. Jabbar, S. Khalid, M. Latif, F. Al-Turjman, AND L. Mostarda [11] proposed a deep learning approach to detect malware-infected files and pirated software across the IoT network. This paper proposes TensorFlow deep neural network to identify pirated software using the source code and the paper proposes an architecture model for cybersecurity threats and countermeasures in industrial IoT. It uses the data set from Google Code Jam (GCJ) to analyze the proposed methodology. G. Verma, and S. Prakash [12] provide a detailed analysis of recent state-of-the-art security issues of different layers in Industrial Internet of Things (IIoT) architecture. It discusses a list of countermeasures against IIoT issues. This paper presents a list of future directions. It proposes Machine Learning that can be another way to counter potential threats and attacks in IIoT infrastructure.

Moreover, P. Grammatikis, P. Sarigiannidis, and l. Moscholios [13] provide a comprehensive security analysis of IoT, by assessing the threats and countermeasures. This paper implements a qualitative and quantitative risk assessment, trying to find the security threats in various layers. The authors discuss the security requirements in IoT such as confidentiality, integrity, availability, and authenticity, and the security challenges such as interoperability, resource constraints, resilience to physical attacks and natural disasters, privacy protection, and scalability. In qualitative evaluation, the authors used the probability and impact and the countermeasures to evaluate the risk level; high, medium, and low. Finally, it identifies the suitable countermeasures and provides future work directions. A. bekkali, M. Essaaidi, M. Boulmalf, and D. majdoubi [14] conducted a systematic literature review of Internet of Things (IoT) Security. This paper presents a comprehensive analysis of IoT security, taking into consideration the IoT generic architecture that includes (the perception layer, network layer, middleware layer, and application layer) and discusses the security issues and solutions for each layer. The authors discuss some IoT cybersecurity challenges such as confidentiality, authentication, availability, integrity, detection, and heterogeneity. Furthermore, This SLR provides an overview of current trends and future direction.

Furthermore, J. Brajones, J. Murillo, J. Valdés, and F. Valero [15] detect and mitigate DoS and DDoS attacks on the Internet of Things (IoT) by an experimental approach using a stateful Software Defined Networking (SDN) data plane. B. Kim, B. Khan, M. Burhan, and R. Rehman [16] performed a comprehensive survey on security issues in the Internet of Things (IoT). This paper presents an overview of different layers in IoT which are (the perception layer, network layer, and application layer) and presents the attacks on each layer. In addition, it reviews mitigation techniques for these attacks. Furthermore, they suggest new IoT architecture layers to overcome these issues and they are (Perception Layer, Observer Layer, Processing Layer, Security Layer, Network Layer, Application Layer) where the Observer improves the security by providing authentication, as well as the Security Layer it improves the privacy by adding Encryption, Decryption, and Hash Encryption. L. Wu, Y. Yang, G. Yin, L. Li, and H. Zhao [17] surveyed the security and privacy issues of the Internet of Things (IoT). IoT provides benefits that make our life much easier but those

benefits, come with a huge number of risks. The survey consists of four parts. The first part, explore the limitation and solutions of IoT devices. The second part classifies the attacks in IoT. The third part focuses on mechanisms and architecture for access control and authentication. The last part, present the security issues in different layers. K. Li, Y. Fan, G. Zhao, B. Zhang, G. Tan, X. Sun, and F. Xia [18] propose a security scheme, Securing Nodes in IoT Perception Layer (SNPL) to protect the nodes in the perception layer. The authors have done a series of experiments, and the result shows that SNPL is effective to counter faulty and malicious nodes. The scheme meets the cybersecurity requirements such as Confidentiality, Integrity, and Availability (CIA). H. Aslan, A. Nasr, S. Abdel-Magid, and H. Ahmed [19] performed a survey on IoT security threats and proposed defense. The authors address the security threats, challenges, and defenses in different layers of IoT such as the perception layer, network layer, and applications layer. M. Tabari and Z. Mataji [20] proposed a distributed Intrusion Detection System (IDS) to detect sinkhole attacks in RPL-based IoT networks. The accuracy of the experiment could reach up to 99.35 rates of accuracy.

Z. Dvorak, Z. Cekerevac, L. Prigoda, and P. Cekerevac [21] present an overview of the Internet of Things (IoT) and what most common attacks. This paper focuses on one attack which is the Man-in-the-Middle (MITM) attack. It also presents some examples of MITM attacks and identifies the possible protection methods against MITM attacks. Then, it discusses how MITM attacks can be conducted and what are the available tools to strike a MITM attack such as Ettercap, Evilgrade, SSLstrip, Dsniff, Cain, and Abel. It provides an overview of available types of MITM attacks, and they are MIT-cloud (MITC), MIT-browser (MITB), MIT-mobile (MITMO), MIT-app (MITA), MIT-IoT. W. Abbass, Z. Bakraouy, A. Baina, and M. Bellafkih [22] provide a novel approach based on ESK (Elastic-search Stack Solution) and the PDCA (Plan, Do, Check, Act) cycle to assess the IoT security risks efficiently. The also authors identified the IoT vulnerabilities. M. Calore, F. Meneghello, D. Zucchetto, M. Polese, and A. Zanella [23] performed a survey on security risks and threats on the Internet of Things (IoT) and discuss the possible counteractions. The authors discuss the security mechanisms that are adapted in some communication protocols. Then, they analyze some attacks in different layers of IoT. They conclude this paper with compression of IoT technologies with respect to the cybersecurity requirements, namely confidentiality, integrity, availability, authentication, and authorization. S. Rekha, L. Thirupathi, S. Renikunta, and R. Gangula [24] performed a study of security and solutions on the Internet of Things (IoT). This study discusses how to examine the main parts of IoT. And how professionals conducted mitigation techniques like encryption to secure the privacy of information. K. Sha, W. Wei, T. Yang, Z. Wang, and W. Shi [25] analyze some security challenges that resulted from new features of Internet of Things (IoT) applications. Moreover, the authors proposed and analyzed architectural security designs, and discuss how to implement this design. Finally, they identified the open issues for each layer. A. Ali, F. Köylü, M. Hassan, M. Sabriye, A. Osman, A. Hilal, Q. Abdullah [26] conducted a review of the architecture, technologies, and application of the Internet of Things (IoT). Then the authors discuss the security challenges and threats in IoT that need to be addressed. C. Hu, Xiuzhen Cheng, A. Alrawais, and A. Alhothaily [27] discuss the security and privacy challenges on the Internet of Things (IoT) and propose a mechanism using fog to improve some security problems in the distribution of certificate revocation information in IoT environments and can enhance the security of security devices. The authors also discuss some IoT challenges such as authentication, trust, privacy, access control, intrusion detection, data protection, and other challenges.

K. Skouby, R. Tadayoni, and S. Koduah [28] addressed the major cybersecurity concerns on the Internet of Things (IoT) environment, application, and domain. In addition, the authors analyze the cybersecurity challenges such as application services attacks, data integrity attacks, trust, privacy, identity, and standardization. The authors have done an experimental evaluation of two kinds of attacks scenarios, they are SQL injection and DoS attack against IoT devices. A. Djenna, S. Harous, and D. Saidouni [29] present an analysis of the recent cybersecurity challenges for the Internet of Things (IoT). Then, discuss some of the potential threats and vulnerabilities, and exploitation techniques adopted by cybercriminals. In addition, the authors provide a taxonomy of cyberattacks that may cause harm to IoT infrastructure. Lastly, they present some security requirements and recommendations to enhance IoT security. J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao [30] performed a survey on the Internet of Things (IoT) by presenting a

comprehensive overview of IoT architecture, available technology, security, and privacy issues and challenges, and IoT applications. This paper presents the technology and attacks that have a high potential to happen in three main layers of IoT which are the perception layer, network layer, and application layer. Then, explore the relationship between IoT and Cyber-Physical Systems (CPS). H. Lakhlef, A. Bouabdallah, and D. Kouicem [31] provide a comprehensive top-down survey of recent proposed security and solutions for the Internet of Things (IoT). The authors discuss the benefits of new technologies and approaches such as blockchain and Software-Defined Networking (SDN) that can enhance the security and privacy of IoT in terms of flexibility and scalability. Lastly, they provide a classification of existing solutions and compare them. V. Rangan, S. Srinivas, K. Kandasamy, K. Achuthan [32] reviewed existing cybersecurity risk assessment methodologies. The authors also review and present IoT risks based on their category and impact. They discuss the risks in systems IoT in the financial and healthcare sector because they have a high-risk exposure and discuss the risk vectors of the Internet of Medical Things (IoMT). Finally, they introduce a risk ranking method. M. Khana and K. Salah [33] performed a survey on major security problems for IoT. The authors reviewed and categorized widespread security problems in various Internet of Things (IoT) layers. They outline the cybersecurity requirements for IoT along with current threats, attacks, and potential solutions. G. Verma and S. Prakash [34] performed a systematic literature review on IoT security threats, countermeasures, and issues in various layers. This paper analyzes the previous papers in IoT security and list the contribution of each paper. It discusses the threats, features, and limitations in the perception layer, transport layer, and application layer. It provides aspects that can be conducted in future research. Finally, P. Parashar and S. Tandon [35] performed a study on the Internet of Things (IoT), the authors present an overview of IoT architecture such as (The things layer, Connectivity/Edge computing layer, Global infrastructure layer, Data ingestion layer, Data analysis layer, and People and Process layer), and related security issues in various layers such as perception layer, network layer, and application layer [41-47].

5. ANALYSIS AND RESULTS

Before answering the research questions, based on our findings in Figure 3, which indicated that 23 of selected studies have used a qualitative method, 11 studies used a quantitative method, and only 1 study used a mixed type of qualitative and quantitative methods.

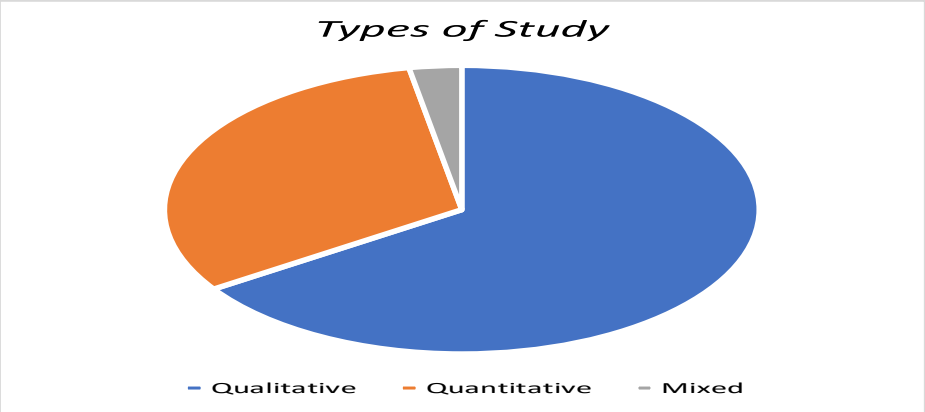

Figure 3: Types of Study.

5.1 Q1: To review what are the common types of cybersecurity threats and attacks in IoT environment?

In this section, we have analyzed the most common types of cyberecurity threats and attacks based on classifying the IoT architecture. The standard IoT architecture is divided into three main layers: The perception layer, The network Layer, and the Application Layer. A high level of security should be provided to all the layers. These layers must meet the cybersecurity requirements: Confidentiality, Integrity, and Availability. In this section, we present the results of the most common threats and mitigation techniques, and countermeasures based on the three types of IOT layers as the subsections below.

5.1.1 The common cyber attacks on IOT-Perception Layer

IoT needs a layer to communicate with the environment. Therefore, this layer consists of sensors and actuators such as (RFID, ZigBee, WSN, GPS, and others.) which collect the data from the environment and transmit it to the next layer to be processed [14]. The most common threats in this layer are shown the Figure 4, they are Jamming, Physical attacks, Eavesdropping, Injection attacks, Tampering, Cloning, and Interference Attacks. Jamming attacks is the most common one that could affect the availability of the device [48-55].

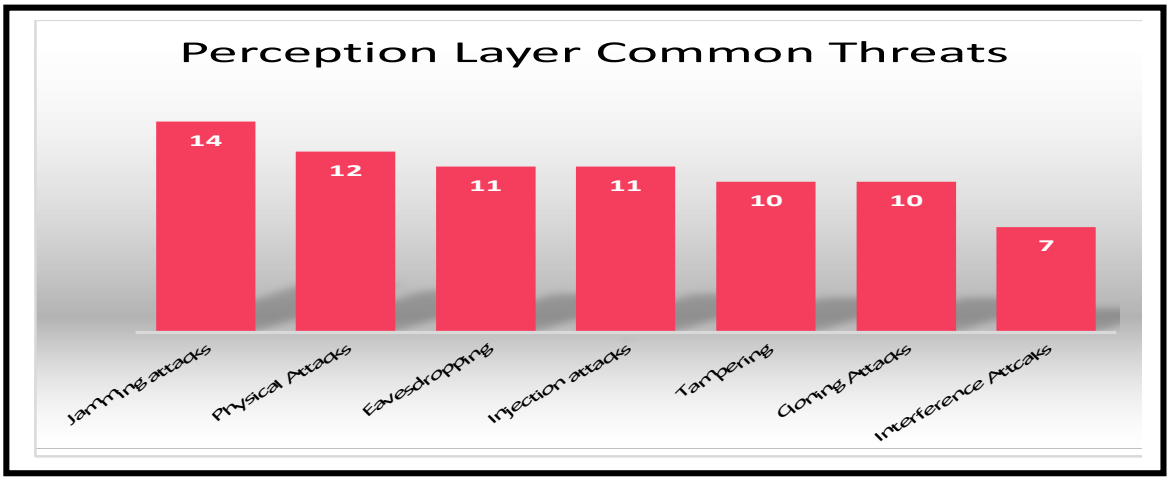

Figure 4: Findings of The most common types of Cyber threats and attacks in IOT-Perception layer.

5.1.2 The common cyber attacks on IOT-Network Layer

This layer is the second layer, which receives the data from the perception layer and transmits it to the application layer. This layer is made of wired and wireless networks such as (WiFi, 3G, Bluetooth, LTE, and others.) [14], [19]. It maintains the reliable delivery of data by supporting connection-oriented service [56-60]. Based on the results, the top seven common attacks are shown in Figure 5 Denial of Service (DoS) Attacks and Distributed Denial of Service (DDoS) attacks are at the top of the list. Then, Man-in-the-Middle (MITM) Attacks, Sinkhole attack, Sybil attacks, Spoofing attacks, Traffic Analysis, and Routing Attacks [60-64].

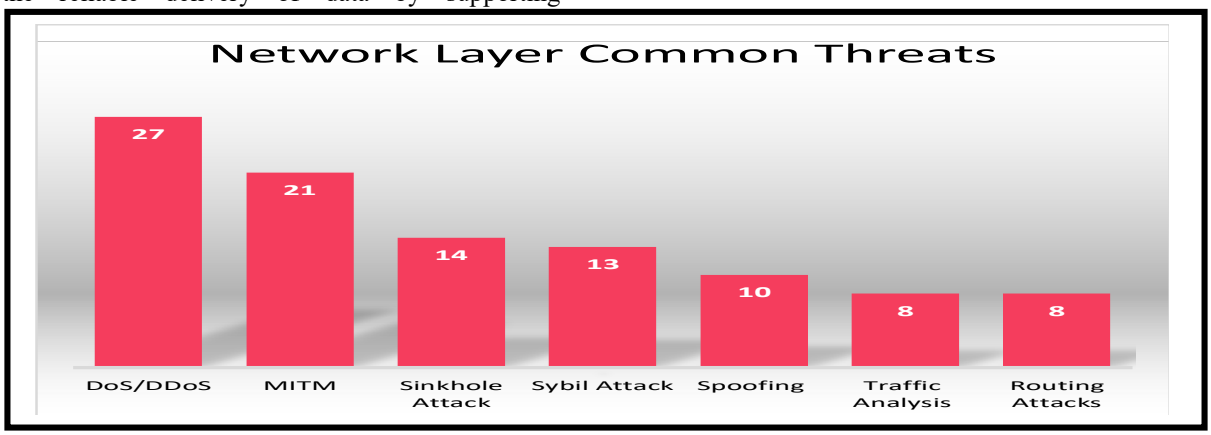

Figure 5: Findings of The most common types of Cyber threats and attacks in IOT-Perception layer.

5.1.3 The common cyber attacks on IOT-Application Layer

This layer provides the interface to the end-user which is made up of services areas such as (healthcare, smart homes, connected cars, etc.) [14]. This layer can recognize the spam, malicious, and valid data by using some methods that provide filtering features [19]. Based on our findings, the most common types of security threats need to be addressed in this layer are DoS/DDoS attacks, code injection attacks, phishing attacks, Malware attacks, malicious scripts attacks, buffer overflow attacks, cross-site scripting (XSS) attacks, and spyware attacks need to be addressed, but DoS/DDoS attacks are the most common threats in this layer. Figure 6 presents the findings of the most common types of security threats in IOT-application layer.

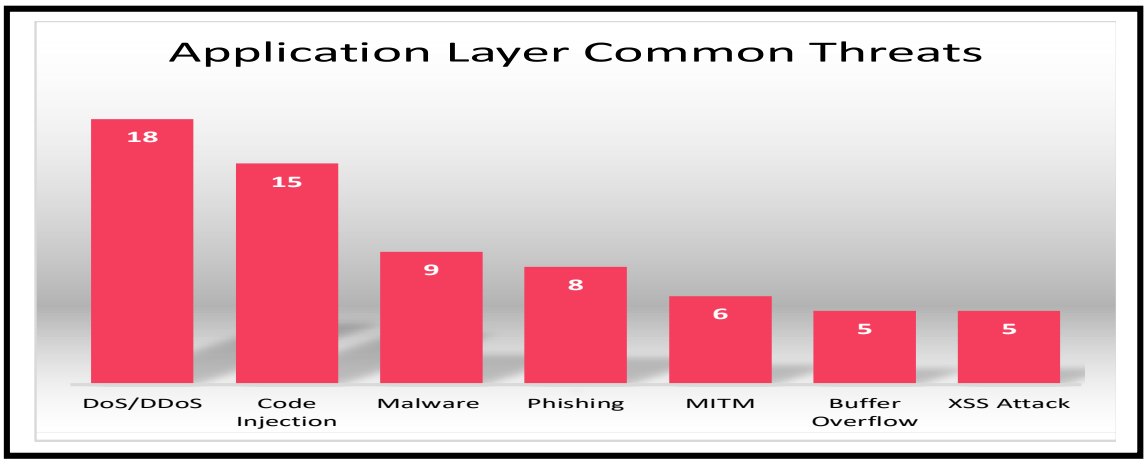

Figure 6: Findings of The most common types of Cyber threats and attacks in IOT-Application layer.

Table 2: Reviewing the common types of IOT threats based on three types of IOT layers

Reference	Title	Layer	Type of Threats and attacks
T. Thalawattha **et al.,** [1] **2021**	A Defense Against an Internet of Things (IoT) Attacks Based on Current Vulnerabilities	**General**	Leakage of privacy, Sniffing Service information manipulation, Lack of encryption, Weak default password, The rise of Botnets.
		Network	Denial of Service (DoS) attacks.
		Application	Denial of Service (DoS) attacks.
A. Assiri **et al.,** [2] **2018**	IoT Security and Privacy Issues	**Perception**	Physical Attacks, Tampering, Cloning Attacks, Timing Attacks.
		Network	Eavesdropping, Denial of Service (DoS) attacks, Viruses attacks, Man-in-the-Middle (MITM) Attacks, Traffic Analysis, Spoofing attacks.
		Application	lack of standards, Denial of Service (DoS) Attack, Man-in-the-Middle (MITM) Attacks.
M. Obaidat **et al.,** [3] **2020**	AComprehensive and Systematic Survey on the Internet of Things: Security and Privacy Challenges,	**Perception**	Social Engineering, Node Jamming attack, Malicious Node Injection, False Data Injection attacks, Eavesdropping, Interference, Sleep Deprivation, Tag Cloning.
		Network	Denial of Service (DoS) attacks, Spoofing attacks, Selective forwarding, Packet replication attack, Man in the middle (MITM) attacks, Sinkhole attacks, Routing

	Security Frameworks, Enabling Technologies, Threats, Vulnerabilities and Countermeasures		information attacks, Wormhole attacks, Sybil attacks, Sniffing attack, Traffic Analysis.
		Application	Phishing attack, Malicious virus/worm/trojan horse, spyware, Malicious scripts, DoS attacks, Software vulnerabilities, Code Injection, Buffer Overflow, Sensitive Data Manipulation, Data leakage
F. Azam **et al., [4]** **2019**	Internet of Things (IoT), Security Issues and Its Solutions	**Perception**	Unauthorized Access, Tag Cloning, Eavesdropping, Interference, Jamming attack, Sleep Deprivation attack, Node Catching, False Data/Code Injection attack, Side-Channel attacks, Booting Attack.
		Network	Denial of Service (DoS) Attack, Distributed Denial of Service (DDoS), Sybil Attack, Sinkhole attack, Sniffing Attack, Traffic analysis, Replay Attack, Man-in-the-Middle (MITM) Attacks, Data Transit Attack, Routing Attacks.
		Application	Phishing Attacks, Buffer Overflow, Sensitive Data Permission/Manipulation, Data Theft, Access Control Attacks, Service Interruption Attacks, Malicious Code Injection Attacks, Sniffing Attacks, Reprogram Attacks.
N. Jhanjhi **et al.,** [5] **2020**	A Review on Security and Privacy Issues and Challenges in Internet of Things	**Perception**	Unauthorized Access to Tags, Tag Cloning, Eavesdropping, Spoofing, RF Jamming, Timing Attack, Replay Attack, Node Capture Attack, Malicious Node Injection Attack, Brute-force Attack, Radio Interference, Tampering.
		Network	Sybil Attack, Sinkhole Attack, Sleep Deprivation Attack, Denial of Service (DoS) Attack, Malicious code injection, Man-in-the-Middle (MITM) Attack, Traffic Analysis, Passive Monitoring, Eavesdropping
		Application	Malicious Code Injection, DoS Attack, Spear-Phishing Attack, Sniffing Attack, Overwhelm, Reprogram
O. Abiodun **et al.,** [6] **2021**	A Review on the Security of the Internet of Things: Challenges and Solutions	**Perception**	Social Engineering, Physical Damage, Node Tempering, Sleep Deprivation, Malicious node injection, RFID Unauthorized access, RFID interference on RFID, RFID cloning, RFID spoofing
		Network	Traffic analysis, Sinkhole attack, Man-in-the-Middle (MITM) attacks. Routing attacks.
		Application	Phishing Attacks, Malicious Script Injection, Denial of Service (DoS) Attacks, Worm, Spyware, and Virus Attacks.
E. Ezema **et al.,** [7] **2018**	A Comprehensive Survey of Security Related Challenges in Internet of Things	**Network**	Denial of Service (DoS) attacks, Distributed Denial of Service (DDoS) attacks, Packets forwarded.
		Application	Denial of Service (DoS) attacks, Distributed Denial of Service (DDoS) attacks.

M. Hameed **et al.,** [8] **2018**	A Review on Security Challenges and Features in Wireless Sensor Networks: IoT Perspective	**Perception**	Eavesdropping, Jamming attack, Tampering attack.
		Network	Denial of Service (DoS) Attacks, Spoofed, Altered, or Replayed Routing Information Attacks, Selective Forwarding Attack, Blackhole Attack, Sinkhole Attack, Sybil Attack, Wormholes Attack, Hello flood attacks, Acknowledgment spoofing attack.
		Application	Denial of Service (DoS) Attacks.
W. Zhou et al., [9] 2018	The Effect of IoT New Features on Security and Privacy: New Threats, Existing Solutions, and Challenges Yet to Be Solved	**Network**	Man-in-the-Middle (MITM) Attack, Distributed Denial of Service (DDoS) Attack, Stuxnet, Malicious Code Injection.
		Application	Man-in-the-Middle (MITM) Attack, Distributed Denial of Service (DDoS) Attack Malicious Code Injection.
A. Bashir **et al.,** [10] **2019**	Internet of Things Security: Issues, Challenges and Counter-Measure	**Perception**	Node Tempering, RF Interference on RFIDs, Node Jamming, Frequency Jamming, Malicious Node Injection/Fake Node, Sleep Deprivation Attack, Malicious Code Injection, Social engineering, Physical attack, Side-Channel Attack, RFID Spoofing, RFID Cloning, RFID Unauthorized Access.
		Network	Traffic Analysis Attacks, Sinkhole Attack, Man in the Middle (MITM) Attack, Denial of Service (DoS), Routing Information Attacks, Sybil Attack, Heterogeneity Problem, Network Congestion problem.
		Application	Phishing Attacks, Malicious Active X Scripts, Malware attacks, Distributed Denial of Service (DDoS).
S. Pal et al., [12] 2021	Analysis of Security Issues and Countermeasures for the Industrial Internet of Things	**Perception**	Jamming Attack, Eavesdropping.
		Network	DNS Spoofing, Session Hijacking, Blackhole Attack, Wormhole Attack, Sybil Attack, Injecting Malicious Codes, MITM Attacks, DoS/DDoS Attacks.
		Application	DoS/DDoS Attacks, Injecting Malicious Codes, MITM Attacks.
l. Moscho **et al.,** [13] **2018**	Securing the Internet of Things: Challenges, Threats and Solutions	**Perception**	Social Engineering, Jamming Attacks, Physical attack, Environmental Threats, Natural Disasters.
		Network	Selective Forwarding attacks, Sinkhole attack, Wormhole attacks, Sybil attack, Hello Flood attack, Traffic Analysis attacks, Man-in-the-Middle (MITM) attacks, Denial-of-service (DoS) attacks, Botnets, Rootkit.
		Application	Buffer Overflow, Backdoor, Spyware.
M. Essaaidi **et al.,** [14]	Systematic Literature Review of	**Perception**	Node Capture, Unauthorized Access to Tags, Tag cloning, Fake Node Injection, Malicious Data Injection, Eavesdropping, Spoofing, RF Jamming,

2022	Internet of Things (IoT) Security		Replay Attack, and Side-Channel Attack (SCA).
		Network	Spoofing, Denial of Service (DoS) Attack, Eavesdropping, Man-in-the-Middle (MITM) Attack, Sybil Attack, Cluster Security Problems, Sinkhole Attack, Sleep Deprivation Attack, Sniffing and Altered or Replayed Routing Information.
J. Murillo **et al.,** [15] **2020**	Detection and Mitigation of DoS and DDoS Attacks in IoT-Based Stateful SDN: An Experimental Approach	**Network**	Denial of Service (DoS) Attacks, Distributed Denial of Service (DDoS), Man in the Middle attack (MITM), Blackholes Attack, Spoofing, Repudiation, Elevation of privileges).
B. Kim **et al.,** [16] **2018**	IoT Elements, Layered Architectures and Security Issues: A Comprehensive Survey	**Perception**	Eavesdropping, Node Capture, Fake Node Injection, Replay Attack, Timing Attack.
		Network	Denial of Service (DoS) Attack, Main-in-The-Middle (MITM) Attack, Storage Attack, Exploit Attacks.
		Application	Cross-Site Scripting Attack, Malicious Code Injection Attack, the ability to deal with Mass Data Spear-Phishing, Social Engineering.
L. Wu **et al.,** [17] **2017**	A Survey on Security and Privacy Issues in Internet-of-Things	**Perception**	Physical Attack, Faulty Nodes Injection, Eavesdropping Attacks, Active Attacks.
		Network	Man-in-the-Middle (MITM) Attack, Distributed Denial of Service (DDoS) Attack, Replay Attack.
		Application	Viruses, Malware, Distributed Denial of Service (DDoS) Attack
K. Li et al., [18] 2020	SNPL: One Scheme of Securing Nodes in IoT Perception Layer	**Perception**	Cryptoanalysis Attacks, Timing Attacks, Side-channel Attacks, Forgery Attacks, Substitution Attacks.
H. Aslan **et al.,** [19] **2019**	A survey of IoT security threats and defenses	**Perception**	Physical attacks, Jamming Attacks, Tampering attack, RF Interference, Object Replication, Tag Cloning.
		Network	Traffic Analysis Attack, Spoofing, Sinkhole Attack, HELLO Flood, Blackhole Attack, Man-in-the-Middle (MITM) Attacks, Sybil attacks.
		Application	Virus, Worms, Trojan Horse, Spyware, Malicious Code Injection, Denial of Service (DoS), Distributed Denial of Service (DDoS), Cross-site Scripting Attack, Buffer overflow, Privacy Leak Attacks.
M. Tabari **et al.,** [20] **2020**	Detecting Sinkhole Attack in RPL-based Internet of Things Routing	**Network**	Sinkhole Attacks.

	Protocol		
Z. Dvorak **et al.,** [21] **2017**	Internet of Things and The Man-in-the-Middle Attacks - Security and Economic Risks	**Network**	Man-in-the-Middle Attacks, Denial of Service (DoS), Compromised-key Attacks, Manipulation Attacks. MITM can be conducted in several ways: Address Resolution Protocol (ARP) cache poisoning, DNS spoofing, Session hijacking including side-jacking, evil twin, sniffing, DNS spoofing, SSL Hijacking, Session hijacking, SSL hijacking.
W. Abbass **et al.,** [22] **2019**	Assessing the Internet of Things Security Risks	**Perception**	Node Jamming, Tampering, Malicious Node Injection.
		Network	DoS/DDoS, Sinkhole, Selective Forwarding, Packets altering, and Worm.
		Application	DoS/DDoS, Viruses, Malicious scripts, Phishing attacks Man in the Middle (MITM) Attacks.
M. Calore **et al.,** [23] **2019**	IoT: Internet of Threats? A Survey of Practical Security Vulnerabilities in Real IoT Devices	**Network**	Sybil Attacks, Sinkhole Attack, Selective Forwarding and Blackhole Attacks, Hello Flooding Attack, Local Repair Attack, Version Number Attack, Attacks from the Internet side.
S. Rekha **et al.,** [24] **2021**	Study of security issues and solutions in Internet of Things (IoT)	**Network**	Distributed Denial of Service (DoS) Attacks, Denial of Service (DDoS) Attacks.
		Application	Distributed Denial of Service (DoS) Attacks, Denial of Service (DDoS) Attacks.
K. Sha **el al.,** [25] **2018**	On security challenges and open issues in Internet of Things	**Network**	Man-in-the-Middle (MITM) Attack, Sybil attack, Replay Attack, Side-channel Attacks.
A. Ali **et al.,** [26] **2021**	Review of Internet Things (IoT) of Security Threats and Challenges	**Perception**	Tampering attacks, Eavesdropping.
		Network	Man-in-the-Middle (MITM) Attacks, Denial-of-Service (DoS) Attacks.
C. Hu **et al., [27] 2017**	Fog Computing for the Internet of Things: Security and Privacy Issues	**Network**	Denial of Service (DoS) Attacks.
		Application	Malware-based Attacks.
K. Skouby **et al.,** [28] **2017**	Cyber Security Threats to IoT Applications and Service Domains	**Network**	Wireless Scrambling, Eavesdropping, Man-in-the-Middle (MITM) Attacks, Denial of Service (DoS) Attacks, Message Modification Attacks, Injection Attacks, IP Misconfiguration,
		Application	Denial of Service (DoS) Attacks, SQL injection, Code Execution, XSS, and CSRF attacks.
A. Djenna **et**	Internet of Things Meet	**Perception**	RFID attacks: RFID Spoofing, RFID Cloning, RFID Modification, RFID Tag Alteration. Botnet Attacks:

al., [29] **2021**	Internet of Threats: New Concern Cyber Security Issues of Critical Cyber Infrastructure		Centralized Attacks, P2P Attacks, Hybrid Attacks, Random Attacks. Session Med-jacking, Physical Attacks.
		Network	Denial of Service Attacks: Classic Attacks, Massive Attacks.
		Application	Web Injection: SQL Injection, NoSQL Injection, LDAP Injection, OS Update Injection. Cross-Site Scripting (XSS): Reflected XSS, Persistent XSS, DOM-based XSS. Malware: APT, Autonomic Malware, Advanced Malware, Ransomware, Backdoor.
J. Lin **et al.,** [30] **2017**	A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications	**Perception**	Node Capture Attacks, Malicious code Injection Attacks, False Data Injection Attacks, Replay Attacks, Cryptoanalysis Attacks, and Side-Channel Attacks, Eavesdropping and Interference.
		Network	Denial of Service (DoS) Attacks, Spoofing Attacks, Sinkhole Attacks, Wormhole Attacks, Man in the Middle (MITM) Attacks, Routing Information Attacks, Sybil Attacks.
		Application	Phishing Attack, Malicious Virus/worm, Malicious Scripts.
H. Lakhlef [31] **2018**	Internet of things security: A top-down survey	**Perception**	Jamming Attacks, Physical Attacks.
		Network	Denial of Service (DoS) Attacks, Distributed Denial of Service (DDoS) Attacks, Injection attacks.
		Application	Denial of Service (DoS) Attacks, Distributed Denial of Service (DDoS) Attacks, Injection attacks.
V. Rangan **et al.,** [32] **2020**	IoT cyber risk: a holistic analysis of cyber risk assessment frameworks, risk vectors, and risk ranking process	**Perception**	Device tampering, tag cloning, sensor tracking, Jamming Attacks.
		Network	Distributed Denial of Service (DDoS) Attack, Denial of Service Attack (DoS), Man-in-the-Middle (MITM) Attacks, Replay Attacks, Side-Channel Attacks.
		Application	SQL Injection, Account Hijacking, Ransomware, Brute-force Attack, Buffer Overflows.
M. Khana **et al.,** [33] **2017**	IoT Security: Review, Blockchain Solutions, and Open Challenges	**Perception**	Jamming Attacks
		Network	Denial-of-Service (DoS) Attacks, Man-in-the-Middle (MITM) Attack, Sinkhole and Wormhole attacks, Spoofing Attacks, Sybil attacks, Sleep deprivation attacks.
		Application	Denial-of-Service (DoS) Attacks, Man-in-the-Middle (MITM) Attack.
G. Verma et al., [34] 2021	Emerging Security Threats, Countermeasures, Issues and Future Aspects on Internet of Things (IoT): A	**Perception**	Node Tempering, Impersonation.
		Network	Routing Attacks, Data Transit Attacks.
		Application	Denial of Service (DoS) Attack, Data Leakage, Data Transit Attacks.

	Systematic Literature Review		
S. Tandon **et al.,** [35]	A study on Internet of Things (IOT) security issues and solutions	**Perception**	Eavesdropping, Node Capture, Fake Node Injection, Replay Attack.
		Network	Denial of Service (DoS) Attack, Main-in-The-Middle (MITM) Attack, Storage Attack
		Application	Cross-Site Scripting, Malicious Code Attack.

5.2 Q2: To review what are the suitable cybersecurity mitigation techniques for IOT threats and attacks?

In this section, we presented the study findings related to the most common mitigation techniques that have been used in previous studies to address the several types of cybersecurity attacks in IOT as mentioned in section above. Figure 7 showed the suggested mitigation techniques to address IoT threats. The results indicated that 17 studies focused on authentication techniques in order to mitigate the threats and attacks in IOT environment. Number of studies (10) have been used encryption techniques to address cybersecurity attacks in IOT domain. Six of studies employed the access control techniques, five of previous studies used the Artificial Intelligent (AI), few of papers have been used the Blockchain technology and only one study employed the Digital Signature.

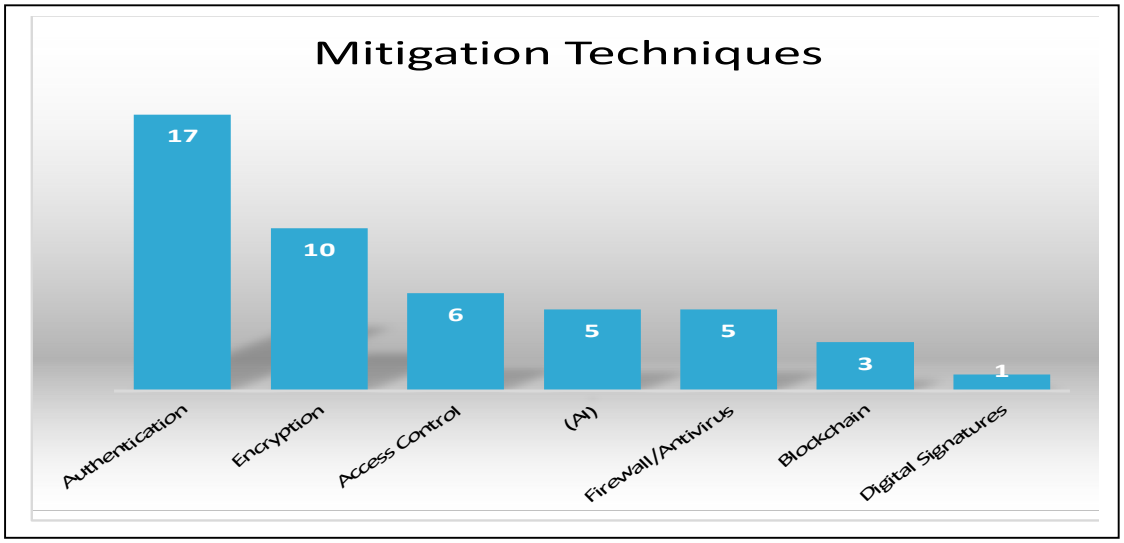

Figure 7: Findings of the most common types of Mitigation Technique for IOT threats and attacks.

Table 3: Reviewing the common types of Suggested Mitigation Technique for IOT threats and attacks.

Reference	Title	Type of Study	Suggested Mitigation
T. Thalawattha **et al.,** [1] **2021**	A Defence Against an Internet of Things (IoT) Attacks Based on Current Vulnerabilities	Qualitative	Remote safe configuration, Security patches, Two-Factor Authentication, Biometrics Authentication, Encryption, and Enhanced API security.
A. Assiri **et al.,** [2] **2018**	IoT Security and Privacy Issues	Qualitative	Encryption, Stenography, Access Control, and Authentication, Good protocols and software, the number of users and data must be considered when designing the applications.
M. Obaidat **et al.,** [3] **2020**	A Comprehensive and Systematic Survey on the Internet of Things: Security and Privacy Challenges, Security Frameworks, Enabling Technologies, Threats, Vulnerabilities and Countermeasures	Qualitative	Physical security, Zero-Knowledge, Risk Assessment, Security Aware Ad-hoc Routing (SAR), Pathing algorithms, TLS/SSL, Key Distribution, Cryptography and Encryption, Digital Signatures, Processing Protocols, Access Control, Patching, Intrusion and Threat Detection, Antivirus/Firewall, Blockchain, Honeypot Detection, Standardization, Traffic Filtering, Authentication, Trust Establishment, Location-based Data Security.
F. Azam **et al., [4] 2019**	Internet of Things (Iot), Security Issues and Its Solutions	Qualitative	Encryption, Identity-based authentication protocols, Data Analysis, Artificial intelligence (AI), Connect only to trusted networks.
N. Jhanjhi **et al.,** [5] **2020**	A Review on Security and Privacy Issues and Challenges in Internet of Things	Qualitative	pint-to-point or end-to-end encryption, Digital Signature, Symmetric, and Asymmetric Encryption, Encryption Algorithms, Risk assessment, Delayed disclosure of keys, tamper-poofing, hiding, Authentication, Encryption, Routing Algorithms, Firewall, Anti-virus, Intrusion Detection System (IDS), Rate-limiting, Authentication.
O. Abiodun **et al.,** [6] **2021**	A Review on the Security of the Internet of Things: Challenges and Solutions	Qualitative	Spam Prevention, Digital Signatures.

E. Ezema **et al.,** [7] **2018**	A Comprehensive Survey of Security Related Challenges in Internet of Things	Qualitative	OAuth, 2.0-basedoneM2M, afine-grained policymutually.
W. Zhou et al., [9] 2018	A Review on Security Challenges and Features in Wireless Sensor Networks: IoT Perspective	Qualitative	Physical Unclonable Functions (PUF), Intrusion Detection System (IDS) and Intrusion Prevention System (IPS), Encryption, Authentication, ARM TrustZone.
A. Bashir **et al.,** [10] **2019**	Internet of Things Security: Issues, Challenges and Counter-Measures	Qualitative	Trust Management, Adaptive Security and Trust Management solution (ASTM), Heterogeneity management, Trust-Based Access Control model (TBAC), Secure Mediation GateWay (SMGW), Authentication control, Identity Authentication and Capability Access Control (IACAC).
F. Ullah **et al.,** [11] **2019**	Cyber Security Threats Detection in Internet of Things Using Deep Learning Approach	Quantitative	Deep-Learning.
S. Pal et al., [12] 2021	Analysis of Security Issues and Countermeasures for the Industrial Internet of Things	Qualitative	Trust-management-based Routing Protocol, Context-aware, and secure multi-hop routing protocol, Intrusion detection system (IDS)-based security architecture, Privacy-preserving Data Mining (PPDM) techniques, Privacy-preserving authentication and data control, Devices must be checked and evaluated frequently. In addition, components should meet the NIST standard.
l. Moscho **et al.,** [13] **2018**	Securing the Internet of Things: Challenges, Threats and Solutions	Mixed	User authentication systems (password-based schemes, token-based schemes such as electronic keycards, smart cards, static or dynamic biometric such as fingerprints, retina, iris, facial characteristics, hand geometry, voice). physical access control mechanisms, (Access control mechanisms determine the access privileges of the authenticated users and objects) and a trust framework, firewall, DPS systems.
M. Essaaidi **et al., [14] 2022**	Systematic Literature Review of Internet of Things (IoT) Security	Qualitative	Blockchain, Authentication and key establishment protocol, Lightweight Identity-Based Encryption System, IoT-OAS Architecture.

J. Murillo **et al.,** [15] **2020**	Detection and Mitigation of DoS and DDoS Attacks in IoT-Based Stateful SDN: An Experimental Approach	Quantitative	Deep Packet Inspection (DPI).
B. Kim **et al.,** [16] **2018**	IoT Elements, Layered Architectures and Security Issues: A Comprehensive Survey	Quantitative	Authentication, Access Control Mechanisms such as (OpenHab Technology, IoTOne Technology), Cluster-based intrusion detection and prevention system, adaptive risk management, adaptive security monitoring, analytics, a predictive model, and adaptive security decision-making models.
L. Wu **et al.,** [17] **2017**	A Survey on Security and Privacy Issues in Internet-of-Things	Quantitative	Localized fault detection algorithm, Decentralized Intrusion Detection, End-to-End (E2E) secure communication, Authentication, Encryption, Standardized IPv6 mechanisms, Encapsulating Security Payload (ESP).
K. Li et al., [18] 2020	SNPL: One Scheme of Securing Nodes in IoT Perception Layer	Quantitative	Machine Learning Algorithms, Security Node in the Perception Layer (SNPL) Scheme.
H. Aslan **et al.,** [19] **2019**	A survey of IoT security threats and defenses	Qualitative	Clone Attacks: DCTD, BASE, DeClone and DeClone +, GREAT, DTD, Traffic Analysis Attack: Adaptive Link Padding, Dependent Link Padding, Honeypots, Honey-tokens, Decoy Documents, Decoy WiFi Traffic. Spoofing Attack: Received signal strength (RSS) mechanism and IDOL model, K-means cluster algorithm. Sinkhole Attack: INTI, SVELTE, VeRA. HELLO Flood Attack: A signal strength and time threshold based AODV-HFDP, Neighborhood based IDS, GIDS and NIDS. Blackhole Attacks: DPRAODV, Neighborhood-based and routing recovery, CUSUM, Hint based probabilistic approach. MITM attacks: Client-side bottleneck bandwidth analysis, A passive approach, radius authentication server.
			Sybil Attack: Detection based on network features, Detection Based on Cryptography, Detection Based on the Relationship Between Neighbors. RF Interference and Jamming: Signal strength, Carrier Sensing Time, Packet Delivery Ratio, Adaptive CCA, DynCCA. Malicious Code Injection - Antivirus software, update patches for operating systems, security policy and Security updates, Control flow, Protective Software, Verify software integrity, Side-channel analysis. Denial of Service

			Attacks: Flow rate statistics, User browsing behaviors analysis, Cluster analysis. Software Vulnerabilities Attacks: Fuzzing, Scanners of Web Application, Static Analysis Techniques, Brick, CRED. Buffer Overflow: Static analysis technique, Dynamic analysis, Hybrid analysis. XSS attacks: Skip list, Hybrid Program Analysis, xHunter, Penetration Testing and Fault Injection, Secure Web Application Proxy. Privacy Leak Attacks: Strong Passwords, Access Control, Re-authentication Mechanism.
M. Tabari **et al.,** [20] **2020**	Detecting Sinkhole Attack in RPL-based Internet of Things Routing Protocol	Quantitative	Distributed Intrusion Detection System (IDS) in the RPL-based IoT networks
Z. Dvorak **et al.,** [21] **2017**	Internet of Things and The Man-in-the-Middle Attacks - Security and Economic Risks	Qualitative	Update the operating system patches regularly, Firewall, SSL certificates, and strong encryption, IDS, DNSSEC, being cognizant and keeping an eye out for things that seem unusual, HTTPS.
W. Abbass **et al.,** [22] **2019**	Assessing the Internet of Things Security Risks	Quantitative	Logstash, Elasticsearch, Kibana.
M. Calore **et al.,** [23] **2019**	IoT: Internet of Threats? A Survey of Practical Security Vulnerabilities in Real IoT Devices	Quantitative	Authentication, 6LoWPAN and LoRaWAN, CryptoCoP.
S. Rekha **et al.,** [24] **2021**	Study of security issues and solutions in Internet of Things (IoT)	Qualitative	Authentication, Encryption.
K. Sha **el al.,** [25] **2018**	On security challenges and open issues in Internet of Things	Qualitative	Authentication, Intrusion Detection Algorithms, 6LoWPAN Protocol, Frame Counter, DTLS based End-to-End security architecture.
C. Hu **et al., [27] 2017**	Fog Computing for the Internet of Things: Security and Privacy Issues	Quantitative	Fog Computing.
A. Djenna **et al.,** [29] **2021**	Internet of Things Meet Internet of Threats: New Concern Cyber Security Issues of	Qualitative	Strong Authentication, Self-healing Mechanism, Firewall, Adoption of a defense-in-depth strategy, Artificial Intelligence, Machine Learning and Deep Learning, Resilience, Penetration Testing.

	Critical Cyber Infrastructure		
J. Lin **et al.,** [30] **2017**	A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications	Qualitative	
H. Lakhlef **et al.,** [31] **2018**	Internet of things security: A top-down survey	Qualitative	Encryption, Artificial Intelligence (AI), IP Traceback, Access Control Mechanism.
V. Rangan **et al.,** [32] **2020**	IoT cyber risk: a holistic analysis of cyber risk assessment frameworks, risk vectors, and risk ranking process	Quantitative	Authentication, Access Control, Trust Management Techniques, Encryption.
M. Khana **et al.,** [33] **2017**	IoT Security: Review, Blockchain Solutions, and Open Challenges	Qualitative	Blockchain technology
G. Verma et al., [34] 2021	Emerging Security Threats, Countermeasures, Issues and Future Aspects on Internet of Things (IoT): A Systematic Literature Review	Qualitative	Authentication techniques
S. Tandon **et al.,** [35]	A study on Internet of Things (IOT) security issues and solutions	Qualitative	Improved layered architecture of IoT, Encryption and Hashed Based Security, Third party security services such as (OpenHab, NOZOMI networks, Zingbox).

6. CONCLUSION AND FUTURE WORK

This study aimed to conduct a systematic review on the common types of cybersecurity threats and attacks on IoT and to review the suitable mitigation techniques for IOT threats and attacks. To achieve that, a systematic review has been conducted on 35 recent paper which have published in top ranking journal like IEEE, Elsevier and Springer. Based on our findings, which indicated that Jamming attack is the most common threats on the perception layer or sensors layer, and DoS/DDoS attacks are the most common method at the Network and Application layer. In addition, the results revealed that the most

suitable mitigation technique for addressing the IOT attacks is the authentication technique. In addition, some of studies have been employed the AI methods to reduce IoT threats to reduce risks that cannot be addressed with traditional mitigation techniques. Finally, few of IOT studies used the blockchain technology for mitigating the cybersecurity threats and attacks in IOT environment. Therefore, this paper recommends future studies to conduct more research with the focus on blockchain mechanisms.

FUNDING: This work was funded by King Faisal University, Saudi Arabia [Project No. GRANT592].

ACKNOWLEDGMENTS: This work was supported through the Annual Funding track by the Deanship of Scientific Research, Vice Presidency for Graduate Studies and Scientific Research, King Faisal University, Saudi Arabia [Project No. GRANT592].

CONFLICTS OF INTEREST: All authors declare no conflict of interest.

REFERENCES:

[1] T. Thalawattha, P. Rodrigo, D. Dissanayake, K. Jayasinghe and R. Kathriarachchi, “A Defense Against an Internet of Things (IoT) Attacks Based on Current Vulnerabilities”, International Conference on Advancement of Development Administration 2020 (Thailand), 2021.

[2] A. Assiri and H. Almagwashi, “IoT Security and Privacy Issues”, International Conference on Computer Applications and Information Security (ICCAIS), 2018.

[3] M. Obaidat, J. Brown, S. Obeidat, J. Holst, and A. Hayajneh, “A Comprehensive and Systematic Survey on the Internet of Things: Security and Privacy Challenges, Security Frameworks, Enabling Technologies, Threats, Vulnerabilities and Countermeasures”, Computer, 2020.

[4] F. Azam, R. Munir, M. Ahmed, M. Ayub, A, Sajid, and Z. Abbasi, "Internet of Things (IoT), Security Issues And Its Solutions", Science Heritage Journal, 2019.

[5] D. Alferidah and N. Jhanjhi, "A Review on Security and Privacy Issues and Challenges in Internet of Things", IJCSNS International Journal of Computer Science and Network Security, 2020.

[6] O. Abiodun, E. Abiodun, M. Alawida1, R. Alkhawaldeh, and H. Arshad, "A Review on the Security of the Internet of Things: Challenges and Solutions", Springer, 2021.

[7] E. Ezema, A. Abdullah, and N. Sani, "A Comprehensive Survey of Security Related Challenges in Internet of Things", International Journal of New Computer Architectures and their Applications (IJNCAA), 2018.

[8] M. Burhanuddin, A. Mohammed, R. Ismail, M. Hameed, A. Kareem, and H. Basiron, "A Review on Security Challenges and Features in Wireless Sensor Networks: IoT Perspective", Journal of Telecommunication, Electronic and Computer Engineering (JTEC), 2018.

[9] W. Zhou, Y. Zhang, and Peng Liu, "The Effect of IoT New Features on Security and Privacy: New Threats, Existing Solutions, and Challenges Yet to Be Solved", IEEE Internet of Things Journal, 2018.

[10] A. Bashir, S. Sholla, and A. Nazir, "Internet of Things Security: Issues, Challenges and Counter-Measures", International Journal of Computing and Network Technology, 2019.

[11] F. Ullah, H. Naeem, S. Jabbar, S. Khalid, M. Latif, F. Al-Turjman, AND L. Mostarda, "Cyber Security Threats Detection in Internet of Things Using Deep Learning Approach", IEEE Access, 2019.

[12] S. Pal and Z. Jadidi, "Analysis of Security Issues and Countermeasures for the Industrial Internet of Things", Applied Sciences, 2021.

[13] P. Grammatikis, P. Sarigiannidis, and l. Moscholios, "Securing the Internet of Things: Challenges, Threats and Solutions", Internet of Things, 2018.

[14] A. bekkali, M. Essaaidi, M. Boulmalf, and D. majdoubi "Systematic Literature Review of Internet of Things (IoT) Security", Advances in Dynamical Systems and Applications (ADSA), 2022.

[15] J. Murillo, J. Brajones, J. Valdés, and F. Valero, "Detection and Mitigation of DoS and DDoS Attacks in IoT-Based Stateful SDN: An Experimental Approach", Sensors, 2020.

[16] B. Kim, B. Khan, M. Burhan, and R. Rehman, "IoT Elements, Layered Architectures and Security Issues: A Comprehensive Survey", Sensors, 2018.

[17] L. Wu, Y. Yang, G. Yin, L. Li, and H. Zhao, "A Survey on Security and Privacy Issues in Internet-of-Things", IEEE Internet of Things Journal, 2017.

[18] K. Li, Y. Fan, G. Zhao, B. Zhang, G. Tan, X. Sun, and F. Xia, "SNPL: One Scheme of

Securing Nodes in IoT Perception Layer", Sensors, 2020.

[19] H. Aslan, A. Nasr, S. Abdel-Mageid, and H. Ahmed, "A survey of IoT security threats and defenses", International Journal of Advanced Computer Research, 2019.

[20] M. Tabari and Z. Mataji, "Detecting Sinkhole Attack in RPL-based Internet of Things Routing Protocol", Journal of AI and Data Mining, 2020.

[21] Z. Dvorak, Z. Cekerevac, L. Prigoda, and P. Cekerevac, "Internet of Things and The Man-in-the-Middle Attacks - Security and Economic Risks", MEST Journal, 2017.

[22] W. Abbass, Z. Bakraouy, A. Baina, and M. Bellafkih, "Assessing the Internet of Things Security Risks", Journal of Communications, 2019.

[23] M. Calore, F. Meneghello, D. Zucchetto, M. Polese, A. Zanella, "IoT: Internet of Threats? A Survey of Practical Security Vulnerabilities in Real IoT Devices", IEEE Internet of Things Journal, 2019.

[24] S. Rekha, L. Thirupathi, S. Renikunta, R. Gangula, "Study of security issues and solutions in Internet of Things (IoT)", Materials Today: Proceedings, 2021.

[25] K. Sha, W. Wei, T. Yang, Z. Wang, W. Shi, "On security challenges and open issues in Internet of Things", Future Generation Computer Systems, 2018.

[26] A. Ali, F. Köylü, M. Hassan, M. Sabriye, A. Osman, A. Hilal, Q. Abdullah, "Review of Internet Things (IoT) of Security Threats and Challenges", International Conference on Emerging Smart Technologies and Applications (eSmarTA), 2021.

[27] C. Hu, Xiuzhen Cheng, A. Alrawais, and A. Alhothaily, "Fog Computing for the Internet of Things: Security and Privacy Issues", IEEE Internet Computing, 2017.

[28] K. Skouby, R. Tadayoni, and S. Koduah, "Cyber Security Threats to IoT Applications and Service Domains", Wireless Personal Communications, Springer, 2017.

[29] A. Djenna, S. Harous, and D. Saidouni, "Internet of Things Meet Internet of Threats: New Concern Cyber Security Issues of Critical Cyber Infrastructure", Applied Sciences, 2021.

[30] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, "A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications", IEEE Internet of Things Journal, 2017.

[31] H. Lakhlef, A. Bouabdallah, and D. Kouicem, "Internet of things security: A top-down survey", Computer Networks, 2018.

[32] V. Rangan, S. Srinivas, K. Kandasamy, K. Achuthan, "IoT cyber risk: a holistic analysis of cyber risk assessment frameworks, risk vectors, and risk ranking process", EURASIP Journal on Information Security, Springer, 2020.

[33] M. Khana and K. Salah "IoT Security: Review, Blockchain Solutions, and Open Challenges", Future Generation Computer Systems, 2017.

[34] G. Verma, and S. Prakash, "Emerging Security Threats, Countermeasures, Issues and Future Aspects on Internet of Things (IoT): A Systematic Literature Review", Advances in Interdisciplinary Engineering, 2021.

[35] P. Parashar and S. Tandon, "A study on Internet of Things (IOT) security issues and solutions", ResearchGate, 2020.

[36] J. Lewis "Managing Risk for the Internet of Things," CSIS, 2016.

[37] S. Sicari, A. Rizzardi, D. Miorandi, and A. Porisini, "A Risk Assessment Methodology for the Internet of Things", Computer Communications, 2018.

[38] Hany F. Atlam, Ahmed Alenezi, Robert J. Walters, and Gary B. Wills, "An Overview of Risk Estimation Techniques in Risk-based Access Control for the Internet of Things", In Proceedings of the 2nd International Conference on Internet of Things, Big Data and Security, 2017.

[39] Alamer, Maryam, and Mohammed Amin Almaiah. "Cybersecurity in Smart City: A systematic mapping study." 2021 International Conference on Information Technology (ICIT). IEEE, 2021.

[40] Al Nafea, Roaa, and Mohammed Amin Almaiah. "Cyber security threats in cloud: Literature review." 2021 International Conference on Information Technology (ICIT). IEEE, 2021.

[41] Bubukayr, Maryam Abdulaziz Saad, and Mohammed Amin Almaiah. "Cybersecurity concerns in smart-phones and applications: A survey." 2021 International Conference on Information Technology (ICIT). IEEE, 2021.

[42] Almaiah, Mohammed Amin, and Ahmad Al-Khasawneh. "Investigating the main determinants of mobile cloud computing adoption in university campus." Education and

Information Technologies 25.4 (2020): 3087-3107.

[43] Almaiah, Mohammed Amin, et al. "Classification of cyber security threats on mobile devices and applications." Artificial Intelligence and Blockchain for Future Cybersecurity Applications. Springer, Cham, 2021. 107-123.

[44] Adil, Muhammad, et al. "An anonymous channel categorization scheme of edge nodes to detect jamming attacks in wireless sensor networks." Sensors 20.8 (2020): 2311.

45]] Adil, Muhammad, et al. "MAC-AODV based mutual authentication scheme for constraint oriented networks." IEEE Access 8 (2020): 44459-44469.

[46] Almaiah, Mohammed Amin. "A new scheme for detecting malicious attacks in wireless sensor networks based on blockchain technology." Artificial Intelligence and Blockchain for Future Cybersecurity Applications. Springer, Cham, 2021. 217-234.

[47] Adil, Muhammad, et al. "An efficient load balancing scheme of energy gauge nodes to maximize the lifespan of constraint oriented networks." IEEE Access 8 (2020): 148510-148527.

[48] Adil, Muhammad, et al. "An energy proficient load balancing routing scheme for wireless sensor networks to maximize their lifespan in an operational environment." IEEE Access 8 (2020): 163209-163224.

[49] Khan, Muhammad Nawaz, et al. "Improving energy efficiency with content-based adaptive and dynamic scheduling in wireless sensor networks." IEEE Access 8 (2020): 176495-176520.

[50] Qasem, Mais Haj, et al. "Multi-agent system combined with distributed data mining for mutual collaboration classification." IEEE Access 9 (2021): 70531-70547.

[51] Almaiah, Mohammed Amin, et al. "A new hybrid text encryption approach over mobile ad hoc network." Int. J. Electr. Comput. Eng.(IJECE) 10.6 (2020): 6461-6471.

[52] Al Hwaitat, Ahmad K., et al. "Improved security particle swarm optimization (PSO) algorithm to detect radio jamming attacks in mobile networks." Quintana 11.4 (2020): 614-624.

[53] Almaiah, Mohammed Amin, et al. "A Lightweight Hybrid Deep Learning Privacy Preserving Model for FC-Based Industrial Internet of Medical Things." Sensors 22.6 (2022): 2112.

[54] Almaiah, Mohammed Amin, et al. "A Novel Hybrid Trustworthy Decentralized Authentication and Data Preservation Model for Digital Healthcare IoT Based CPS." Sensors 22.4 (2022): 1448.

[55] Almudaires, Fajer, and Mohammed Almaiah. "Data an overview of cybersecurity threats on credit card companies and credit card risk mitigation." 2021 International Conference on Information Technology (ICIT). IEEE, 2021.

[56] Siam, Ali I., et al. "Secure Health Monitoring Communication Systems Based on IoT and Cloud Computing for Medical Emergency Applications." Computational Intelligence and Neuroscience 2021 (2021).

[57] AlMedires, Motaz, and Mohammed AlMaiah. "Cybersecurity in Industrial Control System (ICS)." 2021 International Conference on Information Technology (ICIT). IEEE, 2021.

[58] Almomani, Omar, et al. "Machine Learning Classifiers for Network Intrusion Detection System: Comparative Study." 2021 International Conference on Information Technology (ICIT). IEEE, 2021.

[59] Ali, Aitizaz, et al. "An Industrial IoT-Based Blockchain-Enabled Secure Searchable Encryption Approach for Healthcare Systems Using Neural Network." Sensors 22.2 (2022): 572.

[60] Khan, Zard Ali, et al. "A Neighborhood and Machine Learning-Enabled Information Fusion Approach for the WSNs and Internet of Medical Things." Computational Intelligence and Neuroscience 2022 (2022).

[61] Almaiah, Amin, and Omar Almomani. "An investigation of digital forensics for shamoon attack behaviour in FOG computing and threat intelligence for incident response." Journal of Theoretical and Applied Information Technology 98.07 (2020).

[62] Qasem, Mais Haj, et al. "Multi-agent Systems for Distributed Data Mining Techniques: An Overview." Big Data Intelligence for Smart Applications (2022): 57-92.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[63] Ali, Aitizaz, et al. "Big Data Based Smart Blockchain for Information Retrieval in Privacy-Preserving Healthcare System." Big Data Intelligence for Smart Applications: 279.

[64] Almaiah, Mohammed Amin, and Mohammed Al-Zahrani. "Multilayer neural network based on MIMO and channel estimation for impulsive noise environment in mobile wireless networks." Int. J. Adv. Trends Comput. Sci. Eng 9.1 (2020): 315-321.