electronics

MDPI

Review

Cybersecurity Risk Analysis in the IoT: A Systematic Review

Thanaa Saad AlSalem [1], Mohammed Amin Almaiah [2,3] and Abdalwali Lutfi [4,5,*]

[1] Department of Information Systems, King Faisal University, Al-Ahsa 31982, Saudi Arabia
[2] Department of Computer Science, Aqaba University of Technology, Aqaba 11947, Jordan; malmaiah@kfu.edu.sa
[3] King Abdullah the II IT School, The University of Jordan, Amman 11942, Jordan
[4] School of Business, King Faisal University, Al-Ahsa 31982, Saudi Arabia
[5] Applied Science Research Center, Applied Science Private University, Amman 11931, Jordan
* Correspondence: aalkhassawneh@kfu.edu.sa

Abstract: The Internet of Things (IoT) is increasingly becoming a part of our daily lives, raising significant concerns about future cybersecurity risks and the need for reliable solutions. This study conducts a comprehensive systematic literature review to examine the various challenges and attacks threatening IoT cybersecurity, as well as the proposed frameworks and solutions. Furthermore, it explores emerging trends and identifies existing gaps in this domain. The study's novelty lies in its extensive exploration of machine learning techniques for detecting and countering IoT threats. It also contributes by highlighting research gaps in economic impact assessment and industrial IoT security. The systematic review analyzes 40 articles, providing valuable insights and guiding future research directions. Results show that privacy issues and cybercrimes are the primary concerns in IoT security, and artificial intelligence holds promise for future cybersecurity. However, some attacks remain inadequately addressed by existing solutions, such as confidentiality, security authentication, and data server connection attacks, necessitating further research and real-life testing of proposed remedies.

Keywords: Internet of Things (IoT); cybersecurity; cybersecurity frameworks; cybersecurity approaches

Citation: AlSalem, T.S.; Almaiah, M.A.; Lutfi, A. Cybersecurity Risk Analysis in the IoT: A Systematic Review. *Electronics* **2023**, *12*, 3958. https://doi.org/10.3390/electronics12183958

Academic Editor: Seokjoo Shin

Received: 16 July 2023
Revised: 8 September 2023
Accepted: 16 September 2023
Published: 20 September 2023

1. Introduction

The Internet of Things (IoT) has permeated numerous sensitive disciplines, including the health sector and the economic sector. However, the IoT is emerging at home, in large cities, and in other, different domains of life, which are not of less importance. In addition, the IoT provides connections to intelligent objects, applications, and cloud computing; 50 billion IoT devices were connected to the internet in 2020 [1]. This huge source of data, as well as the future trend of artificial intelligence, which the world has come to rely on, has put pressure on vendors and designers of IoT devices to secure this technology in order to enable it to meet upcoming demands. However, trusting a device starts with ensuring its security, which has become a necessity, especially when these devices are connected to the internet, exposing them to many threats and cyberattacks [2]. The security threats include cybercrimes, software piracy, and malware attacks [1], as well as various damaging attacks. However, this continuous field of improvement cannot adopt existing approaches to provide security. New risks keep on arising, which requires updates to new frameworks and solutions in parallel with updating IoT disciplines [3]. Furthermore, an updated review of the applied techniques and approaches is recommended regularly. For this reason, the proposed study reviews recent progress in the literature regarding cybersecurity risk analysis for the IoT. It also identifies various cybersecurity frameworks and approaches proposed for IoT cybersecurity risk analysis by identifying the various types of attacks and challenges facing IoT devices. In addition, it highlights the most important techniques that have been used in detecting IoT risks, identifying the new trends in IoT cybersecurity, and identifying the gap found in the literature to recommend possible solutions.

The key novelty of this study lies in its focused exploration of machine learning techniques in the context of IoT security. We delve into specific algorithms and methodologies, shedding light on their practical implementation and efficacy. Additionally, we identify critical research gaps in the assessment of economic impacts resulting from IoT cybersecurity incidents, and the need for tailored security solutions in the industrial IoT domain.

A. Motivation

As the world is witnessing a turning point towards a new era of virtual reality, there will be no limits to the IoT in the future. The IoT is a rapidly growing sector and is considered a revolution in technology and artificial intelligence, wherein the usage of IoT devices is increasing exponentially [4]. Concerns about the privacy and cybersecurity challenges of the IoT are the most prioritized issues for risk management professionals. The IoT will change the world soon, but security concerns will still be arising. However, if security issues and challenges, for example, privacy and authentication, in addition to other challenges like confidentiality, are treated properly, then everything will change with the IoT [5]. Huge amounts of daily data produced from dealing with the IoT are transmitted with high susceptibility to risks and threat attacks, which require a profound strategy of risk management for the IoT with a focus on cybersecurity issues.

The motivation behind this research stems from the urgency of addressing the escalating cybersecurity concerns surrounding IoT systems. With cyberattacks becoming more pervasive and evolving in complexity, it is imperative to thoroughly examine the various types of threats affecting IoT devices and systems. By delving into the existing literature and gaining insights from previous studies, we aim to provide a comprehensive understanding of the landscape of IoT cybersecurity, including the types of attacks and challenges that have emerged.

This investigation seeks to serve as a reference point for researchers, policymakers, and industry practitioners in their efforts to bolster IoT security. By analyzing the proposed frameworks, approaches, and detection techniques put forth in the literature, we aspire to identify potential avenues for enhancing the protection of IoT ecosystems. Moreover, the review will shed light on any existing gaps in the research, offering directions for future investigations and innovations in the field of IoT cybersecurity.

Our primary objective is to consolidate and present a well-structured literature review that not only highlights the prevalent attacks and challenges but also provides valuable insights into the proposed solutions and their effectiveness. With a specific focus on identifying the most vulnerable aspects of IoT security, we aim to offer a comprehensive analysis that contributes to the growing body of knowledge concerning IoT cybersecurity.

By emphasizing the significance of IoT security and the criticality of mitigating potential threats, this study endeavors to raise awareness of the importance of robust cybersecurity measures for IoT devices and systems. Ultimately, we aspire to foster a more secure and resilient IoT environment that can continue to evolve and thrive in the face of emerging cyber risks.

B. Problem Statement

The IoT is extremely exposed to risks and threats due to its highly connective nature, the ongoing development in this discipline, and the rising global demand for it in the future. New risks and vulnerability issues are presented [2], which require updated reviews of the existing risk assessment and analysis frameworks and approaches. In addition, the nature of the IoT, such as the way in which it is connected to many systems and dealing with huge amounts of data, has increased the likelihood of exposure to attackers. What is more, concerns regarding the cybersecurity of the IoT are not limited to vendors. However, consumers require trustworthy technology [6]. There is an insistent demand for the ultimate solutions for securing this growing technology [7]. On the other hand, the variety of recommended and proposed approaches and solutions offered by the recent studies regarding the cybersecurity of the IoT has raised the following questions. What are

the most important techniques that have been used in detecting IoT risks? What are the new trends in IoT cybersecurity? What are the attacks that the IoT is vulnerable to?

C. Scope

The scope of the current study focuses on the frameworks and approaches that have been proposed recently by professionals and scholars for the risk assessment and analysis processes for the cybersecurity of the IoT. To collect the data for the literature review, the study focused on the usage of the following keywords: IoT, cybersecurity, cybersecurity frameworks, and cybersecurity approaches.

D. Expected Outcomes

Cybersecurity in the IoT has caught the attention of many scholars; numerous articles have been published, especially in the last five years. Several solutions and frameworks were proposed by previous studies, tackling the most threatening cyberattacks. In addition, an updated review of the cybersecurity of the IoT is essential, as this field is rapidly evolving and spreading. The proposed paper makes a significant contribution to summarizing the state-of-the-art studies and identifying the progress of research in this field. The aim of this research is achieved by meeting the following objectives:

- Identify various cybersecurity frameworks and approaches proposed for IoT cybersecurity risk analysis.
- Identify the various types of attacks and challenges facing IoT devices.
- Highlight the most important techniques that have been used in IoT risk detection.
- Identify the new trends in IoT cybersecurity.
- Identify the gap found in the literature review and recommend expected solutions.

2. Methodology

This section presents the research methodology that is followed in this study; it represents a sequence of steps, starting with the eligibility criteria of the research article selection, and then addressing the information sources, search strategy, and selection process. Moreover, data analysis and synthesis are discussed in this section.

The review process followed the steps of systematic literature review as outlined in the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) guidelines [8].

2.1. Eligibility Criterion

The current review research selected previous studies according to an eligibility criterion, based on research articles that have discussed the cybersecurity of the IoT, research that has addressed the challenges facing IoT cybersecurity, and studies that have proposed frameworks and new approaches in an attempt to resolve cybersecurity issues. Furthermore, previous review papers that have addressed the risk assessment of IoT cybersecurity were included.

2.2. Information Sources

The author depended on reliable databases, such as Science Direct and IEEE, in addition to papers and articles that have been published in a high-impact-factor international journal.

2.3. Search Strategy and Selection Process

The authors used the following keywords (IoT, cybersecurity, cybersecurity frameworks, cybersecurity approaches) in trusted research engines (Google Scholar, Academia, Science Direct, and IEEE). The research articles fitting the inclusion criterion were then filtered according to the year of publication, which was mainly between 2015 and 2023, focusing on the studies between 2018 and 2023. Another filtering process was undertaken according to the area of research, so that research that offered no contribution towards

tackling the current research questions was discarded. The selected studies were also filtered according to their discussion and depth of analysis, as well as according to their development in the research area. Finally, the authors chose 40 articles that had a systematic review process as shown in Figure 1.

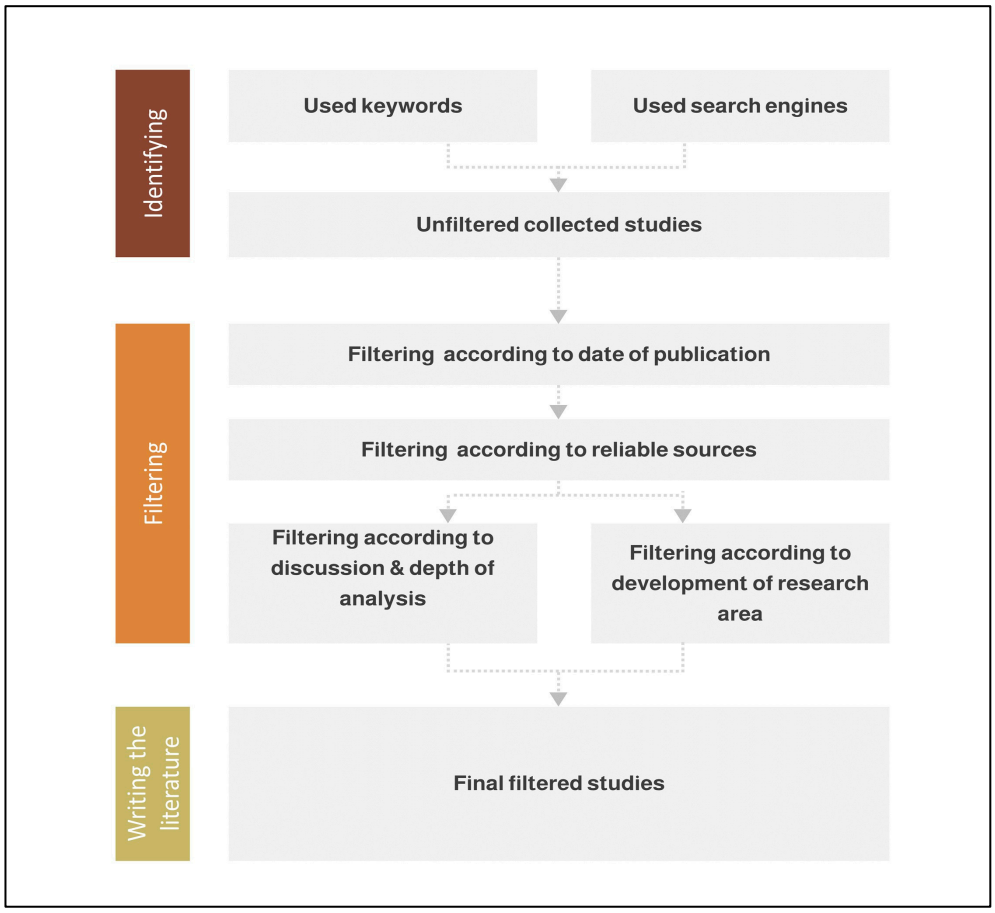

Figure 1. Search strategy framework.

2.4. Data Analysis and Synthesis

Each study of the 40 selected was classified according to its type: empirical study, practical study, survey study, review paper, and so on. Moreover, the objectives and problems discussed were highlighted, and major results and recommendations were extracted. Then, the author used a table to represent the threats and challenges, the impact of these attacks, proposed frameworks and approaches, and the salient detection techniques.

2.5. Findings

The findings included a summary of the knowledge gained from all the reviewed studies. Different types of attacks and challenges were also discussed. In addition, the authors figured out a research gap that had not been included in the previous studies. Finally, the new trends in IoT cybersecurity were extracted from the literature and summarized in the findings.

3. Literature Review

This section presents previous studies that addressed the topic of IoT cybersecurity, providing a critical analysis of the most noteworthy studies done by scholars and focusing on those published in the last decade.

3.1. IoT Risk Assessment

Study [1] discussed the importance of giving attention to the two main threats attacking IoT with serious economic damages; these two threats are software piracy and malware attacks. This study was an empirical one in which the methodology being used was based on experiments conducted to check the proposed solution. However, the study aimed to introduce a new solution approach in which pirated software and malware-infected files across the IoT network were discovered. Moreover, the results of the experimentation showed that the proposed novel solution approach works better than the previous approaches regarding the cybersecurity of the IoT.

Study [2] discussed the deeper everyday involvement of the IoT in our daily lives and how this technology is exposed to numerous risks according to its nature. This empirical study used the EBIOS methodology in order to conduct a risk analysis process for the identification of vulnerabilities in IoT architecture. Its main aim was the identification of the top significant security risk to an IoT application that a developer should take into consideration, and then work on securing it. Its key results showed that the most vulnerable parts of the IoT process are sensors, smart switches, and small actuators in specific contexts.

Study [3] discussed IoT risk assessment concepts. The main aim of this paper was to identify the reason behind the inadequacy of current risk assessment approaches for the IoT. Its results showed that the main reasons for the inadequacy of current risk assessment approaches for the IoT are as follows:

- Shortcomings in periodic assessment.
- Changing system boundaries, yet limited systems knowledge.
- The challenge of understanding the glue.
- Failure to consider assets as an attack platform.

Moreover, automated and constant risk assessment approaches were required, in addition to developing new backup tools that help simulate and model predictive powers.

3.2. Attacks and Challenges

Study [5] was a survey research paper that discussed the challenges and the ongoing situation of the IoT. The main goal of the research paper was to offer an introduction to the security standards and challenging issues, as well as IoT security forthcoming trends. The authors used a methodology that was mainly based on reviewing the related literature. Its results showed that recent studies of the IoT addressed authentication access and control protocols.

Study [9] addressed cybersecurity threats to healthcare services, particularly hospitals and clinics utilizing IoT technology. It introduced an adaptive cybersecurity framework designed for dynamic adaptation to cyber threats. The research focused on leading adaptive security measures that anticipate and respond to adaptive attacks targeting healthcare services and infrastructures. The results demonstrated that the framework effectively provided the best possible defense response against dynamic and adaptive attacks.

Study [10] emphasized the significance of cyber risk in IoT systems and sought to identify risks within the IoT while defining relevant risk assessment techniques. It presented an analysis of existing cyber risk evaluation approaches through a review of related literature. As a foundational study in the field, it provided essential definitions in the context of IoT cybersecurity. The main outcomes included an overview of studies on IoT cyber risk quantification, and strategies for mitigating and transferring cyber risks.

Study [11] discussed the privacy issues facing the IoT and how computational intelligence (CI) can be part of cybersecurity. The study aimed to explore the relevance of using CI technologies for solving IoT cybersecurity issues. This survey research paper collected secondary data from a review of the related literature. The main contribution of this paper was in highlighting the challenges facing the CI technologies involved in the cybersecurity of the IoT.

Study [12] addressed the pressing need for novel solutions to combat cybercrimes impacting IoT systems globally. The authors offered their insights and solutions concerning

cybercrimes. Its primary contribution lay in providing a comprehensive summary of diverse cybersecurity challenges in IoT, benefiting researchers and professionals interested in IoT systems. The challenges are categorized based on IoT security features, and the study proposes blockchain as an ideal solution, offering integrity, authentication, and encryption.

Study [13] discussed the various concerns related to IoT devices, mainly the robbery of data and data violation forms. This review article aimed to identify IoT security challenges and requirements as well as various solutions proposed. The main results showed that the security of the IoT is affected by the cybersecurity solution's cost, data volume, and data sensitivity.

Study [14] discussed the IoT's background and security. The study also discussed the potential cybersecurity attacks on the IoT and the available solutions. In addition, the study aimed to introduce a novel solution composed of three layers: lower, IoT; middle, edge; and top, cloud. The study was empirical and the solution proposed took place as an assessing process. The main results showed that the introduced solution model can cut out certain potential vulnerabilities.

Study [15] aimed to provide a taxonomy of the types of threats affecting IoT devices and systems, and an analysis of attacks and intruders. The results showed that issues like confidentiality, privacy, and organization trust were of the highest priority regarding IoT cybersecurity. Furthermore, the paper contributed to opening the way for future research in digging further into the consequences of the mentioned threats.

3.3. Detection Techniques

Study [16] discussed the issue of stealing the information of users, as IoT technology, according to the authors, is highly vulnerable to such issues. The purpose of the research article was to upgrade the advancement of IoT studies by focusing on various types of IoT security issues, as well as to identify the available solutions. The study discussed the presence of physical, network, application, Zigbee, and Z-wave attacks. The major results showed that authentication, secure communication solutions, and application security are the existing solutions nowadays. However, the authors recommended a digital signature as the ultimate solution, due to the nature of IoT devices.

Study [17] discussed IoT users' lack of awareness of its risks, especially regarding information loss and violation. The article was a review paper, in which authors relied on previously published studies to extract the needed information. The study was limited to devices unsupported by their manufacturers. The findings presented 12 different attacks, including low-grade attacks, average-level attacks, great attacks, and high-intensity attacks. In addition, it showed that the lack of appropriate security has led to a great concern that any attacker with good expertise can benefit from the weaknesses in ecosystems.

- CI-enabled cybersecurity architecture.
- CI algorithms and tools.
- CI-enabled data mining in cybersecurity.
- Cognitive security with IoT devices.
- Efficient CI algorithms in cybersecurity.
- CI-enabled malware detection and classification.
- General data protection regulation vs. CI.

At the end of the research, the authors offered new trends in facing these challenges, that is, using privacy-preserving data techniques and having a 5G IoT environment, in addition to CI cyber defenses.

Study [18] discussed the importance of the flexibility of the techniques used in the cybersecurity of the IoT. For this reason, the study aimed to introduce a technique for risk detection, which combines the fuzzy inference system with the validation of experts, which allows for the evaluation of security risks of IoT systems. The authors used interviews as the data collection tool from experts. The research article was empirical and the proposed techniques were subjected to simulation and evaluation via scenarios. The results showed that the recommended technique was more accurate than the existing fuzzy techniques.

Study [19] discussed the importance of using machine learning in the process of securing the IoT. The study's main aim was to identify the advantages of machine learning technology in solving cybersecurity issues. The study was a review paper, and the authors' methodology was to review the related literature in order to fulfill the research objective. The findings of the research paper showed that Random Forest and K-Nearest Neighbor (KNN) algorithms provided the most precise attack detection in the proposed solutions. Moreover, Software Defined Networks (SDN) and the fog layer of networks resulted in many efficient solutions.

3.4. Proposed Solutions

Study [20] conducted a systematic review to investigate cybersecurity incident response in IoT ecosystems within smart city applications. The study aimed to advance the cybersecurity assessment model for IoT solutions in smart cities. It highlighted the increasing reliance of smart cities on IoT, raising concerns about their vulnerability to cyberattacks. The proposed model supports cybersecurity development in smart cities and suggests the incorporation of additional techniques to enhance its effectiveness.

Study [21] discussed the need for IoT devices to be trusted by consumers, especially when it comes to cybersecurity issues. The main aim of the paper was to introduce a cybersecurity solutions assessment approach based on taking advantage of virtual environments and agent-based simulation. This research article was a practical one, based on realistic scenarios. Its results showed that the efficacy of the recommended approach was manifested by a case study of a smart home model setting that was evaluated by the 'SmallWorld' platform.

Study [22] discussed building trusted healthcare services based on IoT, complying with international regulations. This practical study can be considered a case study whose methodology was based on developing a case-oriented cybersecurity assessment, ASAC: Advanced Security Assurance Case. Moreover, the hierarchical cybersecurity model for healthcare IoT systems was developed. The main goal of this article was to build and develop an authentic IoT architecture for healthcare systems. The major result was a detailed model showing how each layer is being secured while obtaining verifiable, traceable, justifiable results for both parties involved.

Study [23] addressed the security concerns attending the integration of industrial control systems into the IoT domain. The empirical study aimed to introduce a novel model for authenticating the security of distributed control systems during their initial design phases. Through experimental scenarios, the model's effectiveness was demonstrated in identifying and mitigating potential cyber threats. The study's main contributions lay in the mechanization of an alloy analyzer and the development of a large-scale IoT assessment framework, enhancing the security of distributed control systems at the early stages of their design.

Study [24] is a review paper. It discussed the mobile computing technique used for the cybersecurity of the IoT. The main aim of the research paper was to provide a holistic analysis of major issues with and the complexities of the cybersecurity of IoT devices in light of mobile computing. The major results of the paper showed the following:

- Devices based on the IoT showed vulnerability related to various attacks.
- A robust security mechanism is recommended to improve cybersecurity for the IoT.
- The suggested mechanism would preferably be based on mobile computing, which covers the software and hardware security.
- New trends in this discipline indicate the importance of mobile computing in cybersecurity, which will be the focus of researchers.

Study [25] discussed the current deficiency of a standardized methodology for aligning the impact and likelihood of cyberattacks in specific IoT-associated disciplines. The study's main aim was to provide improved knowledge of economic impact assessment models for I4.0 by proposing a novel impact assessment model. The authors used grounded theory in their methodology. The main results showed the impact of the method of evaluating

the new risk metrics, together with a novel regulatory framework and standardization of IoT databases.

3.5. Future Trends

Study [4] explored the cybersecurity challenges posed by the IoT and the potential role of artificial intelligence in addressing these challenges. Through a comprehensive literature review, it identified the key areas of concern and proposed strategies for enhancing IoT security using artificial intelligence. The study emphasized the need for continuous development of AI algorithms and highlighted the criminal motives behind IoT and AI-related cyberattacks. The research aimed to equip cybersecurity experts with effective techniques to secure IoT systems and foster a safer IoT environment.

Study [6] discussed the cybersecurity concerns of vendors and consumers in light of the increasing use of IoT devices in our world. The study was an empirical paper, where the authors used data from a review of the related literature and tested two scenarios for different attacks. The main goal of this research was to identify the main IoT applications, as well as to analyze the issues challenging cybersecurity in the near future. The results of the paper showed that the tested scenarios revealed a high vulnerability of the IoT systems.

Study [26] addressed security concerns in organizations working with information systems and extensively utilizing the IoT. It emphasized the importance of effective risk management due to inevitable risk factors. The study identified the inadequacy of current risk assessment approaches for information systems and introduced an advanced algorithm, Improved Cuckoo Search (ICS), for information security risk assessment in a miniature IoT system. The empirical study used a simulation experiment to demonstrate the success of the proposed algorithm, although it is limited to one system.

Study [27] discussed privacy violation issues in smart homes that arise from the use of IoT devices. It proposed an approach to help end-users lacking awareness of IoT risks in assessing and responding effectively to these risks. The study employed a survey to gather available risk approaches and implemented its model using a meta-modeling framework (ADOXX). The main limitation is the focus solely on home devices. The findings provided knowledge and awareness to end-users, empowering them to make informed decisions and be conscious of known and expected risks in their smart homes.

Study [28] discussed the H2020 European research project GHOST, Safe-Guarding Home IoT Environments with Personalized Realtime Risk Control. The main goal of the research was to introduce the GHOST security framework for smart homes and explore the main issues with its cybersecurity. This article is considered a practical study, adopting the methodology of an architecture analysis with real-life trials that show the capabilities of the framework. The study results showed that real-life trials provide crucial feedback on the practicality and authentication of the system in reasonable cybersecurity circumstances.

Study [29] discussed a comprehensive exploration of the IoT cyber risk in Industry 4.0. The study type is a case study, however, the methodology being used was a literature review survey in addition to a case study to extract novel perspectives for the evaluation of the economic impacts of IoT cyber risks, using the grounded theory approach. The main goal of the research article was to narrate the qualitative case study results. Key results showed that, according to the revision undertaken, there was a proportionate deficiency in planning for disaster recovery.

Study [30] discussed the rapid spread of cyber-physical systems and IoT use, which have resulted in different security issues. The main aim of this paper was the recognition of current IoT devices' security vulnerabilities, as well as promoting the development of low-cost IoT security methods. The article discussed two case studies, commercial and industrial IoT devices. Major results showed that both case studies had a high vulnerability to attacks and threats, and there should be an urgent solution before the wider spread of IoT devices in the next few years.

Study [31] discussed related cyber risks and the economic impact assessment of the IoT. The study type is empirical, where the methodology being used was based on calculations

and experiments. Approaches being used were (1) the Cyber Value at Risk (CyVaR) and (2) the MicroMort (MM). The study's main aim was to give insights regarding economic impact evaluation using mathematical calculations. Furthermore, the study's major results showed that economic impact can be evaluated by the following:

- Novel risk standards.
- Specific novel assessment method for the novel risk standards.
- Novel regulatory framework and standardization of IoT databases.
- Novel risk vectors as defined in the form of International IoT Asset Classification and Key IoT Cyber Risk Factors.

Study [32] discussed the integration of sensors and actuators as a form of controlling cyber-physical systems. The article was a case study, aiming to concentrate on an ontology-based advancement of IoT cybersecurity and to introduce a framework based on knowledge reasoning for the cybersecurity of the IoT. The methodology used was the application of the Model-Driven Service Engineering Architecture. The main contribution of the paper was the IoTSec ontology, and key results showed that the evaluation revealed great structural uniformity, in addition to the dynamic order of the classes.

Study [33] discussed the issues related to the security of smart homes based on IoT devices. The main aim was to discuss the different security issues that affect the cybersecurity of smart homes, as well as to introduce a solution for these risky potential attacks. This study is a practical one, in which the authors used the methodology of the OCTAVE Allegro, which is based on information assets. The study results showed that there exist 15 different attacks that threaten smart homes and need a solution.

Study [34] discussed the relationships between humans and their devices as necessary elements of cybersecurity profiles. The main aim of the study was to attain cybersecurity profiles via human factors. The main results of this practical study were:

- Defining the concept of human factors for cybersecurity;
- Proposing a methodology that can be used for different purposes.

Study [35] focuses on cybersecurity issues in the digital economy and introduces two frameworks, one updated from existing risk evaluation and one novel. It adopts a practical approach and employs a theoretical analysis through a literature review. One significant result is the paper's contribution to the domain of the 'digital economy', which was not extensively covered in the literature. However, the study's limitations include its reliance on previous studies with case studies and specific approaches.

Study [36] addresses awareness regarding IoT device cybersecurity among organizations and aims to guide them in improving their cybersecurity practices. It is an introductory study and part of a series of related studies. Notably, the study is accessible to individuals without IoT expertise, requiring only basic knowledge of privacy and cybersecurity. Major findings indicate the need for significant transformations in cybersecurity practices within organizations, emphasizing the importance of risk management for device utilization purposes, irrespective of device type.

Study [37] discussed the rising importance of cybersecurity among IoT systems manufacturers. The paper aimed to mitigate the risks of cybersecurity among entities and end-users based on the protection of IoT assets and privacy considerations. This review paper tried to find a solution for cybersecurity by reviewing the technologies and frameworks of IoT cybersecurity. Then, the authors proposed a framework based on four layers. This study covered a gap regarding the risk management of IoT cybersecurity by providing resource allocation methods to managers.

Study [38] discussed the issue of cybercriminals affecting the IoT infrastructure in addition to the importance of highlighting this issue internationally. For this reason, the study aimed to critically analyze the cybersecurity challenges related to IoT infrastructure by reviewing the related, reliable previous studies. The main contribution of this study was improving cybersecurity solutions. The key results of the research article showed that cybersecurity is an essential concern for the evolution of ecosystems and their appropriate operation.

Study [39] discussed the idea of enhancing the security of IoT devices before offering them for handling and usage, which can limit and mitigate cyberattacks. The study aimed to propose a model using the technique of hardening processes. It is a practical study that surfs the literature and then proposes a solution. It followed a qualitative analysis methodology. The study's main contribution was filling the gap in studies related to hardening and security authentication.

Study [40] aimed to identify advancement areas of the IoT and the related threats to their origin. The paper was a review article, wherein data were collected from the previous related studies. Its key results are listed as follows:

- Public administration is the top sector attacked.
- The education sector had most data violation.
- The industrial sector is the sector which will mostly develop based on IoT systems.

Study [41] aimed to introduce a novel assessment tool for ther risks of attacking IoT systems. The article was a comparative empirical study that relied on grounded theory as the methodology. The framework proposed was drawn from the shortages of the previous related studies. However, as per the authors, the study contributed to evaluating the influence of the IoT cyber risk. Its major results showed that the framework provides a comprehensive advanced knowledge of impact assessment.

Study [42] discussed how the emerging new IoT world is exposing data to violation and loss of confidentiality. The paper aimed to interpret the challenges of securing IoT devices and presented a debate about the technologies used for the purpose of IoT cybersecurity. This paper is a review article, in which the authors depended on collecting data from previous studies. The results of the current article showed that a creditable security technique is required for the purpose of developing IoT services.

3.6. Physical Layer Security Solutions for IoT Devices

In the context of physical layer security, a study focused on improving secrecy–energy efficiency in a satellite–terrestrial integrated network by using secrecy-aware hybrid beamforming schemes. These schemes involved a multibeam satellite system sharing the millimeter wave spectrum with a cellular system. The goal was to maximize achievable secrecy–energy efficiency by jointly designing hybrid and digital beamformers at the base station and satellite, respectively. The researchers used a sequential convex approximation method to handle multiple ESs and converted the original problem into a linear one with matrix inequalities and second-order cone constraints. Their proposed robust beamforming design was shown to be effective and superior through simulations using realistic satellite and terrestrial downlink channel models [43]. In another study, the researchers focused on addressing two critical aspects of future satellite communications: security and energy efficiency. They investigated secure energy efficient beamforming in multibeam satellite systems, where each satellite user was vulnerable to eavesdroppers attempting to intercept confidential information. The researchers employed the signal-to-leakage-plus-noise ratio metric to derive closed-form normalized beamforming weight vectors. Additionally, they utilized the successive convex approximation method to efficiently solve the power allocation subproblem. By combining these techniques, they proposed an iterative algorithm to obtain suboptimal solutions for the design [44].

To meet the increasing demands of Internet-of-Things (IoT) devices, multiple access techniques have been a focus of research. A study aimed to maximize the overall data transmission rate in the system while satisfying signal-interference-plus-noise-ratio requirements for IoT devices and power constraints for the UAV and satellite. The optimization problem was initially non-convex, but the researchers used sequential convex approximation and first-order Taylor expansion to transform it into a solvable one with a rank-one constraint. They then developed an iterative penalty function-based algorithm to solve this transformed problem. Simulations were conducted, and the results showed that the proposed method effectively reduced mutual interference and improved the system's overall data transmission rate compared to existing benchmark schemes. In essence, the

study focused on optimizing multiple access techniques for IoT devices in a satellite-UAV communication system to enhance overall performance and accommodate explosive access demands [45–51]. Whereas 6G networks offer customized end-to-end network services and support emerging cloud-edge applications, 5G networks do not. As the resource allocation problem in 6G is of utmost importance and requires more research attention, a study introduced an efficient resource allocation algorithm called TailoredSlice-6G. This algorithm is designed to enable tailored slices in 6G networks. When a slice request is received, the TailoredSlice-6G algorithm first identifies the slice resource type. Based on this information, it selects the most suitable sub-algorithm for resource allocation and slicing deployment. Each type of slice is associated with a specific resource allocation sub-algorithm incorporated into TailoredSlice-6G. A crucial aspect of the proposed algorithm is that each sub-algorithm is designed to operate within polynomial time, ensuring efficient and timely resource allocation for different slice types. In summary, the study focuses on addressing resource allocation challenges in 6G networks by introducing the TailoredSlice-6G algorithm, which allows for tailored end-to-end network services and supports diverse cloud-edge applications [52–57].

This literature review section provides a comprehensive summary of the most important previous studies related to the cybersecurity of the IoT. This summary encompasses the study's aims, identified problems, study types, major results, and limitations. Additionally, this section thoroughly examines the proposed frameworks and approaches, as well as the various cyberattacks discussed, which were used to populate the table below.

4. Evaluation and Analysis

Table 1 represents a comprehensive overview of the previous articles. We analyzed the studies based on two primary dimensions. (1) Identification of the attacks and challenges outlined in each article, (2) the proposed approach and framework.

The reviewed literature has addressed a wide range of attacks posing threats to the IoT. The content of the studies varied, with some focusing on specific attacks, while others addressed broader challenges in IoT cybersecurity. This section presents in-depth findings and analysis of the different attacks identified in the literature, along with a comprehensive discussion of the various frameworks and proposed solutions to mitigate these threats.

Starting with smart cities and smart homes, smart cities had concerns regarding keeping their systems under control. Cybersecurity attacks can threaten the power grid and water supply, resulting in the collapse of essential daily needs [20]. Staying in the same domain, smart homes were attacked by privacy violations, which impacted the physical world as a result [27]. Moreover, [28] mentioned that there are physical, network, and software attacks that impact the safeguarding of smart homes. In addition, smart homes had concerns about eavesdropping and impersonation attacks, as well as network routing and service availability challenges [33]. The proposed solutions for the smart cities and smart homes were OCTAVE Allegro evaluation methodology and GHOST safeguarding homes. In addition, a smartphone application was proposed for monitoring the household devices' state.

The next discipline is the economic impact of cybersecurity, as cybersecurity attacks created concerns regarding the impacts and consequences on the economy and industrial devices. Industrial devices based on the IoT were widely used [25,29,30,35]. Proposed solutions for this domain included mapping interactions among various factors in the IoT devices, as well as the IoT MicroMort model for economic impact calculation.

Moreover, the health sector has suffered from cyberattacks, which were addressed by the previous literature, as cybersecurity attacks threaten healthcare services and include data loss and physical attacks [9,22]. Proposed solutions included a normative hierarchical model of international cybersecurity standards. The authors also suggested supporting dynamic adaptation to cyber threats.

Table 1. The literature review summary table.

References	Attacks/Challenges	Proposed Framework/Approaches
[1]	Software piracy and malware attacks Challenges: economic and reputational damages	- Approach to check the existence of pirated software and malware-infected files in the IoT network. - The TensorFlow deep neural network to recognize the pirated software. - Tokenization and weighting characteristics to get rid of the noisy data. - Deep learning approaches to check the source code plagiarism.
[2]	Confidentiality concerns and data exploitation	Risk analysis based on EBIOS methodology.
[3]	Organization's assets attacks	A form of runtime, near-real-time risk assessment support.
[20]	Controlling traffic light attacks against smart vehicles Collapsing the power grid Surveillance cameras Water supply (chemical levels) Power outage Smart cities lose control of their systems as a result of the attacks	An evaluation model to assess the cybersecurity (level of maturity) of IoT solutions used in a smart city.
[23]	Eavesdropping attack Identity faking attack Disclosure of sensitive data	A proposed framework for the security verification of distributed industrial control systems. The framework is based on modeling industrial IoT infrastructures. Patterns made by the attacks and mitigation techniques to stop the attacks. Using an alloy analyzer to prove mitigation techniques.
[9]	Healthcare services attacks including physical attacks and data loss	The dynamic adaptive cybersecurity framework.
[26]	Context privacy leakage Staff lack of operation and abuse of power Lack of user awareness of protection Privacy cognition	The algorithm Improved Cuckoo Search (ICS) for a back-propagation neural network (BPNN) to enhance the accuracy and stability.
[27]	Profiling attacks Privacy violating Lifecycle transitions Inventory attack It shows the impact on the physical world	A smartphone application that allows users to monitor the household devices that use the IoT in a quick process, while also checking the state of the security of these devices instantly.
[11]	IoT systems' vulnerability Malware detection Data security concerns Personal and public physical safety risk issues	Privacy-preserving data techniques and a 5G IoT environment, in addition to computational intelligence cyber defenses.
[12]	Cybercrimes Impact on the global economy	Blockchain technology.
[22]	Healthcare services and cybersecurity challenges	Normative hierarchical model of the international cybersecurity standards.
[28]	Cybersecurity issues in smart homes: Physical attack Network attack Software attack Impact on safeguarding homes	GHOST, Safe-Guarding Home IoT Environments with Personalized Real-Time Risk Control security framework.

Furthermore, cybercrimes were a main concern and a significant field of study that caught the attention of many scholars [3,12,17,34,38,42]. Attacks included impact on the global economy, organizations' assets, profiling of human data, and confidential data.

Proposed methods included blockchain technology, runtime near real-time risk assessment support, and human factor concept method to obtain cybersecurity profiles.

On the other hand, an important issue addressed by previous studies was privacy concerns and attacks [6,11,13,15,16,18,19,21,23,24,26,32,36,37]. The privacy concerns included eavesdropping, identity faking, exploitation, fabrication, theft, data integrity and falsification, and access to sensitive information. Proposed solutions included a mitigation strategy using an alloy analyzer, Improved Cuckoo Search, exploitation of the virtual environment, hardware, software solutions, knowledge reasoning for the IoT, software-defined networks, risk estimation techniques, privacy-preserving data techniques, a 5G IoT environment, and computational intelligence cyber defenses.

5. Results and Discussion

This section aims to present and discuss the findings from the literature review, the attacks and challenges, the frameworks and approaches proposed, and the detection techniques according to each study (Table 1). This section also presents the gap found in the systematic review and the future trends in IoT cybersecurity.

5.1. Most Frequent Attacks That IoT Is Vulnerable to

Different attacks on and challenges to IoT cybersecurity that were identified by the previous studies were discussed in Table 1. The table represents the various approaches and frameworks proposed, in addition to the attacks or vulnerability detection techniques. Moreover, their percentages are shown in Figure 2. Results showed that the most-tackled issues and concerns with IoT cybersecurity were the privacy issues [11,15,27,36,37] in addition to the concerns related to cybercrimes [12,17,38]. Details related to the top two issues concerning the cybersecurity of IoT are explained in Figure 3. Another notable issue discussed in the literature was denial-of-access attacks [5,15,21,24,39]. Data exploitation was also one of the critical challenges detected concerning IoT security [6,11,13,19,26,40], followed by a Man-in-the-Middle attack as detected by [24].

5.2. Most Important Techniques That Have Been Used in IoT Risk Detection

Regarding detection techniques, the current study summarized a few techniques that have been found in the literature as shown in Figure 4, such as artificial intelligence [1,4], cognitive security technique [20], novel meta-heuristic technique [26], cloud computing [24], and machine learning [19].

5.3. New Trends in IoT Cybersecurity

The literature review revealed several emerging trends and future directions in IoT cybersecurity. While the available literature provided valuable insights, it is important to note that the number of studies explicitly focusing on specific trends was limited. Nonetheless, the identified trends are indicative of the potential advancements in securing IoT systems. We discuss the prominent trends below:

- Integration of artificial intelligence (AI): artificial intelligence has emerged as a promising technique in addressing the challenges of IoT cybersecurity. Several studies [19,38,40] highlighted the role of AI, particularly machine learning algorithms, in detecting and mitigating cybersecurity threats in IoT environments. AI-based solutions offer the ability to analyze vast amounts of data from IoT devices, identify patterns, and proactively respond to potential attacks. Future research in this area should focus on refining AI algorithms, exploring ensemble learning approaches, and implementing real-time adaptive cybersecurity systems.
- Blockchain technology for enhanced security: blockchain technology has gained significant attention for its potential to enhance the security and privacy of IoT devices and data [12]. By providing decentralized and tamper-resistant data storage and communication, blockchain can reduce the risk of data manipulation and unauthorized access. Research efforts should concentrate on optimizing blockchain solutions for

IoT, addressing scalability issues and ensuring interoperability with existing IoT architectures.

- Dynamic adaptive cybersecurity frameworks: as the IoT ecosystem evolves, static cybersecurity measures may become inadequate to defend against constantly evolving threats. Dynamic adaptive cybersecurity frameworks, as proposed by some studies [9], offer the ability to continuously assess and adjust security measures based on real-time threat intelligence. Future research should focus on developing intelligent and context-aware cybersecurity frameworks that can adapt to the changing IoT environment while minimizing the impact on system performance.
- Privacy-preserving techniques: with increasing concerns over data privacy in IoT, several studies [6,11,37] emphasized the need for privacy-preserving techniques. These techniques aim to protect sensitive user data while still enabling meaningful data analysis for IoT applications. Future research should explore novel cryptographic protocols, privacy-enhancing technologies, and privacy-aware data sharing mechanisms to strike a balance between data privacy and utility.
- Secure firmware and hardware design: the security of IoT devices heavily depends on the integrity of their firmware and hardware components [39]. Studies emphasized the importance of implementing secure development practices and utilizing hardware security modules to safeguard against physical attacks and firmware tampering. Future research should address the challenges of secure firmware updates, hardware-based attestation, and supply chain security.

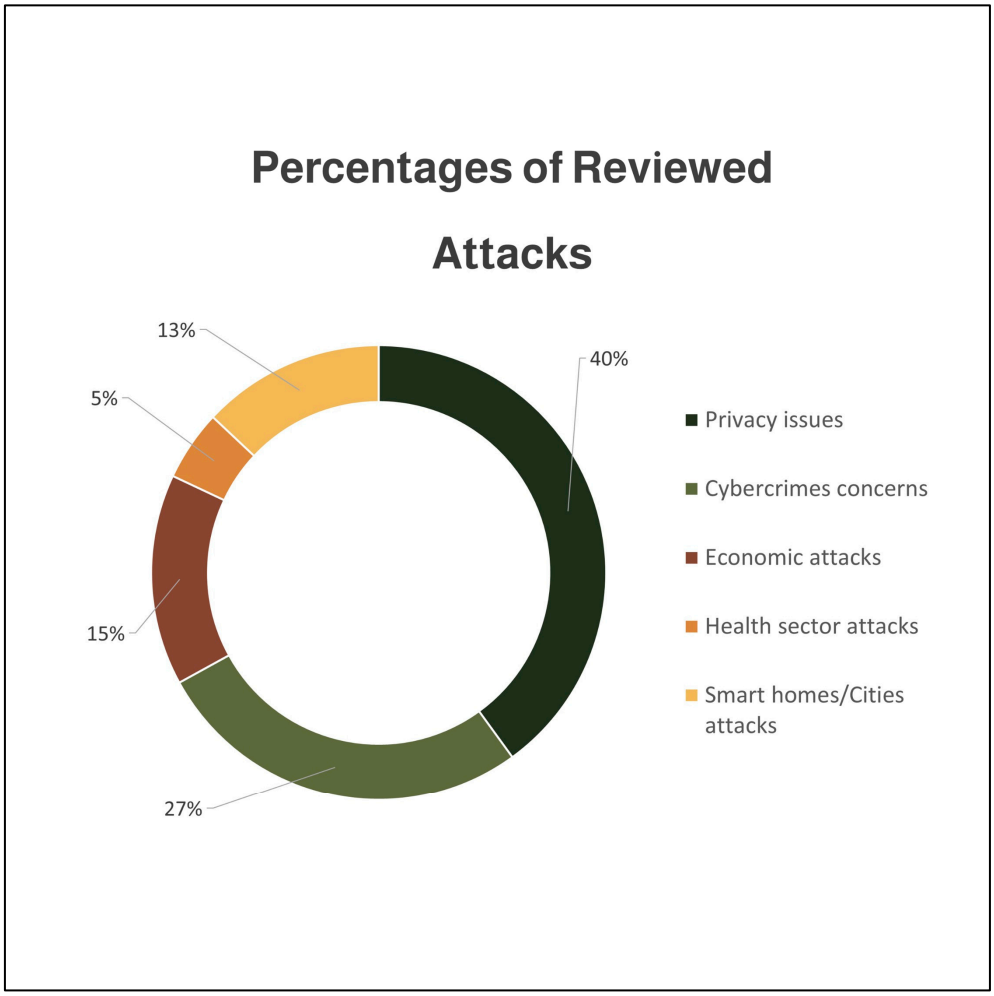

Figure 2. Percentages of reviewed attacks.

Despite the identified trends, it is essential to acknowledge that the field of IoT cybersecurity is continually evolving, and new trends may emerge over time. Additionally, the limited number of studies addressing specific trends indicates the need for further research to explore and validate the effectiveness of proposed solutions in real-world IoT scenarios.

Therefore, the identified trends in IoT cybersecurity hold significant potential in addressing the challenges posed by the expanding IoT landscape. Research efforts should continue to focus on these trends, exploring innovative approaches, and collaborating across disciplines to create a robust and resilient IoT security ecosystem.

5.4. Literature Review Gap

The machine learning techniques used in IoT cybersecurity were not tackled deeply by previous studies. Their role must be better identified and described. Moreover, there are still some attacks not fully covered by the proposed solutions, for which we recommend wider research and real-life examples to test the effectiveness of each proposed solution, in agreement with the perspectives of [12,28]. These attacks include data server connection attacks [4] in addition to confidentiality and security authentication [39].

Figure 3. Top two cybersecurity concerns.

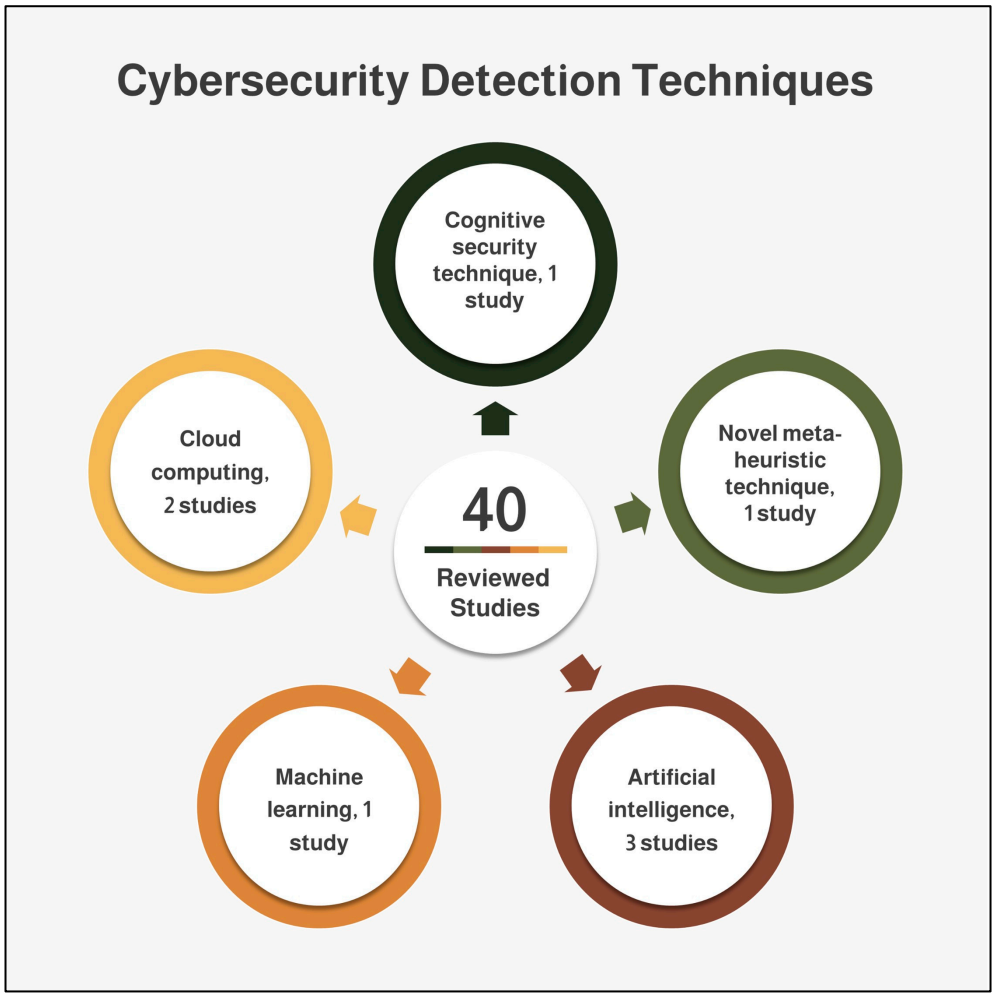

Figure 4. Cybersecurity detection techniques.

6. Conclusions

In conclusion, this systematic review has shed light on the diverse and evolving landscape of IoT cybersecurity. The analysis of the reviewed literature revealed that IoT devices and systems face a wide range of cyber threats, with privacy issues and cybercrimes standing out as the most significant concerns. While this finding aligns with common knowledge, it underscores the critical need for continuous efforts in addressing these challenges.

Furthermore, the literature review highlighted the potential of artificial intelligence as a promising technique for enhancing IoT cybersecurity. As the IoT ecosystem grows in complexity and scale, traditional security measures alone may not suffice to protect against sophisticated attacks. The integration of artificial intelligence and machine learning offers the potential for more adaptive, proactive, and effective security solutions to counter evolving threats.

However, while the review provided valuable insights into the existing research, there are still important areas where further exploration is needed. For instance, some attacks and vulnerabilities were not comprehensively covered by the proposed solutions, indicating the need for more tailored and targeted approaches.

Therefore, future research should focus on interdisciplinary collaborations, real-world validation of proposed solutions, and exploration of emerging technologies beyond artificial intelligence.

The field of IoT cybersecurity is dynamic and ever evolving, requiring constant vigilance and innovation to protect against cyber threats effectively. This review provides

a foundation for future researchers to build upon and underscores the importance of collective efforts to secure the IoT for the benefit of society at large.

Author Contributions: Conceptualization, T.S.A.; methodology, T.S.A., A.L. and M.A.A.; validation, T.S.A., A.L. and M.A.A.; formal analysis, T.S.A.; investigation, T.S.A.; resources, T.S.A.; writing—original draft preparation, T.S.A.; writing—review and editing, T.S.A., A.L. and M.A.A.; visualization, T.S.A.; supervision, M.A.A. and A.L.; project administration, M.A.A. and A.L. All authors have read and agreed to the published version of the manuscript.

Funding: 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. Grant No. 4241).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

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. Grant No. 4241).

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Ullah, F.; Naeem, H.; Jabbar, S.; Khalid, S.; Latif, M.A.; Al-Turjman, F.; Mostarda, L. Cyber Security Threats Detection in Internet of Things Using Deep Learning Approach. *IEEE Access* **2019**, *7*, 124379–124389. [CrossRef]
2. Zahra, B.F.; Abdelhamid, B. Risk Analysis in Internet of Things Using EBIOS. In Proceedings of the 2017 IEEE 7th Annual Computing and Communication Workshop and Conference (CCWC), Vegas, NV, USA, 9–11 January 2017; pp. 1–7.
3. Nurse, J.R.C.; Creese, S.; De Roure, D. Security Risk Assessment in Internet of Things Systems. *IT Prof.* **2017**, *19*, 20–26. [CrossRef]
4. Kuzlu, M.; Fair, C.; Guler, O. Role of Artificial Intelligence in the Internet of Things (IoT) cybersecurity. *Discov. Internet Things* **2021**, *1*, 7. [CrossRef]
5. Mahmoud, R.; Yousuf, T.; Aloul, F.; Zualkernan, I. Internet of Things (IoT) Security: Current Status, Challenges and Prospective Measures. In Proceedings of the 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST), London, UK, 14–16 December 2015; pp. 336–341.
6. Tweneboah-Koduah, S.; Skouby, K.E.; Tadayoni, R. Cyber Security Threats to IoT Applications and Service Domains. *Wirel. Pers. Commun.* **2017**, *95*, 169–185. [CrossRef]
7. Gonzalez, L.; Ruggia, R. Policy-Based Compliance Control Within Inter-Organizational Service Integration Platforms. In Proceedings of the 2018 IEEE 11th Conference on Service-Oriented Computing and Applications (SOCA), Paris, France, 20–22 November 2018; pp. 202–209.
8. Moher, D.; Liberati, A.; Tetzlaff, J.; Altman, D.G. Preferred reporting items for systematic reviews and meta-analyses: The PRISMA statement. *Int. J. Surg.* **2010**, *8*, 336–341. [CrossRef]
9. Boudko, S.; Abie, H. Adaptive Cybersecurity Framework for Healthcare Internet of Things. In Proceedings of the 2019 13th International Symposium on Medical Information and Communication Technology (ISMICT), Oslo, Norway, 8–10 May 2019; pp. 1–6.
10. Radanliev, P.; De Roure, D.; Maple, C.; Nurse, J.R.; Nicolescu, R.; Ani, U. Cyber Risk in IoT Systems. *Univ. Oxford Comb. Work. Pap. Proj. Rep. Prep. PETRAS Natl. Cent. Excell. Cisco Res. Cent.* **2019**, *169701*, 1–27. [CrossRef]
11. Zhao, S.; Li, S.; Qi, L.; Da Xu, L. Computational Intelligence Enabled Cybersecurity for the Internet of Things. *IEEE Trans. Emerg. Top. Comput. Intell.* **2020**, *4*, 666–674. [CrossRef]
12. Abdullah, A.; Hamad, R.; Abdulrahman, M.; Moala, H.; Elkhediri, S. CyberSecurity: A Review of Internet of Things (IoT) Security Issues, Challenges and Techniques. In Proceedings of the 2019 2nd International Conference on Computer Applications & Information Security (ICCAIS), Riyadh, Saudi Arabia, 1–3 May 2019; pp. 1–6.
13. Rizvi, S.; Kurtz, A.; Pfeffer, J.; Rizvi, M. Securing the Internet of Things (IoT): A Security Taxonomy for IoT. In Proceedings of the 2018 17th IEEE International Conference on Trust, Security and Privacy, New York, NY, USA, 31 July–3 August 2018; pp. 163–168.
14. Tawalbeh, L.; Muheidat, F.; Tawalbeh, M.; Quwaider, M. IoT Privacy and Security: Challenges and Solutions. *Appl. Sci.* **2020**, *10*, 4102. [CrossRef]
15. Abomhara, M.; Køien, G.M. Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks. *J. Cyber Secur. Mobil.* **2015**, *4*, 65–88. [CrossRef]
16. Islam, M.R.; Aktheruzzaman, K.M. An Analysis of Cybersecurity Attacks against Internet of Things and Security Solutions. *J. Comput. Commun.* **2020**, *8*, 11–25. [CrossRef]

17. Gurunath, R.; Agarwal, M.; Nandi, A.; Samanta, D. An Overview: Security Issue in IoT Network. In Proceedings of the 2018 2nd International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Palladam, India, 30–31 August 2018; pp. 104–107.
18. Atlam, H.F.; Wills, G.B. An efficient security risk estimation technique for Risk-based access control model for IoT. *Internet Things* **2019**, *6*, 100052. [CrossRef]
19. Strecker, S.; Van Haaften, W.; Dave, R. An Analysis of IoT Cyber Security Driven by Machine Learning. In *Proceedings of the International Conference on Communication and Computational Technologies: ICCCT 2021*; Springer: Singapore, 2021; pp. 725–753.
20. Andrade, R.O.; Yoo, S.G.; Tello-Oquendo, L.; Ortiz-Garces, I. A Comprehensive Study of the IoT Cybersecurity in Smart Cities. *IEEE Access* **2020**, *8*, 228922–228941. [CrossRef]
21. Furfaro, A.; Argento, L.; Parise, A.; Piccolo, A. Using virtual environments for the assessment of cybersecurity issues in IoT scenarios. *Simul. Model. Pract. Theory* **2017**, *73*, 43–54. [CrossRef]
22. Strielkina, A.; Illiashenko, O.; Zhydenko, M.; Uzun, D. Cybersecurity of Healthcare IoT-Based Systems: Regulation and Case-Oriented Assessment. In Proceedings of the 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT), Ukraine, Kyiv, 24–27 May 2018; pp. 67–73.
23. Kulik, T.; Tran-Jorgensen, P.W.V.; Boudjadar, J.; Schultz, C. A Framework for Threat-Driven Cyber Security Verification of IoT Systems. In Proceedings of the 2018 IEEE International Conference on Software Testing, Verification and Validation Workshops (ICSTW), Västerås, Sweden, 9–13 April 2018; pp. 89–97.
24. Liao, B.; Ali, Y.; Nazir, S.; He, L.; Khan, H.U. Security Analysis of IoT Devices by Using Mobile Computing: A Systematic Literature Review. *IEEE Access* **2020**, *8*, 120331–120350. [CrossRef]
25. Radanliev, P.; De Roure, C.; Cannady, S.; Montalvo, R.M.; Nicolescu, R.; Huth, M. Economic impact of IoT cyber risk-analysing past and present to predict the future developments in IoT risk analysis and IoT cyber insurance. In *Living in the Internet of Things: Cybersecurity of the IoT*; Institution of Engineering and Technology: London, UK, 2018. [CrossRef]
26. Li, S.; Bi, F.; Chen, W.; Miao, X.; Liu, J.; Tang, C. An Improved Information Security Risk Assessments Method for Cyber-Physical-Social Computing and Networking. *IEEE Access* **2018**, *6*, 10311–10319. [CrossRef]
27. Ryoo, J.; Tjoa, S.; Ryoo, H. An IoT Risk Analysis Approach for Smart Homes (Work-in-Progress). In Proceedings of the 2018 International Conference on Software Security and Assurance (ICSSA), Seoul, Republic of Korea, 26–27 July 2018; pp. 49–52.
28. Augusto-Gonzalez, J.; Collen, A.; Evangelatos, S.; Anagnostopoulos, M.; Spathoulas, G.; Giannoutakis, K.M.; Votis, K.; Tzovaras, D.; Genge, B.; Gelenbe, E.; et al. From Internet of Threats to Internet of Things: A Cyber Security Architecture for Smart Homes. In Proceedings of the 2019 IEEE 24th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), Limassol, Cyprus, 11–13 September 2019; pp. 1–6.
29. Radanliev, P.; De Roure, D.; Nurse, J.R.C.; Nicolescu, R.; Huth, M.; Cannady, S.; Montalvo, R.M. Integration of Cyber Security Frameworks, Models and Approaches for Building Design Principles for the Internet-of-Things in Industry 4.0. In *Living in the Internet of Things: Cybersecurity of the IoT*; Institution of Engineering and Technology: London, UK, 2018.
30. Wurm, J.; Hoang, K.; Arias, O.; Sadeghi, A.-R.; Jin, Y. Security Analysis on Consumer and Industrial IoT Devices. In Proceedings of the 2016 21st Asia and South Pacific Design Automation Conference (ASP-DAC), Macao, China, 25–28 January 2016; pp. 519–524.
31. Radanliev, P.; De Roure, D.C.; Nicolescu, R.; Huth, M.; Montalvo, R.M.; Cannady, S.; Burnap, P. Future developments in cyber risk assessment for the internet of things. *Comput. Ind.* **2018**, *102*, 14–22. [CrossRef]
32. Mozzaquatro, B.A.; Agostinho, C.; Goncalves, D.; Martins, J.; Jardim-Goncalves, R. An Ontology-Based Cybersecurity Framework for the Internet of Things. *Sensors* **2018**, *18*, 3053. [CrossRef]
33. Ali, B.; Awad, A.I. Cyber and Physical Security Vulnerability Assessment for IoT-Based Smart Homes. *Sensors* **2018**, *18*, 817. [CrossRef] [PubMed]
34. Nieto, A.; Rios, R. Cybersecurity profiles based on human-centric IoT devices. *Hum.-Centric Comput. Inf. Sci.* **2019**, *9*, 39. [CrossRef]
35. Radanliev, P.; De Roure, D.C.; Nurse, J.R.C.; Mantilla Montalvo, R.; Cannady, S.; Santos, O.; Maddox, L.T.; Burnap, P.; Maple, C. Cyber Risk Impact Assessment-Assessing the Risk from the IoT to the Digital Economy. *SN Appl. Sci.* **2020**, *2*, 1–12. [CrossRef]
36. Boeckl, K.; Fagan, M.; Fisher, W.; Lefkovitz, N.; Megas, K.N.; Nadeau, E.; O'Rourke, D.G.; Piccarreta, B.; Scarfone, K. *Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks*; US Department of Commerce, National Institute of Standards and Technology: Gaithersburg, MD, USA, 2019.
37. Lee, I. Internet of Things (IoT) Cybersecurity: Literature Review and IoT Cyber Risk Management. *Future Internet* **2020**, *12*, 157. [CrossRef]
38. Djenna, A.; Harous, S.; Saidouni, D.E. Internet of Things Meet Internet of Threats: New Concern Cyber Security Issues of Critical Cyber Infrastructure. *Appl. Sci.* **2021**, *11*, 4580. [CrossRef]
39. Echeverría, A.; Cevallos, C.; Ortiz-Garces, I.; Andrade, R.O. Cybersecurity Model Based on Hardening for Secure Internet of Things Implementation. *Appl. Sci.* **2021**, *11*, 3260. [CrossRef]
40. Scarfò, A. The Cyber Security Challenges in the IoT Era. In *Security and Resilience in Intelligent Data-Centric Systems and Communication Networks*; Elsevier: Amsterdam, The Netherlands, 2018; pp. 53–76.
41. Almomani, O.; Almaiah, M.A.; Alsaaidah, A.; Smadi, S.; Mohammad, A.H.; Althunibat, A. Machine learning classifiers for network intrusion detection system: Comparative study. In Proceedings of the 2021 International Conference on Information Technology (ICIT), Amman, Jordan, 14–15 July 2021; pp. 440–445.

42. Wahab, A.; Ahmad, O.; Muhammad, M.; Ali, M. A Comprehensive Analysis on the Security Threats and their Countermeasures of IoT. *Int. J. Adv. Comput. Sci. Appl.* **2017**, *8*, 489–501. [CrossRef]
43. Lin, Z.; Lin, M.; Champagne, B.; Zhu, W.-P.; Al-Dhahir, N. Secrecy-Energy Efficient Hybrid Beamforming for Satellite-Terrestrial Integrated Networks. *IEEE Trans. Commun.* **2021**, *69*, 6345–6360. [CrossRef]
44. Lin, Z.; An, K.; Niu, H.; Hu, Y.; Chatzinotas, S.; Zheng, G.; Wang, J. SLNR-based Secure Energy Efficient Beamforming in Multibeam Satellite Systems. *IEEE Trans. Aerosp. Electron. Syst.* **2022**, *59*, 2085–2088. [CrossRef]
45. Lin, Z.; Lin, M.; de Cola, T.; Wang, J.-B.; Zhu, W.-P.; Cheng, J. Supporting IoT With Rate-Splitting Multiple Access in Satellite and Aerial-Integrated Networks. *IEEE Internet Things J.* **2021**, *8*, 11123–11134. [CrossRef]
46. Almaiah, M.A.; Ali, A.; Hajjej, F.; Pasha, M.F.; Alohali, M.A. A Lightweight Hybrid Deep Learning Privacy Preserving Model for FC-Based Industrial Internet of Medical Things. *Sensors* **2022**, *22*, 2112. [CrossRef]
47. Al Nafea, R.; Almaiah, M.A. Cyber security threats in cloud: Literature review. In Proceedings of the 2021 International Conference on Information Technology (ICIT), Amman, Jordan, 14–15 July 2021; pp. 779–786.
48. Bubukayr, M.A.; Almaiah, M.A. Cybersecurity concerns in smart-phones and applications: A survey. In Proceedings of the 2021 international conference on information technology (ICIT), Amman, Jordan, 14–15 July 2021; pp. 725–731.
49. Alamer, M.; Almaiah, M.A. Cybersecurity in Smart City: A systematic mapping study. In Proceedings of the 2021 International Conference on Information Technology (ICIT), Amman, Jordan, 14–15 July 2021; pp. 719–724.
50. Lutfi, A.; Alrawad, M.; Alsyouf, A.; Almaiah, M.A.; Al-Khasawneh, A.; Al-Khasawneh, A.L.; Alshira'H, A.F.; Alshirah, M.H.; Saad, M.; Ibrahim, N. Drivers and impact of big data analytic adoption in the retail industry: A quantitative investigation applying structural equation modeling. *J. Retail. Consum. Serv.* **2023**, *70*, 103129. [CrossRef]
51. Ali, A.; Almaiah, M.A.; Hajjej, F.; Pasha, M.F.; Fang, O.H.; Khan, R.; Teo, J.; Zakarya, M. An industrial IoT-based blockchain-enabled secure searchable encryption approach for healthcare systems using neural network. *Sensors* **2022**, *22*, 572. [CrossRef]
52. Cao, H.; Du, J.; Zhao, H.; Luo, D.X.; Kumar, N.; Yang, L.; Yu, F.R. Toward Tailored Resource Allocation of Slices in 6G Networks With Softwarization and Virtualization. *IEEE Internet Things J.* **2022**, *9*, 6623–6637. [CrossRef]
53. Alrawad, M.; Lutfi, A.; Alyatama, S.; Al Khattab, A.; Alsoboa, S.S.; Almaiah, M.A.; Ramadan, M.H.; Arafa, H.M.; Ahmed, N.A.; Alsyouf, A.; et al. Assessing customers perception of online shopping risks: A structural equation modeling–based multigroup analysis. *J. Retail. Consum. Serv.* **2023**, *71*, 103188. [CrossRef]
54. Almaiah, M.A.; Hajjej, F.; Ali, A.; Pasha, M.F.; Almomani, O. A Novel Hybrid Trustworthy Decentralized Authentication and Data Preservation Model for Digital Healthcare IoT Based CPS. *Sensors* **2022**, *22*, 1448. [CrossRef] [PubMed]
55. Siam, A.I.; Almaiah, M.A.; Al-Zahrani, A.; Elazm, A.A.; El Banby, G.M.; El-Shafai, W.; El-Samie, F.E.A.; El-Bahnasawy, N.A. Secure Health Monitoring Communication Systems Based on IoT and Cloud Computing for Medical Emergency Applications. *Comput. Intell. Neurosci.* **2021**, *2021*, 8016525. [CrossRef] [PubMed]
56. Almaiah, M.A.; Al-Zahrani, A.; Almomani, O.; Alhwaitat, A.K. Classification of cyber security threats on mobile devices and applications. In *Artificial Intelligence and Blockchain for Future Cybersecurity Applications*; Springer International Publishing: Cham, Switzerland, 2021; pp. 107–123.
57. Almaiah, M.A. A new scheme for detecting malicious attacks in wireless sensor networks based on blockchain technology. In *Artificial Intelligence and Blockchain for Future Cybersecurity Applications*; Springer International Publishing: Cham, Switzerland, 2021; pp. 217–234.