STAP
Smart Technologies Academic Press

Journal of Cyber Security and Risk Auditing

https://www.jcsra.thestap.com/

Check for updates

Towards Trustworthy IoT Systems: Cybersecurity Threats, Frameworks, and Future Directions

Thanaa Alsalem [1], Mohammed Amin[2]

[1] *College of Computer Sciences and Information Technology, King Faisal University, Saudi Arabia*
[2] *Fellowship Researcher, INTI International University, Nilai 71800, Malaysia*

ARTICLE INFO

Article History

Received: 15-01-2023
Revised: 30-01-2023
Accepted: 08-02-2023
Published: 10-02-2023

Vol.2023, No.1

DOI:
https://doi.org/10.63180/jcsra.thestap.2023.1.2

***Corresponding author.**
Email:
m.almaayah@aau.edu.jo

Orcid:

https://orcid.org/0000-0002-2215-2481

ABSTRACT

The Internet of Things (IoT) is becoming increasingly integrated into our daily lives. However, this rapid expansion raises significant concerns about future cybersecurity risks and the trustworthiness of this promising technology. This study aims to consolidate existing knowledge on the various cyberattacks and challenges facing IoT security, as well as to review the frameworks and solutions that have been proposed to address them. Additionally, it explores emerging trends and identifies gaps in the current IoT cybersecurity landscape. The literature review revealed that privacy breaches and cybercrimes remain the most pressing concerns. Artificial intelligence has emerged as a promising approach to enhancing cybersecurity in IoT environments. Nevertheless, several threats such as those targeting confidentiality, authentication, and server connectivity remain insufficiently addressed. This highlights the need for broader research and the application of real-world case studies to evaluate the effectiveness of proposed security measures.

Keywords: Internet of Things (IoT), IoT security, Cyberattacks, Confidentiality, Authentication.

How to cite the article
Alsalem, T., & Amin, M. (2023). Towards Trustworthy IoT Systems: Cybersecurity Threats, Frameworks, and Future Directions. Journal of Cyber Security and Risk Auditing, 2023(1), 3–18. https://doi.org/10.63180/jcsra.thestap.2023.1.2

1. Introduction

Internet of Things (IoT) devices have become increasingly integrated into sensitive sectors such as healthcare and finance. However, their influence extends far beyond these industries, reaching homes, smart cities, and many aspects of daily life. IoT enables connectivity among intelligent objects, applications, and cloud services, with an estimated 50 billion devices projected to be connected to the Internet by 2020 [1]. This massive connectivity, combined with the growing reliance on artificial intelligence, places immense pressure on vendors and device manufacturers to ensure the security and reliability of these technologies. Trust in IoT begins with security—particularly because these devices are constantly exposed to cyber threats when connected to the internet. Examples include cybercrimes, malware, software piracy, and other damaging attacks [1] [2]. However, the rapidly evolving nature of IoT makes it difficult for existing security solutions to remain effective. New threats emerge daily, requiring continuous development of security frameworks and approaches [3]. Therefore, regular reviews and updates of cybersecurity techniques are essential. This study aims to review recent advancements in cybersecurity risk analysis for IoT, identify various attack types and challenges, and evaluate proposed frameworks and solutions. Furthermore, it highlights the most widely used risk detection techniques, explores emerging trends in IoT cybersecurity, and addresses gaps found in the literature with recommendations for future research.

1.1 Motivation of the Research

As the world stands on the verge of a new era shaped by virtual reality and hyper connectivity, IoT is rapidly emerging as a transformative force in both technology and artificial intelligence. The exponential growth in the use of IoT devices [4] raises significant concerns about privacy and cybersecurity, which have become top priorities for risk management professionals. Although IoT is set to revolutionize various domains, unresolved security issues—such as privacy, authentication, and confidentiality—continue to hinder trust and full adoption [5]. Massive volumes of data are transmitted daily through IoT networks, making them highly vulnerable to cyberattacks. As such, a robust and forward-looking cybersecurity risk management strategy is urgently required to secure the future of IoT.

1.2 Problem Statement

Due to their highly interconnected nature and evolving technological landscape, IoT devices are increasingly exposed to a wide range of cyber risks and vulnerabilities [2]. As global attention shifts toward IoT innovation, new threats continuously emerge, necessitating updated and comprehensive reviews of current risk assessment frameworks and strategies. The complexity of IoT systems—along with their integration into numerous platforms and data-driven environments—elevates their susceptibility to cyberattacks. Security concerns are no longer limited to manufacturers; end-users now demand trustworthy, secure technologies [6]. This demand is driving the need for practical and effective cybersecurity solutions [7]. Furthermore, the diversity of approaches and frameworks proposed in recent studies raises critical questions: What are the most effective techniques for IoT risk detection? What are the emerging trends in IoT cybersecurity? Which types of attacks pose the greatest threats to IoT systems?

This study focuses on identifying and analyzing the most recent frameworks and approaches for cybersecurity risk assessment and management in the context of IoT. Specifically, it seeks to: Review key techniques used for detecting cybersecurity risks in IoT. Identify the most common and dangerous types of cyberattacks targeting IoT devices. Explore emerging trends and strategies in the field of IoT cybersecurity. The literature review was conducted using keywords such as IoT, cybersecurity, cybersecurity frameworks, and cybersecurity approaches. Cybersecurity in IoT has attracted significant scholarly attention, especially over the past five years, resulting in a wealth of literature proposing various solutions and frameworks to address critical security threats. Given the dynamic nature of IoT, frequent and updated review studies are essential. This research aims to contribute meaningfully by synthesizing the state-of-the-art studies in the field and tracing the progress of IoT cybersecurity research. The main objectives are to:

Identify various cybersecurity frameworks and approaches proposed for IoT cybersecurity risk analysis.

Categorize the different types of attacks and challenges facing IoT devices.

Highlight the most important risk detection techniques used in IoT security.

Identify current trends in IoT cybersecurity.

Expose gaps in the literature and recommend future directions for research and practical implementation.

2. Literature review

This section presents a critical analysis of key studies conducted over the past decade on cybersecurity in the Internet of Things (IoT). The selected works provide insights into the major challenges, threats, and solutions proposed to secure IoT systems across various domains. A study by [1] this empirical study emphasized two major threats to IoT systems software piracy and malware attacks—due to their significant economic impact. The authors introduced a novel detection approach for pirated software and malware-infected files within IoT networks. Experimental results demonstrated that the proposed solution outperformed existing methods in enhancing IoT cybersecurity. [2] Highlighting the daily integration of IoT into our lives, this study used the EBIOS methodology to conduct a risk analysis focused on vulnerabilities in IoT architecture. The key contribution lies in identifying the most critical security risks developers should prioritize, especially vulnerabilities in sensors, smart switches, and small actuators within specific contexts. [3] This review paper investigated why existing risk assessment approaches are inadequate for IoT environments. The analysis revealed several limitations, including. The periodic nature of assessments, Evolving system boundaries and limited knowledge, Lack of attention to systems integration ("the glue"), overlooking the potential use of assets as attack vectors. The authors advocate for continuous, automated risk assessment mechanisms and the development of predictive simulation tools.

Another study [4] this literature-based study explored the rapid growth of IoT and its connection with artificial intelligence (AI). It examined both the use of AI to secure IoT systems and the threats AI itself may pose. While many AI algorithms show promise in enhancing IoT security, others require further development. The paper also addressed the misuse of AI and IoT technologies for malicious purposes. [5] This survey focused on current IoT security challenges and standards. The authors reviewed authentication protocols and access control mechanisms, highlighting the importance of security standardization and predicting trends in IoT cybersecurity. [6] Addressing the growing concern of cybersecurity among vendors and consumers, this empirical study simulated attack scenarios to assess the vulnerability of IoT applications. The findings revealed significant exposure to cyber threats, emphasizing the urgent need for stronger security solutions. [8] This systematic review examined the development of cybersecurity frameworks for smart cities. The authors proposed a model to assess the cybersecurity capabilities of IoT-based smart city solutions. Their findings suggest that smart cities, heavily reliant on IoT, are highly vulnerable to cyberattacks. The proposed model supports enhancing cybersecurity resilience, especially when integrated with additional technologies. [9] Focused on industrial control systems within IoT environments, this empirical study proposed a framework to evaluate the security of distributed control systems at the design stage. Using an experimental setup and alloy analyzer, the authors demonstrated the framework's utility in identifying and mitigating cyber threats during system development. [10] This empirical research introduced an adaptive cybersecurity framework for IoT-based healthcare systems. Using game theory simulations, the authors showed that their framework could effectively predict and respond to dynamic cyberattacks. The study underscores the importance of proactive defense strategies in critical healthcare infrastructure.

In a study by [11] explored the risk management in IoT-dependent organizations, this empirical study developed an Improved Cuckoo Search (ICS) algorithm for cybersecurity risk assessment. Simulation results confirmed the algorithm's effectiveness, although the evaluation was limited to a single IoT system. [12] This practical study addressed privacy violations in smart homes due to IoT usage. The authors proposed a user-centric risk assessment model implemented via the ADOXX metamodeling platform. While the study was limited to smart home devices, it contributed significantly by raising user awareness and empowering informed decision-making regarding IoT risks. [13] This review paper highlighted users' lack of awareness regarding IoT security risks, especially related to data privacy and integrity. Drawing on secondary data, the authors identified 12 types of attacks with varying severity. The study emphasized the growing concern over IoT vulnerabilities and the ease with which skilled attackers can exploit security weaknesses—particularly in unsupported or outdated devices. A study discussed the issues of software piracy and malware attacks as two of the most critical threats facing IoT systems, with substantial economic implications. It proposed a novel solution to detect pirated and malware-infected files in IoT networks. The empirical results demonstrated improved performance over existing techniques [1]. Another research used the EBIOS methodology to conduct a risk analysis focused on vulnerabilities in IoT architectures. It emphasized the need for developers to secure specific application components such as sensors and actuators, which were identified as the most vulnerable [2]. A review identified limitations in existing IoT risk assessment methods, citing issues

such as infrequent evaluations, evolving system boundaries, and the failure to account for systems as potential attack platforms. The study concluded that automated and continuous risk assessment tools are necessary [3]. Artificial intelligence's role in IoT security was explored in another paper, which reviewed how both attackers and defenders are using AI. The study found that while some AI techniques are effective, many require further research. It also highlighted the criminal exploitation of AI in targeting IoT systems [4].

Recent IoT research has focused on authentication, access control, and security protocols, as highlighted in a survey study. The paper also projected future trends in IoT security [5]. Another empirical study examined IoT systems' vulnerabilities by simulating two attack scenarios. It concluded that many applications remain highly vulnerable and emphasized the need for stronger consumer and vendor awareness [6]. In a systematic review of cybersecurity frameworks for smart cities, researchers proposed a model for assessing IoT security in urban settings. The paper found that as smart cities become more dependent on IoT, their vulnerability to attacks increases significantly [8]. Industrial control systems entering the IoT landscape were the focus of another empirical study. It proposed a security framework for early-stage distributed control system design, helping to prevent threats before deployment [9]. A healthcare-focused paper introduced an adaptive cybersecurity framework that reacts to dynamic and intelligent cyber threats using game theory. The proposed system was tested and proved effective against adaptive attacks [10]. Information system organizations that heavily rely on IoT were the subject of a study proposing an improved cuckoo search algorithm for risk assessment. Though effective, the study's limitation was its application to only one system [11]. Privacy risks in smart homes were explored in a practical study using ADOXX to model how non-expert users could assess and respond to their own cybersecurity risks. Findings highlighted the importance of end-user awareness [12].

Another review identified twelve types of attacks on IoT systems and noted that manufacturers often do not provide ongoing security support, making devices easy targets for skilled attackers [13]. A survey paper explored the role of computational intelligence (CI) in IoT cybersecurity. It identified key challenges for CI integration, such as algorithm efficiency and compliance with data regulations. The authors proposed 5G and privacy-preserving techniques as future solutions [14]. Cybercrimes targeting IoT were the focus of another review, which categorized IoT challenges and recommended blockchain for its integrity and encryption benefits [15]. In a healthcare context, researchers developed a hierarchical cybersecurity model for IoT systems that complies with international standards. This case-based study ensured traceability and verification in its layered security model [16]. The GHOST research project introduced a smart home cybersecurity framework. Practical trials confirmed the framework's ability to adapt to real-life threats [17]. Another case study combined a literature survey with grounded theory to evaluate cyber risks in Industry 4.0. It found a major gap in disaster recovery planning for industrial IoT systems [18]. A review examined data privacy issues in IoT systems and concluded that the high volume and sensitivity of data significantly increase security concerns [19]. Security vulnerabilities in both commercial and industrial IoT devices were discussed in a dual-case study. The authors advocated for affordable security solutions before widespread IoT adoption [20]. To assess smart home cybersecurity solutions, researchers simulated realistic attack scenarios using the SmallWorld platform. Their proposed framework improved user trust and provided accurate risk evaluation [21]. An economic impact analysis of IoT cyber risks used two models—Cyber Value at Risk and MicroMort—to suggest a standardized framework for assessing IoT-related financial threats [22]. A holistic review examined how mobile computing can enhance IoT security by integrating hardware and software defenses. The study found that mobile computing is a key trend in this field [23]. Ontology-based cybersecurity for IoT was proposed in a case study using a knowledge-reasoning framework. The IoTSec ontology was shown to be structurally sound and effective [24]. Smart home cybersecurity was assessed using the OCTAVE Allegro methodology, revealing 15 significant threats and contributing a foundational model for future security designs [25]. The influence of human behavior on cybersecurity profiles was investigated through a human-factor model. The study proposed that human considerations should be integrated into cyber-risk strategies [26]. Cybersecurity risks in the digital economy were addressed in a theoretical analysis that updated an existing evaluation framework and introduced a new one. It emphasized the lack of existing literature on digital economy cybersecurity [27]. Another review synthesized risk assessment models for IoT. It defined common risk types, evaluation approaches, and suggested future strategies for mitigation and transfer of risk [28]. A study targeted at organizations and federal agencies introduced a practical guide for enhancing IoT cybersecurity. It emphasized that trust depends on both usage context and device functionality [29].

A comprehensive review classified threats to IoT devices and emphasized issues like confidentiality and organizational trust. It concluded with a taxonomy of attack types [30]. Data theft and privacy breaches were central to another review. The authors outlined existing countermeasures such as authentication and secure communications but favored digital signatures for better protection [31]. A framework consisting of four cybersecurity layers was proposed to mitigate IoT risks while ensuring efficient resource allocation. It also addressed a gap in existing literature on risk management [32]. In

another critical analysis, cyber threats to IoT infrastructure were classified, and various attack methods were discussed. The authors highlighted that cybersecurity is essential for a stable IoT ecosystem [33]. Device-level hardening was proposed as a method to enhance IoT security before deployment. The qualitative analysis demonstrated the benefits of this proactive approach [34].

An empirical study introduced a layered security model combining IoT, edge, and cloud technologies. It reduced potential vulnerabilities through multi-layered defense [35]. Fuzzy inference combined with expert validation was used in a new technique for risk detection. Simulation results showed it outperformed traditional fuzzy models [36]. A review highlighted sectors most affected by IoT threats: public administration, education, and industry. The authors suggested these sectors should be priorities for future security developments [37]. A grounded theory-based study proposed a new assessment framework for cyber risk in IoT. It filled gaps in prior research and provided comprehensive impact insights [38]. A review of emerging IoT technologies concluded that data confidentiality remains the most pressing challenge. The authors advocated for a reliable, standardized security framework [39].

Finally, a new impact assessment model for Industry 4.0 was proposed using grounded theory. The model emphasized regulatory alignment and economic evaluation of cyber risks [40]. A review of machine learning applications for IoT security concluded that Random Forest and K-Nearest Neighbors are the most accurate detection techniques. It also stressed the effectiveness of SDN and fog-layer networks [41].

3. Research methodology

This section outlines the methodology adopted in this study, detailing the sequence of steps undertaken for selecting, analyzing, and synthesizing relevant literature. It includes the eligibility criteria for study selection, information sources, search strategy, selection process, data analysis procedures, and key findings.

3.1 Eligibility Criteria

The review was guided by specific eligibility criteria to ensure the inclusion of relevant and high-quality studies. The selected research articles primarily addressed the cybersecurity of the Internet of Things (IoT), focusing on challenges, attack vectors, risk factors, and proposed frameworks or approaches to mitigate cybersecurity issues. Additionally, review papers that discussed IoT cybersecurity risk assessment and management frameworks were included.

3.2 Information Sources

The study relied on reputable databases such as ScienceDirect, IEEE Xplore, Google Scholar, and Academia.edu. Only peer-reviewed journal articles and conference papers published in high-impact, internationally recognized venues were considered to ensure the credibility and academic rigor of the sources.

3.3 Search Strategy and Selection Process

A systematic search strategy was employed using key terms such as “IoT,” “cybersecurity,” “cybersecurity frameworks,” and “cybersecurity approaches.” These keywords were applied across selected academic databases. The inclusion criteria filtered articles published between 2015 and 2022, with a particular emphasis on studies from 2018 to 2022 due to the rapid evolution of IoT technologies and associated security concerns during this period. Further screening was conducted based on the relevance to the research objectives, contribution to the field, and depth of discussion. Articles lacking substantive analysis or practical contribution were excluded. This rigorous process resulted in the selection of 40 relevant articles, which were then included in the systematic review.

3.4 Data Analysis and Synthesis

Each of the 40 selected studies was classified according to its research design empirical, practical, survey-based, or review. The key research objectives, problem statements, findings, and recommendations were extracted. The author developed a structured synthesis by organizing the studies into a comparative framework that captured: Key cybersecurity challenges and threats in IoT. The impact of various types of attacks. Proposed frameworks and technical solutions. Detection and mitigation techniques used. A summary table was constructed to provide a consolidated view of the above elements, facilitating a thematic analysis of emerging trends and gaps.

3.5 Findings

The findings present a consolidated overview of the insights derived from the reviewed literature. Multiple categories of cyberattacks and their corresponding impacts on IoT systems were identified. Furthermore, the review highlighted significant research gaps, particularly regarding the effectiveness and coverage of existing security frameworks in real-world IoT deployments.

Emerging trends such as the application of artificial intelligence, blockchain, and edge computing in enhancing IoT security were also identified. These trends and gaps serve as a foundation for proposing future research directions and informing the development of more robust IoT cybersecurity solutions. The overall methodology followed in this study is visually summarized in Figure 1.

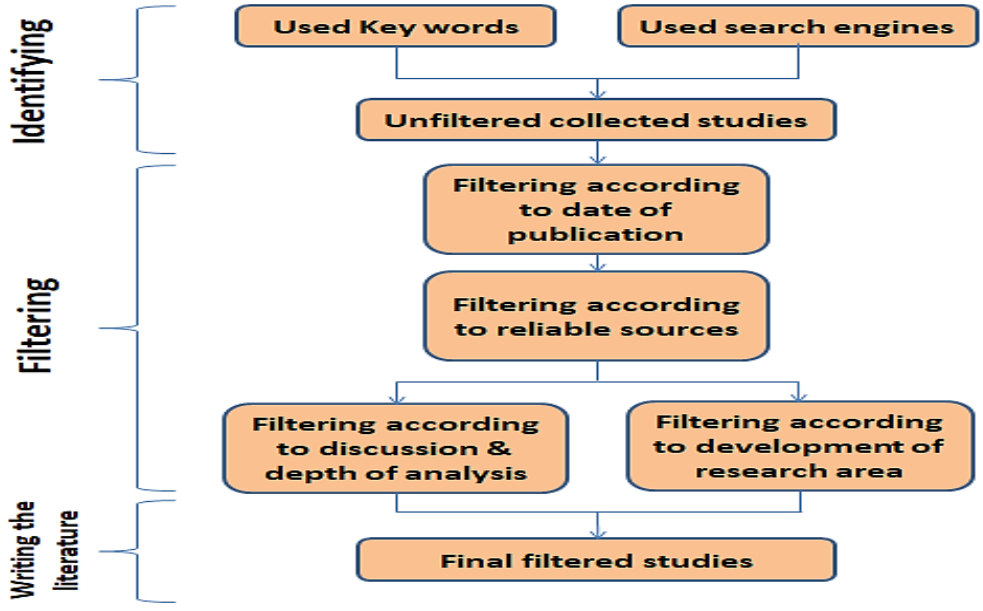


Figure 1. Literature review search strategy framework

4. Evaluation and Analysis

Table 1 presents a comparative summary of the 40 reviewed articles. The comparison is based on three key dimensions: (1) the types of cybersecurity attacks or challenges identified in each study, (2) the frameworks or approaches proposed to address these challenges, and (3) the detection techniques employed or recommended. The table highlights the diversity of solutions and methodologies adopted across the literature, offering insights into how different studies have approached IoT cybersecurity and responded to specific threat vectors.

Table 1. Related works on IoT.

Studies	Comparison Factors		
	Attacks/challenges	***Proposed framework/approaches***	***Detection techniques***
[1]	Software piracy and malware attacks.	Approach to check the existence of the pirated software and malware-infected files in the IoT network:	Artificial Intelligence

Studies	Comparison Factors		
	Attacks/challenges	***Proposed framework/approaches***	***Detection techniques***
	Challenges: economic and reputational damages.	- 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	
[4]	Network gateway attacks cloud data server connections attacks	N/A	Artificial Intelligence
[5]	Active attacks Passive attacks Denial of Service (DoS) attacks Man-in-the-Middle attacks Replay attack Timing attack Node capture attack Impact on the services provided by the IoT	N/A	
[6]	Application services attack, data integrity attack, privacy, trust, identity, standardization	N/A	Cloud computing
[8]	Controlling traffic lights/ 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	Cognitive security technique
[9]	Eavesdropping attack Identity faking attack Disclosure of sensitive data	A proposed framework for the security verifying of distributed industrial control systems. The framework is based on modelling industrial IoT infrastructures,	

Studies	Comparison Factors		
	Attacks/challenges	***Proposed framework/approaches***	***Detection techniques***
		patterns made by the attacks, and mitigation techniques to stop the attacks. And using Alloy analyzer to prove mitigation techniques	
[10]	Health care services attacks including physical attacks/ Data loss	The dynamic Adaptive Cybersecurity Framework	
[11]	context privacy leakage/ staff disoperation and abuse of power/ the protection awareness lack of users/ privacy cognition	Algorithm improved cuckoo search (ICS) for a back- propagation neural network (BPNN) to enhance the accuracy and stability	Novel meta-heuristic technique
[12]	Profiling attacks/ Privacy-violating / Lifecycle Transitions/ Inventory attack/ It shows Impact on the physical world	A smart-phone application, that allows users to monitor their household devices that uses IoT, in a quick process, also they can check the state of security of these devices instantly.	
[13]	Cybercriminal attacks Impact on the server	N/A	
[14]	IoT systems' vulnerability Malware detection Data security concerns Personal & public physical safety risk issues.	Privacy preserving data techniques and a 5G IoT environment, in addition to computational intelligence cyber defenses	Computational intelligence/ cyber defense technologies/intrusion detection Techniques.
[15]	Cybercrimes Impact on global economy	Blockchain technology	
[16]	Healthcare services cybersecurity challenges	Normative hierarchical model of the international cybersecurity standards	
[17]	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	
[18]	Cyber physical attacks Economic impact	A novel introduced design principles map interactions among various factors in the IoT devices	
[19]	Identity and data theft	N/A	

Studies	Comparison Factors		
	Attacks/challenges	***Proposed framework/approaches***	***Detection techniques***
	Device manipulation, Data falsification Network manipulation Impact on application platforms		
[20]	Commercial and industrial IoT devices vulnerability concerns	N/A	
[21]	Physical attacks (DoS) identity fabrication	A proposed approach which relies on the virtual environments' exploitation, as well as, agent-based simulation, to assess cybersecurity solutions for the next generation of IoT applications in real life scenarios	
[22]	Economic impact concerns caused by cybersecurity issues	IoT MicroMort model with current cyber risk valuation frameworks, to calculate the economic impact of IoT cyber risk	
[23]	Attacks related to smartphones/Phishing/Spoofing/Malware attacks/Physical attacks/DoS/Man in middle/eavesdropping, replay attacks	Hardware and software-based solutions	Mobile computing
[24]	Access to sensitive information challenge.	An ontology-based cybersecurity framework using knowledge reasoning for IoT, composed of two approaches: design time and run time	
[25]	Flooding attacks Jamming attacks Replay attacks Unauthorized routing update and wormhole attacks). Eavesdropping and impersonation attacks	OCTAVE Allegro methodology.	
[26]	Profiling of human attacks	Methodology based on the concept of Human Factors to obtain Cybersecurity profiles	
[27]	Economic impact concerns as a result of cybersecurity	Digital economy specific novel framework for impact evaluation of IoT cyber risk.	
[28]	N/A	Effective risk assessment	
[29]	Privacy issues concerns	N/A	
[30]	Physical attacks	N/A	

Studies	Comparison Factors		
	Attacks/challenges	***Proposed framework/approaches***	***Detection techniques***
	DoS attacks Reconnaissance attacks Access attacks Privacy attacks Cybercrimes attacks Destructive attacks SCADA Attacks		
[31]	Eavesdropping, injection of fraudulent packets, and non-authorized conversations. Exploiting the software, access to sensitive data physical attacks Network attacks Application attacks Zigbee attacks Z-Wave attacks	N/A	
[32]	Privacy issues Protection of IoT assets concerns	A linear programming method for the allocation of financial resources to multiple IoT cybersecurity projects	
[33]	Cybercrimes	N/A	
[34]	Viruses (DoS)	Evaluating the level of security of an IoT solution based on a checklist that considers the security aspects in the three layers of the IoT architecture	
[35]	Main challenges: Improper device updates Lack of effective and robust security protocols	IoT layered model: generic and stretched with the privacy and security components and layers identification.	
[36]	Security and privacy challenges	Risk estimation technique which integrates the fuzzy inference system with expert judgment to evaluate security risks of access control operations in the IoT system	
[37]	Data loss attacks	N/A	
[38]	High impact cyber attacks	Novel model for impact assessment of IoT cyber risk	
[39]	Security and confidentiality of data concerns	N/A	
[40]	Economic risks related to IoT attacking's concerns Privacy concerns Ethics concerns Trust concerns	Impact assessment model of IoT cyber risk in Industry 4.0	

Studies	Comparison Factors		
	Attacks/challenges	***Proposed framework/approaches***	***Detection techniques***
	Reliability concerns Acceptability, and security concerns		
[41]	BOT Net attack Data exploitation concerns	Utilized Software Defined Networks (SDN) and the fog layer of networks	Machine learning

The reviewed literature revealed a wide range of cybersecurity threats targeting the Internet of Things (IoT). The focus of the studies varied, with some addressing specific attacks while others explored broader challenges associated with IoT cybersecurity. This section presents a detailed analysis of the various types of attacks identified in the literature, along with the corresponding frameworks and solutions proposed to mitigate these threats.

Beginning with smart cities and smart homes, the primary concern within smart cities is maintaining control over critical infrastructure. Cybersecurity breaches in this context can disrupt power grids and water supplies, leading to the collapse of essential services ([8]). Similarly, smart homes face serious privacy violations that can have real-world consequences ([12]). In addition, [17] identified physical, network, and software-based attacks as significant threats to home security systems. Further threats to smart homes include eavesdropping, impersonation, network routing manipulation, and service availability disruptions ([25]). Proposed solutions for mitigating these threats include the OCTAVE Allegro risk evaluation methodology, the GHOST safeguarding framework for smart homes, and smartphone-based applications for monitoring household device activity.

In the economic and industrial domain, several studies emphasized the growing concern over the financial implications of IoT-related cyberattacks. As IoT devices become increasingly integrated into industrial infrastructure, the risk of economic disruption rises ([18], [20], [27], [40]). Proposed solutions in this area included mapping the interactions among critical IoT components and adopting the IoT MicroMort model for assessing the economic impact of cyber incidents.

The healthcare sector also emerged as a critical area of concern. Cyberattacks in this context pose threats not only to sensitive patient data but also to the physical safety of healthcare infrastructure ([10], [16]). Recommended solutions include the development of normative, hierarchical models aligned with international cybersecurity standards, as well as frameworks that enable dynamic adaptation to emerging cyber threats.

Cybercrime was another prominent topic across multiple studies ([3], [13], [15], [26], [33], [39]). The scope of these attacks ranged from targeting organizational assets and critical data to large-scale economic disruption and human profiling. Proposed approaches included the implementation of blockchain-based security protocols, real-time and near real-time risk assessment mechanisms, and the integration of human factor modeling to create comprehensive cybersecurity profiles.

Privacy concerns were extensively addressed across numerous studies ([6], [9], [11], [14], [19], [21], [23], [24], [29]–[32], [36], [41]). Identified threats in this domain include eavesdropping, identity theft and impersonation, data falsification, unauthorized access to sensitive information, and integrity violations. To counter these threats, various solutions were proposed, including mitigation strategies utilizing Alloy Analyzer, optimization techniques such as improved cuckoo search, and the use of virtual environments for vulnerability simulation. Other notable recommendations include hybrid hardware-software solutions, reasoning frameworks for IoT knowledge modeling, Software-Defined Networks (SDN), and advanced risk estimation methodologies. Additionally, several studies suggested adopting privacy-preserving data techniques, deploying cybersecurity defenses within a 5G IoT environment, and leveraging computational intelligence to enhance protection mechanisms.

5. Results and Discussions

This section presents and discusses the key findings of the literature review, including the types of attacks and challenges identified (summarized in Table 1), the proposed frameworks and approaches, as well as the detection techniques used across various studies. Furthermore, this section addresses the gaps identified in the reviewed literature and outlines the anticipated future trends in IoT cybersecurity.

5.1 Attacks on IoT

The reviewed studies revealed a wide array of cybersecurity challenges and attacks affecting IoT systems, as outlined in Table 1. These challenges were further categorized and quantified, with their distribution illustrated in Figure 2. The most frequently discussed issue was privacy violation, prominently featured in studies such as [12], [14], [29], [30], and [32]. This was closely followed by concerns related to cybercrime, highlighted in studies including [13], [15], and [33]. Figure 3 provides further insight into these two dominant concerns.

Additional threats addressed in the literature included denial-of-access (DoA) attacks ([5], [21], [23], [30], [34]), which can disrupt service availability, and data exploitation ([6], [11], [14], [19], [37], [41]), which remains a critical issue due to IoT systems' extensive data collection and communication. Man-in-the-middle (MitM) attacks were also identified, particularly in [23], as another serious threat impacting data integrity and confidentiality.

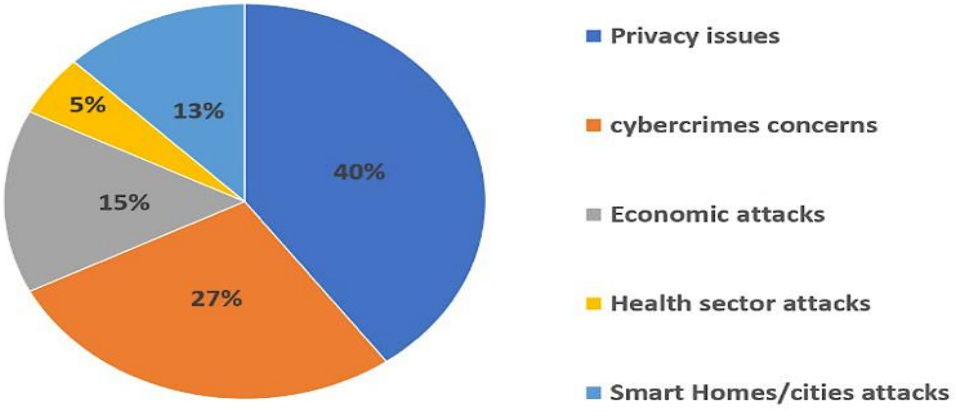


Figure 2. Percentages of reviewed attacks

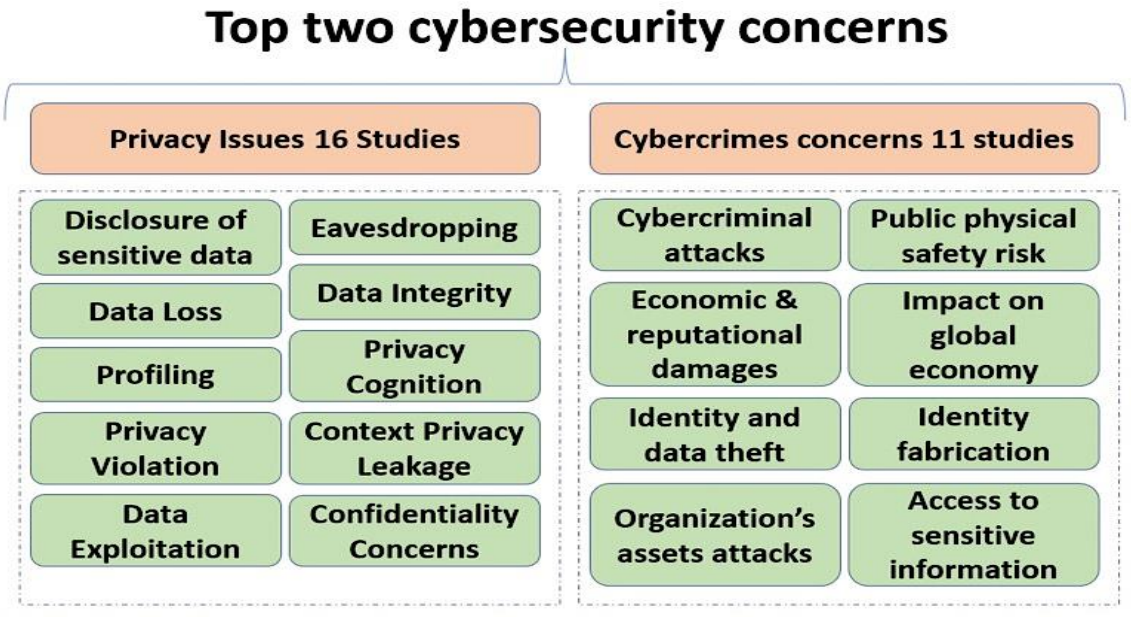


Figure 3. Top two cybersecurity concerns

5.2 Prominent Techniques for IoT Risk Detection

In terms of threat detection methodologies, the reviewed studies presented several advanced techniques. As depicted in Figure 4, artificial intelligence (AI) was widely recognized for its potential in identifying and mitigating cyber threats in IoT environments ([1], [4]). Other notable methods include cognitive security techniques ([8]), novel meta-heuristic algorithms ([11]), cloud computing-based approaches ([23]), and machine learning models ([41]). These methods reflect the increasing reliance on adaptive, data-driven strategies to address the dynamic nature of cybersecurity threats in IoT systems.

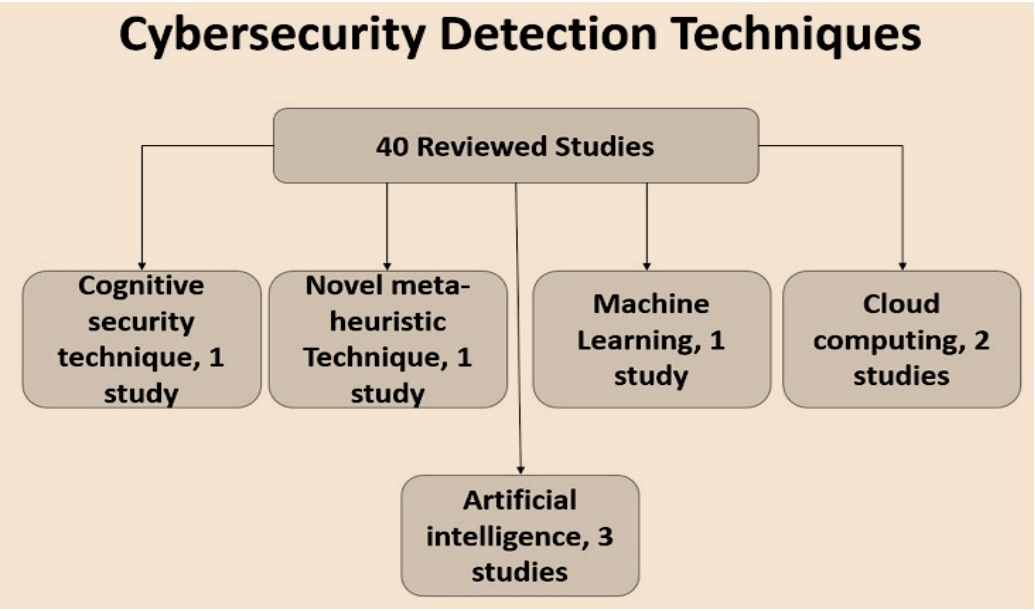


Figure 4. Cybersecurity detection techniques

5.3 Emerging Trends in IoT Cybersecurity

The reviewed literature pointed toward several emerging trends expected to shape the future of IoT cybersecurity. One prominent trend is the growing integration of artificial intelligence, which is anticipated to play a critical role in enhancing threat detection and response capabilities ([37]). Despite current advances, existing cybersecurity solutions are often insufficient to fully protect IoT environments, emphasizing the need for more sophisticated AI-based techniques ([33]). Additionally, several studies ([10]) underlined the importance of machine learning as a foundational tool for developing intelligent and scalable cybersecurity solutions.

5.4 Identified Gaps in the Literature

Despite the substantial contributions of the reviewed studies, several gaps remain. Notably, the role of machine learning techniques in IoT cybersecurity was not thoroughly examined. There is a pressing need to further explore, evaluate, and contextualize these techniques in real-world settings. Moreover, certain types of cyberattacks remain insufficiently addressed by existing frameworks, calling for expanded research and empirical validation of proposed solutions ([15], [17]). These under-addressed threats include data server connection attacks ([4]), confidentiality breaches, and weaknesses in security authentication mechanisms ([34]).

6. Conclusion

This study offered a systematic review of the literature regarding the IoT cybersecurity issues, challenges, attack types, detection techniques, frameworks, and approaches. Artificial intelligence has shown to be a promising technique in which future research is going to focus on for the purpose of achieving cybersecurity solutions for the IoT discipline. Yet, the current research is limited to the published articles in the duration between 2015-2022, also limited to the time restriction, in which wider review requires a longer duration of the study. Another limitation was that the identification of the frameworks and approaches being proposed was not discussed deeply from a perceptive of an expert in cybersecurity, the study was limited to a general discussion according to the expected outcomes identified at the beginning of the research.

Corresponding author

Dr. Mohammed Amin
m.almaayah@aau.edu.jo

Acknowledgements
Not applicable.

Funding
This work was supported by the Deanship of Scientific Research, Vice Presidency for Graduate Studies and Scientific Research, King Faisal University, Saudi Arabia.

Contributions
T.A; Conceptualization, A.A; Investigation, T.A; Writing (Original Draft), T.A; and T.A; Writing (Review and Editing) Supervision, M.A; Project Administration.

Ethics declarations
This article does not contain any studies with human participants or animals performed by any of the authors.

Consent for publication
Not applicable.

Competing interests
The author declares no competing interests.

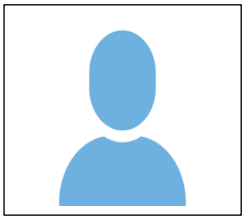
References

[1] Ullah, F., et al. (2019). Cyber security threats detection in Internet of Things using deep learning approach. *IEEE Access*, 7, 124379–124389.
[2] Zahra, B. F., & Abdelhamid, B. (2017). Risk analysis in Internet of Things using EBIOS. In *2017 IEEE 7th Annual Computing and Communication Workshop and Conference (CCWC)* (pp. 1–7). IEEE.
[3] Nurse, J. R., Creese, S., & De Roure, D. J. (2017). Security risk assessment in Internet of Things systems. *IT Professional*, 19(5), 20–26.
[4] Kuzlu, M., Fair, C., & Guler, O. (2021). Role of artificial intelligence in the Internet of Things (IoT) cybersecurity. *Discover Internet of Things*, 1(1), 1–14.
[5] Mahmoud, R., Yousuf, T., Aloul, F., & Zualkernan, I. (2015). Internet of Things (IoT) security: Current status, challenges and prospective measures. In *2015 10th International Conference for Internet Technology and Secured Transactions (ICITST)* (pp. 336–341). IEEE.
[6] Tweneboah-Koduah, S., Skouby, K. E., & Tadayoni, R. J. (2017). Cyber security threats to IoT applications and service domains. *Wireless Personal Communications*, 95(1), 169–185.
[7] González, L., & Ruggia, R. (2018). Policy-based compliance control within inter-organizational service integration platforms. In *2018 IEEE 11th Conference on Service-Oriented Computing and Applications (SOCA)* (pp. 202–209). IEEE.
[8] Andrade, R. O., Yoo, S. G., Tello-Oquendo, L., & Ortiz-Garcés, I. A. (2020). A comprehensive study of the IoT cybersecurity in smart cities. *IEEE Access*, 8, 228922–228941.
[9] Kulik, T., Tran-Jørgensen, P. W., Boudjadar, J., & Schultz, C. (2018). A framework for threat-driven cyber security verification of IoT systems. In *2018 IEEE International Conference on Software Testing, Verification and Validation Workshops (ICSTW)* (pp. 89–97). IEEE.
[10] Boudko, S., & Abie, H. (2019). Adaptive cybersecurity framework for healthcare Internet of Things. In *2019 13th International Symposium on Medical Information and Communication Technology (ISMICT)* (pp. 1–6). IEEE.
[11] Li, S., Bi, F., Chen, W., Miao, X., Liu, J., & Tang, C. J. (2018). An improved information security risk assessments method for cyber-physical-social computing and networking. *IEEE Access*, 6, 10311–10319.

[12] Ryoo, J., Tjoa, S., & Ryoo, H. (2018). An IoT risk analysis approach for smart homes (work-in-progress). In *2018 International Conference on Software Security and Assurance (ICSSA)* (pp. 49–52). IEEE.
[13] Gurunath, R., Agarwal, M., Nandi, A., & Samanta, D. (2018). An overview: Security issue in IoT network. In *2018 2nd International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)* (pp. 104–107). IEEE.
[14] Zhao, S., Li, S., Qi, L., & Da Xu, L. J. (2020). Computational intelligence enabled cybersecurity for the Internet of Things. *IEEE Transactions on Emerging Topics in Computational Intelligence*, 4(5), 666–674.
[15] Abdullah, A., Hamad, R., Abdulrahman, M., Moala, H., & Elkhediri, S. (2019). Cybersecurity: A review of Internet of Things (IoT) security issues, challenges and techniques. In *2019 2nd International Conference on Computer Applications & Information Security (ICCAIS)* (pp. 1–6). IEEE.
[16] Strielkina, A., Illiashenko, O., Zhydenko, M., & Uzun, D. (2018). Cybersecurity of healthcare IoT-based systems: Regulation and case-oriented assessment. In *2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT)* (pp. 67–73). IEEE.
[17] Augusto-Gonzalez, J., et al. (2019). From Internet of threats to Internet of Things: A cyber security architecture for smart homes. In *2019 IEEE 24th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD)* (pp. 1–6). IEEE.
[18] Radanliev, P., et al. (2018). 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* (pp. 1–6). IET.
[19] Rizvi, S., Kurtz, A., Pfeffer, J., & Rizvi, M. (2018). Securing the Internet of Things (IoT): A security taxonomy for IoT. In *2018 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/12th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE)* (pp. 163–168). IEEE.
[20] Wurm, J., Hoang, K., Arias, O., Sadeghi, A.-R., & Jin, Y. (2016). Security analysis on consumer and industrial IoT devices. In *2016 21st Asia and South Pacific Design Automation Conference (ASP-DAC)* (pp. 519–524). IEEE.
[21] Furfaro, A., Argento, L., Parise, A., & Piccolo, M. P. (2017). Using virtual environments for the assessment of cybersecurity issues in IoT scenarios. *Simulation Modelling Practice and Theory*, 73, 43–54.
[22] Radanliev, P., et al. (2018). Future developments in cyber risk assessment for the Internet of Things. *Computers in Industry*, 102, 14–22.
[23] Liao, B., Ali, Y., Nazir, S., He, L., & Khan, H. U. (2020). Security analysis of IoT devices by using mobile computing: A systematic literature review. *IEEE Access*, 8, 120331–120350.
[24] Mozzaquatro, B. A., Agostinho, C., Goncalves, D., Martins, J., & Jardim-Goncalves, R. J. (2018). An ontology-based cybersecurity framework for the Internet of Things. *Sensors*, 18(9), 3053.
[25] Ali, B., & Awad, A. I. (2018). Cyber and physical security vulnerability assessment for IoT-based smart homes. *Sensors*, 18(3), 817.
[26] Nieto, A., Rios, R. J. H.-C., & Sciences, I. (2019). Cybersecurity profiles based on human-centric IoT devices. *Human-centric Computing and Information Sciences*, 9(1), 1–23.
[27] Radanliev, P., et al. (2019). Cyber risk impact assessment—assessing the risk from the IoT to the digital economy. *Proceedings of the Living in the Internet of Things: Cybersecurity of the IoT 2019*, IET.
[28] Radanliev, P., De Roure, D. C., Maple, C., Nurse, J. R., Nicolescu, R., & Ani, U. (2019). Cyber risk in IoT systems. *Living in the Internet of Things 2019*. IET.
[29] Boeckl, K., et al. (2019). *Considerations for managing Internet of Things (IoT) cybersecurity and privacy risks*. U.S. Department of Commerce, National Institute of Standards and Technology (NIST).
[30] Abomhara, M., & Køien, G. M. J. (2015). Cyber security and the Internet of Things: Vulnerabilities, threats, intruders and attacks. *Journal of Cyber Security and Mobility*, 65–88.
[31] Islam, M. R., & Aktheruzzaman, K. J. (2020). An analysis of cybersecurity attacks against Internet of Things and security solutions. *Journal of Communications and Computer*, 8(4), 11–25.
[32] Lee, I. J. F. I. (2020). Internet of Things (IoT) cybersecurity: Literature review and IoT cyber risk management. *Future Internet*, 12(9), 157.
[33] Djenna, A., Harous, S., & Saidouni, D. E. J. A. S. (2021). Internet of Things meets Internet of threats: New concern cybersecurity issues of critical cyber infrastructure. *Applied Sciences*, 11(10), 4580.
[34] Echeverría, A., Cevallos, C., Ortiz-Garces, I., & Andrade, R. O. J. A. S. (2021). Cybersecurity model based on hardening for secure Internet of Things implementation. *Applied Sciences*, 11(7), 3260.
[35] Tawalbeh, L. A., Muheidat, F., Tawalbeh, M., & Quwaider, M. J. A. S. (2020). IoT privacy and security: Challenges and solutions. *Applied Sciences*, 10(12), 4102.
[36] Atlam, H. F., & Wills, G. B. J. I. o. T. (2019). An efficient security risk estimation technique for risk-based access control model for IoT. *Internet of Things*, 6, 100052.
[37] Scarfò, A. (2018). The cybersecurity challenges in the IoT era. In *Security and Resilience in Intelligent Data-Centric Systems and Communication Networks* (pp. 53–76). Elsevier.
[38] Radanliev, P., et al. (2020). Future developments in standardisation of cyber risk in the Internet of Things (IoT). *Internet of Things*, 2(2), 1–16.
[39] Ahmed, A. W., Ahmed, M. M., Khan, O. A., Shah, M. A. J. I. J. o. A. C. S., & Applications. (2017). A comprehensive analysis on the security threats and their countermeasures of IoT. *International Journal of Advanced Computer Science and Applications*, 8(7), 489–501.

[40] Radanliev, P., De Roure, D., Cannady, S., Montalvo, R. M., Nicolescu, R., & Huth, M. (2018). Economic impact of IoT cyber risk—analysing past and present to predict the future developments in IoT risk analysis and IoT cyber insurance. *Living in the Internet of Things 2018*, IET.
[41] Strecker, S., Van Haaften, W., & Dave, R. (2021). An analysis of IoT cyber security driven by machine learning. In *Proceedings of International Conference on Communication and Computational Technologies* (pp. 725–753). Springer.

Biographies



Thanaa Alsalem received a master degree in Cybersecurity from King Faisal University. He has an excellent experience in the cybersecurity field in both theoretical and practical. He has several certificates in cybersecurity like CEH and others. He several publications in cyber risk assessment. His research interests including cyber security, risk assessment and cyber-attacks. 220003189@student.kfu.edu.sa

Dr. Mohammed Amin is an Associate Professor in the Department of Computer Science at University of Jordan. Almaayah is among the top 2% scientists in the world from 2020 up to now. He is working as Editor in Chief for the International Journal of Cybersecurity and Risk Assessment. He has published over 115 research papers in highly reputed journals such as the Engineering and Science Technology, an International Journal, Education and Information Technologies, IEEE Access and others. Most of his publications were indexed under the ISI Web of Science and Scopus. His current research interests include Cybersecurity, Cybersecurity-Risk Assessment and Blockchain. m.almaayah@aau.edu.jo