STAP Smart Technologies Academic Press

STAP Journal of Security Risk Management

https://www.jsrm.thestap.com/


# Cyber Risk Management in the Internet of Things: Frameworks, Models, and Best Practices

**Mohammed Almaayah** [1], **Rejwan Bin Sulaiman**[2]

[1] *Fellowship Researcher, INTI International University, Nilai 71800, Malaysia*
[2] *School of Computer science and Technology, Northumbria University, Newcastle Upon Tyne, UK*

**ARTICLE INFO**

**Article History**

**Received: 25-06-2024**
**Revised: 04-10-2024**
**Accepted: 05-10-2024**
**Published: 06-10-2024**

**Vol.2024, No.1**

**DOI:**
https://doi.org/10.63180/jsrm.thestap.2024.1.1

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

**Orcid:**

https://orcid.org/0000-0002-2016-1093



**ABSTRACT**

This paper contributes to the ongoing discourse by identifying key risks associated with IoT devices and environments and proposing strategies to mitigate them. The study focuses on three main objectives: (1) identifying the primary security threats affecting IoT devices, (2) outlining best practices for mitigating these risks, and (3) exploring the role of cyber risk management in securing IoT ecosystems. By addressing these aspects, the paper aims to support stakeholders in implementing more robust security frameworks, ensuring confidentiality, integrity, and safety in IoT deployments. Based on an analysis of 35 previous studies, it is evident that a variety of complementary risk management frameworks and models are available to support the secure deployment and operation of IoT devices. These frameworks have been developed for both governmental and commercial use, enabling organizations to tailor their risk management strategies to specific IoT contexts. Among the reviewed studies, seven utilized the ISO framework for risk management in IoT environments, while six applied the NIST framework. Additionally, three studies implemented the OCTAVE framework to assess and mitigate risks. Notably, nine studies each employed a distinct risk management model, including ELK Stack, PDCA Cycle, Cyber Kill Chain (CKC), CSRF, CRAMM, COBIT 5, IoTSRM2, and the Cyber Value at Risk (CVaR) model. These diverse approaches highlight the growing recognition of the need for structured, adaptable, and sector-specific risk management strategies in the rapidly evolving IoT landscape.

**Keywords:** Internet of Things (IoT), Risk Management, ISO Framework, NIST Framework, Threats in IoT.

**How to cite the article**
Almaayah, M., & Sulaiman, R. B. (2024). Cyber Risk Management in the Internet of Things: Frameworks, Models, and Best Practices. STAP Journal of Security Risk Management, 2024(1), 3–23. https://doi.org/10.63180/jsrm.thestap.2024.1.1

## 1. Introduction

Nowadays we live in the era of technology that embedded in our daily routine and one of these technologies is Internet of Things. Internet of things allows billion devices to sense, share information and communicate over the internet. These devices have data, which collect, analyze and use in order to provide perfect planning, Management and decision making for different type of users. Thus, IoT is used in different field such education, medical, entertainment… etc. The aim of IOT is to make things able to connect anytime, anywhere with any person and anything. The common IoT architecture has three layers, which are perception layer, network layer and application layer. There is common IoT architecture, which has three layers. Figure 1, illustrated the IoT layers which are application layer, network layer and perception layer. The perception layer is the first layer, which used in order to link to the physical world to collect data and sense of its surroundings. It measures the value like light, temperature and so on. The second layer is the network layer, which can provide the user with the specific service requested. It connects the perception layer and application layer. The third layer is an application layer, which is a set of interface methods that hosts in a communication network use to communicate with one another.

The rapid growth of IoT devices leads to increase the number of cyber risks, which must consider. The attackers always find a way to exploit any vulnerabilities to attack the IoT devices in order to satisfy his /her desire. Thus, this paper aims to identify the main risks with IoT and find the best mitigation technique in order to reduce these risks. In addition, finding the best risk management frameworks and models in IoT. The paper organized as follows. Section2 introduces the background of IoT. Section 3 introduces motivation of paper. Followed by section 4, which is problem statement and then section5 research methodology. Then followed by section6, which discusses Literature Review. Finally, section7 and eight, which are Result and discussion and future work.

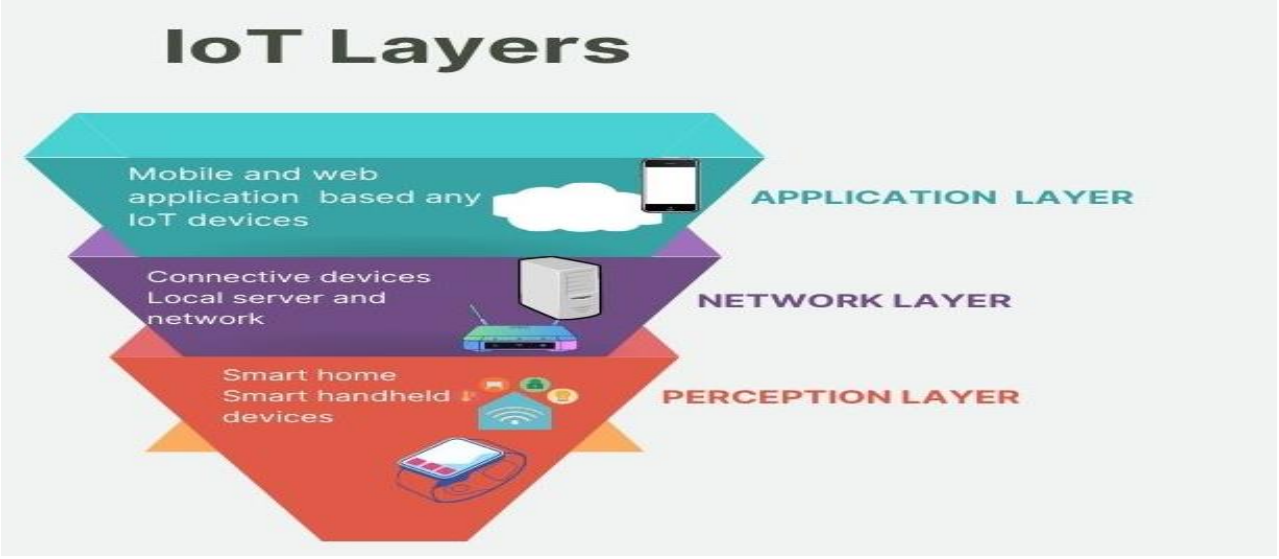


**Figure 1.** Architecture of IoT layers.

## 2. Background

Internet is affordable and widely available to everyone in the world. These Internet of Things (IoT) objects (clouds/web servers/hosts/sensors/machines/applications) connect directly to the internet and send data to other users over the intern. IoT will turn things in the real world into intelligent things. IoT connects everything in the world within a common infrastructure, allowing us to control the things around us, as well as provide information about the state of things [9].

The concept of IoT exists since 1999, and its exponential growth leads to raise security and privacy risks. For example, ebay admitted in 2017 that all 3 billion-user accounts had been hacked. [3]. Many of these risks result from device vulnerabilities caused by hackers' cybercrime and improper use of system resources. The IoT should configure to ensure

simple and secure usage control. Consumers need trust to get the most out of the IoT, enjoy its benefits, and avoid security and privacy risks. As mentioned earlier, most IoT devices and services are exposed to many common threats such as viruses and denial of service attacks.

IoT and risk management research focuses on providing the best tools for complete IoT security. However, it is not enough to take simple steps and tools to avoid such threats and address system vulnerabilities. Therefore, it is important to ensure a smooth process of policy implementation, supported by rigorous procedures. The security development process requires a thorough understanding of system resources to identify various possible vulnerabilities and threats. You need to identify the system assets [8].

## 3. Motivation for the paper

The significant growth of the IoT provides many chances such as social network and intelligent things to provide specific applications or services to the end users. However, IoT leads to increase the security challenges and risk management. Thus, the aim of IoT cybersecurity is to decrease the cybersecurity risks and protect the users and organizations through the protection of IoT. Therefore, the purpose of this paper focused on the IoT and risk management.

## 4. Problem statement

The contribution of the paper is to identifying the risks and mitigate safety risks. The security and confidentiality of Internet of Things (IoT) raises the discussion these days due to IoT occurs when rising and dominant and driving technological progress. IoT is provided a huge number of things in the form of other smart devices that promote smart TV and life. [8] As a result, the purpose of this paper is to examine the security issues facing IoT devices and the IoT environment in order to recommend strategies to mitigate these issues. Three key issues considering in this study are:

1- What are the main risks of that security that corresponds to the IoT device?
2- What best practices can apply to mitigate these risks?
3- What does role of cyber risk management with IoT?

## 5. Research Methodology

This paper has been conducted Systematic Literature Review (SLR) methodology. It was evaluating and interpreting all available previous researches' results that related to the role of risk management with IoT. It also identifies and analyzes key cybersecurity attacks in IoT to achieve the objective of cybersecurity, which are confidentiality, integrity and availability.

This paper used PRISMA in order to select the suitable paper to analyze. First, the research strings formatted as IoT AND Risk management, (vulnerabilities OR risks OR attacks) on IoT. The research applied on Google scholar and research gate website and it focuses on papers published during 2016 to 2022 with content related to IoT and cyber risk management. There are three stages in PRISMA, which are identification, screening and included stages. First, in identification stage, we removed 50000 duplicated records and removed 100,000 for other reasons from google scholar database. Also, we removed 9025 records from research gat website. Next stage, which is screening, we removed 3550 papers which have data duplication and 1555 papers contains only abstract. Also, we excluded 895 papers which have unspecific goal. Twenty-five papers written in foreign language executed. Finally, in included stage, we selected 25 papers from google scholar database and 10 papers from research gate. (See figure2)

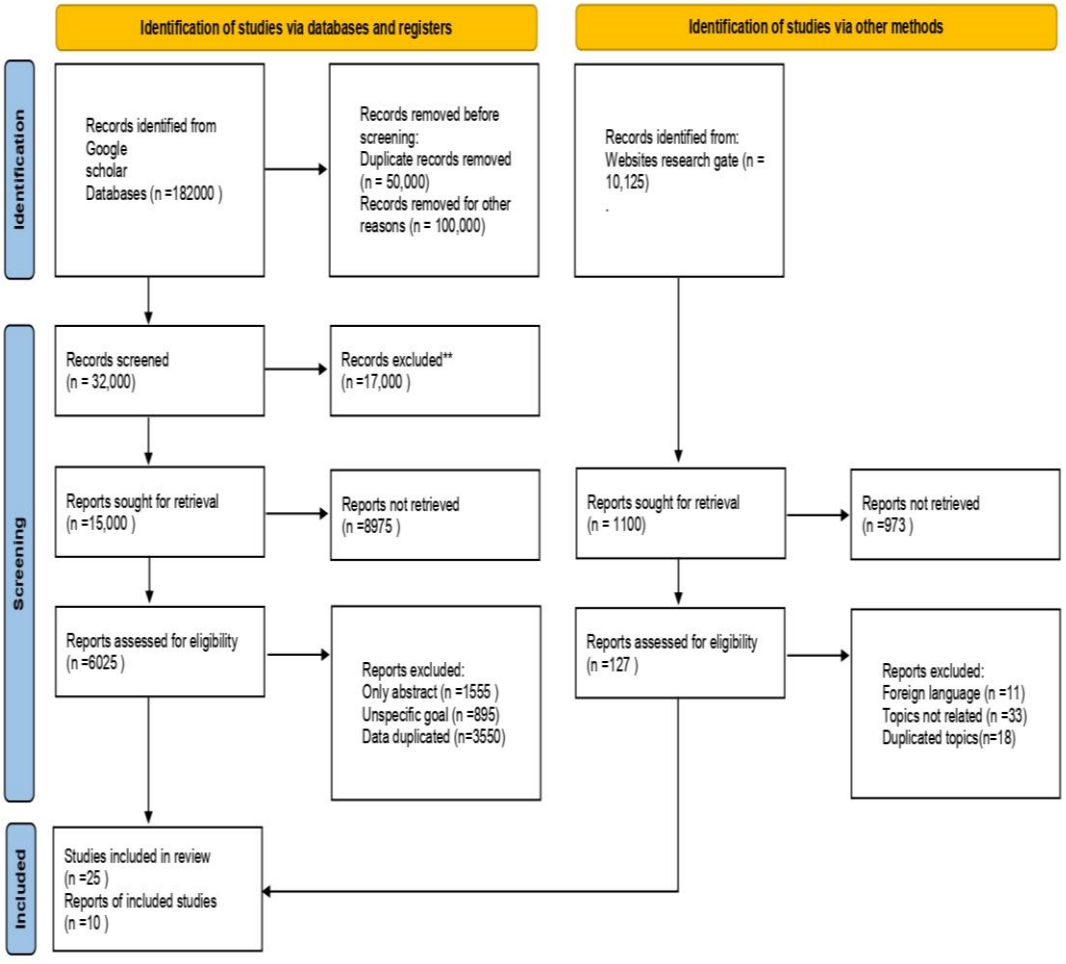


**Figure 1**. PRISMA

## 6. Literature Review

The following is a brief explanation that describe the related works and findings in order to achieve the purpose of this paper. The purpose of the study of Atlam et al was to conduct a review of various risk estimation techniques related to dynamic access control models in order to perform and select the appropriate risk estimation technique for the IoT. Moreover, it contributed to the fact that security and privacy are regarded as the most difficult challenges to address due to the dynamic and heterogeneous nature of the IoT system. Access control models are the fundamental building blocks for addressing the IoT's security and privacy challenges. The access control model is used to ensure that only authorized users have access to system resources in order to achieve the cyber security objectives of system integrity and confidentiality. Traditional and dynamic access control models are the two types of access models. Traditional access models rely on predefined policies that produce predictable results in a variety of situations. As a result, these approaches are useless in the IoT system. Dynamic access control approaches, on the other hand, are based on policies and dynamic contextual features that are estimated in real-time. As a result, these approaches are beneficial in the IoT system. These approaches are based on trust, history, risk, and operational necessity. NIST demonstrated that the Risk Adaptable Access Control (RAdAC) model dynamically permits or denies access requests based on the estimated risk of each access request. As a result, it has greater flexibility in accessing system resources, making it a suitable model for IoT. The paper discovered that there are requirements for selecting the appropriate risk estimation technique of the risk-based access control model for the IoT system. These requirements include dynamic interaction, scalability, limited resources, and data availability. [1]

The purpose of the study of Abbass et al, was conducting the efficient Security Risk Assessment (SRA) to analyze security risks of IoT infrastructure. It contributed that IoT connects with devices have vulnerabilities that may exploit by attackers and affect sensitive data. There are variety of SRA approaches, which are standards and methods. Adopting these approaches will affect IoT performance and security. As the result it needed to adopt a new SRA approaches which is ELK stack and Plan Do Check Act (PDCA) cycle to proactive and reactive towered the risks of IoT in order to reduce the spreading impact. ELK stack reduced the tangible and intangible security risks by fast assessment. It contains three components that are Logstash, Elasticsearch and Kibana. It is a real time fast assessment. PDCA cycle incorporated with ELK stack to make the approach systematically documented. The study discovered that the approach emphasizes SRA knowledge, but it lacks a systematic knowledge protection strategy. [2]

The purpose of the study of Radanliev et al was to provide new risk assessment models for IoT and calculating their economic impact. It contributed that with the growth of IoT, the attack increase. Thus, it must safe the IoT deployment. For calculating the economic impact of IoT cyber risks, this study adapted two established models for predicting MicroMort and uncertainty - the Cyber Value at Risk model. MicroMort used to identify the level of financial risk. Cyber value at risk used to calculate the cost of averting a fatality. As the result, the risk model allows for the determination of an acceptable level of IoT risk. In the future, the proposed assessment approach and IoT MicroMort model could serve as a valid model for calculating IoT cyber risk. [3]

The purpose of the study of Vashi et al was identifying the architecture of IoT in intelligent world, the security challenges in IoT and their countermeasures. It contributed that IoT has five layers, which are Perception Layer, Network Layer, Middleware Layer, Application Layer and Business Layer. Each layer has its own security issues that need to control. Due to nodes in the perception layer operate in the external environment, it is vulnerable to attackers by intercept the sensor nodes of IoT devices. The transport layer is a primary part in IoT because it transmits a lot of information through the layers. Thus, it faces many security issues such Authentication problems, Sybil Attack, Sinkhole Attack, Sleep Deprivation Attack and Denial of Service (DoS) Attack. The security issues of the application layer are Malicious Code Injection, Denial-of-Service (DoS) Attack, Spear-Phishing Attack and Sniffing Attack. As a result, the study identified IoT security controls such as Encryption, which used to provide security of the network layer. In addition, RFID electronic tag used to ensure that sensitive information accessed by authorized reader. This achieved the confidentiality. Sensor nodes in perception layer must authenticate to prevent DoS attacks. In addition, OpenID framework used to provide authentication. OAuth is a standardization framework for approval purposes. Access control used to prevent unauthorized to access the resources. Filtration devices between the transmission layer and the application layer to ensure the network is unblocked. Finally, it discovered the challenges in the study could be the direction of research on future work of IoT security due to it is very important in the modern life. [4]

The purpose of the study of Abu Bakar et al was identifying security risks and challenges in IoT in healthcare. Moreover, it was providing security risk model of IoT in healthcare sector. It provided comprehensive process of risk management. It contributed that IoT used in wide range of applications such as healthcare sector. In addition, IoT reduces the cost of services in healthcare and provides high quality of services. Healthcare database created health records, which used to provide services to patients. Therefore, using IoT in healthcare will make it vulnerable to threats and exploitation by attackers because there is no awareness. Privacy in Healthcare application is a challenge in healthcare IoT implementation because it contains sensitive information like personal details and history medical for Patient that need to be confidential. Thus, the healthcare applications that depend on IoT may be vulnerable to threat by attackers. Another challenge is sensitive information send directly to the cloud or datacenter, which lead to increase the costs and unlock security. The IoT security risks management model considered three things, which are IoT Security Technology, IoT Safety and System Security Assurance and IoT Network Infrastructure Safety. This study recommended using ISO/IEC 27005:2018 standard in order to build an efficient risk management [5].

The purpose of the study Traian was to study to support IoT adopters and propose an effective IoT risk management strategy to eliminate security problems. The study also discussed the best security practices that fall under the IoT SRM2 model. These practices have been classified in the form of a hierarchical intrusion in three stages, and these stages contain 16 goals and 30 controls in order to design a good methodology to manage the risks of the Internet of Things. This study also discussed the critical evaluation of some security best practices for the risks of the Internet of Things [6].

The purpose of the study of In Lee was discussing IoT cybersecurity tools and cyber risk management frameworks. The study indicates that the IoT security market is expected to grow by 33% from 2018 to 2023, as IoT technologies are still evolving and the lack of IoT cybersecurity has resulted in an increase in attacks. In addition, the study provided a four-layer IoT network risk management framework, namely network IoT ecosystem layer, IoT network infrastructure layer, IoT network risk assessment layer, and IoT network performance to identify users, internal , external technologies and risks, and define IoT solutions. Furthermore, it applied the LP model in risk assessment with a smart room scenario, like a smart room in a hotel, containing accessible voice commands and optimized for mobile devices. LP model allocates resources in different types of IoT projects. It recommends improving the LP model to prevent risks from IoT devices that support 5G technology [7].

The purpose of the study of Kandasamy et al was to review risk assessment methodologies and how they fit with IoT. In addition, it identified the risks of IoT in term of risks category and impacts. The Open Web Application Security Project (OWASP) used to identify the vulnerabilities for the IoT architecture. The physical security in IoT is the basic vulnerability that exploited by attackers. The IoT security risks ranked into three layers, which are application, network, and hardware layers. He discussed several examples of risk types such as ethical IoT risks, security and privacy IoT risks, and technical IoT risks. This study uses DempsterShafer Theory and Cybersecurity Game Theory, which are IoT risk assessment theories to examine IoT cybersecurity risks. Furthermore, he reviewed four types of frameworks namely IOS, NIST, OCTAVE and TARA. Finally, he introduces the risks of the Internet of Medical Things (IoMT) and uses ranking methods to devise effective risk reduction strategies and techniques. This study developed a computational approach to computing network risk for IoT systems, providing opportunities for other researchers to investigate IoMT risk. [8]

The purpose of the study of Nurse et al was to identify new cybersecurity risk assessment approaches for IoT. It contributed there are strong need for new risk assessment approaches due to the existing cybersecurity risk assessment approaches are not suitable for IoT. There are tools used periodically to risk assessment such as NIST SP800-30, ISO/IEC 27001 and OCTAVE. Risk assessment approaches are not suitable for IoT because their periodic assessment emerge new system each time. In addition, the risk assessment focused on identifying the risks of exist system and challenge of understanding the glue. Finally, the asset could not be considered an attack platform. The challenges of IoT is a complex technology, it is able to expand or shrink in scale, remote control that means out scope for future of IoT. The existing risk assessment failure to determine the risks in IoT. It recommended in IoT risk assessment to provide early warning of risks. [9]

The purpose of the study of Salami was to discuss the concept of IoT and how it does us full in the life. In addition, it contributed how smart home and smart car used IoT in order to perform the function of smart home and car. Finally, it discussed the importance of risk assessment for IoT. [10]

The purpose of the study of Almousa et al was to provide a new approach to manage the risks of IoT. At the beginning, it contributed the risks and vulnerabilities of IoT such as data flow in memory. It divided the security challenges of IoT into four layers, which are security challenges in application layer, security challenges in architecture, security challenges in communication and security challenges in data protection. Moreover, it reviewed some of risk management framework such as NIST published well-crafted risk management technique. This technique starts by framing the risk and end with monitoring the risk. Finally, it proposed a new approach, which is, integrate the risk management process in the development life cycle of the IoT device itself. This allows evaluating the risk management in all functions of the IoT device. It is effective and required less user [11].

The purpose of the study of Latifi et al was discussing a COBIT5 (Control Objectives for Information and related Technology) framework for IoT risk management. It is a good framework due to it is in line with other framework. At the beginning, it discussed some risks of IoT and the role of COBIT5 with them such as third party suppliers and vendors' risk. The role of COBIT5 is reducing action; this is useful for data loss reduction and cost optimization. In addition, it provided the best practices of COBIT5 framework in IoT such as how does this framework fit with other standard frameworks. It provided better performance, save time and cost [12].

The purpose of the study of Ahmed et al was to identify the basic threats and attacks of IoT. In addition, the basic architectural issues such as lack of data encryption in perception layer, DDoS attacks, man-in-the-middle attacks in network layer and weak interface of IoT devices in application layer. In addition, it reviewed some countermeasures to secure IoT such as improved and redesigned IoT security algorithm. Finally, it discussed the future security of IoT. [13]

The purpose of the study of Köylü et al was to identify the architecture and basic and new applications and technologies of IoT and their challenges, which need to control. It contributed that distributed computing will hacked due to incorporated information stockpiling and registering structure such as Google. The cloud sellers can manage and provide good tools for clients, but the programmers can use any technique to achieve their goals. Moreover, it discuss 8 types of attacks that need to consider in fog computing which are Forgery , Tampering, Collusion, Spam, Man-in-the-Middle, Eavesdropping, Impersonation and Denial-of-Service. It discussed the challenges and security of IoT that are bandwidth, regulation, and compatibility, with continuous of innovation of IoT and needs the technologies to converse with one another are running distinctive programming forms, a wide range of execution issues and security weaknesses can result. Customer expectation, if the product of IoT not like customer expectation, it will be a challenge to IoT companies. Security and privacy are the most challenges in IoT. [14]

The purpose of the study of Millar and Rapid was to review the IoT topologies, IoT layers and IoT standardization efforts and protocols. In addition, it reviewed the vulnerabilities of IoT like malware worm, which caused massive disruption to Iranian nuclear centrifuges. In addition, it reviewed common IoT attacks such as the sinkhole attack, the HELLO flood, DDoS and man in the middle attack. It reviewed CISCO's IoT model, which has seven layers and aimed to secure all process and communication and movement. The suggested countermeasures are Intrusion detection systems (IDS) and RFID specific mitigations. The need for channel-based security solutions and standardized protocols is clear and backed by regulatory guidelines. [15] The purpose of the study of Lam K and Chi C was identify the concept of Identity in the Internet-of- Things (IDOT) which is multi factors authentication in IoT and compared it with Identity of Users (IDoU) in order to use IDOT in practical implementation. Finally, it introduced the related issues of IDOT such as cost of large IoT network. [16]

The purpose of the study of Efe et al. was to discuss that IoT faced many type of attacks. It discussed how to provide smart security against the common attack in IoT which ia DDoS. IoT used in daily life and provides convenience for example, smart car, health care…etc. This leads to appear the security challenges of IoT such as authentication, Denial of Service (DoS) attacks and Data Aggregation. [17]

The purpose of the study of Tandon S was to illustrate the privacy Security is the source of security risks and it recommended some relevant ways to prevent IoT risks. It started with IoT architecture and its security issues. Finally, it reviewed the security measures like encryption and hashed based security and SDN & IoT, which provides one single efficient architecture. [18]

The purpose of the study of Yang Y et al. was to present the limitations of IoT devices and their solutions such as battery life extension issues by increasing the capacity of battery, although the design of IoT devices is lightweight and small. It discussed IoT attacks classification and security issues in the application layer, transport layer, network layer and perception layer. [19]

The purpose of the study of Shah P et al. was to review many applications of IoT such as Industrial IoT, connected home and CoAP protocol, which used in GPS for transportation. It presented the challenges of these networks. In addition, the future of IoT. [20]

The purpose of the study of Ștefan V et al. was to identify the security and safety of IoT. This study reviewed the layered of ZigBee wireless sensor network model. The layered of model are application, Data, TCP, UDP, IP, Adaption, Network, Data link and physical. In addition, it presented the threats which could affect the security of IoT layered model such as DDoS and DoS affected IP layer. Finally, it presented the suitable measures for these threats in order to achieve the efficient security such as using firewalls, filtering for DDoS attack. [21]

The purpose of the study of Azrour. M was to present the security issues and challenges of IoT environment in order to ensure that authentication techniques used in proper way to secure IoT service. It discussed the connected devices increase and it will be more than 50 billion by 2030. The examples of security challenge and issues in IoT are DoS, replay attack, spoofing attack, password guessing attack and insider attack. Finally, it presented the authentication techniques for IoT such as one time password (OTP), certificate-based authentication, encryption cryptography and blockchain. [22]

The purpose of the study of Rekha S et al. was to discuss some security issues of IoT, which are data integrity, encryption capabilities, privacy issues, authentications and common framework. It illustrated that there are around 70% limitations in IoT products. Therefore, it must create suitable strategies. It provided solutions to security of IoT like building security in IoT development, authentications, develop a security mindset and encryption technology. [23]

The purpose of the study Prokofiev et al was to identify the compromised IoT devices. In addition, it discussed the basic security problems for IoT, which is allowing unauthorized access. It discussed the basic cybercriminals in IoT, which is botnets and its lifecycle. Finally, it proposed logistic regression model in order to estimate the probability of attack. [24]

The purpose of the study of Toka K et al. was to identify how blockchain provides security to IoT. This study used Hyper ledger Fabric blockchain network in order to achieved the objective of cybersecurity which are availability, integrity, confidentiality, accountability and authorization in IoT devices. In addition, the approach in this study presented in term of network security dimensions. Finally, it discussed that Hyper ledger Fabric blockchain network approach will solve IoT security issues. [25]

The purpose of the study of Dilawar et al. was to identify the role of blockchin in the internet of medical things (IoMT). Blockchain is providing security between connected nodes in order to transmit data. In addition, it discussed that blockchain stores small amount of data and IoMT data is huge and sensitive. Therefore, the solution would be storing the data in separate off-chain storage system. [26]

The purpose of the study of Kokkonis was to discuss that internet of things is growing and transmitting a huge amount of data. Therefore, it must make sure the IoT devices to be secure. Thus, it reviewed blockchain security features. It will be the best solution for decentralized, and trustless. It achieved the security principle, which are availability, confidentiality and integrity. [27]

The purpose of the study of Emam et al. was to identify how security is very important to ensure the sustainability of IoT technologies and confidentiality, integrity, availability (CIA) and privacy. It presented the security issues of IoT devices such as DDoS, SQL injection and physical theft. It presented blockchain, which based on security and trust. Then, it proposed IoT with blockchain framework to ensure strong validation and security process based on integration between consensus algorithms of blockchain. Moreover, it reviewed how to direct IoT transactions to suitable Bitcoins algorithm by using direction algorithm. The proposed framework includes fives elements which are IOT Sensors , Smart Contract , Direction Sensor, Blockchain Network and Blockchain Node. Finally, the study concluded that proposed framework is very useful due to it provides high level of performance by providing high level of security, stability and respond time. [28]

The purpose of the study of Haque et al. was to using blockchain to secure IoT technologies. It discussed that IoT shares information and authenticate data through the central server. Therefore, the security issues increased. Thus, it proposed integrate blockchain with IoT in order to enhance the security, privacy and reliability because the blockchain decentralized and verify all transactions of IoT technologies. Finally, it concluded that the blockchain also has limitations like difficulties with scalability, but it still the suitable solution for IoT security issues. [29]

The purpose of the study of Dorri et al. was to study the benefit of using blockchain in smart home. It discussed the transactions and basic component of smart home. It concluded that costs worth because it provides high level of security and privacy. [30] The purpose of the study of Ayed et al. was to discuss that IoT technologies basic thing in daily life, but they have problems. Moreover, it discussed the layers of IoT, which are sensor layer, network and gateway layer, service management layer and application layer. It reviewed the challenges of IoT such as unsecured devices and provided solutions such as using ideal cryptography algorithm. The study proposed security framework based on blockchain in IoT, which includes physical layer, Communication Layer and interface layer. [31]

The purpose of the study was to present that IoT devices provide different types of services that impact the life, the security issues will be appear. It review the security issues such as DDoS and data authorization .therefore, the paper suggested using blockchain in IoT in order to collect, transit, and process data without any security issues. Finally, it reached that integrate blockchain with IoT provide features like security, decentralization and transparency. [32]

The purpose of the study Yeasmin and Baig was to present the suitable security solutions for IoT, which used in industrial field (IIoT). It proposed to use Hyperledger Fabric Blockchain in IIoT, which called permissioned blockchain in order to ensure the security, authentication and authorization. It contains three component that are Certificate Authority, Membership Service Provider and Peers. [33]

The purpose of the study was to discuss how blockchain is useful in identifying security issues of IoT. It discussed the blockchain types, which are public, private and Consortium. In addition, it discussed the needs for integrate IoT with blockchain. In other side, it discussed the challenges of integrations such as Data Privacy and Anonymity. [34]

The purpose of the study Sagirlar et al was to identify P2P botnets, which compromise the IoT. The study proposed botnets in order to detect the botnets in IoT devices. In addition, it discussed AutoBotCatcher's BFT blockchain. Blockchain used in order to create dynamic network and allow multiple devices collaborate to discover botnets. Finally, it discussed the future work and it will be AutoBotCatcher by based Hyperledger blockchain to ensure the privacy and detect botnets. [35]

**Table 1.** Literature Review IoT and Cybersecurity Risk Management

| NO | Reference | Type of the article | Risk of IoT | Countermeasure | Findings |
|---|---|---|---|---|---|
| 1 | Atlam et al | Review | Security and privacy of IoT challenges. | Access Control Models. | RAAC has greater flexibility in accessing system resources, making it is a suitable model for IoT. |
| 2 | W. Abbass et al | Review | IoT tangible and intangible security risks such as DDos breaches that lead to loss sensitive data. | ELK stack And Plan, Do, Check, Act (PDCA) cycle. | The approach emphasizing SRA knowledge, but it has a lack systematic knowledge protecting strategy. |
| 3 | Radanliev et al. | Review | DDoS attack | updating the CMMI with the ISO 9001 criteria – NIST - FAIR approach- Cyber Value at Risk model and the MicroMo. | Provide acceptable level of risk after using proposed model which is Cyber Value at Risk model and the MicroMo. |

| | | | | | |
|---|---|---|---|---|---|
| 4 | Vashi et al | Practical | leakage of confidential information, tampering, terminal virus. and Denial of Service (DoS) Attack, Malicious Code Injection etc. | Encryption - RFID electronic tag-authenticate - OAuth- Access control - Filtration | The controls prevent unauthorized access; provide confidentiality, authentication. More over prevent DoS attack. |
| 5 | Abu Bakar et al | Case study | Privacy , Asset Security Management and lack of awareness | ISO/IEC 27005:2018 standard<br><br>Intrusion prevention system and firewall Education and Policies | After using ISO/IEC 27005:2018 standard and other controls, it can build an efficient risk management in IoT. |
| 6 | Popescu et al | Survey | data breaches | ENISA- NIST framework- Model (IoTSRM2) | The proposed model provide good risk management practice. |
| 7 | Lee | Review | Risks in smart hotel such as password cracking and email hacking in order to gain access to user accounts. DDOs . | LP model NIST ISO/IEC 27005 Cyber Kill Chain(CKC) (OCTAVE) is a security evaluation framework. | LP model can adapt to the unique situations of each organization. |
| 8 | Kandasamy et al. | Review | IoT and Internet of Medical Things risks | RAP frameworks like NIST, ISO/IEC, and OCTAVE , CSRF. | The existing technique useful but it needs to provide a new approaches. |
| 9 | Nurse et al | Review | The risk of IoT and risk assessment. | NIST SP800-30, ISO/IEC 27001, OCTAVE, CRAMM and EBIOS. | The risk assessment approaches must fit with nature of IoT technologies. |
| 10 | Salami | Review | Not discussed | Not discussed | It must perform risk assessment for IoT. |
| 11 | Almousa et al. | Review | IoT risks such as data flow, Physical Attacks - Network Attacks - | NIST SP 800-30 ISO 27005. Integrate the risk management process in the development life | The recommended countermeasures fit with IoT devices. |

| | | | | | |
|---|---|---|---|---|---|
| | | | Software Attacks - Encryption Attacks. | cycle of the IoT device itself. | |
| 12 | Latifi et al | Review | Data and application, Physical environment, Change management, Third-party supplier and vendors, Security and Privacy, Infrastructure, Legal and regulatory. | COBIT5 framework for IoT risk management. | Using this framework will reduce loss data, increase cost effectiveness, and mitigate the risks. |
| 13 | Ahmed et al | Review | bandwidth - regulation- compatibility- customer expectation- Security and privacy | Not discussed | There is issues related to IoT customers, which need to consider. |
| 14 | Köylü et al | Review | DDos , Man in the middle, Weak interface of IoT. | Improved and redesigned IoT security algorithm.<br><br>Enhance the architecture of IoT. | It is a theoretical aspects, and not practical implementation. |
| 15 | Millar and Rapid. | Survey | DDoS , Man in the middle , Hello flood , sinkhole attack | Application data security, Intrusion detection systems, Choice of protocol, RFID specific mitigations, Reducing risk with legislation. | In the future, the IoT will face different attacks. |

| | | | | | |
|---|---|---|---|---|---|
| 17 | Efe et al. | Review | Authentication<br><br>Denial of Service (DoS) attacks,<br><br>Man in the Middle Attacks<br><br>DDos | Durable hardware<br><br>Updating/patching<br><br>Cryptographic | There are deficiencies in some IoT security solutions. |
| 18 | Tandon et al. | Review | Man in the Middle , DDoS , Stoarge attack, Malicious Code Attack, )Replay Attack | encryption and hashed based security and SDN & IoT | Risk management in IoT develops gradually. |
| 19 | Yang Y et al | Survey | Nodes physically attacked (faulty node)<br><br>Dynamic ecosystem issues<br><br>Authentication issues<br><br>DDoS | Using WSN<br><br>lightweight Mobile IPv6 with IPSec<br><br>Pre-validation, session resumption, and handshake delegation.<br><br>Using compromised IoT devices running the Mirai malware. | It must to develop strong security standard for IoT. |
| 20 | Shah. et al | Survey | IoT is interoperability risk. | unified standard for various technologies is required | There are wide range of IoT applications that needs to communicate with each other. |

| | | | | | |
|---|---|---|---|---|---|
| 21 | Ștefan et al | Review | Tampering<br>Jamming<br><br>Eavesdropping<br><br>Spywares<br><br>DoS, DDoS<br><br>System failure | Isolation<br>Frequency spread<br><br>Unsophisticated encryption<br><br>Antispyware software<br><br>Firewalls, filtering<br><br>Replication and recovery | The security related to power and cost need to consider. |
| 22 | Azrour et al | Review | DoS, replay attack, spoofing attack, password guessing attack and insider attack | One time password (OTP), certificate-based authentication, encryption cryptography and blockchain. | It must enhance the countermeasures of IoT . |
| 23 | Rekha et al | Review | data integrity, encryption capabilities, privacy issues, authenticatios | Building security in IoT development, authentications, develop a security mindset and encryption technology. | The security countermeasure in the study reduce the security issues of IoT. |
| 24 | Prokofiev et al | Review | DDoS attack | logistic regression model | The proposed model useful to detect the IoT compromise. |
| 25 | Toka et al | Review | Not dised | Hyper ledger Fabric blockchain network | The proposed approach can solve IoT security issues. |

| | | | | | |
|---|---|---|---|---|---|
| 26 | Dilawar et al. | Review | Not discussed | Blockchain IoMT architecture. | The proposed architecture does not solve the storage problem. |
| 27 | Kokkonis. | survey | Confidentiality , integrity and availability issues | Blockchain | Blockchain is not suitable solution in all IoT devices issues. |
| 28 | Emam et al. | Practical | SQL injection and XSS, Coding errors, buffer overflow, Clear text protocols and unnecessary open ports, DoS / DDoS, Physical theft and Sybil attack. | IoT with Blockchain algorithm framework (direction algorithm) | The proposed framework is useful to secure IoT devices, but in the future the authors will experiment different blockchain algorithm. |
| 29 | Haque et al. | Review | There are security issues, privacy issues, legal issues and economic issues. | Integrate Blockchain with IoT | It is the suitable solution for iot security issues. |
| 30 | Dorri et al. | Case study | DDoS and linking attack | Blocchain in smart home | The cost worth due to it provides high level of security and privacy. |
| 31 | Ayed et al. | Review | Unsecure devices – privacy | Blockchain | The blockchain is good solution for iot security issue but it needs coding algorithm due to blockchain is variety. |
| 32 | Kumar et al. | Review | DDoS Authorization issue | Blockchain and IoT Reference Model layers. | It used to secure the IoT ecosystem. |

| | | | | | |
|---|---|---|---|---|---|
| 33 | Yeasmin and Baig. | Practical | Not discussed | use Hyperledger Fabric Blockchain in IIoT | The proposed solution allows to achieve the objective of cybersecurity CIA with access control. |
| 34 | Ekanayayake and Premarathne. | Review | Heterogeneity , Interoperability and Autonomous control | Blockchain | Integrating iot with blockchain has challenges. |
| 35 | Sagirlar et al | Review | DDoS attack | AutoBotCatcher' s BFT blockchain | The proposed solution used to detect botnets in IoT devices. |

## 7. Result and discussion

This section illustrated the findings of analyzing previous studies in order to answer the main questions of this paper.

### 7.1 Q1: What are the main cyber risks that corresponds to the IoT device?

This section illustrated the findings of analyzing previous studies; there are many types of risks in IoT, which are privacy risks, security risks, technical risks and ethical risks. The below table provides summary definitions and some examples of risks with IoT. Table
There are three previous studies indicates that privacy risks represent in data breach, data flow and email hacking. (See figure 3)

In security risks, there are 15 studies have been indicated DDoS attack is the most security risk in IoT and five studies have been indicated that DoS attack is another security risk in IoT. There are four studies have been indicated that Man in the middle attack and Malicious code injection are security risks in IoT. In addition, there are two studies indicated that virus, password cracking and encryption attack are the security risks in IoT. There is one study indicated that linking attack is a security risk in IoT. Also, there is one study indicated that confidential issues, spoofing attack, insider attack, spyware, replay attack and software attack are security risks in IoT. (See figure 4) For Technical risks, there are two studies have been indicated authentication is a technical risk in IoT which must consider. Two studies have been indicated that authorization issue is another technical risk in IoT. Availability issue also consider in two studies as technical risk in IoT. One study has been indicated that open unnecessary port is another technical risk in IoT. Coding error is another technical risk in IoT which indicated by one previous study. In addition, one study has been indicated that the weak interface is technical risk in IoT. The system failed mentioned in one study as technical risk. (See figure 5)

For Ethical risks, there is one study indicate that integrity issue is an ethical risk in IoT. In addition, there is one study indicate that the honesty is the ethical risk in IoT. Finally, there is one study indicated that fraud is another ethical risk in IoT. (See figure 6)

**Table 2.** Summery of IoT risks

| Type of risk | Definition | Key words |
|---|---|---|
| Privacy risks | When an organization loses control of its data, whether temporarily or permanently. | Data breach- data flow Email hacking |
| Security risks | Taking advantage of system flaws to gain access to assets with the intent of causing harm. | DDoS- Dos - Man in the middle attack - Malicious code injection – Virus- password cracking encryption attack - linking attack - Confidential issues spoofing attack- insider attack spyware- reply attack - software attack |
| Technical risks | This is caused by hardware or software failure as a result of poor design, evaluation, or other factors. | Authentication - Open unnecessary port - coding error - weak interface - system failed - Authorization - availability issues. |
| Ethical risks | This refers to the unanticipated negative consequences of unethical behavior using IoT devices. | Integrity issues- honesty- fraud |

,

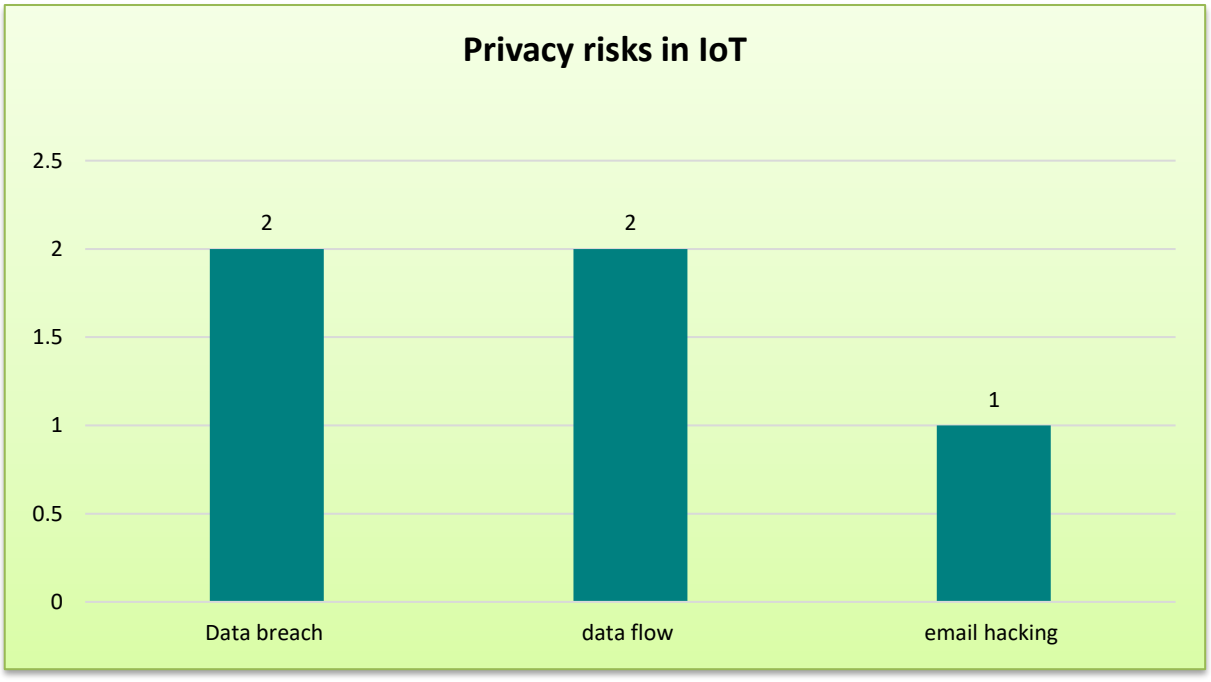


**Figure 2**. Privacy risks in IoT

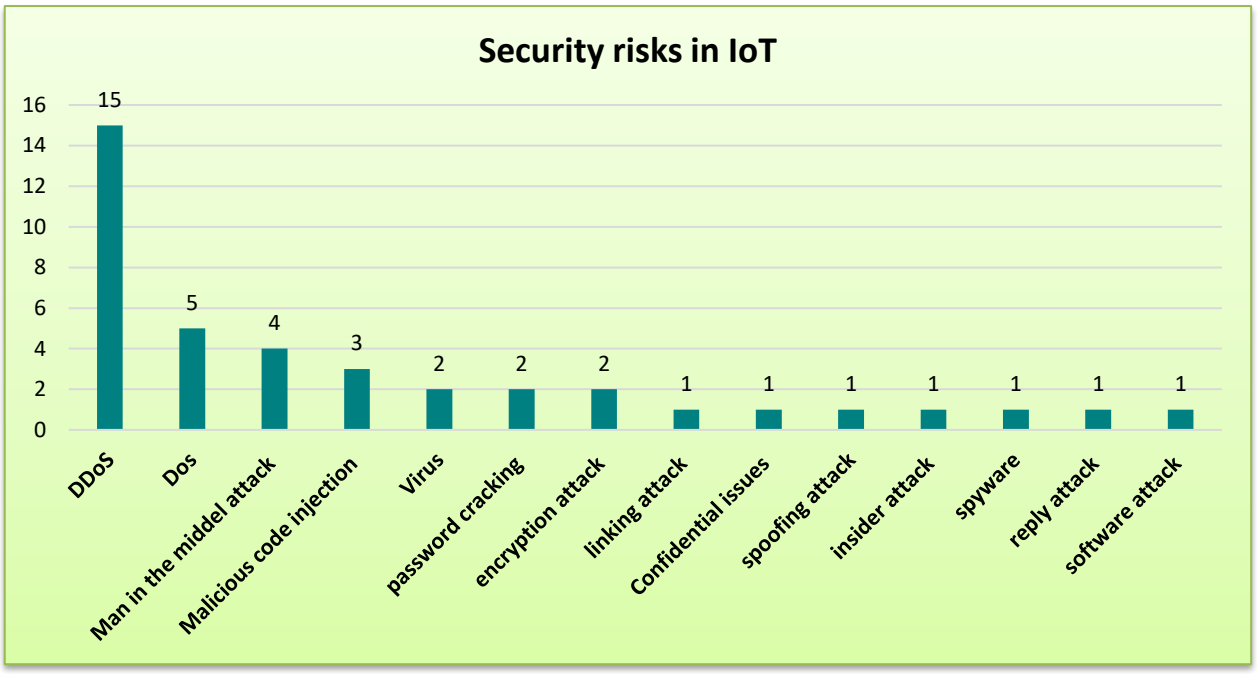


**Figure 3.** Security risks in IoT

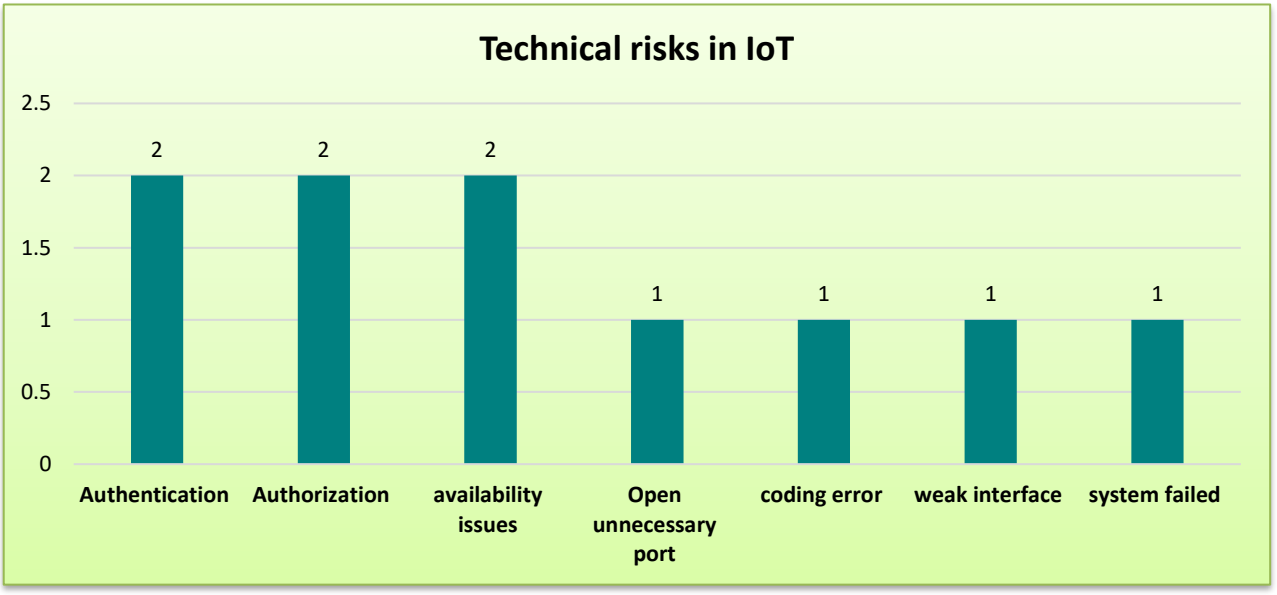


**Figure 4.** Technical risks in IoT

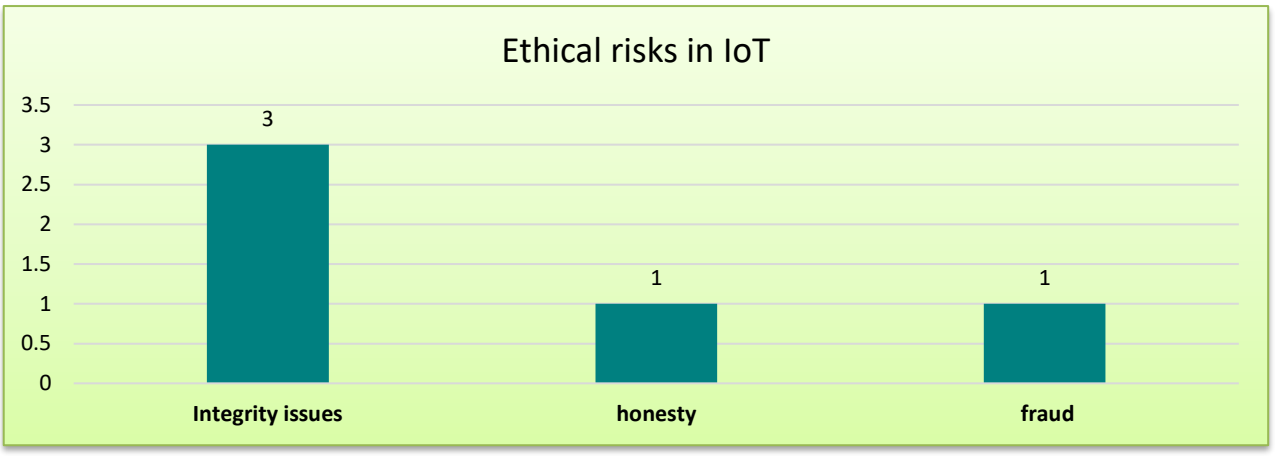


**Figure 5.** Ethical risks in IoT

### 7.2 Q2: What are best practices can apply to mitigate security risks in IoT?

This section illustrated the most important findings reached through the analysis of 35 previous studies, namely that there are many common ways to mitigate the risks of IoT. The below figure2 indicates that (12) previous studies have been used blockchain to mitigate security risks of IoT devices because it provide a single point of failure. In addition, there are around (6) studies have been used authentication technique and (5) studies have been used encryption in order to mitigate the security risks of IoT devices. Two studies illustrated that WSN used to mitigate the security risks and other two studies illustrated that firewall filtering used to reduce the security risks in IoT devices. The other study illustrated that access control, recovery, logistic regression model, antispyware virus and intrusion detection system have been used to mitigate the security risks in IoT devices. See figure 7)

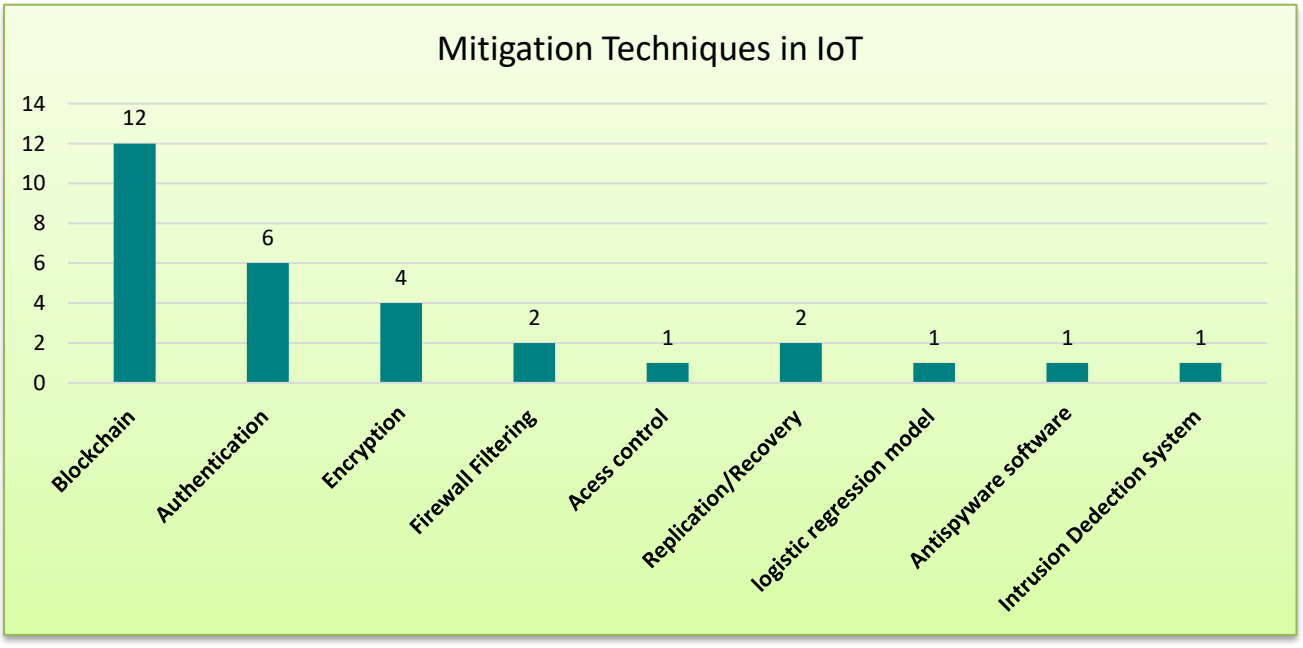


**Figure 6.** Mitigation Techniques in IoT

### 7.3 Q3: What does role of cyber risk management in IoT?

Based on analyzing 35 previous studies, we conclude that there are many and complimenting risk management frameworks and models that can be used in IoT devices. Theses risk management frameworks and models created to government and commercial organizations in order to be able to customize and manage risks in IoT devices. The previous studies indicated that there are (7) studies have been used ISO framework in IoT devices to manage the risks. In addition, there are around (6) studies have been used NIST framework in risk management of IoT devices. Three studies used OCTAVE framework in risk management of IoT devices. There are nine studies, each of them contains a specific model of risk management models, which are ELK stack, PDCA cycle, CKC, CSRF, CRAMM, COBIT5,IoTSRM2 model and cyber value at risk model. See figure 8)

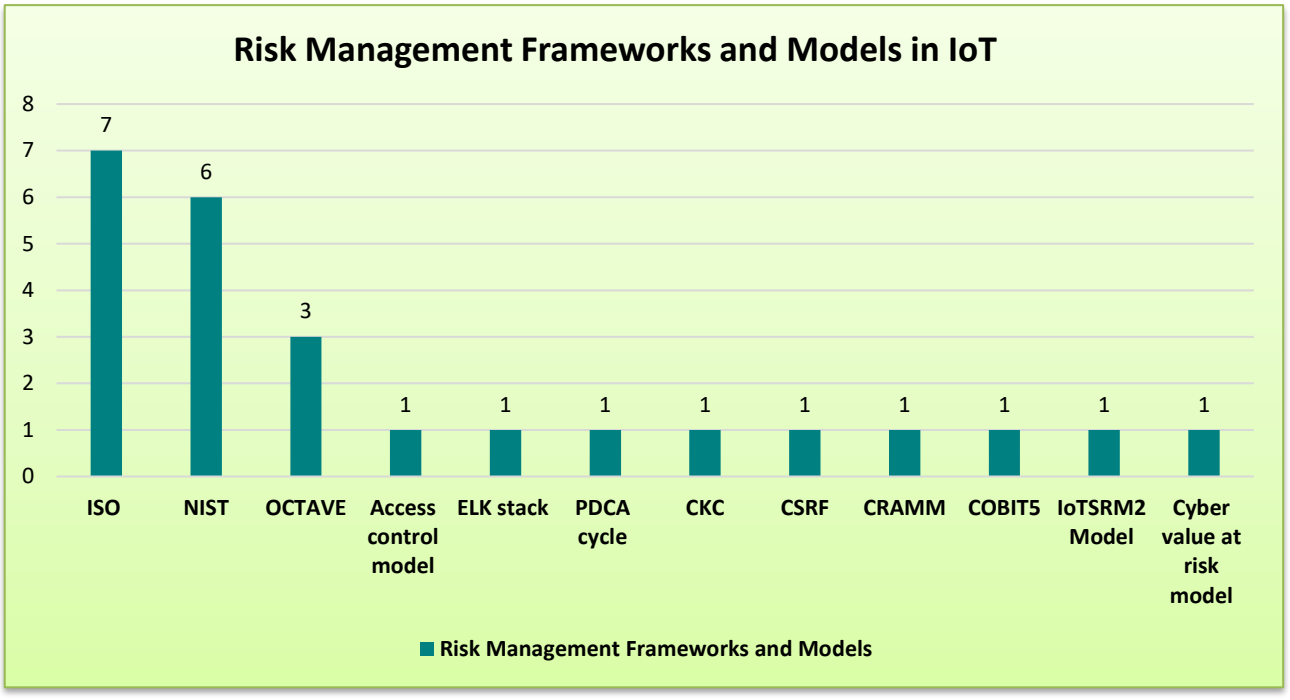


**Figure 7.** Risk management frameworks and models in IoT

## 8. Conclusion and Future work

This paper provides a comprehensive view of IoT risks, which represented in four categories. They are technical risk, security risk, ethical risk and privacy risk. As well as it reviewed the best practices, to mitigate the risks of IoT and it found that blockchain technique is the most tools used to reduce the risks of IoT. In addition, this paper indicates the cyber risk management in IoT. It introduces some of the frameworks that used to manage the risks in IoT such as NIST, ISO and OCTAVE. Finally, this paper concludes that it must consider and address the new risks in IoT devices in order to extending the existing frameworks and designing a new framework for IoT devices and prevent risks.

**Corresponding author**
**Mohammed Almaayah**
m.almaiah@ju.edu.jo

**Acknowledgements**
All authors would like to thank King Faisal University, Saudi Arabia for all supports in terms of labs, funding etc.

**Funding**
This work was supported by the Deanship of Scientific Research, Vice Presidency for Graduate Studies and Scientific Research, King Faisal University, Saudi Arabia (Grant No. KFU 210001).

**Contributions**
M.A; Conceptualization, M.A; Investigation, M.A; Writing (Original Draft), M.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] Atlam, H. F., Alenezi, A., Alharthi, A., Walters, R. J., & Wills, G. B. (2017). An overview of risk estimation techniques in risk-based access control for the Internet of Things. *Proceedings of the 2nd International Conference on Internet of Things, Big Data and Security (IoTBDS 2017)*, 254–260.
[2] Abbass, W., Bakraouy, Z., Baina, A., & Bellafkih, M. (2019). Assessing the Internet of Things security risks. *Journal of Communications*.
[3] Radanliev, P., De Roure, D. C., Walton, R., Van Kleek, M., & Nurse, J. R. C. (2018). Future developments in cyber risk assessment for the Internet of Things. *Computers in Industry, 102*, 14–22.
[4] Vashi, S., Ramani, V., Modi, J., Verma, S., & Prakash, C. (2017). Internet of Things (IoT). *2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)*.
[5] Abu Bakar, M. A., Roslan, N. F., & Abd Rahman, N. H. (2019). The Internet of Things in healthcare: An overview, challenges and model plan for security risks management process. *Indonesian Journal of Electrical Engineering and Computer Science*.
[6] Popescu, G. H., Nica, E., & Mocanu, R. (2021). Leaders' perspectives on IoT security risk management strategies in surveyed organizations relative to IoTSRM2. *Applied Sciences, 11*(9206).
[7] Lee, I. J. (2020). Internet of Things (IoT) cybersecurity: Literature review and IoT cyber risk management. *Future Internet, 12*(157). https://doi.org/10.3390/fi12090157
[8] Kandasamy, V., Kandasamy, K., & Vasan, A. (2020). IoT cyber risk: A holistic analysis of cyber risk assessment frameworks, risk vectors, and risk ranking process. *EURASIP Journal on Information Security*.
[9] Nurse, J. R. C., Creese, S., & De Roure, D. (2017). Security risk assessment in Internet of Things systems. *IT Professional, 19*(5), 20–26.
[10] Salami, F. (2021). Risk management techniques on the Internet of Things. *Journal of Computer Science and Information Systems, 2*(5).
[11] Almousa, M., Althunibat, A., & Almalki, A. (2020). Environment-based IoT security risks and vulnerabilities management. *International Conference on Computing and Information Technology, University of Tabuk*, Saudi Arabia.
[12] Latifi, M., Abhari, A., & Bagheri, E. (2017). A COBIT5 framework for IoT risk management. *International Journal of Computer Applications, 170*(8).
[13] Ahmed, A., Shah, B., & Khan, A. (2020). Internet of Things (IoT): Vulnerabilities, security concerns and things to consider. *11th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*.
[14] Köylü, M., Gökalp, E., & Demir, C. (2021). Review of Internet of Things (IoT) security threats and challenges. *1st International Conference on Emerging Smart Technologies and Applications (eSmarTA)*.
[15] Millar, J., & Rapid, A. (2021). IoT security challenges and mitigations: An introduction.
[16] Lam, P., & Chi, H. (2016). Identity in the Internet-of-Things (IoT): New challenges and opportunities. *Springer International Publishing*.
[17] Efe, A., Aydin, M., & Yıldırım, H. (2018). Smart security of IoT against DDoS attacks. *International Journal of Innovative Engineering Applications, 2*(2), 35–43.
[18] Tandon, N., Sharma, A., & Jain, R. (2020). A study on Internet of Things (IoT) security issues and solutions. *ResearchGate*.
[19] Yang, Y., Wu, L., Yin, G., Li, L., & Zhao, H. (2017). A survey on security and privacy issues in Internet-of-Things. *IEEE Internet of Things Journal*.
[20] Shah, R., & Patel, D. (2017). Applications and challenges faced by Internet of Things – A survey. *ICST Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*.
[21] Ștefan, S., Costin, A., & Bădău, D. (2020). Considerations regarding the security and safety of Internet of Things. *Journal of Computer Science and Control Systems*.

[22] Azrour, M., El Ouahidi, B., & El Ghazi, H. (2021). Internet of Things security: Challenges and key issues. *Security and Communication Networks, 2021*, Article ID 5533843.
[23] Rekha, K., Rani, K. U., & Shobha, G. (2021). Study of security issues and solutions in Internet of Things (IoT). *International Conference on Nanoelectronics, Nanophotonics, Nanomaterials, Nanobioscience & Nanotechnology*.
[24] Prokofiev, I., & Grinchuk, A. (2018). A method to detect Internet of Things botnets. *ResearchGate*.
[25] Toka, L., Cinkler, T., & Forczek, G. (2021). Securing IoT with blockchain. *6th International Conference on Smart City Applications, Karabuk University*.
[26] Dilawar, M. N., et al. (2019). Blockchain: Securing Internet of Medical Things (IoMT). *International Journal of Advanced Computer Science and Applications*.
[27] Kokkonis, G. (2020). Securing IoT systems using the blockchain. *ResearchGate*.
[28] Emam, A. Z., et al. (2020). Securing IoT systems using blockchain algorithms. *Communications on Applied Electronics (CAE)*.
[29] Haque, M. H., et al. (2021). Blockchain technology for IoT security. *Turkish Journal of Computer and Mathematics Education*.
[30] Dorri, A., et al. (2017). Blockchain for IoT security and privacy: The case study of a smart home.
[31] Ayed, A. B., et al. (2020). Blockchain and IoT: A proposed security framework. *17th International Conference on Information Technology–New Generations*.
[32] Kumar, A., et al. (2021). A review on securing IoT with blockchain technology. *Science, Technology and Development*.
[33] Yeasmin, F., & Baig, Z. (2021). Permissioned blockchain: Securing industrial IoT environments. *International Journal of Advanced Computer Science and Applications, 12*(4).
[34] Ekanayake, E., & Premarathne, U. S. (2022). Securing IoT devices using blockchain technology: A review. *ResearchGate*.
[35] Sagirlar, G., Carminati, B., Ferrari, E., Shehab, M., & Lu, H. (2018). AutoBotCatcher: Blockchain-based P2P botnet detection for the Internet of Things. *ResearchGate*.

## Biographies

**Dr. Mohammed Maayah** 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@ju.edu.jo

**Dr. Rejwan Bin Sulaiman** is a highly skilled researcher in the field of artificial intelligence and cybersecurity. Currently serving as a lecturer and module leader at Northumbria University London. His teaching approach combines theoretical foundations with practical applications, fostering an interactive and engaging learning environment. Rejwan believes in equipping students with both conceptual understanding and hands-on skills, enabling them to excel in their academic pursuits and future careers. Rejwan specializes in the areas of cybersecurity, machine learning, and artificial intelligence. He has actively contributed to the field through his research, attending conferences and seminars to present his work and staying up to date with the latest advancements in his domain. https://orcid.org/0000-0002-3037-7808