TMP UNIVERSAL JOURNAL OF RESEARCH AND REVIEW ARCHIVES

VOLUME 4 | ISSUE 2 | YEAR 2025 | APRIL – JUNE 2025

RECEIVED DATE	ACCEPTED DATE	PUBLISHED DATE
10/03/2025	01/04/2025	15/04/2025

Article Type: Research Article

Available online: www.tmp.twistingmemoirs.com

ISSN 2583-7214

CYBER THREATS ANALYSIS IN THE INTERNET OF THINGS

[1]Ali Rafiei Taghanaki

[1] *Department of Information security technology engineering, Applied Scientific Informatics Institute of Iran*

Corresponding Author: Ali Rafiei Taghanaki

ABSTRACT

The present study aims to analyze cyber threats in the Internet of Things (IoT). A descriptive-analytical methodology based on library resources is used in this research. IoT security is a multidimensional subject requiring comprehensive solutions and coordination between manufacturers, policymakers, and users. Through more collaboration in this field, it is possible to transform IoT into a sustainable and secure ecosystem. Although IoT security challenges still exist, with collaborative efforts, we can turn it into a source of wealth to improve lives. Due to the resource limitations of IoT devices, it is difficult to implement strong security protocols. To solve this challenge, various security strategies should be employed, such as lightweight security protocols. The design of cryptographic algorithms compatible with the hardware and resource limitations of IoT devices should be considered by manufacturers.

Keywords: Internet of things, Cyber threats, Security solutions

INTRODUCTION

Nowadays, the Internet of Things (IoT) is recognized as one of the most imperative achievements in the field of information technology. By definition, IoT refers to a set of devices and physical objects capable of connecting to the Internet and exchanging data with each other. These devices are used in various fields, including smart homes, smart cities, industries, health, transportation, and agriculture. Given the increasing number of connected devices and the large volume of data being collected, security has become one of the most imperative challenges in implementing the Internet of Things (Mooha 2021). Basically, IoT security is defined as protecting existing data, information, devices, and communications against various threats, especially cyber-attacks (Hassan 2019). Since most of these devices contain sensitive information and control critical systems such as health, transportation, and energy, a security

breach can lead to serious and irreparable consequences.

Cybersecurity challenges and solutions for the Internet of Things are very important due to the rapid growth of this technology and the increasing number of devices connected to the Internet. In the digital age, the Internet of Things is considered a key concept in realizing smart cities, optimizing industries, and facilitating daily life. However, along with the expansion of this technology, security threats have also increased dramatically. Due to security weaknesses, IoT devices are often exposed to cyberattacks, including data theft, network intrusion, and even distributed attacks such as DDoS. Since most of these devices carry sensitive information, protecting them becomes an essential concern (Madakam et al. 2015). Addressing such challenges requires multifaceted approaches such as educating users, implementing strong security protocols, and regularly updating software. Using encryption for transmitted data and multi-factor authentication can help strengthen the security of these devices. Also, developing global standards for designing and implementing security in IoT seems crucial. Ultimately, collaboration between governments, organizations, and private companies in this field can help establish a more secure ecosystem. Given the growing trend of IoT, defining cybersecurity as a strategic priority helps the sustainable and secure development of this technology (Hassan 2019). Ghobadi (2024) examined the security challenges of the Internet of Things in his research. With the expansion of communication networks, IoT emerged as a platform for connecting objects, machines, and people to each other. The challenges of security and information confidentiality in IoT are of particular importance. The key objective of the paper was to present an efficient model for enhancing security in the IoT context by considering the existing security challenges (Ghabadi 2024). Magami (2023) also defined the Internet of Things as the connection of physical objects to the Internet network for the purpose of data exchange and intelligent control in various systems. Despite significant advances in this field, security challenges are of great concern to researchers and technologists. The paper also examined security problems in IoT and analyzed various security solutions to protect devices and data (Magami 2023).

According to Zarafshan and Shirbandi (2021), the emergence of smart homes, smart cities, and smart objects has been realized based on the concept of the Internet of Things, which has experienced significant growth due to its incredible potential. According to predictions, nearly 50 billion devices will be connected to each other by 2020. However, devices have limited computing, storage, and network capacity, making them vulnerable to attacks. In general, this article has reviewed the major security issues in the Internet of Things and has proposed some innovative solutions (Zarafshan and Shirbandi 2021). Saeidi and Khateri (2021) defined, analyzed, and investigated the key challenges of using the Internet of Things. The identified challenges include security and privacy, laws, technology, culture and business model, and human resources. Using interpretive structure modeling, the identified challenges have been classified based on importance and relevance. The results proved that human resource and technology challenges and security challenges are classified as the first and second priorities, respectively (Saeidi and Khateri 2021). Karimzadeh and Karimzadeh (2010) defined the Internet of Things as a high-potential and rapidly developing field, referring to the emergence of smart homes and smart cities, which will connect 50 billion devices in the future. Despite these advances, the security of such devices with technical limitations is a major challenge that is easily exploited. This article has generally reviewed the significant security issues of the Internet of Things and assessed the state of threats and new and innovative solutions (Karimzadeh and Karimzadeh 2010). In light of the above, this research analyzes cyber threats in the Internet of Things in the form of a descriptive-analytical methodology.

Internet of Things (IoT):

The Internet of Things (IoT) refers to a network of objects and devices that can connect and exchange data via the Internet. Such objects include a variety of smart devices, sensors, home

appliances, vehicles, and even urban structures that communicate with each other and collect and transmit information. IoT enables remote control and monitoring of devices, creating a smarter and more efficient life. For example, a smart home uses smart thermostats to adjust temperature, smart bulbs to control lighting, and security cameras for surveillance. IoT applications have penetrated various fields, including industry, healthcare, agriculture, and transportation (Madakam et al. 2015). IoT can help improve production processes and reduce costs in the industry. Also, in healthcare applications, connected medical devices are used to monitor the condition of patients. However, the expansion of IoT imposes challenges, including security and privacy concerns. Therefore, the development of standards, security protocols, and privacy policies is essential for the safe and effective use of IoT.

Security threats in IoT:

The increasing connectivity of devices to public networks has exposed IoT to cyber threats and made security a serious concern. As IoT usage expands to all aspects of life from smart home devices to industrial systems, protecting these devices from cyber-attacks has become a critical issue. Therefore, understanding the key concepts of cyber-security in IoT is essential for designing and implementing secure systems (Zhang et al. 2014) (Figure 1).

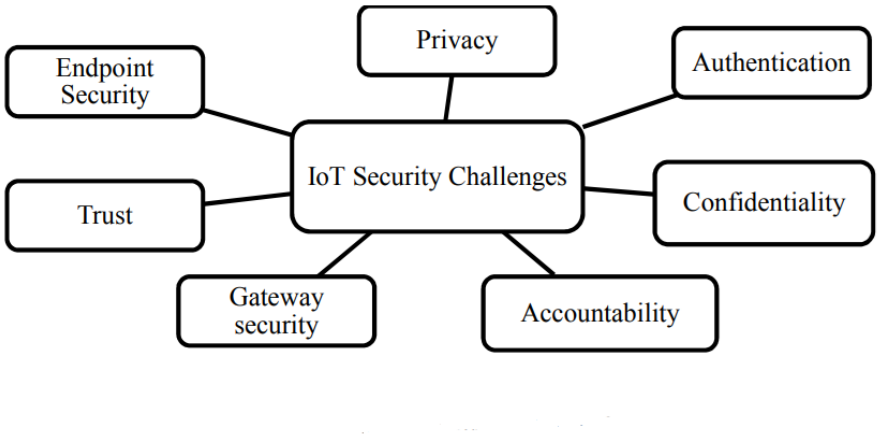

Figure 1: Security Challenges in the Internet of Things

IoT cyber-security encompasses three fundamental principles: confidentiality, integrity, and availability, as follows. Confidentiality ensures that information is only accessible to authorized individuals. IoT devices often transmit sensitive data, such as medical information or user location. As a result, such information must be encrypted to prevent disclosure. Therefore, it is essential to use strong encryption protocols to protect data during transmission and storage.

Integrity ensures that data is not corrupted during transmission or storage. Alteration of data can lead to device malfunctions, such as generating false data by medical systems. Therefore, data integrity helps to ensure the accuracy and reliability of information. Availability ensures that data and devices are always available. DDoS attacks or network disruptions can disrupt availability and lead to critical systems crashes. The solution to this problem is to design resilient networks and systems, as well as rely on advanced security solutions (Figure 2).

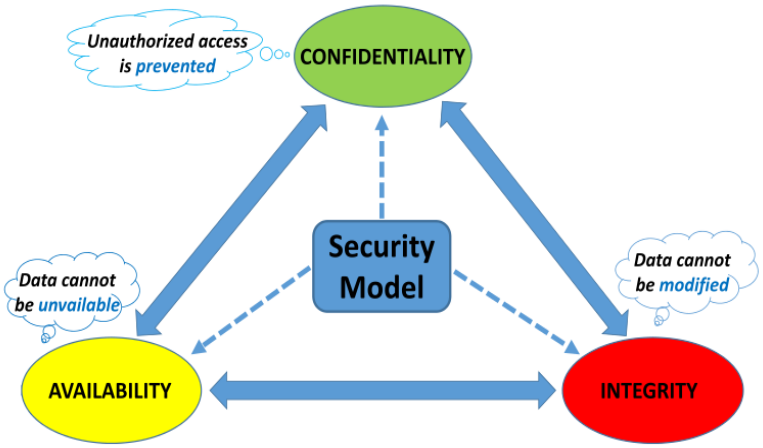

Figure 2: Security models in the Internet of Things

Thus, implementing these principles in the design and development of IoT devices and related systems leads to enhanced security and trust in the virtual world. However, cyber threats are evolving and there is a need for advanced and up-to-date security techniques to protect IoT devices and sensitive data (Thakur et al. 2021).

Security challenges identified in the literature:

Several studies have investigated the vulnerabilities of IoT devices and identified significant challenges in this area. These challenges severely impact the security and reliability of devices. Some of the prominent challenges are discussed below.

- Lack of universal security standards: IoT devices are manufactured by different manufacturers based on different protocols and standards. Heterogeneity and lack of a common security framework led to reduced security of devices. The lack of established standards can cause problems in communication and interaction between devices and make security solutions ineffective.
- Hardware resource limitations of IoT devices: Due to limited hardware resources, many devices cannot easily implement complex security protocols. This limitation can lead to vulnerabilities being exploited by attackers. As a result, manufacturers must consider the trade-off between security and available resources when designing such devices.

Conventional cyber-attacks:

- Brute force attacks: Generally, such attacks are designed to gain unauthorized access to devices by trying different password combinations. This class of threats is especially common in IoT devices with weak passwords.
- Man-in-the-Middle (MITM) attacks: In this type of attack, the attacker can secretly monitor the communication between two parties and extract sensitive information. This process can be easily achieved through security vulnerabilities in the communication protocols of IoT devices.
- Botnet attacks like Mirai: Such attacks often use internet-connected devices as malicious bots to carry out widespread attacks like DDoS. The Mirai attack is one of the most famous Botnet attacks, which disrupted thousands of IoT devices and became the largest DDoS attack in history.

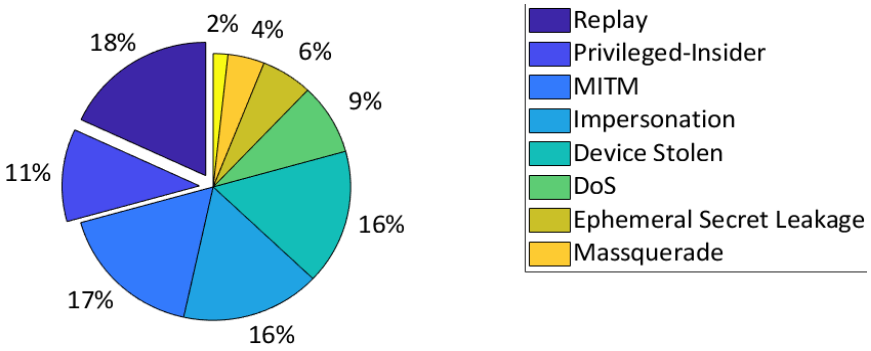

Figure 3: Cyber-attacks on the Internet of Things

In general, the challenges presented highlight the need for greater attention to security in the design and implementation of IoT devices. Addressing these vulnerabilities requires the development of global security standards, the improvement of hardware capabilities, and the implementation of robust security solutions (Roman et al. 2013).

Protecting IoT Security:

Protecting security in IoT is possible by relying on multiple methods, such as strong encryption of transmitted and stored data, implementing strong authentication for users and devices, enforcing appropriate access control policies, and regularly updating device software and operating systems to prevent vulnerabilities. Also, secure protocols such as TLS and DTLS to protect communications, employing firewalls and intrusion detection systems (IDS) to monitor network traffic, and isolating the IoT network from public networks lead to enhanced security. Monitoring device behavior and identifying unusual patterns can help detect threats early. Using security signals and alerts, implementing comprehensive security policies, and educating users about cyber risks are crucial. In addition, selecting trusted and threat-resistant devices should be considered. Combining these methods can achieve broader IoT network security (Roman et al. 2013).

METHODOLOGY

The present study is categorized as descriptive-analytical research. Data collection to study the challenges and solutions of IoT cyber-security requires a multidimensional approach. The study can use various sources including quantitative and qualitative data. Quantitative data can include statistics on cyber-attacks, the number of vulnerabilities discovered, the costs of security breaches, etc. Such data can be collected from reports of security organizations, research papers, and public databases. It is also necessary to study evidence and documents related to policies and regulations related to IoT security. These documents can be queried from government sources, standardization organizations, and private companies. The results of data analysis, including key points, challenges, and solutions identified in the literature, are presented in the form of a systematic and detailed report.

Data Analysis:

Analysis of cyber threats in IoT:

Due to security vulnerabilities, IoT devices are exposed to various attacks. In botnet attacks, attackers use unsecured IoT devices to create a network of bots and carry out DDoS attacks. In MITM attacks, communications between IoT devices and servers are disrupted and data is modified due to weaknesses in encryption. Also, in code injection attacks, attackers exploit software vulnerabilities to execute malicious code and take complete control of devices. In addition, eavesdropping collects sensitive information such as medical data and location by

intercepting communications. Finally, in phishing attacks, attackers use deceptive techniques to gain login credentials from IoT users (Jani and Chaubey 2020).

Table 1: Cyber threats in IoT

Type of attack	Description
Botnet attacks	Attackers use insecure IoT devices to create a network of bots and launch DDoS attacks.
Man-in-the-middle (MITM) attacks	▪ Communications between IoT devices and servers are disrupted and data is altered. ▪ Most such attacks occur due to weak encryption or lack of authentication.
Code injection attacks	▪ Attackers exploit software vulnerabilities in IoT devices to inject malicious code. ▪ This code allows the attacker to gain complete control of the device or sensitive data.
Eavesdropping	By intercepting communications between IoT devices, attackers collect and steal sensitive information such as medical data or location.
Phishing	Using deceptive techniques, attackers seek login credentials or other sensitive information from IoT users.

Security solutions:

Adopting appropriate solutions is crucial to maintain security in IoT devices. Strong authentication helps to strengthen the security of users and devices. At the same time, encryption of user data enables information security. Regular software updates help prevent intrusions. Improved firewalls and intrusion detection systems can detect and block attacks. In addition, educating users about cyber threats and countermeasures can help increase the security of IoT networks (Table 2) (Sahu et al. 2024).

Table 2: Security solutions

Solution	Description
Strong authentication	Using sophisticated methods to authenticate users and devices, such as two-factor authentication and biometric authentication
Data encryption	Encryption protocols to protect data during transmission and storage
Regular software updates	Continuously updating device firmware and software to block vulnerabilities
Firewalls and intrusion detection systems	Launching firewalls and intrusion detection systems to identify and block attacks before they enter the network
User training	Educating users about security risks and how to detect attacks to increase awareness and mitigate risks

Analysis of the effectiveness of security methods:

Analysis of the effectiveness of security methods in IoT shows that each method has its advantages and disadvantages. Strong authentication effectively prevents unauthorized access and subsequently imposes challenges on users. Data encryption significantly protects sensitive information. However, this approach requires more resources. Regular software updates are very effective in reducing weaknesses and vulnerabilities. However, this method may be forgotten. Although they require fine-tuning, firewalls and intrusion detection systems help to detect and block attacks. Finally, user education and awareness help to strengthen security, although it may not have an immediate effect (Table 3) (Bhoi et al. 2024).

Table 3: Analysis of the effectiveness of security methods

Method	Effectiveness	Advantages	Disadvantages
Strong authentication	Very effective in preventing unauthorized access	Increase security and prevent unauthorized access	This method may cause problems for users during use
Data encryption	Effective in protecting sensitive information	Protecting information during transmission and storage	This method requires more resources for processing and storage
Regular software updates	Updating the system and blocking vulnerabilities	Reducing risks from known vulnerabilities	This method may be forgotten or delayed
Firewalls and intrusion detection systems	Effective in detecting and blocking attacks	Identifying advanced threats and preventing their entry	This method requires fine-tuning and permanent resources
User training	Effective in increasing awareness and preventing human errors	Improving safe behaviors and reducing risks from slackness	This approach may not have an immediate impact.

Assessing IoT security challenges and limitations:

Security challenges in IoT arise from multiple reasons and can impose serious vulnerabilities. The limited resources of IoT devices reduce the ability to implement complex security protocols. Also, default and weak passwords are easily mined by attackers. The lack of security updates and the lack of globally unified standards lead to the persistence of vulnerabilities and a lack of coordination between devices. In addition, the centralization of data and the large volume of information produced complicate threat detection and compromise user privacy (Al-Fuqaha et al. 2015).

Table 4: Assessment of challenges and limitations in IoT security

Challenge	Description	Impact
Limited resources of IoT devices	IoT devices typically have limited processing and memory resources.	This challenge makes it difficult to implement complex security protocols.
Default and weak passwords	Many devices have default, fixed passwords.	This problem makes it easy for attackers to infiltrate through brute force attacks.
Insufficient security updates	Some devices are not updateable or manufacturers do not provide security updates.	This challenge makes devices vulnerable to new attacks.
Lack of unified global standards	Lack of common security standards between different manufacturers	Reduced collaboration and synchronization between devices and increased security risks
Diversity of IoT technologies and architectures	Diverse IoT device architectures require different security solutions.	Complexity in designing and implementing effective security solutions
Data centralization	Sending data to a central server under cyber-attack	This challenge leads to a general disruption in the system.
High volume of	The large volume of data	This challenge makes detecting

data	generated by devices complicates threat identification.	and responding to threats time-consuming and difficult.
Excessive data collection	Excessive data collection may violate users' privacy.	Growing concerns about privacy and data misuse
Lack of comprehensive rules	Lack of adequate regulations in many countries to protect IoT security	Lack of transparency and weakness in confronting legal threats
Manufacturers responsibility	Manufacturers take little responsibility for device security and updates.	Users are at risk and manufacturers easily escape accountability.

The lack of comprehensive regulations and limited liability of manufacturers also lead to new challenges for IoT security (Table 4).

DISCUSSION

According to the results, this technology is rapidly renovating and transforming various industries with its unique capabilities. Also, its numerous applications in medicine, agriculture, smart homes, and transportation have positive impacts on improving the quality of life and increasing productivity. However, the increase in the connectivity of devices to public networks leads to increased security vulnerabilities and imposes serious challenges in the field of privacy and data security. Given that many IoT devices have limited resources, it is difficult to implement stronger security protocols. According to the findings of this research, IoT devices are vulnerable to cyber-attacks due to resource constraints and insecure designs. Threats such as botnet attacks, man-in-the-middle (MITM) attacks, and code injection are considered major risks for IoT devices and networks. The lack of global standards and comprehensive regulations makes IoT security more complex. This requires serious efforts to develop effective security solutions. Subsequently, several solutions such as encryption, multi-factor authentication, intrusion detection systems, and reliance on technologies such as artificial intelligence and blockchain can improve IoT security. Such technologies not only ensure data security but also are effective in preventing cyber-attacks and identifying threats. Ultimately, this research proves that IoT security is a multidimensional issue requiring comprehensive solutions and coordination among manufacturers, policymakers, and users. Through greater collaboration in this area, it is possible to transform IoT into a sustainable and secure ecosystem. Although IoT security challenges still exist, with collaborative efforts, we can turn it into a source of wealth to improve lives.

Given the limited resources of IoT devices, it is difficult to implement stronger security protocols. To solve this challenge, various security strategies should be considered. One such solution is to rely on lightweight security protocols. Manufacturers should consider designing cryptographic algorithms that are compatible with the hardware and resource constraints of IoT devices. Secure protocols such as MQTT with TLS and CoAP with DTLS can also play an important role in ensuring data security. In addition, regular software updates are an important factor in increasing IoT security. Manufacturers should provide mechanisms to automatically deliver and install security updates. Users should use devices with regular updates. Another security solution is to implement edge computing. This method proposes to transfer part of the data processing to the network edge to reduce latency and increase security.

Organizations should develop policies to manage IoT devices in the network, including access control, password management, threat detection, and information leakage management. It is also necessary to hold periodic meetings to review and update the policies. Manufacturers are required to produce devices with minimum security standards and respond to security flaws.

This includes providing regular security reports and making product security data available.

CONCLUSION

The present study aims to analyze existing security challenges and provide practical solutions in technical, managerial, and legal areas to improve IoT security. IoT security is a dynamic and evolving issue that requires continuous efforts and cooperation between all stakeholders, including manufacturers, users, and policymakers. Ignoring these challenges can lead to serious threats to privacy and data security. In order to address these threats, comprehensive security strategies, the development of global standards, and the promotion of cyber-security culture among users and organizations should be implemented. Manufacturers also have a responsibility to provide devices with minimum security standards and respond to critical security flaws.

One of the limitations of this study is the limited access to library resources and the need for more time to collect accurate data. Also, bias in interpreting information and selecting sources can affect the results.

REFERENCES

1. Zarafshan, Farzaneh and Shirbandi, Ramin (2010), A review of attacks and security solutions for the Internet of Things (IoT), https://civilica.com/doc/1638889
2. Saeidi, Farahnaz and Khateri, Amirhossein (2010), A review of key challenges in using the Internet of Things. Journal of New Research Approaches in Management and Accounting 5(19), 1-16.
3. Ghobadi, Mostafa (2014), Information security challenges in the Internet of Things (IoT), 7th National Conference on New Technologies in Electrical, Computer, and Mechanical Engineering of Iran, Tehran, https://civilica.com/doc/2050208
4. Karimzadeh, Saeid and Karimzadeh, Amir (2010), A new approach to methods for increasing security in smart homes, National Conference on Civil Engineering, Architecture, and Information Technology in Urban Life, https://sid.ir/paper/900225/fa
5. Maghami, Bijan (1402), Security in the Internet of Things (IOT): Challenges and Solutions, 9th International Conference on Knowledge and Technology of Mechanical, Electrical and Computer Engineering of Iran, Tehran, https://civilica.com/doc/1969045
6. Al-Fuqaha, A., Guizani, M., Mohammadi, M., Ayyash, M., & Saberi, M. (2015). Internet of Things: A survey on enabling technologies, protocols, and applications. IEEE Communications Surveys & Tutorials, 17(4), 2347-2376.
7. Bhoi, S. K., Ghugar, U., Dash, S., Nayak, R., & Bagal, D. K. (2024). Exploring The Security Landscape: A Comprehensive Analysis of Vulnerabilities, Challenges, And Findings in Internet of Things (Iot) Application Layer Protocols. *Migration Letters*, *21*(S6), 1326-1342.
8. Hassan, W. H. (2019). Current research on Internet of Things (IoT) security: A survey. *Computer networks*, *148*, 283-294.
9. Jani, K. A., & Chaubey, N. (2020). IoT and cyber security: introduction, attacks, and preventive steps. In *Quantum Cryptography and the Future of Cyber Security* (pp. 203-235). IGI Global.
10. Madakam, S., Ramaswamy, R., & Tripathi, S. (2015). Internet of Things (IoT): A literature review. *Journal of Computer and Communications*, *3*(5), 164-173.
11. Roman, R., Zhou, J., & Lopez, J. (2013). On the security of wireless sensor networks in the context of the Internet of Things. International Journal of Computer Science & Information Technology, 5(6), 116-123.
12. Sahu, S. K., & Mazumdar, K. (2024). Exploring security threats and solutions

Techniques for Internet of Things (IoT): from vulnerabilities to vigilance. *Frontiers in Artificial Intelligence*, *7*, 1397480.

13. Thakur, K., & Pathan, A. S. K. (2020). *Cybersecurity fundamentals: a real-world perspective*. CRC Press.
14. Zhang, Y., Deng, R. H., & Preneel, B. (2014). Security and privacy in the Internet of Things: Challenges and solutions. Future Generation Computer Systems, 42, 25-33.