



ANALYSIS OF CYBERSECURITY THREATS IN THE INTERNET OF THINGS, FOCUSING ON BANKS

¹Ali Rafiei Taghanaki

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

Corresponding Author: Ali Rafiei Taghanaki

ABSTRACT

This study aims to examine and analyze cybersecurity threats within the Internet of Things (IoT), specifically focusing on the banking sector. The data for this research is collected through simulations of cyberattacks and secure transfers within an IoT system linked to a bank. These data are recorded across 50 repetitions, during which the patterns of attacks and security within the system are tracked. Each device in the system can operate in either an active or IoT state. A separate dictionary is utilized to monitor the progression of attacks in each repetition, with relevant data added whenever an attack or secure transfer occurs. The simulation results indicate a consistent rise in the number of DDoS and MITM attacks over time. In the first repetition, there were 3 MITM attacks and 2 DDoS attacks, but by the 50th repetition, these numbers had increased to 41 and 51, respectively. The findings related to the occurrence of security events show a sharp increase in all variables around the 30th repetition. This rise may be attributed to changes in security policies, the intensification of attacks, or the growing number of IoT devices in the system. Additionally, it was observed that after the 40th repetition, there was a significant increase in the number of anomalies, indicating greater complexity in the attacks and tactics employed by intruders. The correlation matrix between attacks, secure transfers, and anomalies revealed a very low correlation between MITM and DDoS attacks. The analysis of cumulative trend charts for attacks and secure transfers showed that while the cumulative number of MITM and DDoS attacks steadily increased over time, there were also instances of sudden spikes.

Keywords: Cybersecurity threats, Internet of Things, Banks, MITM attacks, DDoS attacks.

INTRODUCTION

The concept of the Internet of Things (IoT) was introduced in the 1990s by Kevin Ashton. The rapid advancement of communication technologies, the decreasing cost of hardware, and the

growing demand for smart devices have all played a significant role in the development of this technology (Sharma et al., 2019). As IoT technology continues to evolve, there is an increasing need to examine and address the security threats and defense strategies within this field. Cybersecurity in IoT systems faces numerous challenges, such as the massive amounts of data generated, the diversity of connected devices, and the limited computational resources. Key security threats in this domain include Distributed Denial of Service (DDoS) attacks, Man-in-the-Middle (MITM) attacks, and data breaches, all of which can disrupt device functionality and compromise user data security. In recent years, emerging technologies have been introduced to bolster IoT security, offering potential solutions to enhance protection and minimize vulnerabilities (Hasan, 2019). These technologies assist in identifying and predicting threats by analyzing data patterns. Advanced machine learning algorithms can detect abnormal behaviors and potential cybersecurity risks. Additionally, intelligent Intrusion Detection Systems (IDS) that learn from traffic patterns are employed to identify and prevent attacks in real-time. Lightweight cryptography is designed specifically for devices with limited resources and low power. Due to the computational limitations of these devices, high-efficiency algorithms such as PRESENT and SPECK are used. These methods ensure security while minimizing the impact on system performance, helping to safeguard sensitive data in IoT devices. In edge computing, data processing occurs closer to IoT devices, reducing response time and locally managing large volumes of data instead of sending them to central servers. This shift decreases reliance on cloud servers, which may be vulnerable to cyberattacks, thereby improving security, protecting information, and lowering the risks of privacy breaches. These technologies represent the ongoing transition toward a more secure and resilient IoT ecosystem in the face of evolving cybersecurity threats (Roman, 2013).

To enhance IoT security, various standards and protocols have been developed. The ISO/IEC 27001 standard provides an international framework for information security management, helping organizations organize their security processes and address risks related to security and privacy protection. The MQTT (Message Queuing Telemetry Transport) protocol is lightweight and efficient, commonly used in IoT applications. Due to its simplicity, it requires additional security layers, such as TLS (Transport Layer Security), to protect data traffic. CoAP, designed for resource-constrained devices, uses DTLS (Datagram Transport Layer Security) to encrypt and secure communications. The Zigbee standard, a communication protocol for low-power networks, is frequently used in smart home devices. Zigbee employs encryption algorithms to protect data, making it valuable for securing information in IoT networks (Thakur, 2020).

Khan and Saleh (2018) discussed the rise of the Internet of Things (IoT) within smart homes and cities, citing Cisco's prediction that the number of connected devices would reach 50 billion by 2020. They highlighted that hacking and compromising many of these devices is relatively easy, as these devices, due to their computational, storage, and network limitations, are more vulnerable to threats than other devices. This paper explores the main security issues in IoT, categorizes threats, and examines new solutions. It also looks into the impact of blockchain technology on improving IoT security and identifies existing research challenges in the field.

IoT security remains one of the most complex challenges in the digital world, requiring focused attention and targeted efforts to improve the current state. Analysis of findings reveals a direct correlation between technological advancements and the rise in cyber threats. As IoT devices become more sophisticated, cyberattacks also grow in complexity and precision. This is particularly evident in attacks like IoT malware, Distributed Denial of Service (DDoS) attacks, and data manipulation. On the other hand, the lack of global and unified standards in the design and development of IoT devices has emerged as one of the key factors contributing to the vulnerability of these systems. Analyses suggest that devices relying on proprietary protocols without security support are prime targets for cyberattacks. Furthermore, an assessment of security solutions reveals that techniques such as encryption, multi-factor authentication, and the use of artificial intelligence have proven effective in many cases. However, these methods

face challenges due to the hardware limitations of IoT devices, such as reduced performance and increased costs. Additionally, user awareness and knowledge should not be overlooked in this context (Sahu, S, 2024). Analyses show a low level of user awareness regarding IoT device security settings and the failure to change default passwords, which facilitates cyberattacks. Ultimately, these factors contribute to a vulnerable security environment, and thus, improving user awareness, establishing global standards, and adopting advanced security techniques are crucial steps in enhancing IoT security. There is an increasing need for a comprehensive approach and collaboration among various stakeholders—from manufacturers to users—to transform the Internet of Things into a secure and sustainable ecosystem.

Continuous research and development to identify emerging threats and offer innovative solutions is crucial. Additionally, raising user awareness and understanding of security risks and how to mitigate them is equally important. This research has aimed to identify and analyze cyber threats within the Internet of Things (IoT), with a particular focus on the banking sector. It also strives to provide practical and effective solutions to counter these threats. However, it is essential to recognize that the IoT security field is still evolving, with new challenges arising daily. Therefore, there are numerous opportunities for improvement and progress in this area, and future research should focus on these opportunities. These may include the development of new security technologies, enhancement of communication protocols, and the establishment of stronger protective policies. Furthermore, user education and raising public awareness are critical factors in improving IoT cybersecurity. The ultimate goal of these efforts is to create a secure and reliable environment for harnessing the benefits of IoT technology. Ultimately, IoT security is not only a technical challenge but also a social responsibility that requires the involvement of all stakeholders, including governments, international organizations, technology companies, and end-users.

RESEARCH METHODOLOGY

The data is collected through the simulation of cyberattacks and secure transmissions within an Internet of Things (IoT) system related to a bank. These data are recorded over 50 iterations, during which the attack patterns and security status of the system are defined. Each device can be in one of two states: active or inactive. Initially, three devices are inactive. A dictionary is used to track the number of attacks and secure transmissions:

- MITM (Man-in-the-Middle Attack)
- DDoS (Distributed Denial of Service Attack)
- Secure Transmissions (Secure Data Transfers)
- Anomalies (Detected Anomalies in Devices)

Additionally, another dictionary is created to monitor the attack trends during each iteration. Each time an attack or secure transmission occurs, the relevant value is added to this dictionary. When devices are active, data is transmitted securely. The status of the devices is regularly checked, and if any device unexpectedly becomes inactive, an anomaly is logged. The objective is to analyze the impact of various attacks and track the system's security over time.

FINDINGS

The number of MITM attacks increased from 3 in the first iteration to 41 in the 50th iteration, while DDoS attacks grew from 2 to 51. The number of secure transmissions, initially zero, rose to 109 by the end of the process, reflecting an improvement in system security. However, anomalies also showed an upward trend, rising from 2 at the start to 149 by the end, indicating that the system faced a broader range of threats.

Table 1: Analysis of Cyberattack Trends and Secure Transmissions in the IoT Security System of the Bank

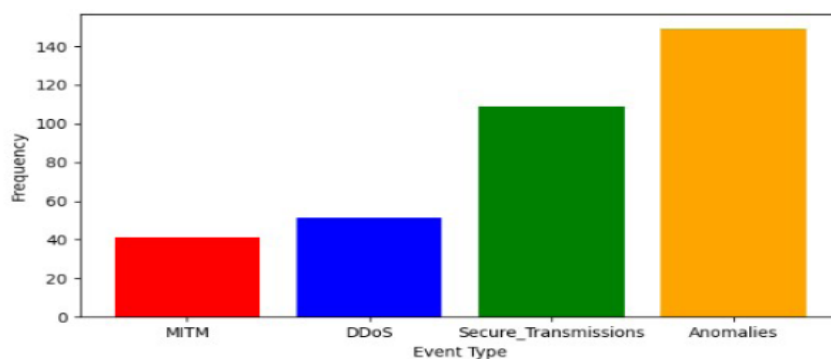
Anomalies	Secure Transmissions	DDoS	MTTM	Iteration
2	0	2	3	1
29	19	12	11	10
59	45	22	15	20
89	68	28	22	30
119	85	40	35	40
149	109	51	41	50

Around iteration 30, all variables saw significant growth, which could suggest changes in security policies or an intensification of the attacks. Moreover, after iteration 40, there was a notable increase in the number of anomalies, likely due to the increasing complexity of the attacks (Table 1).

Figure 1 displays the frequency distribution of different types of security events throughout the simulation process. These events are divided into four main categories:

- **Man-in-the-Middle (MITM) Attack:** The number of times this type of attack was detected, where the attacker attempts to intercept or alter the communication between two parties.
- **Distributed Denial of Service (DDoS) Attack:** The frequency of attacks that simultaneously target and disrupt a system by overwhelming it with traffic from multiple malicious sources.
- **Secure Transmissions:** The number of times data was securely transmitted without interference from attackers.
- **Anomalies:** The number of instances detected where abnormal behavior occurred, which could indicate a potential cyber-attack.

This chart shows the trend of each of these events throughout the simulation process and provides an opportunity for quick comparison between the occurrence rates of attacks and security events.

**Figure 1: Attacks and Secure Transmissions**

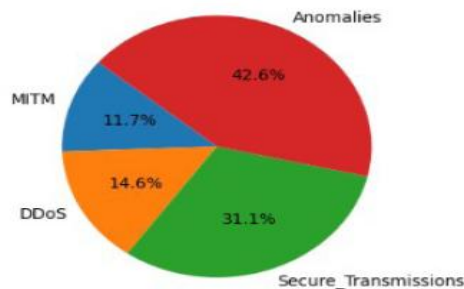


Figure 2: Shows an increase in anomalies

Figure 2 depicts the Distribution of Events. Figure 3 This chart displays the trend of security event occurrences over time (measured in simulation iterations). The horizontal axis represents the number of execution iterations, while the vertical axis shows the frequency of each security event. Each line tracks the changes in the frequency of a specific event over time, including MITM attacks (red), DDoS attacks (blue), secure transmissions (green), and anomalies (orange), providing a comparison of the security fluctuations throughout the system's execution.

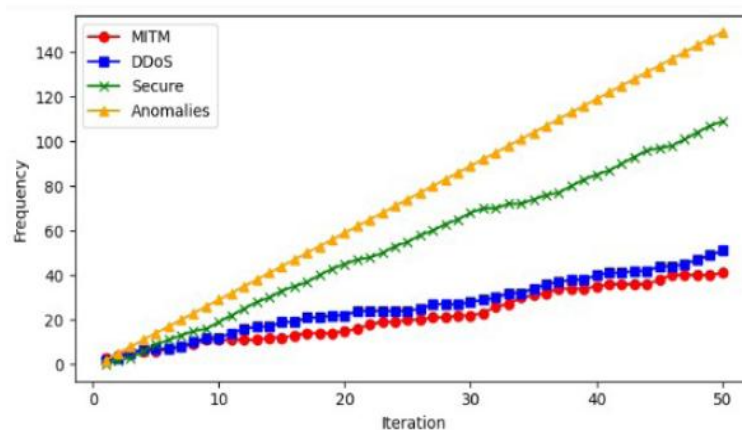


Figure 3: Trend Chart of Security Event Occurrences

Figure 4: The chart shows the distribution of the frequency of various security events. Each point on the chart represents the number of occurrences of a specific security event. The horizontal axis includes four types of events (MITM, DDoS, secure transmissions, and anomalies), while the vertical axis indicates the number of times each event occurred. This chart allows us to visually compare the distribution and frequency of each event.

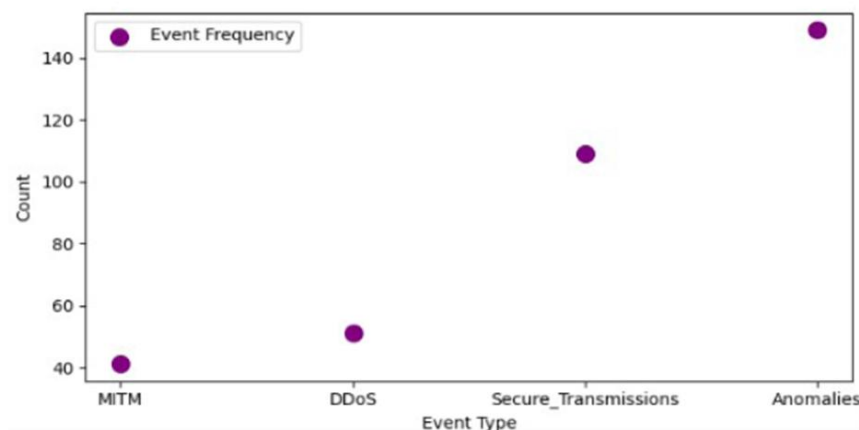


Figure 4: Scatter plot of event types.

Analysis of the Correlation Matrix Between Attacks and Secure Transmissions

The correlation matrix illustrates the relationships between different types of attacks (MITM, DDoS), secure transmissions, and detected anomalies throughout the simulation. Analyzing this matrix aids in understanding the attack patterns and their effects on data security. (Table 2).

Table 2: Correlation Between Attacks and Secure Transmissions

Anomalies	Secure-Transmission	DDoS	MTTM	Iteration	Variables
0.02	-0.15	0.07	-0.06	1.00	Iteration
-0.03	0.12	0.03	1.00	-0.06	MTTM
-0.02	0.10	1.00	0.03	0.07	DDoS
-0.02	1.00	-0.10	0.12	-0.15	Secure-Transmission
1.00	-0.02	-0.02	-0.03	0.02	Anomalies

A weak positive correlation is observed between MITM attacks and secure transmissions, indicating that as the frequency of these attacks increases, the number of secure transmissions also slightly rises. This is likely due to the strengthening of security measures following the attack. Similarly, attacks may prompt devices to secure their data for recovery, as some IoT system devices increase their security. On the other hand, the negative correlation between secure transmissions and the number of simulation repetitions suggests that, over time, as attacks increase, some devices become non-functional, leading to a decline in secure data transmissions during DDoS and MITM attacks. Additionally, the very low correlation between the two types of attacks indicates their independence from one another. The minimal correlation between anomalies and other variables suggests that anomaly detection occurs independently of other network events and attacks.

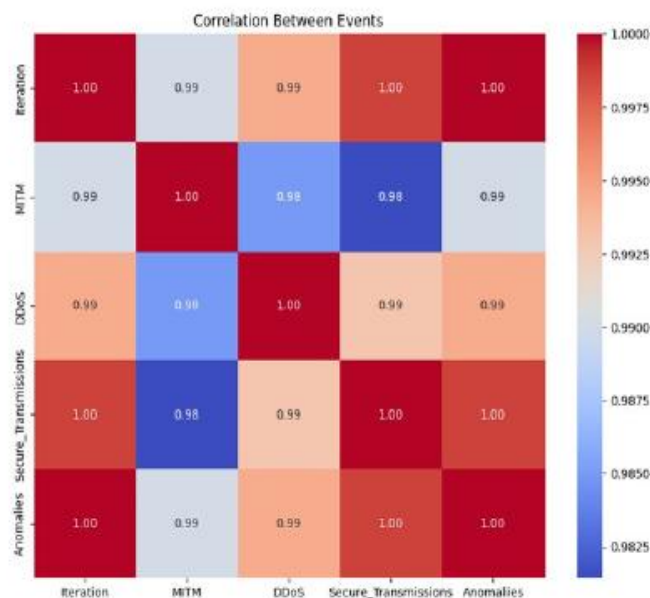


Figure 5: Correlation Matrix between Events

As a result, DDoS and MITM attacks have a slight effect on secure transmissions, but this impact is not particularly significant. Over time, secure transmissions decrease, which could be attributed to the deactivation of IoT devices following the attacks. Meanwhile, anomalies show little to no correlation with attacks and secure transmissions, likely indicating random or independent detection of these events.

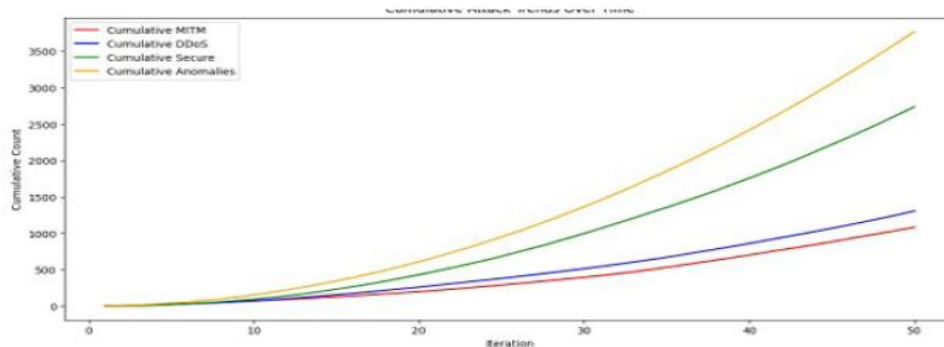


Figure 6: Cumulative Trend of Attacks and Secure Transmissions Over Time

Figure 6 shows the cumulative trend of attacks and secure transmissions over time. The horizontal axis represents the number of simulation iterations, while the vertical axis displays the cumulative value of the variables.

The *red line (Cumulative MITM)* shows the cumulative amount of MITM attacks over time. The *blue line (Cumulative DDoS)* illustrates the cumulative trend of DDoS attacks. The *green line (Cumulative Secure Transmissions)* represents the cumulative value of secure transmissions. The *orange line (Cumulative Anomalies)* shows the cumulative number of anomalies over time.

An increase in these lines indicates a rise in cumulative attacks and secure transmissions across the simulation iterations. If the slope of a line increases at a certain point, it indicates a faster growth of that variable during that time period.

Table 3: Attack and Security Report Table

Event	Frequency
MITM	41
DDoS	51
Secure- Transmissions	109
Anomalies	149

- **MITM Attacks (41 occurrences):** The frequency of these attacks is relatively lower compared to other events, which could suggest that security measures have successfully reduced MITM attacks or limited the opportunities for their occurrence.
- **DDoS Attacks (51 occurrences):** These attacks occurred more frequently than MITM attacks, indicating that distributed denial-of-service (DDoS) attacks had a significant impact on the network. This may be due to the increased number of devices connected to the system.
- **Secure Transmissions (109 occurrences):** This figure is notably higher than the total number of attacks, showing that the system remains capable of conducting secure data transfers, although it may be vulnerable to attacks under certain circumstances.
- **Anomalies (149 occurrences):** The highest count is related to unusual events or anomalies, suggesting that the system may have experienced unexpected behavior patterns, possibly due to attacks, system errors, or other unidentified causes.

CONCLUSION

The simulation results show that the number of DDoS and MITM attacks has increased over time. In the first iteration, there were 3 MITM attacks and 2 DDoS attacks. By iteration 50,

these numbers had risen to 41 and 51, respectively. This upward trend indicates the growing severity of cyber threats over time. Additionally, the number of secure transmissions rose from an initial value of zero to 109 by the end of the simulation. This suggests that the system's security mechanisms gradually strengthened, improving its ability to prevent attacks and ensure data security. However, the increase in anomalies, from 2 to 149, signals emerging security challenges and the need for more advanced solutions to identify and address threats. The trend charts of security events show a sharp increase in all variables around iteration 30. This spike could be due to changes in security policies, the intensification of attacks, or a rise in the number of IoT devices within the system. Moreover, after iteration 40, there was a significant rise in anomalies, which may reflect the increasing complexity of attacks and evolving attacker methods. The correlation matrix between attacks, secure transmissions, and anomalies revealed that the correlation between MITM and DDoS attacks was very low, meaning these two types of attacks occurred independently. However, the correlation between the number of secure transmissions and the number of MITM and DDoS attacks was weak but positive, indicating that an increase in attacks led to stronger security measures and more secure transmissions. Nonetheless, it was observed that as attacks increased, some IoT devices became nonfunctional, causing a reduction in secure transmissions.

Additionally, anomalies showed no significant correlation with other variables, suggesting that they were identified independently of the other attacks and security events. The analysis of cumulative trends for attacks and secure transmissions showed that the cumulative increase in MITM and DDoS attacks remained consistent over time, although there were occasional sudden spikes. These jumps could be the result of more complex attacks or an increase in the number of attackers. In contrast, the trend of secure transmissions showed a significant rise, suggesting that the system gradually adopted more effective security mechanisms to handle the attacks. These results indicate that for improving security in the Internet of Things (IoT), more advanced methods are required to detect and counteract attacks. Enhancing machine learning techniques for anomaly detection, strengthening data encryption, and implementing smart firewalls are strategies that could help improve IoT security in the future. The data analysis highlights that while the security challenges of IoT are complex and varied, appropriate measures can significantly reduce the vulnerabilities of this technology. One of the key steps is to implement advanced security techniques such as data encryption, multi-factor authentication, and the creation of intrusion-resistant networks, which can prevent unauthorized access and cyberattacks. Additionally, improving system monitoring and continuous surveillance using AI algorithms and machine learning can play a critical role in early threat detection, enabling quicker responses. Furthermore, utilizing innovative authentication and encryption methods, such as blockchain and distributed security protocols, could enhance the security of transactions and data exchanges. Overall, a comprehensive approach that combines advanced technologies, effective monitoring strategies, and preventive security measures can effectively manage these threats and enhance safety and trust within the IoT ecosystem. Users must be aware of cyber threats and the security measures needed for IoT devices. To increase awareness, educational campaigns and public workshops can be organized. Furthermore, organizations should provide continuous training programs for their employees and promote a cybersecurity culture, including cyberattack simulations and anomaly detection. Organizations should also develop policies for managing IoT devices within their network, including access control, password management, threat detection, and information leakage management. Regular meetings to review and update these policies are essential.

This research, due to limited access to real data on IoT attacks, relied on simulations and previous studies for many analyses, which may impact the accuracy of the results. Many of the proposed security solutions, especially in areas like encryption and artificial intelligence, are dependent on the hardware limitations of IoT devices. This presents a challenge in implementing security measures on a large scale.

REFERENCES

1. Hassan, W. H. (2019). Current research on Internet of Things (IoT) security: A survey. *Computer networks*, 148, 283-294.
2. Khan, M. A., & Salah, K. (2018). IoT security: Review, blockchain solutions, and open challenges. *Future generation computer systems*, 82, 395-411.
3. Sharma, N., Shamkuwar, M., & Singh, I. (2019). The history, present and future with IoT. *Internet of things and big data analytics for smart generation*, 27-51.
4. 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.
5. 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.
6. Thakur, K., & Pathan, A. S. K. (2020). *Cybersecurity fundamentals: a real-world perspective*. CRC Press.