SWINBURNE UNIVERSITY OF TECHNOLOGY

Swinburne University of Technology

Faculty of Science, Engineering and Technology

ASSIGNMENT AND PROJECT COVER SHEET

Unit Code: COS30015 Unit Title: IT Security

Assignment number and title: No. 1 - Research Project Due date: 18/06/2023

Lab group: Group 2 Tutor: Dr. Anh Ngoc Le Lecturer: Dr. Anh Ngoc Le

Family name: Trac Duc Anh Luong Identity no: 103488117

Other names:

To be completed if this is an INDIVIDUAL ASSIGNMENT
I declare that this assignment is my individual work. I have not worked collaboratively, nor have I copied from any other student's work or from any other source except where due acknowledgment is made explicitly in the text, nor has any part been written for me by another person.

Signature: Trac Duc Anh Luong

To be completed if this is a GROUP ASSIGNMENT
We declare that this is a group assignment and that no part of this submission has been copied from any other student's work or from any other source except where due acknowledgment is made explicitly in the text, nor has any part been written for us by another person.

ID Number	Name	Signature

Marker's comments:

Total Mark:

Extension certification:

This assignment has been given an extension and is now due on

Signature of Convener: Date: / 2022

COS30015 - IT Security

Assignment 1: Research Project

Emerging Attacks on IoTs

Author: Trac Duc Anh Luong

Submission Date: 18/06/2023

1 Abstract

The Internet of Things (IoT) has grown significantly, transforming many industries with its network of interconnected systems and gadgets. However, the growth of IoT has also brought along fresh security concerns and flaws that want immediate attention. The need for solid security solutions is emphasized as this literature review investigates the difficulties and vulnerabilities of new assaults on IoT devices and networks. The review identifies the principal difficulties IoT systems must overcome: supply chain threats, distributed denial of service (DDoS) attacks, device vulnerability, and communication channel attacks. These flaws can cause major infrastructure interruptions, unwanted access, data manipulation, and privacy violations. Several security procedures and tactics have been suggested and implemented to address these concerns. Among the solutions to strengthen IoT security are secure authentication mechanisms, encryption methods, intrusion detection and prevention systems (IDPS), secure over-the-air (OTA) updates, and access control mechanisms. Several actions are taken to build trust, protect communication channels, identify and stop intrusions, maintain secure software upgrades, and manage device access. Collaboration amongst stakeholders, including technology providers, business leaders, policymakers, and researchers, is necessary to achieve adequate security in the IoT ecosystem. It calls for the creation of industry standards and norms, the sharing of information, and the adoption of best practices. Ongoing research and innovation are essential to remain ahead of changing threats and create adaptable security solutions. We can realize the full potential of IoT technology while guaranteeing the privacy, integrity, and security of connected devices by tackling the issues brought on by new attacks on the IoT. Everyone must work together to recognize, reduce, and defeat these dangers to create a robust, secure, and reliable IoT ecosystem.

2 Introduction

The Internet of Things (IoTs) has become an emerging field of technology, leading to a rapid increase in the number of interconnected devices across the globe. This expansion opened up new possibilities for technology, enabling the communication between multiple devices across various systems, which led to the transformation in various industries, namely healthcare, smart homes, transportation, and agriculture, and achieving the ultimate goal of enhancing the quality of life. However, it also led to multiple vulnerabilities and security issues that can be exploited (Abbas et al. 2020). Unprecedented IT security challenges arise with these emerging attacks on IoTs systems.

The definition of emerging attacks on IoTs can be interpreted as security threats that can be exploited through the vulnerability of interconnected IoT systems (Abomhara & Køien 2014). Cyber intruders implement various approaches, including malware attacks, MITM (man-in-the-middle), physical attacks, and zero-day exploits to gain unauthorized access, compromise and manipulate the collected data, or launch DDOS attacks. The key terminologies related to these significant security attacks include malware, data breaches, botnets, and privacy violations.

Understanding and assessing the emerging attacks on IoT is instrumental, and the report will highlight convincing findings related to this issue (Chasaki & Mansour 2015). The reach and coverage of IoTs systems across the industries mentioned above make the attacks on this system a heated issue. If the issue is neglected, there will be dire consequences in numerous domains. Financial losses, system malfunction, compromised security of users, and danger to the mass can be posed. Ensuring the IoTs systems from cyber attacks will provide the maintainability and development for the IoTs field in an interconnected world.

This literature review aims to provide a detailed and insightful analysis of the knowledge surrounding attacks on IoTs. Existing research that has already covered different aspects of this topic will serve as references to this report. In addition, comprehensive knowledge of the latest vulnerabilities and countermeasures will be tackled by incorporating the author's insights and perspective. Possible solutions will be identified to cope with these security breaches.

The report follows a logical structure to present the understanding of emerging attacks on IoTs. It will start with a background overview, covering the importance of current IoTs technologies. Next, the report goes into further detail about the systems' infrastructures, methods, how these attacks leverage the existing vulnerabilities, and how to mitigate the attack and follow-up damages, with a detailed analysis of the pros and cons of these approaches. Finally, the report will conclude the findings and conclusions drawn from research and surveys.

3 Overview

This literature review section will outline how the report is organized and any extra background information relevant to emerging attacks on IoTs. The selection criteria for making use of relevant sources will also be mentioned. Specific criteria were followed during the literature selection process for this review. The main focus was to evaluate the relevance of papers related to the chosen topic of IoTs attacks. Chosen papers for reference will be recent, with peer reviews conducted and authoritative sources in the two fields of IoTs and cybersecurity. We will look at the provided evidence, case studies, research and analysis of IoT attacks and their impact. The involvement of these credible sources will lead to a comprehensive understanding throughout this literature review.

The emerging attacks on IoTs have become an urgent concern due to the vulnerability introduced by the unprecedented amount of interconnected IoT devices. Integrating such devices has increased security threats in several industry sectors, such as healthcare, transportation, agriculture, and smart houses. The serve damage that can be left behind after IoT attacks are illegal access, data manipulation, privacy violations, and the corruption of essential services. The dependence on IoT technologies and the possible repercussions of attacks highlights how urgent it is to comprehend and adequately solve these security concerns.

This literature seeks to offer a thorough knowledge of the rising attacks on IoTs by exploring the background and contextualizing the problem. After thoughtful examination, the review aims to highlight the various attacking paths, their methodology, and their implication to IoT systems using a detailed analysis of published papers in the reference. This literature survey paves the way for a critical study of the issues, effects, and potential solutions related to attacks on IoTs in the following sections.

4 Literature Review

This literature review will examine new IoT security threats' fundamental problems and difficulties. We will examine the systems, methods, strategies, mechanisms, and current solutions to these challenges. A proper analysis of these existing approaches will be conducted to determine what threats have been mutualized and their potential for future mitigation.

4.1 Major Challenges

4.1.1 Device Vulnerability

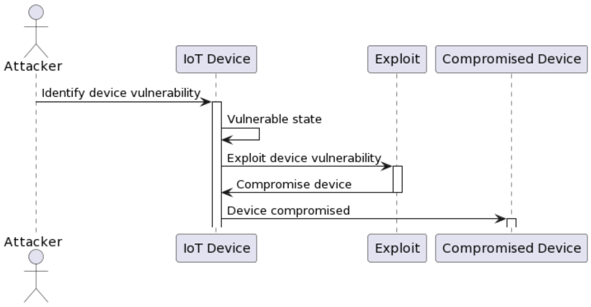

Figure 1: Device Vulnerability

The vulnerability of IoT devices can be comprehended as a weak spot that cyber attackers can exploit (Roesner et al. 2014). The reason leading to this weakness is related to the limitation of computational resources and lack of self-defence security mechanism in the device's structure. IoT devices are often designed with constrained resources, such as low processing power, memory, and energy input. These can be understood as the cost of production can be exorbitant with a network of multiple devices. Also, IoT sensors are often placed in remote environments for environment monitoring, requiring extended battery life, thus reducing the number of processes running, lack of resource-intensive cryptographic operations and susceptibility to breaches.

4.1.2 Communication Channel Attacks

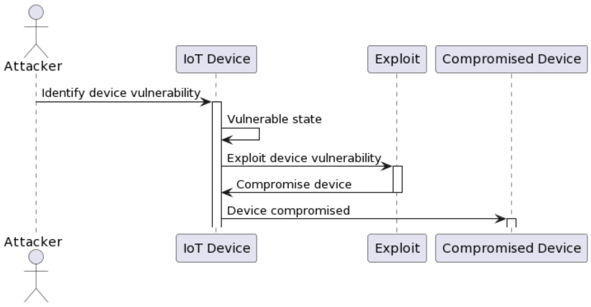

Figure 2: Communication Channel Attacks

An IoT system operates on multiple vital communication protocols to exchange data and connectivity across multiple devices (Sun et al. 2016). However, these various protocols introduce vulnerabilities that hackers can exploit. Some communication protocols that can be listed are MQTT, CoAP, Zigbee, and BLE (Bluetooth Low Energy). Eavesdropping is when attackers intercept and capture wireless communications between IoT devices to gain unauthorized access to data from sensors, the user, or even alter the commands. Jamming is when intruders use high-frequency signals to disrupt the link of communication between IoT nodes and discourage them from communicating or exchanging any data. Another dangerous attack is MitM – Man-in-the-Middle attack. In this attack, the hacker intercepts, relays communication between two IoT devices and secretly monitors or alters the transmitted data. In this attack, sensitive data can be eavesdropped on or manipulated with malicious injections of commands and signals in the network.

4.1.3 Data Privacy and Integrity

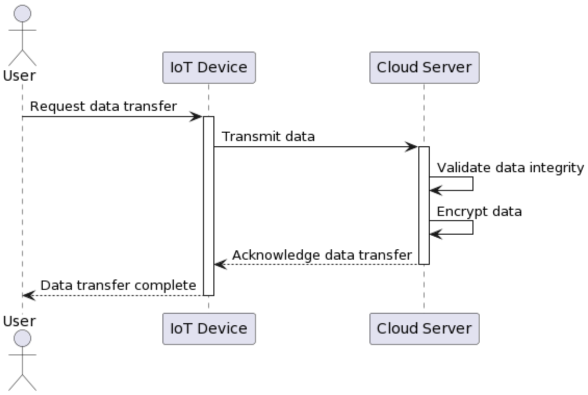

Figure 3: Data Encryption

In the previous sections, we discussed how data and sensitive information could be violated during IoT attacks. Due to the sensitive nature of the data that IoT devices collect and communicate, data privacy and integrity are significant issues in the IoT field (Roman et al. 2013). The device often collects and communicates sensitive data related to financial, health, or personal information, which makes them a vulnerable attack target for cybercriminals. Weak defence mechanisms in IoT devices result in them being exploited to gain unauthorized access to collected and transmitted data. These weaknesses include default credentials, weak authentication methods, and unpatched vulnerability errors. Attackers can manipulate sensor data to achieve malicious goals. Some attacking approaches are false information injection, and control command modification, leading to the malfunctions of individual devices and the entire system. Attackers may get access to the systems or the channels used for communication, extract sensitive information, and then reveal it to uninvited parties. Significant repercussions from these breaches could include identity theft, financial fraud, or unlawful surveillance. Wireless communication can also cause exploitation, as data can be captured and decrypted, compromising confidentiality and integrity. User trust in IoTs systems is also in question as suspicion on the type of information they gather and store.

4.1.4 Distributed Denial of Service (DDoS) Attacks

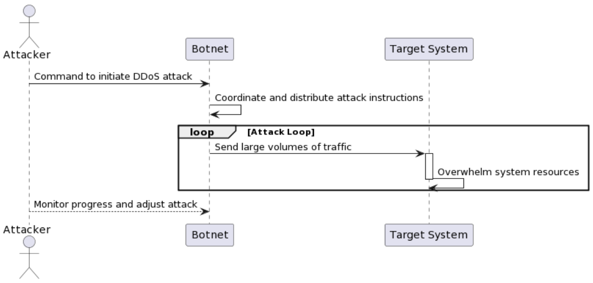
Attacker
Botnet
Target System
Command to initiate DDoS attack
Coordinate and distribute attack instructions
loop
[Attack Loop]
Send large volumes of traffic
Overwhelm system resources
Monitor progress and adjust attack
Attacker
Botnet
Target System

Figure 4: DDoS Attacks

DDoS attacks pose considerable threats in the field of IoT, as IoT botnets have been leveraged to launch widespread DDoS attacks (Antonioli et al. 2018). These breaches badly damage services and the physical infrastructure, causing system corruption and financial downfalls. DDoS attacks aim to overwhelm a system by flooding it with a high volume of illegal traffic, take away the processing power and resources of the targeted system and make it inaccessible to authenticated users. Amplification techniques are often implemented, exploiting the vulnerabilities of specific network protocols and amplifying the volume sent to the traffic. Attacks launched through IoT botnets can result in service disruption and even cause critical damage to the infrastructure. The vulnerabilities among most IoT devices can be due to out-of-date hardware updates and usage of default credentials, turning them into an appealing attack target for cybercriminals.

4.1.5 Supply Chain Attacks

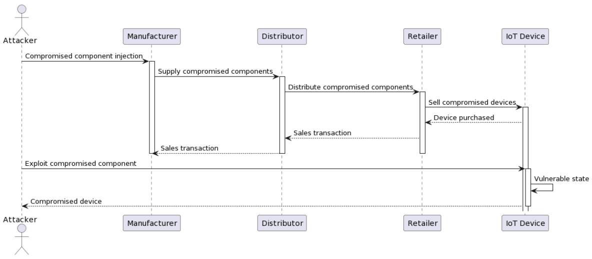

Figure 5: Supply Chain Attacks

Supply chain attacks pose a critical threat to IoT devices due to the number of components in supply chains that can be compromised or injected with malicious commands and malfunctions (Bhasin & Singh 2020). The complexity of IoT supply chains and the involvement of stakeholders, manufacturers, and distributors make them a prime target for significant cyber attacks. Cybercriminals can compromise the devices by replacing different components during production and distribution. These components include malicious hardware or backdoor access to control points. Faulty components that resemble real ones represent an additional risk, as built-in flaws can be included alongside harmful functionalities. These components commonly need the appropriate quality assurance, security assurance, and security precautions, making them more appealing to attackers. Attackers may get unauthorized access to and control IoT devices due to supply chain vulnerabilities, allowing them to compromise important information, stop operations, or use the devices as launching pads for other attacks. These kinds of assaults compromise the integrity and trust of IoT systems, eroding faith in the ecosystem as a whole and harm not only specific devices but also entire networks and vital infrastructure.

4.2 Existing Systems, Methods, Strategies, Mechanisms, and Solutions

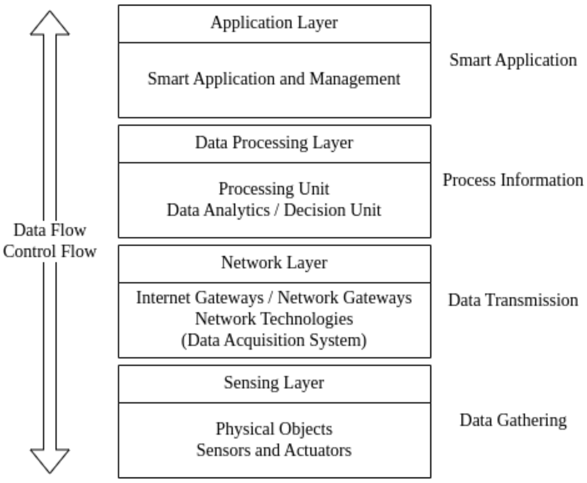

Figure 6: IoT System Architecture

Existing systems, methods, strategies, procedures, and solutions address attacks on Internet of Things (IoT) devices. These strategies seek to reduce weaknesses and defend IoT systems against various dangers. These current systems, approaches, plans, procedures, and remedies are properly described below, examining the problems they address and justifying their potential efficacy.

4.2.1 Secure Authentication

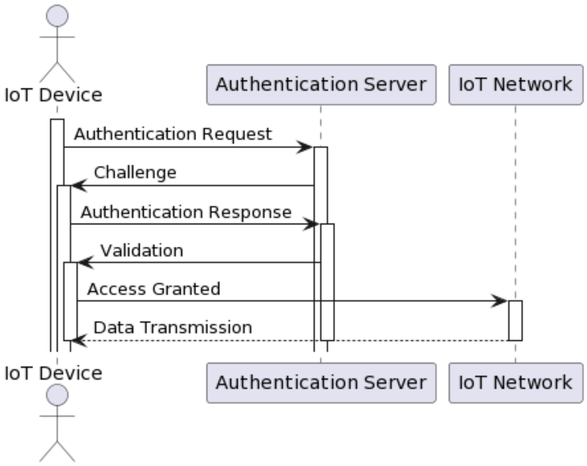

Figure 7: Secure Authentication to IoT Networks

For IoT device security, reliable authentication procedures are essential. Using methods like mutual authentication and digital certificates is essential in the IoT setting, where many connected devices are present (Lang & Letaief 2016). Mutual authentication establishes trust and prevents illegal access by enabling the IoT device and the network to confirm each other's identities. IoT device authenticity can be verified via digital certificates, allowing for secure data transfer and communication. Putting these safeguards in place significantly reduces the danger of unwanted access and potential data breaches. These authentication procedures protect sensitive data and uphold the integrity of IoT networks, making the IoT ecosystem more solid and secure.

4.2.2 Encryption

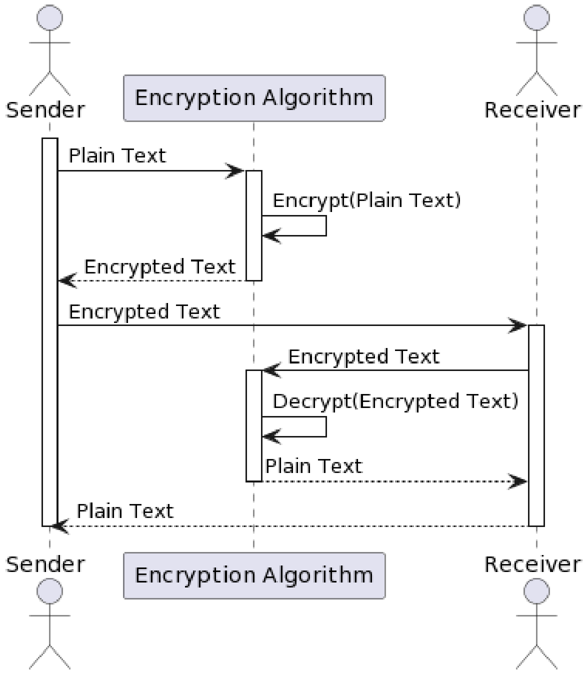

Figure 8: Encryption Procedures

Encryption methods are critical in the IoT field to ensure the privacy and integrity of data transmitted between IoT devices and the entire system (Smith 2022). The amount of sensitive data being exchanged constantly requires effective and secure encryption mechanisms. Symmetric and asymmetric encryption are commonly used to secure communication channels and protect data. Symmetric encryption implements a shared key to carry out data encryption and decryption. The approach assures that encrypted data cannot be decrypted without the key, even when compromised. Asymmetric encryption implements two keys, a public key and a private key. As can be interpreted from their name, the public key is shared publicly while the private key is kept confidential. Data encrypted using the public key can only be decrypted using the private key, which ensures bi-directional communication between devices.

4.2.3 Intrusion Detection and Prevention Systems (IDPS)

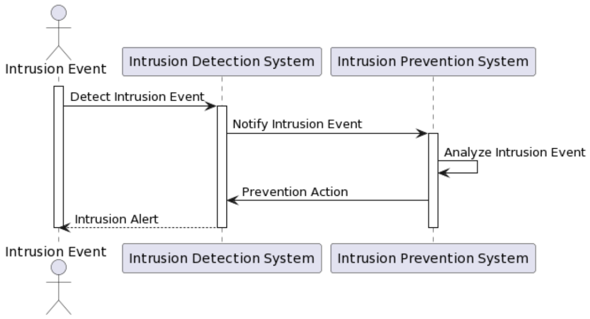

Figure 9: IDPS Procedures

IDPS play an instrumental role in protecting IoT networks from threats and malicious intents (Johnson & Brown 2021). These systems are specifically created to control and monitor the network traffic to detect dishonest behaviours and unauthorized access. IDPS implements various approaches to detect and prevent intrusions: anomaly detection and signature-based detection. Anomaly detection is where the system publishes a baseline of normal behaviour and identifies any abnormal activities that differ from that baseline. Those activities can be potential intrusions and threats. Signature-based detection compares the network traffic and system activities with records stored in a database for signals of attacks. If a record matches the traffic record, it indicates that the threat is known to carry out appropriate action and prevent damage to the system from intrusions. By closely monitoring IoT networks, IDPS can promptly detect and respond to cyber-attacks. The systems provide real-time alerts or programmed actions to deal with the intrusion incident. IDPS has contributed significantly to the enhancement of security measures of IoT systems.

4.2.4 Secure Over-the-Air (OTA) Updates

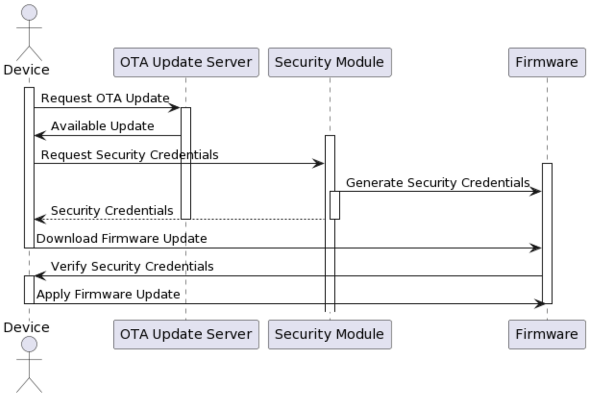

Figure 10: OTA Updates for Firmware

Secure Over-the-Air (OTA) update methods are instrumental for deploying software and hardware updates for IoT devices (Thompson & Patel 2023). These mechanisms ensure that manufacturing companies and system administrators can update their software and hardware promptly, eliminating the task of getting physical access to each device. The goal of OTA updates is to detect vulnerabilities, patch those errors, and enhance the security of IoT devices. By sending updates through secure channels, OTA prevents any emerging unauthorized modifications to the device's software or hardware. Secure updates ensure that malicious injections and actors will be minimized. Encryption and authentication techniques are employed to secure the update repercussion. Each device authenticates the updates using its dedicated certificates or authentication keys. Using OTA, IoT systems and their devices can stay up-to-date with regular patches and security updates. An up-to-date system will reduce the risk of cyber-attacks and enhance the reliability of devices over time.

4.2.5 Access Control

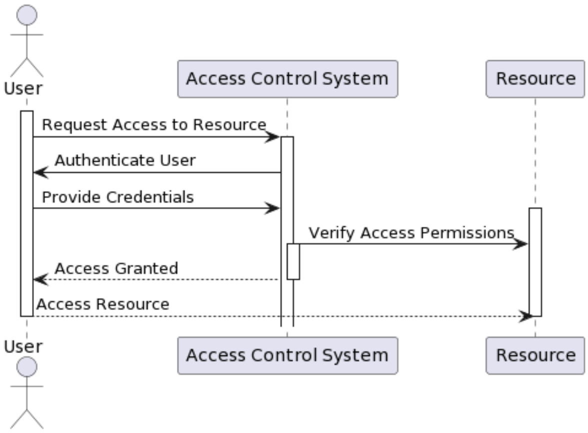

Figure 11: Access Control to Private Resources

Access control mechanisms are critical to ensuring the security and integrity of IoT systems by setting the privileges and permissions granted to IoT devices (Williams & Jones 2022). These methods indicate that only authorized devices and users have the required access rights to control functions and private data within an IoT ecosystem. Upon implementation of access control, companies can establish controls over device permissions. These controls are read, write, execute, and admin for a single device or a group of devices. The techniques used for access control are authentication, authorization, and permission accountability to ensure authoritative access. Credentials, biometric data, or cryptographic keys help achieve the integrity and security control of the IoT system. Authentication determines the actions and resources a device or user can access. On the other hand, accountability keeps records of the authorized device's and user's actions to identify illegal and malicious intent. Implementing an efficient access control system enable organizations to prevent unauthorized access, protect private data, and prevent critical actions from being triggered by cyber attackers.

The problems brought on by new attacks on IoT devices, such as unauthorized access, data breaches, invasions, unauthorized alterations, and illegal control, are partly lessened by these current systems and solutions. Organizations may improve the security of their IoT deployments and safeguard the confidentiality and integrity of IoT systems and data by putting these steps in place. However, ongoing research and development are required to remain ahead of expanding IoT attacks and to investigate fresh ideas for countering new dangers.

The literature review identifies the principal problems and difficulties new IoT-related attacks bring. Authentication, secure communication, and intrusion detection and prevention are the main areas where existing systems, methods, strategies, procedures, and solutions focus. Security, resource limitations, and scalability trade-offs are still important factors. As IoT devices become more integrated into daily life, it is crucial for innovations and research to address emerging IoT attacks and ensure the safety and security of users.

5 Discussion

The literature review has shed important light on the topic on the topic of emerging attacks on IoTs and their possible security implications. This discussion aims to evaluate the given literature view and assess the advantages and disadvantages, as well as the positive and negative aspects of the known attacks and their possible effects on IoT systems. Suggestions and potential recommendations will also be made throughout this discussion.

5.1 Critical Analysis of Selected Literatures

5.1.1 Advantages

5.1.1.1 Comprehensive coverage

It is certainly helpful that the literature covers all attack methods and security issues in detail. The literature identifies the numerous places where IoT systems are vulnerable by examining various forms of attack, such as device exploitation, network vulnerabilities, and social engineering (Roman et al. 2011). Understanding these vulnerabilities is essential for implementing the proper security precautions and creating reliable IoT systems.

5.1.1.2 Real-world examples

The literature considerably improves comprehension of IoT security concerns by incorporating real-life scenarios and case studies. Researchers and practitioners can understand the practical ramifications of security breaches in IoT systems by looking at actual instances and their effects. Examples from everyday life offer palpable proof of the possible impact on privacy, safety, and financial well-being.

5.1.1.3 Technical insights

The literature considerably improves comprehension of IoT security concerns by incorporating real-life scenarios and case studies. Researchers and practitioners can understand the practical ramifications of security breaches in IoT systems by looking at actual instances and their effects. Examples from everyday life offer palpable proof of the possible impact on privacy, safety, and financial well-being.

5.1.2 Disadvantages

5.1.2.1 Limited focus

Some writing on IoT security may have a limited scope, focusing on particular factors while ignoring other crucial ones. This narrow focus might constrain the development of a comprehensive understanding of IoT security concerns, which can lead to knowledge gaps. As an illustration, research might primarily concentrate on network-level security while ignoring device-level vulnerabilities or risks related to social engineering.

5.1.2.2 Lack of standardization

Establishing procedures and regulations for IoT security presents an enormous challenge. Different perspectives and methodologies are frequently used in the literature due to the variety of IoT devices, communication protocols, and deployment scenarios (Rahman et al. 2014). Consistency may lead to clarity and consistency issues when implementing security measures. The industry must cooperate to establish uniform standards, rules, and best practices to give a united approach to IoT security.

5.1.2.3 Time sensitivity

IoT security is an active topic where novel attack methods and vulnerabilities continually appear. The literature, especially older publications, might need to cover the most recent dangers and defences, which makes it less applicable to tackling today's security issues. Continuous study and knowledge exchange are required to get over this obstacle. Researchers, practitioners, and organizations ought to keep up with the latest developments, proactively improve the body of knowledge, and engage in networks and platforms for information sharing.

5.2 Impacts of emerging attacks on IoT systems

5.2.1 Positive Impacts

5.2.1.1 Enhanced security awareness

The literature raises awareness of the security risks and challenges connected with IoT deployments among IoT consumers, manufacturers, and distributors. This awareness encourages proactive IoT security approaches and more robust security solutions.

5.2.1.2 Technological advancement

The outlined security challenges accelerate IoT security technology improvements. Developing creative solutions and defences against new dangers in response to attacks leads to an overall improvement in IoT security technologies.

5.2.2 Negative Impacts

5.2.2.1 Compromised privacy

IoT devices capture a great deal of private data, posing security concerns. Security breaches may provide unwanted access to personal data, jeopardizing user privacy and raising the possibility of fraud or other privacy crimes.

5.2.2.2 Economic damage

IoT security breaches can cost people, companies, and occasionally whole sectors large sums of money. Remediation, system recovery, and reputation damage can be expensive, adversely impacting IoT acceptance and economic expansion.

5.2.2.3 Safety risks

Security vulnerabilities can pose serious safety threats in some IoT applications, particularly in the automotive, healthcare, and essential infrastructure industries. In these circumstances, unauthorized access to or manipulation of data might result in complex cases, highlighting the necessity of solid security measures.

5.3 Possible solutions and recommendations

5.3.1 Robust Device Security

Manufacturers should prioritize device security, who should also use secure authentication methods, frequent firmware updates, and incorporate self-defence features. In addition, IoT device compliance with essential security criteria can be ensured through industry-wide security standards and certifications.

5.3.2 Secure Communication

To ensure safe data transfer between IoT devices and networks, encrypted communication methods like Transport Layer Security (TLS) should be used. Mutual authentication and safe critical exchange implementation can even boost communication route security.

5.3.3 Regular Assessments

Businesses and individuals should regularly conduct inspections and vulnerability assessments to find vulnerabilities in IoT deployments. This proactive strategy enables fast vulnerability mitigation before malicious actors exploit them.

5.3.4 User Awareness and Education

It is crucial to inform IoT users of their devices' security dangers and the recommended methods for protecting their IoT systems. This education may entail using secure passwords, segmenting networks, and being wary of firmware updates and third-party software.

6 Conclusion

In conclusion, the introduction of the Internet of Things (IoT) has transformed technology and benefited many industries in countless ways. However, it has also introduced new vulnerabilities and security threats that must be addressed to ensure IoT systems' long-term viability and trustworthiness. This literature review has clarified the difficulties and weaknesses related to attacks on IoT networks and devices. It has emphasized the dangers of supply chain assaults, device vulnerabilities, communication channel attacks, data privacy and integrity concerns, and DDoS attacks. These dangers can result in significant system disruptions, data manipulation, privacy breaches, and illegal access. Numerous tactics and solutions have been developed to reduce these risks. IoT systems' security has been improved by implementing secure OTA updates, access control systems, intrusion detection and prevention systems, and encryption approaches. These steps are taken to build relationships of trust, and specific communication channels, identify and stop intrusions, guarantee the accuracy of software updates, and manage device access. Collaboration between stakeholders, including technology providers, industry leaders, politicians, and researchers, is necessary to address the latest attacks on IoTs. By promoting guidelines, exchanging threat intelligence, and setting industry standards and laws, it is critical to promote a culture of security. Ongoing research and innovation are required to keep ahead of changing threats and provide robust security solutions that can accommodate the ever-evolving dynamics of the IoT world. The potential of IoT technologies can be fully exploited while protecting vital infrastructures, individual privacy, and the security and integrity of IoT systems by addressing these issues. Our capacity to comprehend and reduce the risks associated with new threats will determine how thriving the IoT ecosystem will be, paving the path for a resilient, secure, and reliable linked world.

References

Abbas, S. G., Husnain, M., Fayyaz, U. U., Shahzad, F., Shah, G. A. & Zafar, K. (2020), Iot-sphere: A framework to secure iot devices from becoming attack target and attack source, *in* '2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)', pp. 1402–1409.

Abomhara, M. & Køien, G. M. (2014), Security and privacy in the internet of things: Current status and open issues, *in* '2014 International Conference on Privacy and Security in Mobile Systems (PRISMS)', pp. 1–8.

Antonioli, D., Le, T., Ochoa, M., Rrushi, J., Abreu, F., Dacier, M. & Stringhini, G. (2018), Detecting credential compromise in enterprise settings, *in* 'Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security', pp. 1873–1875.

Bhasin, S. & Singh, R. (2020), Challenges and security threats in internet of things: A comprehensive review, *in* '2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT)', IEEE, pp. 1–6.

Chasaki, D. & Mansour, C. (2015), 'Security challenges in the internet of things', *International Journal of Space-Based and Situated Computing* **5**, 141–149.

Johnson, A. & Brown, L. (2021), Intrusion detection and prevention systems for iot networks, *in* 'Proceedings of the International Conference on Internet of Things (IoT)', IEEE, pp. 145–154.

Lang, M. & Letaief, K. B. (2016), 'Analysis of security threats and vulnerabilities in mobile environment', *IEEE Wireless Communications* **23**(4), 29–35.

Rahman, M. S., Raju, R. & Buyya, R. (2014), 'A survey on security issues in services computing over cloud computing', *Journal of Network and Computer Applications* **42**, 101–113.

Roesner, F., Kohno, T. & Molnar, D. (2014), 'Security and privacy for augmented reality systems', *ACM Computing Surveys (CSUR)* **47**(4), 1–39.

Roman, R., Zhou, J. & Lopez, J. (2011), 'Security challenges and solutions in the internet of things', *Computer Networks* **57**(10), 2266–2279.

Roman, R., Zhou, J., Lopez, J. & Ning, H. (2013), 'On the features and challenges of security and privacy in distributed internet of things', *Computer Networks* **57**(10), 2266–2279.

Smith, J. (2022), 'Encryption methods for iot security', *Journal of Internet Security* **15**(3), 78–92.

Sun, Y., Wang, Y., Wang, H. & Zhang, Y. (2016), 'Iot security techniques based on network behavior', *IEEE Communications Magazine* **54**(9), 36–41.

Thompson, R. & Patel, A. (2023), 'Secure over-the-air updates for iot devices', *Journal of Security Engineering* **8**(2), 112–128.

Williams, C. & Jones, E. (2022), Access control mechanisms for iot systems, *in* 'Proceedings of the International Conference on Internet of Things (IoT)', IEEE, pp. 231–240.