Southeast Europe Journal of Soft Computing ISSN 2233 – 1859
Available online: http://scjournal.ius.edu.ba

Vol 13, No. x1, March 2024, pp. 69-78

Comprehensive Analysis of the Current State of Cyber Security Measures for IOT Devices

[1*]M.Chithik Raja, [2]Mohamed Musallam Bakhit Al-Mahri [3] Devarajan Veerasamy and [4]Sunil Thomas Karickom

[1-4] Department of Information Technology,
College of Computing and Information Sciences,
University of Technology and Applied Sciences Salalah
Dhofar Region, Salalah, Sultanate of Oman
Corresponding Author: chithik.sinnaiya@utas.edu.om

Article Info

Article history:

Article received on 30 12 2023

Received in revised form 17 01 2024

Keywords:

Internet of Things, Cyber Security, Risk Analysis, Threat Modelling, Vulnerability Analysis, Mitigation Strategies

ABSTRACT: A new era of connectivity has been brought about by the Internet of Things (IoT), which presents unheard-of chances for innovation in a wide range of sectors and applications. IoT device proliferation does, however, also bring with it serious cybersecurity challenges. This systematic review examines the state of cyber security risk in the Internet of Things (IoT) space today, providing a thorough analysis of the research that has already been done and the approaches that have been used to assess and mitigate these risks. We study different aspects of cyber security risk within the IoT context, such as threat modeling, risk assessment techniques, vulnerability analysis, and mitigation strategies, drawing from a wide range of peer-reviewed articles, industry reports, and white papers. Additionally, the review draws attention to the unique qualities of IoT systems—such as heterogeneity, scalability, and resource constraints—that increase the risks associated with cyber security. The current status of cyber security protocols for Internet of Things devices is thoroughly examined in this paper. This paper will examine the distinct difficulties presented by the Internet of Things environment, the security flaws that these gadgets frequently display, and the possible risks they may encounter. Furthermore, the paper will examine the diverse approaches, tools, and methods presently utilized to enhance the security of Internet of Things devices. We will also talk about the regulatory environment that oversees IoT security and the ongoing research and development initiatives aimed at improving it. In order to help direct future efforts in safeguarding our digital, interconnected world, we hope to offer a comprehensive, perceptive analysis.

1. INTRODUCTION

The Internet of Things, or IoT, has become a ground-breaking idea in the quickly changing field of digital technology and has completely changed the way we interact with it. IoT devices are now widely used, bringing previously unthinkable levels of convenience and efficiency to our everyday lives. These devices range from industrial sensors to smart home appliances. But as long as these gadgets are used more and more, cybercriminals will always find them to be appealing targets. In order to protect these devices and the data they handle, it is imperative that strong cybersecurity measures be put in place. Our research shows that even though there has been significant advancement in our knowledge of and response to IoT cyber security threats, there are still a number of important holes. Among these are the absence of standardized risk assessment techniques and the requirement for more successful security measure integration into IoT system architecture. We highlight the need for an all-encompassing strategy to IoT cyber security that takes organizational, regulatory, and technical factors into consideration as we offer recommendations for future research.

2. CHALEENGES POSED BY THE IOT LANDSCAPE

Cybersecurity faces many issues as a result of the wide and constantly changing Internet of Things (IoT) landscape. These difficulties are caused by the distinctive qualities of Internet of Things devices as well as the intricacies of the networks in which they function.

Heterogeneity: The variety of IoT devices is immense. Their manufacturers, operating systems, and capabilities differ greatly between them. Because of this variability, the environment around cyber security is complicated, making it challenging to define consistent security standards or procedures that apply to all devices [1].

Scalability: Another major obstacle is the sheer number of IoT devices. By 2025, there will be more than 30 billion IoT devices worldwide, according to Statistics. It is a difficult undertaking to manage and secure so many gadgets. [2][3].

Resource Constraints: The processing and memory capacity of many Internet of Things (IoT) devices is often limited because they are designed to be small and energy-efficient. Due to resource constraints, some devices might not be able to integrate advanced security features like encryption and intrusion detection systems. [4].

Data Privacy: Sensitive data, including private and corporate information, is frequently gathered by IoT devices. Keeping this data private and secure is a major challenge, especially in light of the possibility that it could be accessed on the device itself or intercepted during transmission. [5].

Lack of Security by Design: Security is not given enough consideration in the design of many IoT devices. Rather, the emphasis is frequently on development speed and functionality. Devices with this condition may have built-in security flaws, such as outdated software and weak default passwords. [6].

Interconnectivity: Because Internet of Things devices are interconnected, a security breech in one device may have an effect on numerous others. Malware may be able to spread swiftly throughout a network of devices thanks to this connectivity. [7].

Complex Supply Chain: The Internet of Things supply chain is frequently intricate, encompassing numerous manufacturers, developers, and service providers. Because of its complexity, it may be challenging to guarantee security at every stage of the device's lifecycle, from deployment and maintenance to design and manufacture. [7],[8].

A multifaceted strategy combining technological advancements, governmental regulations, and a security-conscious culture among IoT device manufacturers and users is needed to address these issues. Establishing an IoT environment where security is a fundamental component of every device's operation and design rather than an afterthought is necessary.

3. LITERATURE REVIEW

Security is a basic need for IoT platforms, according to a thorough examination of the state of cyber security measures for IoT devices as of right now[9]. IoT will grow more globally as a result of the deployment of 5G networks, but there are security issues that must be resolved as well[10]. ACORN is the most efficient scheme in terms of power consumption and resource utilization among the lightweight authenticated encryption (LAE) algorithms developed for Internet of Things (IoT) systems[11]. However, due to resource limitations and heterogeneous protocols, designing reliable intrusion detection systems for IoT environments presents challenges[12]. Maintaining confidentiality, authentication, access control, and integrity in Internet of Things networks requires efficient security and privacy protocol[13]. The shortcomings and difficulties with lightweight authenticated encryption and intrusion detection systems for the Internet of Things require more investigation. The resource limitations and heterogeneous protocol stacks of IoT environments frequently render traditional security methods ineffective. [14]. As a result, there is a need for learning-based approaches, particularly those that combine machine learning and IDS, to address the shortcomings of non-learning based systems [15]. However, there is a lack of production-grade models in this area [16]. Additionally, the integration of cloud computing with IoT has raised security concerns, but deep learning techniques show promise in addressing these challenges [17]. Overall, future research should focus on enhancing cybercrime investigations, improving cloud-based IoT security, and finding innovative solutions to prevent cyber-attacks.

4. IOT THREAT MODELING

Threat modeling is a critical process in the development and maintenance of IoT systems. It involves the identification and quantification of security risks associated with an IoT product and its surrounding ecosystem, ideally conducted during the product design phase, a concept known as "security by design" ("IoT Security Audits 2/4): IoT Threat Modelling - Medium").

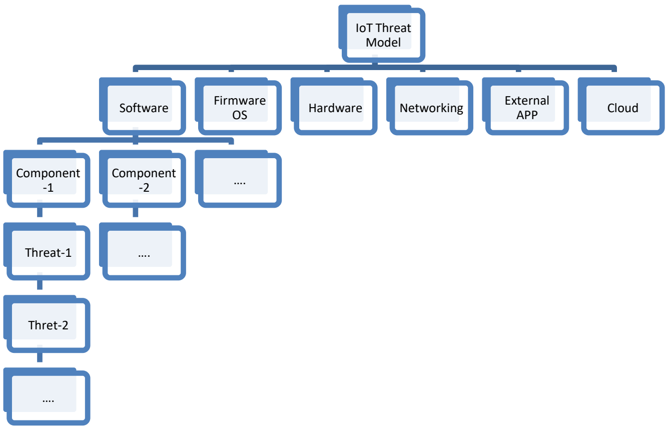


Figure 1 IoT Based Threat Modelling Snap Chart

Partitioning the entire system into multiple components is the first stage in threat modeling. When discussing the Internet of Things, many different types of components may be involved. Hardware components, the IoT device's operating system or firmware, any software that runs on the device, networking protocols and interfaces, Applications on the outside that allow users to interact with Internet of Things devices, like mobile apps, cloud services, and third-party APIs, The next stage is for each of the components to identify the actual threats after they have been identified as the pieces under analysis.

Figure 1 shows the five steps that make up a typical threat modeling process. Threat mapping, risk assessment, asset identification, mitigation capabilities, and threat intelligence are the stages. Different insights and visibility into the organization's security are provided by each of these steps.

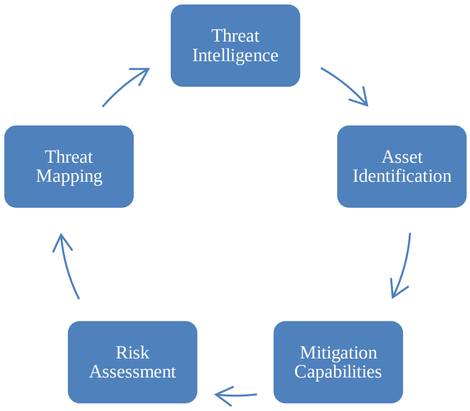


Figure 2 IoT Based Threat Modelling Process

Threat Intelligence: This is the starting point of the diagram. It is an acronym for information gathering regarding possible dangers to the Internet of Things.

Threat Intelligence and Asset Identification are related. In this step, the important IoT system assets that might be attacked by malicious actors are identified. These could consist of data, software, or hardware. The diagram goes from Asset Identification to Mitigation Capabilities. This phase is comprehending the threat and putting precautions in place to lessen its likelihood. Risk assessment, which comes next, has to do with mitigating capabilities. Here, the potential impact of each threat is evaluated based on a number of factors, such as the threat's likelihood of materializing and the severity of its consequences. The final feature on the diagram is Threat Mapping.

5. IOT BASED RISK ASSESMENT TECHNIQUES

S. No.	Risk Assessment Techniques	Description	Method
1	Fault Tree Analysis (FTA)	Determine and evaluate the likelihood of security threats. Logic gates are used to dissect a potential fault (or failure) into its component parts at a lower level.	top-down, deductive analytical
2	Failure Mode and Effect Analysis (FMEA)	Figuring out every potential flaw in a product's design, production method, or manufacture. It can be applied to the analysis of possible failure modes in the context of IoT and their effects on the overall performance of the system.	step-by-step approach
3	Attack Tree Analysis (ATA)	designed specifically to comprehend system security. An attack tree offers an organized method, based on different types of attacks, for characterizing a system's security. The attack's ultimate objective is represented by the root of the tree, and its various means of attainment are symbolized by the leaves.	Tree structure
4	Attack Surface Analysis (ASA)	Identifying all possible points where an unauthorized user could try to enter data to or extract data from an environment. In the IoT context, this could involve any communication interface, such as Wi-Fi, cellular, or Bluetooth.	top-down, deductive analytical
5	Risk Matrix	Graphical method of ranking and measuring risks. Plotting of each risk according to its likelihood and severity on the matrix helps decision-makers concentrate on high-priority risks.	Matrix
6	Security Risk Metrics	Technique to gauge and measure an IoT system's security posture. They can be used to monitor advancements over time, assess security performance in relation to industry norms or benchmarks, and guide risk management choices.	Quantitati ve

Table 1 IoT Based Risk Assessment Techniques

An essential part of the cyber security framework for Internet of Things (IoT) systems is risk assessment. It assists in recognizing, assessing, and ranking risks according to their possible consequences and probability of occurrence. Here, we go over a few methods that are prominently applied to the Internet of Things (IoT) as shown in table 1.

S. No. Risk Assessment Techniques Description Method

1 Fault Tree Analysis (FTA) Determine and evaluate the likelihood of security threats. Logic gates are used to dissect a potential fault (or failure) into its component parts at a lower level. top-down, deductive analytical

2 Failure Mode and Effect Analysis (FMEA) Figuring out every potential flaw in a product's design, production method, or manufacture. It can be applied to the analysis of possible failure modes in the context of IoT and their effects on the overall performance of the system. step-by-step approach

3 Attack Tree Analysis (ATA) designed specifically to comprehend system security. An attack tree offers an organized method, based on different types of attacks, for characterizing a system's security. The attack's ultimate objective is represented by the root of the tree, and its various means of attainment are symbolized by the leaves. Tree structure

4 Attack Surface Analysis (ASA) Identifying all possible points where an unauthorized user could try to enter data to or extract data from an environment. In the IoT context, this could involve any communication interface, such as Wi-Fi, cellular, or Bluetooth. top-down, deductive analytical

5 Risk Matrix Graphical method of ranking and measuring risks. Plotting of each risk according to its likelihood and severity on the matrix helps decision-makers concentrate on high-priority risks. Matrix

6 Security Risk Metrics Technique to gauge and measure an IoT system's security posture. They can be used to monitor advancements over time, assess security performance in relation to industry norms or benchmarks, and guide risk management choices. Quantitative

Every one of these methods adds a unique viewpoint and set of instruments to the risk assessment procedure. In actuality, they are frequently combined to give a thorough picture of the security threats connected to an Internet of Things system. By putting these strategies into practice, companies can improve the security and resilience of their IoT systems by proactively mitigating possible threats.

6. IOT BASED VULNERABILITY ANALYSIS

Although the Internet of Things (IoT) revolution has increased connectivity and convenience, it has also created a number of potential security risks. Malicious actors may take advantage of these vulnerabilities, resulting in service interruptions, data breaches, and other security incidents. We will examine the common vulnerability types discovered in Internet of Things systems in this section, along with the analysis techniques employed.

A.Unsecured Communication: Since many IoT devices communicate over unprotected networks, they are vulnerable to man-in-the-middle attacks and eavesdropping. To protect against these threats, encryption protocols and secure communication channels are crucial.

B.Inadequate Authentication/Authorization: IoT devices are frequently vulnerable to issues like weak passwords, inadequate access controls, and the absence of two-factor authentication. These may make it possible for unauthorized users to take over devices or access private information.

C.Poorly Managed Software Updates: IoT devices are susceptible to known security flaws if they do not receive regular software updates or patches. Some devices require users to manually install updates, or they do not support updates.

D.Device Physical Security: An attacker may be able to disable an IoT device, install malicious firmware, or extract sensitive data if they have physical access to the device.

E.Privacy Concerns: Large volumes of personal data are frequently collected and stored by IoT devices, making them susceptible to abuse or illegal access.

F.Default Settings: The default usernames and passwords that come with a lot of Internet of Things devices are frequently left unmodified by users. Attackers may find this to be a simple way to take over the devices.

G.Insecure Ecosystem Interfaces: Cloud and mobile interfaces for user control and data storage are common in IoT ecosystems. These platforms' lax security protocols make it possible for unauthorized users to access and take control of IoT devices.

H.Lack of Device Identity: A lot of IoT devices don't have a distinct identity or authentication mechanism. As a result, it could be challenging to guarantee that only approved devices are linked to the network and to secure communication between devices.

I.Inadequate Network Security: IoT devices frequently connect to networks that lack adequate security safeguards. This can make them vulnerable to network-based attacks and make it possible for malware to propagate among devices that are linked.

J.Embedded, Hard-Coded Credentials: IoT devices may occasionally include embedded login credentials for cloud interfaces or remote administration. If hackers manage to find these credentials, they can easily access the device and any related data.

Usually, a variety of methods are used to analyze these vulnerabilities, such as threat modeling, static and dynamic code analysis, and penetration testing. In order to find potential vulnerabilities in the system, penetration testing simulates attacks on the system. The process of static and dynamic code analysis entails looking through the IoT device software's source code to find any coding mistakes or unsafe programming techniques that might result in vulnerabilities. The process of threat modeling entails determining possible dangers to the system and evaluating their likelihood and possible consequences.

6.1. Man in the Middle Attack

Two scenarios were available for the MITM attack. Kali Linux and Ubuntu were used by the attacker as the attacker and server virtual machines, respectively, in scenario a). In this case, a Raspberry Pi device was the victim. For focused attacks and to locate victims and server IPs, programs like Ettercap, Advanced IP Scanner, and Wireshark were employed. Comparable experiments were carried out with the Raspberry

Pi operating system acting as the victim. The attacker in scenario b) used Windows 10 virtual machine (VM) and Kali Linux, and Metasploit was used as the server. Ettercap and Wireshark were the tools used in this scenario to spy on the usernames and passwords of the victims.

6.2. Attack model to analyze vulnerabilities

In order to analyze the Man-in-the-Middle (MITM) attack, two scenarios were tested. In case (a), Kali Linux was used on a Raspberry Pi device for the test, while Ubuntu served as the server. The attack used Wireshark and Ettercap as tools. The IP addresses of the Ubuntu server (192.168.0.102) and Raspberry Pi device (192.168.0.115) were found using Advanced IP Scanner. In this attack, ARP poisoning was used, and the Raspberry Pi's IP address was used to use Wireshark to look up the HTTP protocol. On pages that used the HTTP protocol, during the attack, the victim's username and password were seen as unencrypted credentials coming from the browser.

In scenario b), three virtual machines were used: Kali Linux as the attacker, Metasploitable2 as the server, and Windows 10 as the victim. Ettercap and Wireshark were used as tools for the attack. The IP address of the Windows 10 VM (192.168.0.102) was identified as the device to monitor, and the IP address of the Metasploitable2 VM was selected as the IP address to spoof. ARP poisoning was employed in this attack, and Wireshark was used to search for the HTTP protocol using the Windows 10 IP address. Unencrypted credentials, including the victim's username and password, were observed from the browser page during the attack .

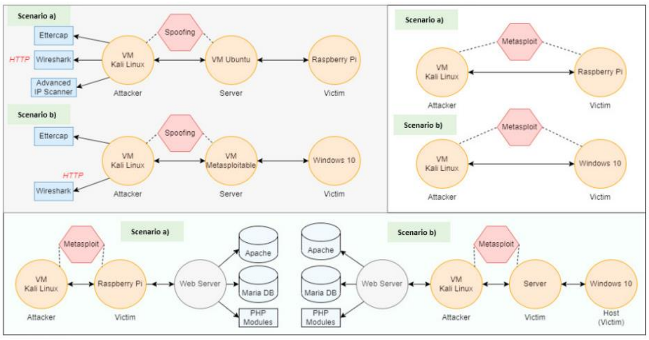
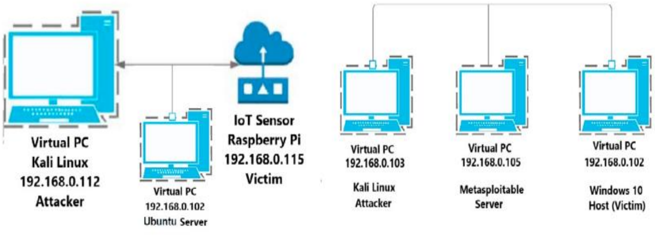


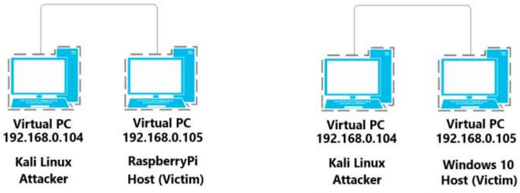
Figure 3 Model for MITM, DoS and Backdoor attacks on a Raspberry Pi.



a) MITM attack from Kali Linux to a Raspberry Pi

b) MITM attack from Kali Linux to Windows10

Figure 4 Network topology: attack Man In The Middle



a) Backdoor attack from Kali Linux to Raspberry Pi using Meterpreter

b) Backdoor attack from Kali Linux to Windows 10 using Meterpreter.

Figure 5 Network topology - Backdoor Attack

6.3. Back Door Attack

Test a) involved two virtual machines.

Kali Linux was used as the attacker and a Raspberry Pi as the victim. Metasploit was used to create a payload from a Kali Linux VM in the following format: msfvenom -p linux/x86/meterpreter/reverse tcp LHOST= [AttackerIP] LPORT=[ListeningPort] -f elf > shell.elf. The payload needed to be executed on the victim's system (in this case his Raspberry Pi), and before executing the file, the attacker had to grant the file execute permissions. Once the file was executed on the victim's system, a listening handler from Kali Linux's Metasploit interface was connected to the victim's computer, allowing remote control over him. System information such as name, operating system, version, and architecture can be obtained using commands such as sysinfo and ipconfig.

Test b) used two virtual machines, Kali Linux as the attacker and Windows 10 as the victim.Metasploit was used to create a payload from a Kali Linux VM using the msfpayload

module for Windows in the following format: msfvenom -p windows/meterpreter/reverse tcp LHOST=[AttackerIP] LPORT=[ListeningPort] -f exe > Shell .EXE. The payload needed to run on the victim's system after disabling Windows Defender Firewall and disabling all virus and threat protection options. Once the file was executed on the victim's system, a listening handler from his Metasploit interface on Kali Linux was connected to the victim's computer, allowing remote control.System information such as name, operating system, version, architecture, and domain can be obtained using commands such as sysinfo. It was possible to take a screenshot of the victim's screen using the screenshot command and navigate to directories and files within the system using shell commands. You can also create, delete, and move files using commands.

6.3. Denial of Service Attack

Two tests were performed to analyze the denial of service attack.

A) a denial of service attack against the Raspberry Pi as a server, and b) a denial of service attack against the server shown in Figure 4 are shown.Figure 5(a) shows a test using a , Kali Linux virtual machine with a Web server installed (as the attacker) and a Raspberry Pi IoT device (as the victim).The server used Apache and MariaDB database manager with PHP module installed. To perform a denial of service (DoS) attack, the Synflood module (TCP SYN flooding) was loaded from a Kali Linux VM using Metasploit.

The attack was carried out using his IP address 192.168.0.106 on the victim server and using the exploit command .The web server was affected by the attack, resulting in a 4 minute and 15 second delay in loading four web pages in the Raspberry's browser.

The server page at address https: //192.168.0.106 took approximately 35 seconds to load.This is because the attack overloaded the number of available connections that the server could establish. Figure 5(b) shows a test using two virtual machines.One machine runs Kali Linux (as the attacker) and the other runs Windows 10 (as the victim), using a web server built with Apache, the MariaDB database manager, and PHP modules.The Synflood utility module (TCP SYN flooding) was loaded from the Kali Linux VM to perform the DoS attack.The attack was carried out using his IP address 192.168.0.103 on the victim server and using the exploit command. The web server was affected by the attack, causing a significant delay in loading the server page with the address https://192.168.0.103 from the browser.

7. RESULT ANALYSIS

Test- 1 MITA : Both Raspberry Pi and Windows 10 machines were vulnerable to the Kali Linux Man In The Middle (MITM) attack.The Ettercap tool was used to perform MITM and wireshark-enabled network traffic capture on eth0 on Kali Linux.As shown in Figure 5, the attack took approximately 15 minutes to devise and successfully eavesdropped on indefinitely.However, it takes 1 second for the attack to complete his MITM.It has been confirmed that if the page being used has the http protocol, it is possible to see the information that the user sends in the browser. We recommend that you only use sites that use the https protocol and find ways to circumvent MITM to prevent attackers from obtaining information from your device.

Test-2 Back door attack: Successful backdoor attacks were performed against Raspberry Pi and Windows 10 using Kali Linux, Metasploit Framework, and payloads. This attack created a backdoor that allowed the attacker to take control of the victim's computer. As shown in Figure 6, devising the attack took 13 minutes on Raspberry Pi and 15 minutes on Windows 10. However, the backdoor attack itself took just one second. Compared to the Raspberry Pi, Windows 10 had additional commands available, such as the screenshot command to capture the screen of a Windows 10 computer. I was able to access shell commands for command line access on both Windows 10 and Raspberry Pi. However, unlike Windows 10, the Raspberry Pi did not have the ability to access directories, folders, or files.

Test-3 Denial of Services : Denial of Service (DoS) attacks can target web servers or Raspberry Pis.An attack on web server accessed from Windows 10 caused websites to load.However, after the attack, the server loaded successfully.Similarly, configuring the Raspberry Pi as a server will increase load times in the event of a DoS attack.'s four web pages took approximately 4 minutes and 15 seconds to load during the attack, compared to the usual 40 seconds.Furthermore, one attack on the server took 35 seconds, and the speed slowed down even further after three additional attacks from different devices.As shown in Figure 6, the attack details took 8 minutes in both cases.However, the DoS attack itself took only 60 seconds to execute.A server connected to the Raspberry Pi can act as a means to obtain information from sensors and other IoT devices, or it can connect directly to the Raspberry Pi itself.If server stops working, you risk losing incoming data.

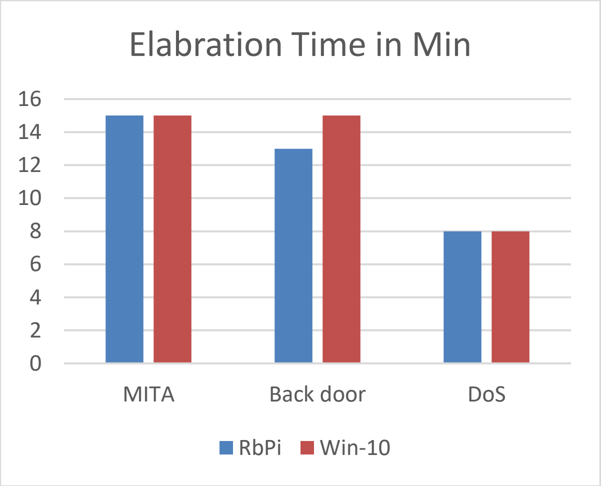


Figure 6 Elabration Time to Detect the Threat

8. IOT BASED THREAT MITIGATION STATEGIES

We go over IoT-based threat mitigation techniques in this section. The numerous risks that the Internet of Things poses must first be understood. These risks can include the potential for physical harm to the devices or networks, unauthorized access to devices or networks, and malicious activity like data theft or manipulation. It is necessary to implement the necessary security measures to mitigate these threats as soon as they are identified.

Using encryption is one method of reducing the risks associated with IoT. Data stored on the device can be secured using encryption, as well as data in transit. Furthermore, it is imperative to incorporate authentication protocols to guarantee that authorized users can access the device or network.

Using intrusion detection and prevention systems is an additional method of mitigating threats. These programs keep an eye out for unusual activity and can notify administrators of possible dangers.Access to specific networks or devices can also be restricted using firewalls. Maintaining the most recent security patches and updates installed on the networks and devices is crucial, to sum up. Additionally, regular audits are necessary to confirm that the latest security measures are being followed. There are several available IoT-based mitigations, such as a comprehensive security strategy that should incorporate firewalls, authentication, encryption, and intrusion detection and prevention in addition to regular audits and updates. To maintain the security of the devices and networks, it is crucial to comprehend potential threats and put the right countermeasures in place.

9. CONCLUSION

But as IoT devices continue to proliferate, hackers will unavoidably find them to be appealing targets. According to our research, there are still a number of crucial gaps in our understanding of and response to IoT cyber security threats, despite significant advancements in this area. These include the requirement for more efficient integration of security measures into IoT system design and the absence of standardized risk assessment methodologies. Cybersecurity faces many challenges as a result of the vast and constantly changing Internet of Things (IoT) landscape. These difficulties are caused by the distinctive qualities of Internet of Things devices as well as the intricacies of the networks in which they function. Their manufacturers, operating systems, and capabilities differ greatly between them. It's a difficult task to manage and secure so many devices. Limitations on Resources: Since many IoT devices are made to be small and energy-efficient, their memory and processing capacity are frequently constrained. The support of advanced security measures like intrusion detection systems and encryption may be limited by these resource limitations on these devices. Devices that have inherent security flaws as a result, like outdated software and weak default passwords, may be produced. Due to its complexity, security may be challenging to maintain throughout the device's lifecycle, including during design, manufacture, deployment, and maintenance. It takes a multifaceted strategy to address these issues, combining technological advancements, governmental regulations, and a security-conscious culture among IoT device manufacturers and users. We highlight the need for an all-encompassing strategy to IoT cyber security that takes organizational, regulatory, and technical factors into consideration as we offer recommendations for future research.

REFERENCES

[1] S. S. Ambarkar and N. M. Shekokar, "A comprehensive survey of existing security techniques in the IOT protocol stack," in Cyber Security Threats and Challenges Facing Human Life, pp. 57–69, 2022. [Online]. Available: https://doi.org/10.1201/9781003218555-7

[2] D.-A. Andrioaia, "Cyber Security Analysis of IOT devices transmitting data in the THINGSPEAK Platform Cloud," in Journal of Engineering Studies and Research, vol. 28, no. 3, pp. 29–33, 2022. [Online]. Available: https://doi.org/10.29081/jesr.v28i3.003

[3] M. Aziz Al Kabir, W. Elmedany, and M. S. Sharif, "Securing IOT devices against emerging security threats: Challenges and mitigation techniques," in Journal of Cyber Security Technology, pp. 1–25, 2023. [Online]. Available: https://doi.org/10.1080/23742917.2023.2228053

[4] S. C.P and M. B.C, "Analysis of security issues, threats and challenges in Cyber–physical system for IOT devices," in SSRN Electronic Journal, 2021. [Online]. Available: https://doi.org/10.2139/ssrn.3882538

[5] C. Kelly, N. Pitropakis, S. McKeown, and C. Lambrinoudakis, "Testing and hardening IOT devices against the Mirai botnet," in 2020 International Conference on Cyber Security and Protection of Digital Services (Cyber Security), 2020. [Online]. Available: https://doi.org/10.1109/cybersecurity49315.2020.9138887

[6] A. Khan and C. Cotton, "Detecting attacks on IOT devices using featureless 1D-CNN," in 2021 IEEE International Conference on Cyber Security and Resilience (CSR), 2021. [Online]. Available: https://doi.org/10.1109/csr51186.2021.9527910

[7] M. Medwed, V. Nikov, J. Renes, T. Schneider, and N. Veshchikov, "Cyber resilience for self-monitoring IOT devices," in 2021 IEEE International Conference on Cyber Security and Resilience (CSR), 2021. [Online]. Available: https://doi.org/10.1109/csr51186.2021.9527995

[8] M. R, G. K, and V. V. Rao, "Proactive measures to mitigate cyber security challenges in IOT based Smart Healthcare Networks," in 2021 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS), 2021. [Online]. Available: https://doi.org/10.1109/iemtronics52119.2021.9422615

[9] A. Bandekar and A. Y. Javaid, "Cyber-attack mitigation and impact analysis for low-power IOT devices," in 2017 IEEE 7th Annual International Conference on CYBER Technology in Automation, Control, and Intelligent Systems (CYBER), 2017. [Online]. Available: https://doi.org/10.1109/cyber.2017.8446380

[10] Z. Minchev and I. Gaydarski, "Cyber Risks, Threats & Security Measures Associated with Covid-19," 2020. [Online]. Available: https://doi.org/10.11610/views.0037

[11] H. Omotunde and M. Ahmed, "A comprehensive review of security measures in database systems: Assessing authentication, access control, and beyond," in Mesopotamian Journal of Cyber Security, pp. 115–133, 2023. [Online]. Available: https://doi.org/10.58496/mjcsc/2023/016

[12] N. Palanivel, P. Sathiyanarayanan, R. Indumathi, and V. Selvi, "IOT health care devices for patient

monitoring," in Cyber Security and Operations Management for Industry 4.0, pp. 109–123, 2022. [Online]. Available: https://doi.org/10.1201/9781003212201-8

[13] C. Rajan, D. Sharma, D. P. Samajdar, and J. Patel, "Low power physical layer security solutions for IOT devices," in Recent Advances in Security, Privacy, and Trust for Internet of Things (IoT) and Cyber-Physical Systems (CPS), pp. 229–248, 2020. [Online]. Available: https://doi.org/10.1201/9780429270567-10

[14] A. Schmitt, T. Chasar, M. Sivagnanam, and F. Kaleem, "Capability Analysis of Internet of Things (IOT) devices in botnets and implications for Cyber Security Risk Assessment Processes," in 2018 ASEE Annual Conference & Exposition Proceedings. [Online]. Available: https://doi.org/10.18260/1-2--30173

[15] A. Tabassum and W. Lebda, "Security Framework for IOT devices against Cyber-attacks," in 6th International Conference on Computer Science, Engineering and Information Technology (CSEIT-2019), 2019. [Online]. Available: https://doi.org/10.5121/csit.2019.91321

[16] A. Tuscano and S. Joshi, "Significance of cyber security of IOT devices in the healthcare sector," in 2023 Somaiya International Conference on Technology and Information Management (SICTIM), 2023. [Online]. Available: https://doi.org/10.1109/sictim56495.2023.10104657

[17] C.-K. Wu, "A comprehensive set of security measures for IOT," in Internet of Things Security, pp. 199–245, 2021. [Online]. Available: https://doi.org/10.1007/978-981-16-1372-2_12