IoT Security: Threats and Forensics

Ayanna Armstrong
Computer Science Department
ampton niversity
ampton A

Abstract - In recent years, the number of Internet of Things (IoT) devices has expanded fast, transforming various industries such as healthcare, manufacturing, and transportation, and delivering benefits to both individuals and industries. However, the increased use of IoT devices has exposed IoT ecosystems to a slew of security risks and digital forensic issues.

This thesis investigates the most common IoT security dangers and attacks, as well as students' understanding of them and mitigation techniques, as well as the key issues involved with IoT forensic investigations.

In this thesis, a mixed-method approach is used, combining a literature review and a survey investigation. The poll measures students' understanding of IoT security threats, mitigation approaches, and perceptions of the most effective ways to improve IoT security. In addition, the survey underlines the importance of user training and awareness in minimizing IoT dangers, highlighting the most effective strategies, such as stronger regulations and increased device security by manufacturers. The literature review provides a complete overview of the most popular IoT security risks and attacks, including malware, malicious code injection, replay attacks, Man in the Middle (MITM), botnets, and Distributed Denial of Service (DDoS).

This paper also emphasizes the definition and process of digital and IoT forensics, the significance of IoT forensics, and various data sources in IoT ecosystems.

The key issues of IoT forensics and how they affect the efficiency of digital investigations in the IoT ecosystem are thoroughly investigated.

Overall, the findings of this study contribute to ongoing research to improve IoT device security, emphasize the necessity of greater awareness and user training, and address the issues of IoT forensic investigations.

I. Introduction

esearch is concerned with oT security concerns and the difficulties involved with oT forensics. A literature review and a survey study are used in the pro ect s mi ed method approach. Furthermore the paper intends to investigate the most fre uent oT security vulnerabilities and assaults as well as their mitigation approaches and implications in real world occurrences. n addition the research will measure students knowledge of oT security threats mitigation strategies and the best ways to improve oT security. t will provide a complete review of the problems connected with oT forensics and their impact on the oT system investigation process.

A. Background

The nternet of Things oT refers to a network of ob ects that are e uipped with software computing power sensors network connectivity and other technologies that allow them to collect and e change data and e ecute activities autonomously. luetooth igbee and Wi Fi are among the wireless protocols used by oT devices to connect with one another. These communication protocols allow devices to communicate data and interface with multiple cloud services for storage and processing 1 .

According to recent predictions the number of oT devices in use worldwide is e pected to reach 1 . billion by 0 4 14 . This figure is predicted to rise to 0. billion by 0 5 illustrating the fast use of oT technology in a variety of industries such as healthcare manufacturing smart cities and transportation 14 .

Despite the numerous benefits of oT devices the rapid e pansion in their use has resulted in numerous security vulnerabilities and privacy concerns . ecause of the vast volume of data created and processed by oT devices they have become a popular target for attackers and cybercriminals. Malware assaults Distributed Denial of Service DDoS attacks Man in The Middle M TM attacks Malware and unauthori ed access are some of the most common security concerns in oT systems 5 . Several real world oT crimes including as the Mirai botnet the erkada hack and the St. ude Medical implant device hack have demonstrated the impact of security breaches on persons healthcare and vital infrastructure . These incidents have had substantial economic and societal conse uences emphasi ing the significance of addressing oT security concerns 1 .

The growing amount of nternet of Things oT crimes and security problems has underlined the need for realistic oT forensic tools and procedures 1 . oT forensics is the collection analysis and preservation of digital evidence from oT devices to aid in cybercrime investigations. owever because the nature of oT systems particularly the array of devices data formats and protocols for communication oT forensics confronts numerous obstacles . Another problem is locating and identifying evidentiary data which can be dispersed over various cloud platforms throughout the world. Furthermore the limited storage space and processing power of oT devices might complicate the forensic procedure by making it difficult to collect and analy e digital evidence .

B. Problem Definition

The rapid e pansion in the number of oT devices has resulted in a spike in security threats assaults and forensic issues. As oT becomes more integrated into our daily lives it becomes increasingly vital to comprehend these ha ards assess human awareness and identify the fundamental issues in oT forensics 14 . As the present body of knowledge is very restricted there is still a substantial research need in this sector. The problem will be formulated in this section by offering the research uestions that will lead the research:

- What are the most fre uent oT security dangers and attacks as well as their mitigation approaches and real world conse uences
- What level of understanding do students have of oT security threats and mitigation approaches and how do they consider the most effective ways to improve oT security
- What are the main obstacles of oT forensics and how do they affect the efficiency of digital investigations in the oT ecosystem

II. Methodology

The goal of this paper is to give a full e amination of oT security threats and attacks as well as the accompanying forensic issues by employing a mi ed method approach to ac uire insights from both theoretical and practical viewpoints. The research approach is structured as a road map with numerous ob ectives to reach the aim and close the knowledge gap. First a literature review will be done to gain an understanding of the theoretical basis and current knowledge of oT security threats and forensic problems. n addition a survey of students will be conducted. t will measure their understanding and awareness of oT security threats mitigation techni ues and udgments of the most effective ways to improve oT security.

A. Literature Review

As the nternet of Things oT e pands linking billions of devices worldwide new security concerns and threats develop posing serious dangers to user privacy data integrity and device operation. This section is based on the findings of the selected studies literature review 10 . t provides an overview of five often mentioned oT security issues and related mitigation solutions in the literature. These oT security dangers and attacks were identified based on their recurrence in the e amined scholarly articles 7 . This illustrates how fre uently various dangers are addressed in the oT security sector not how they rank in importance. Furthermore this section

delves into real world instances related to various oT dangers demonstrating their real world conse uences.

Attacks with Malware and Malicious Code Injection

Malware and malicious code in ection attacks pose serious cybersecurity risks to oT devices and systems 4 . Attackers in ect malicious code into oT devices or networks to compromise their functionality steal sensitive data or gain unauthori ed access.

Malware attacks on oT infrastructure involve the distribution of harmful programs such as viruses worms ransomware or botnets that e ploit weaknesses in oT systems. These attacks fre uently target web apps or oT connection protocols. These e ploits allow attackers to gain unauthori ed access to oT devices giving them control over device operation and eopardi ing data integrity. Attackers can also steal sensitive data stored on oT devices such as passwords and login credentials resulting in data breaches and privacy violations 15 . n addition attackers can infect devices with malware and use them to e ecute other attacks.

False Data Injection (FDI) Attack

The attackers goal in this assault is to modify the data being gathered or transferred between oT devices causing them to produce incorrect outputs or initiate unintended events. FD attacks fre uently take use of flaws in the communication protocols used by oT devices to communicate data such as poor encryption and a lack of authentication 4 .

Some possible outcomes of FD attacks include compromised data integrity which occurs when attackers corrupt or alter data collected and processed by oT devices resulting in incorrect decision making which can have serious conse uences in critical sectors such as healthcare energy and transportation systems 4 . An e ample of FD is an attacker introducing bogus sensor readings into an industrial control system causing e uipment failure.

Another effect would be privacy violations as attackers might ac uire unauthori ed access to sensitive information in oT devices by in ecting bogus data into them and monitoring personal activity. Strong encryption algorithms can be used to secure the confidentiality and integrity of data e changed between oT devices making it more difficult for attackers to in ect bogus data . To validate the identity of communication partners strong authentication and authori ation procedures should be built. Furthermore digital signatures or message authentication codes should be used to detect and prevent the transmission of modified data. To address known vulnerabilities regular security updates and patches should be implemented 14 .

Replay Attack

Attackers target oT devices by capturing and retransmitting legal data packets to ac uire unauthori ed access. Attackers begin by intercepting data packets which fre uently contain authentication data during a valid transaction between two devices in an oT network. The attacker then retransmits the collected data to the system hoping to fool the recipient device into accepting the packets as authentic so e ploiting the system s vulnerability.

eplay attacks can also eopardi e the integrity of oT systems by providing duplicate or outdated data packets allowing the device to make wrong udgments based on the replicated data. Furthermore replay attacks can result in the revelation of sensitive information such as user credentials and device specific information as well as a loss of privacy.

This e ploit can also degrade device performance by causing it to process and reply to redundant data packets using memory and processing power.

Smart home systems and industrial oT devices are e amples of oT e uipment that can be targeted by replay attacks . A replay attack in smart home systems could target the connection between a smart lock and its related mobile application. The attacker might intercept and save a legal unlocking command before replaying it to

obtain access to the residence. Attackers can also target sensor and control system communication in industrial oT devices.

Eavesdropping Attack

The illegal capture and monitoring of data transferred between devices in an oT system constitutes this threat. Attackers employ packet sniffing as one of several approaches to gather and analy e traffic between oT devices and networks. Eavesdropping attacks seek sensitive data such as login credentials credit card numbers personal information and organi ational information which can subse uently be used to launch additional attacks.

Strong encryption techni ues can be applied to secure the confidentiality and integrity of data transported across network devices making it difficult for attackers to decipher data. Secure communication routes such as irtual rivate Networks N can also aid in the mitigation of eavesdropping attempts by offering added security and safety. Furthermore implementing two factor authentication and network segmentation can reduce the impact of an eavesdropping attack .

Distributed Denial of Service (DDoS) Attack

Multiple infected devices flood a target system such as a server or network with traffic rendering it unavailable or unresponsive to genuine users. This attack is particularly worrying because of the rising number of oT devices with varying levels of security which make them an easy target for attackers to e ploit and employ as part of a botnet to perform DDoS attacks .

This attack in addition to disrupting services and making systems inaccessible results in financial losses due to the e penses associated with downtime service offered by the targeted company. During a DDoS assault attackers can also e ploit security flaws in oT devices to get access to and steal critical data resulting in additional attacks .

B. IoT Forensics

As the nternet of Things oT e pands so does the demand for forensic investigations involving oT devices. Digital forensics is the process of locating gathering and organi ing evidence for use in udicial proceedings. dentification collection organi ation and presentation of evidence are the four fundamental stages in digital forensics. The identification phase entails identifying prospective sources of evidence as well as deciding the investigation s ob ectives. To effectively e tract the essential information forensic investigators must understand the types of devices systems and data storage processes involved.

The collection procedure begins once potential evidence is recogni ed. To assure the reliability of the data ac uired forensic investigators use legal and technical approaches. This procedure may include making hard drive copies downloading data from cloud storage or obtaining information from network logs 10 .

Following data gathering the organi ation process entails e amining the obtained data to uncover patterns that can aid in determining the facts of the case 4 . arious approaches are employed by investigators during this step to sort through enormous amounts of data discovering useful information and re ecting irrelevant material.

Finally the presentation phase is compiling the findings into a concise report to present the evidence in court. The report should be understandable to non e perts in the field of digital forensics such as legal professionals and should demonstrate a link between the evidence and the case.

oT forensics is a branch of digital forensics that focuses on the uni ue issues that oT devices provide. oT devices are networked together and fre uently gather process and transfer data to cloud servers and other devices. This interconnectedness creates a comple environment for forensic investigators necessitating the use of speciali ed instruments . oT forensics is separated into three categories: device network and cloud level.

The analysis of oT devices including their memory hardware and physical interfaces is part of oT device forensics. Due to the wide variety of oT devices and their distinct features investigators must be knowledgeable with a wide range of devices and manufacturers to efficiently gather and evaluate data. oT Network forensics e amines the interaction of oT devices and their connections to networks such as Wi Fi luetooth and cellular networks. nderstanding the network architecture and patterns of traffic associated with oT devices is the focus of this area. Network forensics assists investigators in identifying potential oT system vulnerabilities and intrusions 11 .

oT The study of data saved and processed by cloud services that support oT devices is known as cloud forensics. ecause many oT devices rely on cloud computing for storage and processing investigators must be familiar with the various cloud architectures and security standards to successfully gather and analy e data.

C. *Importance of IoT Forensics*

oT forensics has arisen as a sub domain of digital forensics that is critical in recogni ing assessing and responding to security issues involving oT devices 7 . oT forensics e pands on digital forensics techni ues which include the identification collecting organi ation and presentation of digital evidence in court proceedings. owever oT forensics broadens this reach to address the uni ue issues of oT devices. The significance of oT forensics arises from its capacity to adapt traditional forensic methods to the uni ue problems of oT systems allowing investigators to find evidence that would otherwise be unreachable using traditional forensic tools.

oT devices are being integrated into key infrastructure systems such as energy grids transportation and healthcare. The possible compromising of these devices can have serious ramifications for society and public safety. oT forensics plays a key role in securing these important infrastructures by allowing investigators to collect and analy e data discover vulnerabilities and provide guidelines for enhancing the security of oT devices. Forensic investigators can better understand how attackers obtained access to the system and what efforts can be taken to prevent such attacks in the future by studying the evidence left after an attack. Furthermore oT forensics can aid in the discovery of security flaws in the design of oT devices allowing manufacturers to improve the security of oT devices and lower the risk of future attacks.

Another factor emphasi ing the significance of oT forensics is that oT devices generate a tremendous volume of data fre uently in real time. This information can be useful during a forensic in uiry. oT forensics aids in the reconstruction of events the identification of malicious activity and the establishment of a timeline of events. This is useful in forensic investigations because it assists investigators in determining the cause of the incident and identifying security weaknesses.

D. *Challenges of IoT Forensics*

ecause of the lack of standardi ation and diversity of oT devices forensic investigators have found it incredibly difficult to apply efficient procedures while conducting digital investigations involving oT devices. The oT landscape is defined by various oT devices ranging from modest sensors to large industrial control systems. These devices fre uently use disparate hardware operating systems and software applications resulting in discrepancies in data formats and storage systems 11 .

Furthermore the communication protocols utili ed by oT devices can vary greatly. Some devices use well known protocols like Wi Fi luetooth or igbee while others employ proprietary communication protocols. ecause forensic investigators must be able to comprehend and evaluate the communication patterns between diverse oT devices and their accompanying networks this heterogeneity can provide a considerable difficulty.

Another factor to consider is the variety of operating systems and software applications utili ed by oT devices 11 . While some devices utili e well known operating systems such as Linu or Windows others employ proprietary

systems. Traditional tools may not be effective in these scenarios making it challenging for forensic investigators to discover acceptable methods for obtaining and interpreting data from these devices.

The re uirement for greater standardi ation and heterogeneity in oT forensics poses substantial hurdles for forensic investigators as they must be knowledgeable in a wide range of tools and methodologies to properly perform digital investigations using oT devices. This can result in additional comple ity longer in uiry times and incorrect results.

Another key problem in oT forensics is the vast volume of data generated by oT devices which is spread across multiple servers and networks. As a result determining the precise location of the data can be difficult for forensic investigators because data can be stored locally on the device on various cloud services or on other devices and servers in the oT network where more storage is available. This makes it difficult for forensic investigators to gather information from numerous sources and recreate the timeline of events.

Another issue is that the distributed nature of oT forensic data might raise the possibility of data loss or corruption complicating the forensic procedure even further. Furthermore using the cloud might complicate the process further because cloud storage systems which are fre uently used to store and analy e data generated by oT devices can be hosted in various geographical areas throughout the world and administered by different service providers. This complicates the legal and urisdictional procedure even more as forensic investigators may face legal constraints when accessing data housed in other urisdictions. They may need to navigate comple rules and obtain legal authori ations before they can access the data.

Another key obstacle for oT forensic investigations is a lack of technical capabilities which includes insufficient oT forensic tools limits of traditional forensic tools and insufficient training and instruction for investigators. Furthermore the diversity of oT devices makes it difficult for investigators to develop forensic techni ues intended e clusively for oT devices. Another issue is that standard forensic tools designed for personal computers and mobile devices may not be appropriate for analy ing and e tracting data from oT devices resulting in inade uate results during forensic investigations.

The ramifications of a lack of technical capabilities in oT forensics are far reaching. t may cause delays in forensic investigations where investigators re uire assistance in ac uiring and analy ing data from oT devices using typical forensic techni ues. This delay can have an impact on the outcome of an investigation especially when dealing with time sensitive facts. Furthermore the lack of speciali ed forensic tools can result in incomplete or erroneous investigations as investigators may misunderstand data collected from oT devices.

III. Results

This section presents the research findings which are separated into two sections: the findings of the literature review and the survey results. The first section highlights the important findings from a survey of the literature on oT security threats and attacks as well as the issues involved with oT forensics. The results of a survey conducted to e amine students familiarity with oT security risks and vulnerabilities as well as their perspectives of security measures and shared duties in oT security were provided in the second section.

A. Results of Literature Review

ased on an e amination of the literature references that focused on these specific threats and assaults the table below provides a clear overview of various security risks and attacks their descriptions and the potential implications of each threat.

Attack type	**Description**	**Potential Impact**
Attacks with Malware and Malicious	nauthori ed code e ecution in nternet of	tampering with data unauthori e d access

Code Injection	Things devices	system damage and service disruption
FDI Attack	n ecting bogus data into nternet of Things devices	Data integrity erroneous decision making and false alarms
Replay Attack	e transmitting a previously captured legal data transmission	nauthori e d access system failure replay fraud and service disruption
Eavesdropping Attack	ntercepting and listening in on oT communication	rivacy invasion unlawful access and data theft
DDoS Attack	nterfering with the availability of oT devices by overloading them with traffic	Service interruption unavailability financial and reputational harm infrastructure harm

Table 1: oT Security Threats and Attacks

The table below gives a concise overview of the ma or oT forensic difficulties and e plains how they relate to the specific oT security threats and attacks depicted in Table 1.

Challenge	**Description**	**Relationship to IoT Security Threats and Attacks**
Heterogeneity and lack of standardization	The nternet of Things ecosystem is comprised of several devices platforms and communication protocols making it challenging to build standardied forensic processes.	The comple ity of evaluating and mitigating threats such as Man in the Middle attacks spoofing attacks and Sinkhole attacks is e acerbated using many operating systems communication protocols and encryption authentication mechanisms 5 .
Storage and processing capacity limitations	oT devices often have limited storage and processing capacity which can make digital evidence e traction and analysis difficult.	The ability to preserve logs and records is hampered by limited storage capacity which can impede the investigation of assaults such as eavesdropping cryptanalysis and DDoS attacks. Devices with insufficient processing capacity may be unable to run advanced forensic tools complicating investigations into threats such as malware and malicious code in ection replay assaults and side channel attacks.
Identification and location of data	ecause oT devices are scattered it might be challengin	ecause it can be difficult to follow the data flow between components and find the important

	g to locate and identify useful data sources for forensic investigations.	data among big datasets distributed data across devices cloud platforms and networks hinders investigations into threats such as False Data n ection Spoofing and Man in the Middle attacks.
Inadequate Technical Capabilities	Due to the scarcity of speciali ed tools technologies and knowledge suited to oT forensics as well as the uickly e panding oT landscape.	nade uate training in oT forensics as well as the scarcity of speciali ed forensic tools make it difficult to effectively investigate and respond to a wide range of security threats and attacks such as malware and malicious code in ection cryptanalysis side channel attacks and DDoS attacks.

Figure : Challenges in oT Forensics

B. Survey Results

The idea for conducting the survey stems from the need to assess students awareness and understanding of oT security threats and vulnerabilities particularly those that re uire user participation to successfully mitigate. The survey s goal is to bridge the gap between theoretical knowledge of oT security threats and practical steps users may take to ensure a secure oT environment.

The survey findings were categori ed into the following categories:

1. oT nderstanding and Apprehensions egarding Security

This section contains the answers to uestions 1 and which provide vital insights into the student s understanding of oT and their concerns about the security of oT devices.

uestion 1: According to the findings the ma ority of participants are at least somewhat familiar with the notion of oT. There are total respondents. .1 respondents said they were unfamiliar with oT while 0. 10 respondents said they were somewhat familiar with the concept. A bigger proportion of participants . 11 respondents claimed to be relatively familiar with oT while 7. respondents claimed to be highly familiar. This suggests that many respondents comprehend oT which is critical for developing an informed viewpoint on the associated security problems. The three participants who were unfamiliar with the concept of oT were thanked for their participation informed that they were not the intended audience for this survey and their responses were omitted from further research. As a result the second and following poll uestions were based on replies from 0 participants.

uestion : According to the survey results a si able proportion of respondents are concerned about the security of oT devices. .7 participants indicated being somewhat concerned whereas 40 1 participants reported being moderately concerned. Furthermore . of respondents 10 respondents e pressed concern regarding oT device security. These findings demonstrate an increasing awareness of the possible security threats connected with oT devices.

. Security Threats and ulnerabilities in oT

This section of the survey results looks at participants knowledge of common oT security flaws familiarity with oT security risks and perspectives on the most serious security concerns. The responses to uestions 5 and reveal the respondents grasp of the problems connected with oT security.

uestion : As previously stated the number of respondents from uestion and subse uent uestions in the survey is 0. When asked about fre uent oT security vulnerabilities in this topic most participants . 5 respondents indicated weak or readily guessable passwords as a vulnerability. The second most recogni ed issue .7 of 0 respondents was a lack of regular security updates and patches followed by unsecured remote management access a lack of encryption for data transmission and insufficient user authentication and authori ation all of which were acknowledged by 5 . of respondents 1 respondents . Other vulnerabilities cited by one responder . included hardware access inade uate user knowledge abandoned hardware and shared Wi Fi networks.

n terms of awareness with oT security concerns the most identified threat was Man in The Middle M TM attacks which were recogni ed by 7 . of respondents respondents . nauthori ed access was known to .7 of participants 0 respondents whereas Distributed Denial of Service DDoS attacks and Malware attacks were known to . 1 respondents and 0 1 respondents respectively . Spoofing attacks were identified by 4 . of the respondents 1 . Other threats highlighted by two respondents . each included physical attacks and data misuse.

nauthori ed access emerged as the top concern for . of the respondents 10 respondents when asked to name the most severe security danger among those listed. Malware assaults were close behind with 0 of participants citing them as the most serious concern respondents . DDoS assaults were seen the most serious by 0 of respondents respondents while Man in the Middle attacks were deemed the most serious by 1 . 4 respondents . Only one respondent . thought spoofing attacks were insignificant.

. Safety Measures Techni ues and Common esponsibilities

The third section of the survey findings focuses on participants perspectives on the importance of built in security features in oT devices the security measures they use to protect their devices the importance of user education shared responsibility among various collaborators and the most effective ways to improve oT security.

uestion 4: When asked how important built in security mechanisms in oT devices are an overwhelming 70 1 respondents thought it was very important while .7 respondents thought it was important. Only one person . thought it was somewhat important. These findings demonstrate that most participants reali e the importance of including security safeguards in oT devices by default.

uestion 7: The poll also sought to ascertain how individuals secure their oT devices. Changing default passwords was the most popular security step with . 5 respondents doing so. With . 1 respondents the second most popular measure was regularly updating device firmware followed by using strong encryption methods for data transmission 50 15 respondents disabling remote management of devices 40 1 respondents and monitoring network traffic for unusual activity 0 respondents . n addition one respondent . reported using o T certified devices. Another person advised adopting additional security precautions such as uninstalling old devices when they no longer receive updates and using SS with ust key access.

uestion : n terms of the relevance of user education for ensuring oT security 5 . 1 0 respondents thought it was very important while .7 respondents thought it was important. Only 0 people thought it was somewhat important. This demonstrates that many respondents reali e the need of user education in improving oT security.

uestion : When asked if oT security should be shared by consumers manufacturers and service providers 0 1 respondents agreed while .7 respondents disagreed. Surprisingly . 10 respondents responded that it depends on the situation. Most participants agreed that

multiple stakeholders must work together to properly address oT security challenges.

uestion 10: n response to the uestion of the most effective way to improve oT security .7 11 respondents selected improved device security by manufacturers followed by increased user awareness and education . 7 respondents development of better security technologies 0 respondents and stronger regulations 1 .7 5 respondents . One respondent . offered open source hardware as a possible option as well. These findings reflect a range of perspectives on the most effective ways to improve oT security with a particular emphasis on the role of manufacturers and user knowledge.

IV. Analysis

This thesis sought to collect data on the most common oT security risks and attacks as well as the most common obstacles related with oT forensics and to assess students knowledge of oT security threats and mitigation measures. A mi ed method strategy will combine a literature review and a survey study to answer the research uestions. The literature review will answer the first two research uestions 1 and while the survey study will answer the third . n this chapter we discuss the main findings of the literature review and survey study.

esearch uestion 1: Threats to oT Security Mitigation Techni ues and eal World ncidents

This section covers the most fre uent oT security threats and assaults as well as real world occurrences and actions to prevent and mitigate these risks.

Malware and malicious code in ection attacks pose a serious risk to oT devices.

The Mirai otnet Attack for e ample demonstrated how malware could infect numerous oT devices to form a huge botnet that conducted DDoS attacks on targeted servers . To combat malware and malicious code in ection it is critical to install updates antivirus software and network monitoring.

Fake data in ection attacks occur when an attacker in ects fake data or manipulates e isting data causing the system or user to make wrong udgments and actions. To mitigate the risk of this attack data integrity checks encryption and secure communication methods must be implemented.

The attacker captures and resends legal data or commands to induce undesired actions or ac uire unauthori ed access. eplay attacks can be mitigated by employing timestamps and secure communication methods .

Cryptanalysis and side channel attacks break encryption and obtain access to sensitive information by e ploiting flaws in cryptographic methods or seeing side channel data. Strong encryption methods and effective key management are re uired to guard against these attacks 10 .

When an attacker intercepts communication between oT devices or between a device and a user an eavesdropping attack occurs. Data can be protected against eavesdropping assaults by encryption and secure communication protocols.

DDoS attacks seek to overwhelm oT devices or networks with massive amounts of data traffic resulting in service outages or total unavailability. To mitigate these threats traffic filtering rate restriction and intrusion detection systems should be used 1 .

Spoofing attacks entail an attacker impersonating a legitimate oT device user or service to deceive other devices or users. To prevent spoofing attacks authentication digital certificates and secure communication protocols can be used.

M TM attacks enable an attacker to intercept and potentially change communication between two oT devices or between a device and a user. M TM attacks can be mitigated by encryption secure communication protocols and digital certificates.

Sinkhole attacks compromise an oT device or network node allowing the attacker to modify or prevent communication 1 . To prevent this attack intrusion detection systems secure routing protocols and network monitoring should be deployed 1 .

Sleep deprivation attacks prevent oT devices from entering low power sleep mode resulting in fast battery depletion. ntrusion detection systems should be installed to detect and prohibit continual re uests from unauthori ed sources to counteract this assault 1 .

esearch uestion : Students nderstanding of oT Security Threats and Mitigation Methods

The poll results shed light on students awareness of oT security concerns grasp of mitigation measures and perceptions of the most effective ways to improve oT security.

n terms of familiarity with oT 0. 0 out of of respondents indicated being at least somewhat familiar with the concept indicating that most participants have a basic understanding of oT. This outcome is critical because it serves as the foundation for their understanding of oT security threats and mitigation techni ues.

The omission of the three participants who were unfamiliar with the idea of oT from the analysis of the following uestions assures that the results reflect the viewpoints of people who have some awareness of oT and the security challenges that it raises.

Most respondents 7 . were concerned about the security of oT devices uestion with 40 worried and . highly worried. This finding demonstrates a general understanding of the possible risks associated with oT devices which may motivate students to learn more about the sub ect.

According to the results of uestion 1 and uestion the ma ority of participants 0. are moderate to very familiar with the concept of oT uestion 1 and the ma ority 7 . are concerned about the security of oT devices. This link implies that as students grow more ac uainted with oT technology they become more concerned about its security implications.

When asked about prevalent oT security vulnerabilities respondents had a reasonable understanding of the issues. The ma ority of participants . were aware of weak or easily guessable passwords unsecured remote management access 5 . a lack of data transmission encryption 5 . a lack of regular security updates and patches .7 and insufficient user authentication and authori ation 5 . . These findings indicate that students are aware of potential security threats that can compromise oT devices.

n uestion 4 70 of participants rated built in security measures in oT devices as e tremely important .7 rated it as important 4 rated it as fairly important and only . rated it as somewhat important. This research demonstrates that students respect the notion that oT devices must include security measures by default and acknowledge the responsibility of manufacturers in improving oT security.

The respondents were aware of many oT security concerns 5 with Man in the Middle attacks 7 . receiving the most attention followed by illegal access .7 DDoS assaults . Malware attacks 0 and spoofing attacks 4 . . Furthermore when asked to choose the most serious security danger among those listed respondents named unauthori ed access . and malware assaults 0 as the top threats followed by DDoS attacks 0 M TM attacks 1 . and spoofing attacks . . This demonstrates that students grasp the most fre uent oT security concerns. espondents high awareness and comprehension of oT security vulnerabilities and threats should help them make better udgments when utili ing oT devices and urge them to use best practices for securing them.

uestion and uestion 5 results show that participants are largely aware of common oT security vulnerabilities and are familiar with a variety of security risks 5 . This link emphasi es the significance of identifying vulnerabilities and prospective security threats

since understanding both areas can lead to the development of more effective security solutions.

Furthermore uestion 5 and uestion results suggest that students who are familiar with different security concerns 5 regard unauthori ed access and malware attacks as the most serious threats. These findings could imply that students are more concerned about threats to their data privacy and device operation.

The responses to 7 demonstrate the security precautions that students take to protect their oT devices. Changing default passwords was the most used security solution . followed by fre uently updating device firmware . utili ing strong encryption methods for data transmission 50 disabling remote device administration 40 and monitoring network traffic for suspicious activity 0 . These findings indicate that students have a practical awareness of the processes re uired to safeguard oT devices from security threats.

The relationship between and 7 results suggests that participants who are aware of typical oT security risks are more likely to e ecute security measures such as changing default passwords updating device firmware and employing strong encryption methods for data transmission 7 . This research emphasi es the need of informing consumers about potential vulnerabilities and encouraging them to utili e appropriate security measures.

The relationship between and 7 results suggests that participants who are aware of typical oT security risks are more likely to e ecute security measures such as changing default passwords updating device firmware and employing strong encryption methods for data transmission 7 . This research emphasi es the need of informing consumers about potential vulnerabilities and encouraging them to utili e appropriate security measures.

The need of user education in preserving oT security was acknowledged by the ma ority of respondents with 5 . deeming it very important .7 deeming it essential and 0 deeming it somewhat important. This finding indicates that students believe user awareness and education are critical to the safe use and deployment of oT devices.

When comparing 4 and results most respondents agree that built in security features 4 and user education are critical for preserving oT security. This link emphasi es the significance of combining technology and user knowledge to properly address oT security challenges.

n the ma ority of respondents 0 stated that oT security should be a oint responsibility of users manufacturers and service providers while . believed it depends on the conditions. This viewpoint emphasi es the significance of working together to address oT security issues.

The results of 4 and corroborate the notion that students believe in a shared responsibility for oT security by connecting the relevance of built in security features and user education. This validation deepens students understanding of oT security and emphasi es the need of collaboration among collaborators in addressing oT security concerns efficiently.

When asked about the most effective way to improve oT security 10 participants named improved device security by manufacturers as the most important factor .7 followed by increased user awareness and education . development of better security technologies 0 and stronger regulations 1 .7 . These comments demonstrate that students recogni e the comple ity of oT security and the necessity for a holistic approach including multiple stakeholders.

Moreover most participants agree that oT security should be a shared responsibility between users manufacturers and service providers and they believe that improved device security by manufacturers increased user awareness and education and the development of better security technologies 10 are the most effective ways to enhance oT security. This connection highlights the importance of collaboration between different stakeholders to address oT security challenges effectively.

esearch uestion : Several difficulties with oT forensics have been recogni ed which are related to the specific properties of oT devices. The issues mentioned include a lack of standardi ation and heterogeneity storage capacity and processing capability limitations data locali ation and identification and a lack of technological capabilities.

The lack of standardi ation and heterogeneity in oT ecosystems which include a diverse set of devices platforms and communication protocols hampers the development of standardi ed forensic processes. The multiplicity of operating systems communication protocols and encryption methods used in oT devices complicates the forensic process further complicating the process of assessing and mitigating threats such as M TM attacks Spoofing attacks and Sinkhole attacks 1 .

Another problem in oT forensic investigations is the limited storage and processing capacity of oT devices. This constraint has an impact on the process of keeping logs and data as well as the capacity to investigate threats such as eavesdropping and DDoS attacks . Furthermore oT devices with insufficient processing capacity may be incapable of running advanced forensic tools hindering investigations into threats such as Malware and Malicious code n ection eplay assaults and Side Channel attacks.

Another challenge is the distributed nature of oT devices which complicates the process of data location and identification as it makes it difficult to trace the data transfer between devices and sensors and determine the relevant data among large datasets. This issue complicates the investigations into threats such as False Data n ection Spoofing and M TM attacks. Another issue is the data being fragmented when transmitting which can further complicate the investigations of threats like Eavesdropping Sinkhole and Sleep Deprivation attacks 1 .

A lack of technological capabilities such as a scarcity of speciali ed forensic tools and e pertise tailored to oT forensics might hinder the process of oT forensic investigations. This difficulty makes investigating and responding to numerous security threats and assaults such as malware and malicious code in ection DDoS and cryptanalysis attacks difficult .

V. Conclusion

Finally this thesis demonstrates how oT security user awareness and forensic issues are all intertwined. An in depth e amination of the many facets of oT security reveals that e amining these concerns necessitates a thorough approach.

oT security threats pose ma or ha ards to users and systems necessitating stronger security measures and additional research to keep oT systems safe and build robust security solutions. Furthermore the vital role of user knowledge in preventing mitigating and safeguarding oT devices is emphasi ed emphasi ing the significance of incorporating oT security education into educational programs.

The difficulties connected with oT forensics demonstrate the necessity for the development of improved forensic tools and methodologies designed specifically for oT systems. This is critical for conducting effective digital investigations in a more linked environment.

Furthermore the thesis findings emphasi e the need of collaboration among researchers industrial specialists and users in tackling oT security concerns raising awareness and overcoming forensic issues.

f there had been more time the scope of this investigation may have been e panded.

For future research several avenues could be pursued. First a wider poll may be done with a larger audience including academics professionals and members of the public. This will aid in better understanding of user awareness and views of oT security dangers and mitigation solutions. Second investigating the development of standardi ed oT forensic frameworks and tools would help address the current challenges facing oT forensics investigations. Finally further research on the collaboration between users manufacturers and service providers in the oT system could help establish shared

responsibilities for oT security and e amine the responsibilities of each group.

References

1 NTE NET OF T NGS AND T E MAN N T E M DDLE ATTACKS SEC T AND ECONOM C SKS. *MEST Journal 5* 15 15. https: doi.org 10.1 70 mest.05.05.0 .0

Gautam S. Malik A. Singh N. Kumar S. 01 . *Recent Advances and Countermeasures Against Various Attacks in IoT Environment*. https: doi.org 10.110 icspc4 17 . 01 . 7 5 7

Guest Author. 017 December 14 . *Inside the infamous Mirai IoT Botnet: A Retrospective Analysis*. The Cloudflare log The Cloudflare log. https: blog.cloudflare.com inside mirai the infamous iot botnet a retrospective analysis

4 u . Gao W. Li . Wu M. ua F. iao L. 0 . Detection of False Data n ection Attacks in Smart Grids ased on E pectation Ma imi ation. *Sensors 23* 1 . https: doi.org 10. 0 s 0 1

5 aveed D. Mohammed adamasi . 0 0 . Man in the Middle Attacks: Analysis Motivation and revention. *International Journal of Computer Networks and Communications Security 8* 7 5 5 . https: doi.org 10.47 77 i cncs 7 1

Kolias C. Kambourakis G. Stavrou A. oas . 017 . DDoS in the oT: Mirai and Other otnets. *Computer 50* 7 0 4. https: doi.org 10.110 mc. 017. 01

7 Krishna . . S. Gnanasekaran T. 017 . A systematic study of security issues in nternet of Things oT . *2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*. https: doi.org 10.110 i smac. 017. 05 1

Kumari . ain A. K. 0 . A Comprehensive Study of DDoS Attacks over oT Network and Their Countermeasures. *Computers & Security* 10 0 . https: doi.org 10.101 .cose. 0 .10 0

Langner . 011 . Stu net: Dissecting a Cyberwarfare Weapon. *IEEE Security & Privacy Magazine 9* 4 51. https: doi.org 10.110 msp. 011. 7

10 Nabeel N. abaebi M. . slam M. D. . 0 1 . Security Analysis of LNMNT LightWeight Crypto ash Function for oT. *IEEE Access 9* 1 5754 1 57 5. https: doi.org 10.110 access. 0 1. 1 0 7

11 Nath N . Nath . 0 . Critical analysis of the layered and systematic approaches for understanding oT security threats and challenges. *Computers and Electrical Engineering 100* 107 7. https: doi.org 10.101 .compeleceng. 0 . 107 7

1 a a S. Wallgren L. oigt T. 01 . S ELTE: eal time intrusion detection in the nternet of Things. *Ad Hoc Networks 11* 1 74. https: doi.org 10.101 .adhoc. 01 .04.014

1 ehman A. ehman S. . aheem . 01 . Sinkhole Attacks in Wireless Sensor Networks: A Survey. *Wireless Personal Communications*. https: doi.org 10.1007 s11 77 01 040 7

14 Shafiei . Khonsari A. Derakhshi . Mousavi . 014 . Detection and mitigation of sinkhole attacks in wireless sensor networks. *Journal of Computer and System Sciences 80* 44 5 . https: doi.org 10.101 . css. 01 .0 .01

15 ailshery L. S. 0 September . *Global number of connected IoT devices 2015-2025*. Statista. https: www.statista.com statistics 110144 i ot number of connected devices worldwide

1 ekerevac . Dvorak . rigoda L. ekerevac . 017 . NTE NET OF T NGS

Appendix

Survey uestions:

1. ow familiar are you with oT nternet of Things
. ow concerned are you about oT device security

. Are you aware of any prevalent oT security flaws Check all that apply.
4. ow crucial do you think it is for oT devices to come standard with security features
5. Which of the following nternet of Things security risks are you most familiar with Check all that apply
. Which of the security threats in your opinion is the most serious Select one
7. Which of the following security precautions would you implement to protect oT devices
. ow crucial do you think user education is for oT security
. Do you feel that oT security should be shared by users manufacturers and service providers
10. Which of the following can have the greatest impact on oT security

ACKNOWLEDGEMENTS

This work is partly supported by the Nation Science Foundation Cybercorps: Scholarship for Service program under grant award #1754054.