National College of Ireland

IOT Forensics: A Comprehensive Analysis of an IOT Device using Digital Forensic and Penetration Testing Tools and Methodologies

MSc Research Project
MSc Cyber Security

Ivan Ronald Dsouza
Student ID: X22189386

School of Computing
National College of Ireland

Supervisor: Prof. Eugene McLaughlin

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name:	Ivan Ronald Dsouza
Student ID:	X22189386
Programme:	MSc Cyber Security **Year:** 2024
Module:	MSc Research Practicum
Supervisor:	Eugene McLaughlin
Submission Due Date:	12/12/2024
Project Title:	IOT Forensics: A Comprehensive Analysis of an IOT Device using Digital Forensic and Penetration Testing Tools and Methodologies
Word Count:	**8575** **Page Count: 20**

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature: Ivan Ronald Dsouza

Date: 12/12/2024

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

IOT Forensics: A Comprehensive Analysis of an IOT Device using Digital Forensic and Penetration Testing Tools and Methodologies

Ivan Ronald Dsouza

x22189386

Abstract

The domain of Internet of Things has been continuously expanding due to its increasing demand and diverse applications across Smart Homes, Healthcare, Virtual Assistance, and Agriculture. However, the security of these IOT devices is often neglected. In addition, the interconnected nature of these devices across unknown and heterogenous networks leads to an unprecedented number of IoT endpoints. This nature of complexity and security neglection gives rise to several cyber-attacks resulting in huge losses. This research focuses on executing a comprehensive analysis of a Baby Monitoring IOT device using Digital Forensics Tools and Methodologies. In this scenario, the sub-domain of Digital forensics i.e IOT Forensics will be utilised to carry out a comprehensive analysis of a Baby Monitor highlighting its vulnerabilities, behaviour, and operational lifecycle. This research utilizes the NIST framework for digital forensics wherein the phases of Identification, Preservation, Analysis and Documentation will be implemented. In addition, the study also focuses on executing Vulnerability Assessment and Penetration Testing to identify and explore the types of threats and vulnerabilities pertaining to the Baby Monitor and provided mitigation and remediation solutions to minimise the impact for these vulnerabilities.

Keywords: Digital Forensics, IOT Forensics, Vulnerability Assessment and Penetration Testing, NIST Framework, Baby Monitor

Research Question

What type of cyber-attacks can an IOT device such as Smart Cameras be susceptible to and what could be its mitigation strategies?

1. Introduction:

The modern computing world is advancing rapidly in terms of technology and it's use cases. While Quantum Computing and Artificial Intelligence have peaked in terms of diverse l use cases, the domain of Internet of Things (IoT) has revolutionized the technological landscape, embedding connected devices into nearly every aspect of daily life. From smart home systems to wearable devices, IoT technologies have enhanced convenience and ease of life. Among all these applications, baby monitoring devices have gained significant attention, offering parents the ability to remotely monitor their child’s safety and well-being. However, this interconnected convenience also brings forth a host of security and privacy concerns, making these devices potential targets for cyberattacks. Imagine you monitoring your baby through the camera on your computer but, an attacker has the gained unauthorized access to the camera and now the attacker can monitor all the visuals and activities of your house and can plan to execute a crime. The sensitive nature of the data transmitted and stored by such devices—often involving audio,

video, images, and environmental sensors and hence the Confidentiality, Integrity and Availability of the data must be safeguarded.

This research in the field of IoT forensics through a focused analysis of a baby monitoring IoT device. Such devices, while serving as a critical resource for parents, are particularly vulnerable to exploitation due to inadequate security measures, poor encryption standards, and reliance on cloud-based infrastructure. The research explores the forensic methodologies required to extract and analyse data from these devices, providing insights into their operational structure and identifying vulnerabilities that may facilitate unauthorized access or data breaches.

1.1 Background of the Problem:

IoT forensics, a subdomain of digital forensics, focuses on identifying, preserving, analysing, and presenting evidence from IoT devices to investigate incidents of misuse or cybercrime. The complexity of IoT ecosystems, characterized by diverse hardware, firmware, communication protocols, and data storage mechanisms, poses unique challenges to forensic investigators. Traditional forensic techniques, largely designed for standalone devices, often fall short in addressing the dynamic and distributed architecture of IoT environments. The diverse use of IOT technology has resulted in various potential use cases. Due to this heterogenous nature, the firmware of these devices is closed source as well as exposed to the external network. As a result, detection of security vulnerabilities and cyber-attacks is complex on a firmware level. This complexity results in neglecting the firmware security resulting in vulnerability exploitation.

1.2 Motivation for Research:

IOT is an ever-growing domain which has caught the attention of various researchers and individuals in the technological domain due to its diverse applications across various sectors. While the use of IOT devices in terms of smart wearables, smart homes have escalated in recent times, concerns pertaining to the security of the IOT Devices have increased. The executed research is in the domain of IOT forensics on a focused analysis of an IOT device (Baby Monitor). Baby Monitors fall under the smart home category of IOT use cases which allows parents to continuously monitor their children through audio and video sensors while they are away. However, a significant security concern is that what if the security of the Baby Monitor gets compromised to a cyber-attack such as MITM. In this scenario the attacker would have complete visuals of the house which can then be used to execute a crime such as theft. This gives rise to enhancing the security of IOT devices by utilizing specialized methodologies and tools capable of navigating the complexities of IoT systems. Another reason for choosing IOT forensics for research is because there is not much research that has been done specifically in IOT Forensics and hence there is a lot of scope for enhanced research and practical implementation in this domain.

1.3 Gap Analysis

While the researches conducted so far emphasize on the need to enhance IOT security, each of those researches emphasize on various key factors. As per the research carried out by (Bharadwaj, 2023) a comparative analysis of the Firmware of five IOT devices was carried out and the vulnerabilities were assessed. Whereas, in the research carried out by (Almazrouei *et al.*, 2023), a penetration testing methodology was implemented to uncover vulnerabilities in a

Smart Camera. However, in our research we will be analysing a Two Component Baby Monitoring Devie that comprises of two components i.e a camera as well as a monitor. The analysis would be carried out by combing the penetration testing methodology as well as the NIST Digital Forensic Methodology. In addition, the Gap identified was none of the research papers emphasized on mitigation strategies to prevent the cyber-attacks on IOT Devices. However, in this research we will be implementing a risk rating matrix and mitigation strategies based on the finding of the Vulnerability Assessment.

1.4 Research Objectives:

- To implement a digital forensic methodology tailored for IOT Forensics to extract and analyse data from an IOT Device, providing insights into its operational structure and identifying vulnerabilities.
- To execute Vulnerability Assessment and Penetration Testing to identify vulnerabilities and attacks that an IOT device may be vulnerable to resulting in unauthorized access or data breaches
- To develop a risk rating matrix based on those vulnerabilities and suggest mitigation strategies.

2. Related Work:

In the research carried out by (Bhardwaj *et al.*, 2023) , the researchers carried out a forensic analysis and security assessment of IOT camera firmware for smart homes. This research proposes a unique twelve step framework to perform security and firmware analysis of IOT Smart Home Cameras. The IOT device used for analysis was the D-Link DSC-5020L IOT Camera. As a part of initial analysis, a comparative analysis of five IOT firmwares i.e Wyze, Netatmo, Arlo, Blink and Nest. The comparative analysis was carried out on the basis of various parameters such as their compatibility with Alexa and Google Assistant, the diverse applications of these firmware's across diverse IOT devices such as Security Cameras, Smoke Detectors, Thermostats, Doorbells and Smart Locks, if they offered remote monitoring and, and if they had their own mobile application for interaction. After the initial analysis, the firmware image was acquired from the D-Link Support portal. Basic level firmware analysis was carried out on the firmware image to analyse whether the file is compressed, encrypted, or corrupted and if it is a binary executable, ASCII, Video, or Image file. After firmware image analysis, the byte level analysis consisted of a series of tests such as searching keywords inside file system using dd command, recursive file system extraction of the root filesystem, firmware extraction. The finding of this study uncovered the vulnerabilities present in the firmware wherein, when extracted the root directory files the '/etc_ro' folder is found to have the camera's SSL key, the code contents of which can be viewed using 'grep' and 'cat' commands along with some telnet binaries are found to be installed and a new certificate can be generated as the HTTPS is enabled on the config page. This can be used to take over and control the IoT device as part of advanced-level attacks. The Firmwalker tool was used to analyse the firmware by searching for sensitive contents like usernames, passwords, emails, private keys, and IP addresses. The researchers performed a direct filesystem lookup wherein the SSL-related certificate files including the server certificate inside the cpoi-root/etc or folder of the Linux kernel. A few folders containing details about 'admin', 'root and 'password', 'passwd' were extracted. These files are of high critical risk as these contain hard-coded usernames and

passwords, all residing inside the extracted firmware. In addition, IP Addresses, URLs and hardcoded emails were also retrieved which amount to critical information that can be used to execute high level of cyber-attacks. On a whole, the research emphasized on the current vulnerabilities in the IOT device firmware and the need to enhance its security which could prevent the theft and access to critical information.

In the research carried out by (Almazrouei *et al.*, 2023) "Penetration Testing for IoT Security: The Case Study of a Wireless IP Security CAM", the researchers utilize a systematic penetration testing methodology to identify and uncover security vulnerabilities in a Wireless IP Security Camera. The security camera used for this research is the VAVA IOT Camera. The VAVA base station is connected to the Internet via a wired connection (Ethernet) and sends a wireless access point (protected with WPA-2). Once the user installs the mobile app (VAVA Home), it scans the base station to add it to the app and then adds up to four cameras to that base station. Through the mobile app, users can play a live stream at any time. In addition, users can play back their voices or turn on a loud buzzer. The penetration testing methodology began with the information gathering phase wherein the VAVA Camera was searched on the Federal Communication Commissions (FCC) website to retrieve any relevant documentation to study it's structural and technical make. After the information gathering phase two paths were taken viz Software Exploitation and Hardware Exploitation. As a part of the software exploitation, the Cameras Mobile phone application was used. The application required authentication details to securely login into VAVAS cloud service after which the app can be used to interact and monitor the security cameras. Upon executing mobile phone forensics, it was discovered that VAVA stored the login credentials in a database called vava.db, while the username was stored in plaintext, the password was hashed using a MD5 Hashing Algorithm. However, this algorithm can be easily retrieved using tools such as JohnTheRipper and Hashcat. Further on, the network communication protocols were analysed to identify the ports and services running, wherein Telnet, FTP and SHH were the running protocols. The researchers then tried to find any existing exploits for these ports using Metasploit after which it was found that found that vsftpd 2.0.8 (FTP) and sshd 2015.67 (SSH) were vulnerable to some attacks, but could not be successfully exploited. The hardware exploitation phase began by identifying the communication protocols which comprise of communication interfaces with standard protocols such as UART, SPI, JTAG, and I2C. To identify the communication protocol, the base station was removed from its plastic housing and placed on a PCB. USB-to-UART serial cable was used to communicate with the VAVA base station. After connecting VAVA base station, a terminal emulator was used to indicate what data was received and to interact with the device by sending some data. After switching on the base station no data could be read because of incorrect baud rate setting. After determining the correct baud rate using NXP formula the baud rate was set to 57600 after which the data was readable. An analysis of the system revealed some scripts that are executed at boot time and could be changed. After which a reverse shell generator was used from revshells.com to create a reverse shell to a Docker server on the Internet that listens for the connection coming from VAVA. After the system was rebooted, the root shell was obtained from where the "/etc/dropbear/authorized_keys" file was modified by adding our public SSH key, and creating a connection to the VAVA base station via SSH from the internal network. Upon further analysis the main application running on the VAVA was (Ppcs_vava). After running Ppcs_vava, information such user access token was found which allowed to query more info from the VAVA through the API server.

Cybersecurity and Forensic Analysis of IP-Cameras Used in Saudi Arabia was carried out by ((Kim *et al.*, 2024) wherein the research focused on retrieving evidence from cloud-based storages and analyse logs that can be extracted from IP Cameras. The analysis was carried out against most common attacks that were used to target IP Cameras. Two IP cameras, Hanwha, made in Korea and Mobotix, made in Germany were analysed. The methodology adopted for this research comprised of three phases first being cyber security analysis involving identifying, evaluating, and exploiting vulnerabilities followed by digital forensic analysis, identification, preservation, and analysis and finally documenting the results and findings. The results of this research uncovered potential vulnerabilities wherein Hanwha system exhibited vulnerabilities such as rendering content, improper configurations in specific files extending the scope to execute DDOS attacks. The Mobotix, system comprised of vulnerabilities such as missing HTTP headers, device misconfigurations leading to high-risk cyber-attacks.

Research carried out by (Kaur *et al.*, 2024) "Unveiling the core of IoT: comprehensive review on data security challenges and mitigation strategies". This research emphasized on the need to examine the diverse security threats faced by IOT devices trying to enhancing the security posture by assessing the integration of cloud solutions to minimise security threats pertaining to DDOS attacks, malware deployment, and data breaches. The research is executed by diving the IOT ecosystem into subsystems addressing the vulnerabilities in each subsystem. The findings of this research focus on the mitigation strategies against SQL Injections, DDOS Attacks, Malicious Code Injection, Sniffing Attacks and Impersonation.

The research carried out by (Jaafar *et al.*, 2024) , "A Raise of Security Concern in IoT Devices: Measuring IoT Security Through Penetration Testing Framework". This research focused on exploring the diverse use cases of IOT Devices across diverse domain such as Smart Homes, Agriculture and Smart Healthcare and the need to use automated tools for penetration testing to uncover critical security vulnerabilities to enhance the security posture. For this process, the IOT architecture was broken down into different layers such as Application Layer, Network Layer and Sensory Layer addressing security vulnerabilities in each of these layers. The research utilised the OWASP Security Matrix to classify cyber-attacks across each of these layers based on security principles Confidentiality, Integrity, and Availability. Further on, the research explored the need to employ Automated Tools tailored for IOT devices. The findings of this research address the challenges faced in IOT pentesting providing a comparative analysis between Traditional Penetration Methods and Methods Tailored Specifically for IOT Devices after which considerable gaps were identified in the Traditional Penetration Testing Methodology such as lack of emphasis on firmware security, communication protocols that could only be bridged by developing a methodology tailored for IOT Devices.

"Enhancing home security with IoT devices: A vulnerability analysis using the IoT Security Test," was carried out by (Misailov *et al.*, 2024). This research focused on the Smart Homes use case of IOT Devices such as Smart Thermostats, Smart Alarm Systems, Ip Cameras and Smart Door locks which had a vulnerability score of 6.5, 7.9, 8.2 and 5.1 respectively. Penetration testing was conducted using IOT Test Framework across each of these devices applying remediation strategies to reduce the vulnerability score after which the scores were reduced to 2.1, 3.3, 4.5 and 1.9 respectively. The Smart Door Locks and IP Camera consisted of 12 vulnerabilities on a whole while the Smart Alarm System and Smart Thermostat system revealed 6 vulnerabilities.

3. Research Methodology:

The Methodology adopted for this research comprises of three main phases i.e Review of Literature, Forensic Analysis of the IOT Device, Vulnerability Assessment and Penetration Testing. The complete research methodology can be explained by Figure 1

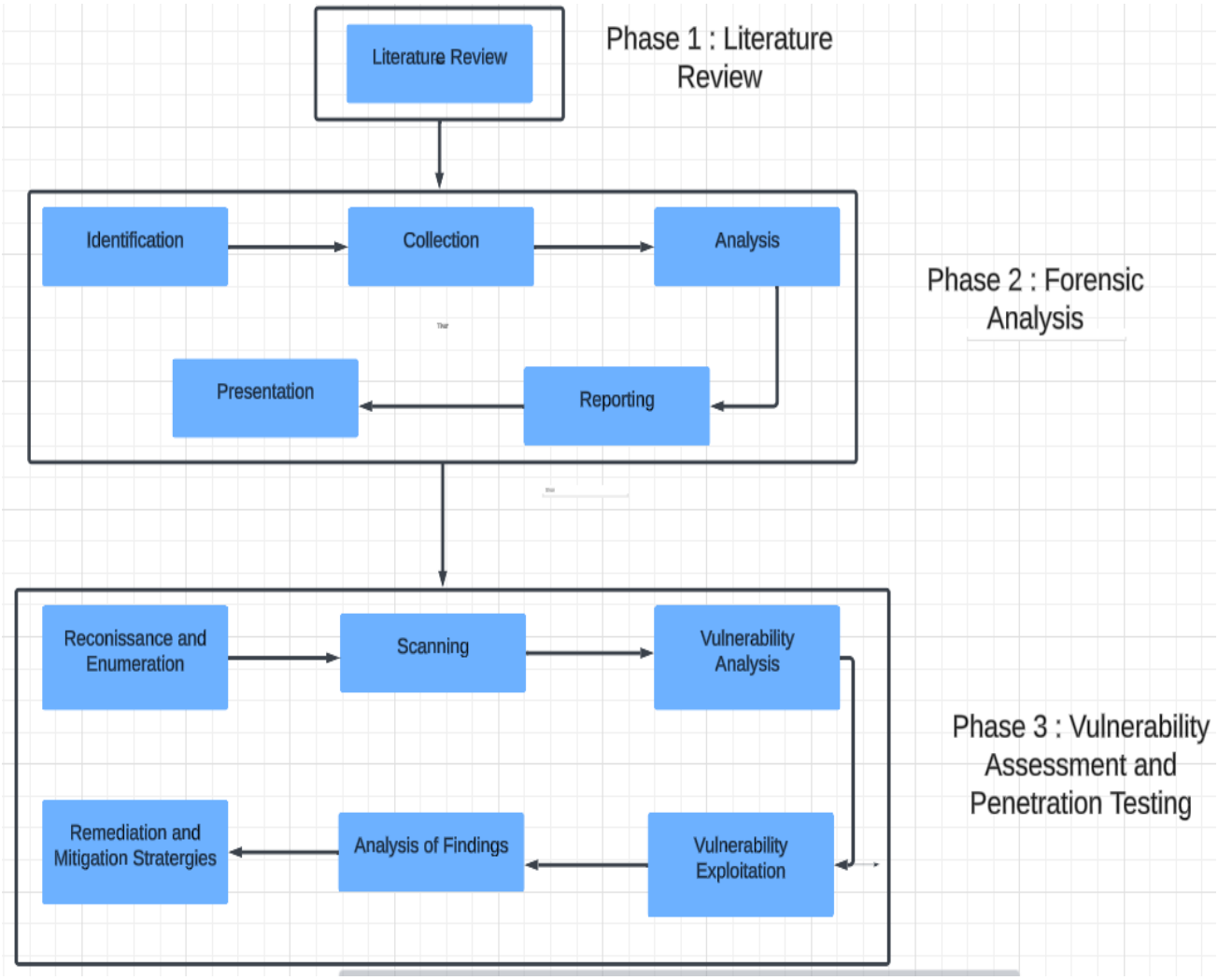

Figure 1 : Research Methodology Flow Diagram

Phase 1: Review of Literature:

The research was initiated by conducting a systematic literature review highlighting the previously done work to act as a point of reference and to identify any existing gaps that could be filled in through our research. For this process, twelve research papers were examined and their process execution and key findings were analyzed and documented. The series of experiments carried out by (Almazrouei *et al.*, 2023) "Penetration Testing for IOT security", is our base paper which is used as a point of reference for our research. After the literature review, we moved onto the next phase of our project which was executing a forensic analysis of the IOT Device.

Phase 2: Forensic Analysis of IOT Device:

In this phase, Forensic Analysis of the IOT Device was executed. For Forensic Analysis, the NIST Digital Forensic Methodology was implemented that comprises of the following phases:

Identification: This phase began by identifying and shortlisting the IOT device that would be forensically analyzed. After thorough research the device shortlisted was a two-component baby monitor that comprised of a smart camera that needed constant power supply and the monitoring device that displayed the footage recorded by the camera. In addition, the baby monitor was allowed to capture footage and operate in the normal environment to carry out behavioral analysis and also explore various functionalities and features of the baby monitor which were feeding reminder, crying detector, playing the lullaby after detecting crying etc.

Collection and Preservation: Once the device was identified, the collection phase was initiated. In the collection phase, information about the device i.e the device makes, the manufacturer, firmware used was collected. In addition, the collection phase also comprised of collection of evidence wherein we used FTK Imager tool to create a logical image of the baby monitor. This logical image would ensure that all the analysis and investigation is only done on the copy and not on the original evidence. For preservation of the evidence, we will be securely storing multiple copies of the logical image to ensure that the evidence is preserved in case the evidence is damaged or corrupted during the analysis process.

Analysis: In the analysis phase, the logical image created by using FTK Imager was analyzed. For analysis we used the Autopsy tool. Autopsy is a prominent tool used in Digital Forensics. Using Autopsy, we were able to analyze the logical image to retrieve any key pieces of evidence which were video files, audio files, any user profiles, hashes, or passwords that could be stored in the baby monitor.

Reporting: In this phase we document all the findings and key pieces of evidence in tabular format which will further be used in the presentation phase.

Presentation: This phase comprises of presenting the findings retrieved from the forensic analysis.

Phase 3: Penetration Testing Methodology:

After executing the forensic analysis, we will be proceeding with the Vulnerability Assessment and Penetrating Testing phase wherein we will try to assess vulnerabilities and exploit them to gain access to the Baby Monitor. This step involves simulating real world cyber-attacks such as DDOS and Man In The Middle Attack to check the security robustness of the IOT Device. After execution of the Vulnerability Assessment and Exploitation we will propose mitigation and remediation strategies to enhance the security of the IOT Device which will help prevent and reduce the impact of cyber-attacks The Entire Vulnerability Assessment and Penetration Testing Phase were divided into various stages which can be given as follows:

Reconnaissance and Enumeration: This is the information gathering phase wherein we will gather as much information as possible about the baby monitor using passive means. In this phase we will understand the design architecture and firmware using online resources and the user manual. Then we will find the IP address using packet capturing tools such as Wireshark and analyze the open ports and services on the IOT device.

Scanning: After the Ip address has been identified we will execute active scanning using Nmap scanning tool to identify open ports, communication protocols and services that are running on the IOT Device.

Vulnerability Analysis: Once the ports and services are identified we will try to find any vulnerabilities that may be caused due to insecure design, software updates, weak credentials, insecure communication protocols. In addition, we will also search for exploits and payloads and try to execute them to exploit the potential vulnerabilities identified.

Vulnerability Exploitation: In this phase the identified vulnerabilities will be actively exploited using various tools provided by Kali Linux. Exploiting the identified vulnerabilities will help us measure the exploitability and impact in case of a cyber-attack. In addition, we will also simulate cyber-attacks to validate the identified vulnerabilities such as bypassing authentication protocols, disrupting communication services by executing DDOS attack, gain unauthorized access to sensitive data, intercept communication by executing MITM attack.

Analysis of Findings: After Vulnerability Exploitation we will analyze the exploited vulnerabilities by documenting the findings which highlight the vulnerabilities identified during the process and also the exploitation methods used to exploit these vulnerabilities. In addition, the potential impact of these vulnerabilities will be compiled in the form of a risk rating matrix highlighting the severity of the vulnerability and it's impact.

Remediation and Mitigation Strategies: In this final phase of the Vulnerability Assessment and Penetration testing methodology we will provide remediation and mitigation strategies against those vulnerabilities. In addition, security issues with regard to enhancing the security of the IOT device from the manufactures end such as releasing software updates, using up to date firmware, using secure communication protocols, utilizing cloud for communication and store instead of storing locally will also be addressed.

4. Design Specifications:

This section provides a brief description of the design specifications highlighting the specifications of the IOT Device and the Architecture diagram of the proposed system.

4.1 IOT Device Specifications:

Table 1: IOT Device Specifications

Name	Babyphone Baby Monitor
Category	IOT Device Smart Camera
Make	Made in China
Manufacturer	Dongguan Anhong Electronic Technology Co. Ltd
WiFi	2.4G WiFi Wireless Transmission
Camera	2 megapixel Night vision Camera
Nominal Voltage	3.7V
Power Supply	5V
Rated Capacity	2000 Mah
Features	360 Rotation, Motion, Detection, Crying Detection, Temperature Monitoring, Two way Intercom, Feeding Reminder, Video Storage

4.2 Architecture Diagram

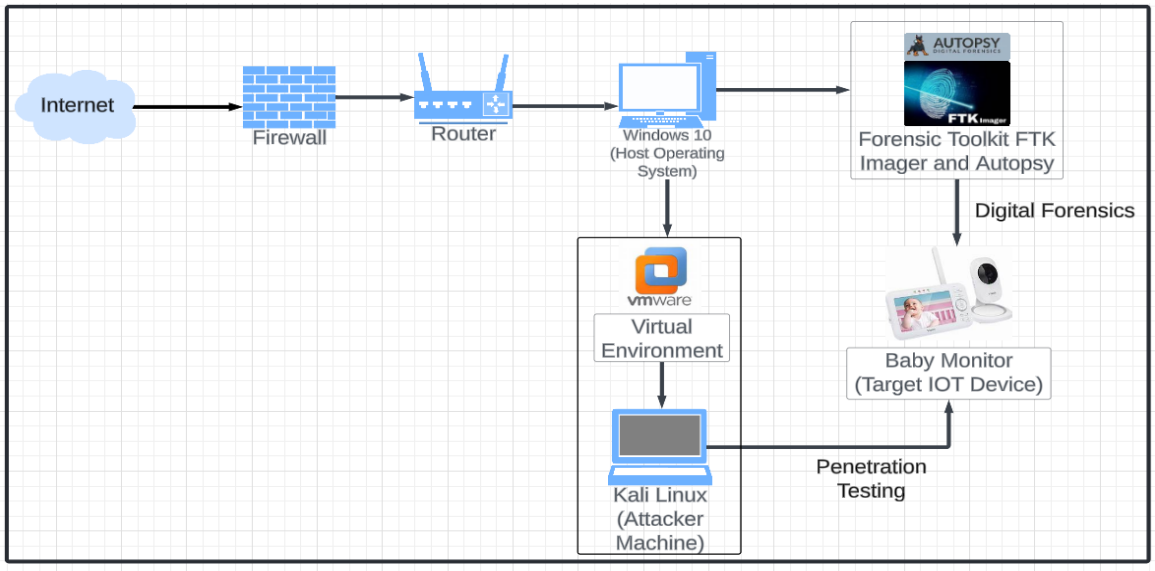

Figure 2: Architecture Diagram

The Architecture diagram highlights the Network Environment in which the IOT Device is connected. In addition, the interaction between the Host and virtual environment via VMWare is also discussed followed by how Kali Linux would interact with the Baby Monitor for executing Vulnerability Assessment followed by Forensic Analysis using Autopsy and FTK Imager .

Network Environment:

Internet: The internet represents the interaction between the network and other services across the system. While the baby monitor is connected directly to the internet, it also ensures that other devices such as the forensic tools and the virtual environment can utilize and retrieve data and resources across the internet.

Firewall: The Firewall ensures that the local network is protected across any unauthorized access. Specially in the case wherein we will be examining the baby monitor, any malicious data, payload or malware which may already be present in the baby monitor could be mitigated by using a firewall.

Router: The router is utilized to connect to the local WiFi (LAN). The Baby monitor is connected to the router via the host operating system ensuring communication between the local area network only.

Host Machine and Virtual Environment:

Windows 10: We have used Windows 10 Version 22H2 as our host operating system wherein we have created a virtualized environment using VMWare to host our Kali Linux Virtual Operating System. In addition, the forensic tools FTK Imager and Autopsy are installed directly upon the host operating system to execute forensic analysis.

Kali Linux: Kali Linux acts as our Attacking Machine for penetration testing and is connected to the Host Operating system via the virtualization software VMWare. To isolate the virtualized environment, we have used the NAT network bridge to ensure that any attack simulation

executed during the security testing does to escape the virtualized environment and affect the host operating system. In addition, Kali Linux and its tools such as Nmap and Wireshark will be used to scan and analyze any vulnerabilities in the baby monitor and then exploit those vulnerabilities.

Baby Monitor: The Baby Monitor is the target IOT device that is used for vulnerability analysis. The Baby monitor will be interacting with the virtual environment via VMWare wherein security testing will be executed by Kali Linux. After security Testing, FTK Imager and Autopsy will be used to carry out forensic analysis of the baby monitor.

Forensic Toolkit: The Digital Forensic toolkit comprises of tools FTK Imager and Autopsy that are installed directly on the host operating system Windows 10. These tools will be utilized for executing forensic analysis by creating a logical image of the baby monitor.

5. Implementation:

5.1 Technical Stack Used

Image Acquisition: Ftk Imager Version 4.7.1.2

FTK Imager is a data preview and imaging tool, widely used in digital forensics for creating images of hard drives, CD's and DVD's and USB devices. It is used to acquire electronic evidence by creating copies of the computer data called images without making changes to the actual evidence. In our analysis, FTK imager was used to create a forensic image of the Baby Monitor IOT Device

Investigation Tool: Autopsy Version 4.21.0

Autopsy is a digital forensics platform that consists of a user interface. Autopsy is widely used by forensic professionals, government appointed forensic investigators in order to investigate, recover and analyse files on a computer. It is free and opensource. In our investigation we used Autopsy to investigate the Forensic Image created by FTK Imager to identify any potential sources of evidence or artifacts.

Nmap: Network Mapper is a open source command line scanning tool that is used to scan ip addressed to identify open ports and services along with its versions and operating systems. Nmap helps users identify which devices are running on their network to identify its open ports, protocols and the services associated with those systems thus facilitating in vulnerability analysis. For this research, Nmap was used in the scanning phase to scan the Ip address of the baby monitor.

Binwalk: Binwalk is a firmware analysis tools which comes pre-installed in kali linux primarily used for searching a given binary image for embedded files and executable code. Specifically, it is designed for identifying files and code embedded inside of firmware images. For our research, Binwalk was used to analyse the Firmware of the Baby Monitor.

Cyber Chef: Cyber chef is an opensource tool also referred to as the Swiss Army Knife in cybersecurity which is used extensively for identifying and decoding hashes such as base 58

or XOR and even encrypted files. In this research, Cyber Chef was used to decode the encoded content in the file “myfiles” which resulted in retrieval of the base 58 encrypted ssh key.

JohnTheRipper: It is a widely used opensource password cracking tool used to perform brute force attacks. It comes preinstalled in Kali Linux Operating System. For our research JohnTheRipper was used to brute force “myfiles” to gain the ssh key.

5.2 Execution

The implementation adopted for this research comprises of two main factors viz, static analysis and dynamic analysis. As a part of our static analysis, we will first understand the firmware and the necessary requirements of the IOT device. Since the IOT device comprises of two parts i.e the Camera which requires constant power supply and the second is the monitor that is used to display the ongoing camera footage. However, both these devices being linked to each other would utilize the same firmware. Hence the first part would be analyzing the firmware and device requirements. For this process, we will connect the IOT camera as well as the monitor to our device using a USB cable to understand its firmware.

Once this is done, an in-depth dynamic analysis is executed which outlines the methodology wherein the forensic analysis of the device is first carried out by NIST Digital Forensic Methodology using tools FTK Imager to create a logical image of the IOT device and Autopsy that is used to analyze the forensic image to retrieve any potential evidence such as any audio files, video files, hash tables or user credentials. Post Forensics, penetration testing methodology will be applied.

5.2.1 Static Analysis:

The IOT Device is connected to the laptop via the USB Cable. Although the IOT device was connected through the USB, the Laptop did not display the established connection. Hence, we reset our drivers in our device manager after which the IOT device was detected. The firmware was then studied after which it was inferred that the device used 2.4Ghz wireless transmission. The firmware file identified was ahx_600m_vx1r3_syscore.bin. However, there was no specific documentation with regard to the AMB600 model we used the Binwalk tool to examine the firmware file after which it was identified that the firmware comprised of hardcoded credentials. A similar result was found in the research carried out by (Bhardwaj *et al.*, 2023) wherein the researchers used the Binwalk Tool which provides offset content details about the firmware image file after which it was confirmed that the firmware file is a Linux OS running MIPS architecture with the ‘U-Boot’ bootloader at the 99,360 offset another uImage offset at 327,744 and the filesystem in LZMA compressed format (Bhardwaj *et al.*, 2023).

5.2.2 Forensic Analysis:

Creation of the Forensic Image:

Once the device was connected to the Windows 10 Device, the baby monitor was allowed to run in the normal environment. This was done to analyse if the baby monitor stored any video, audio, or images locally on the device. Post this, a logical image of the folder was created using FTK Imager. Since the IOT device was discovered in the C Drive, a forensic image containing entire C drive was created. However, the destination for the storage of the forensic image is in

E drive, as the destination of the forensic image cannot be same as that of the source forensic image. The Logical Image is successful created and verified.

Analysis of Forensic Image:

Post Image Acquisition using FTK Imager, the Autopsy tool was used to analyse the forensic image to investigate any artifacts. A new case needs to be created after which the base directory to be selected is the location of the forensic image. Upon examination artefacts such as databases, hast tables, metadata were identified. In addition, several Video and image files were also retrieved. These audio and video files were captured when the monitor was allowed to run in the environment. However, the baby monitor can only store video by provisions of a memory card. This implies that the Baby monitor was able to capture videos and images and store it locally in plain format. This poses as a significant security risk, as these audio and video files can be accessed if an attacker is able to establish a remote connection.

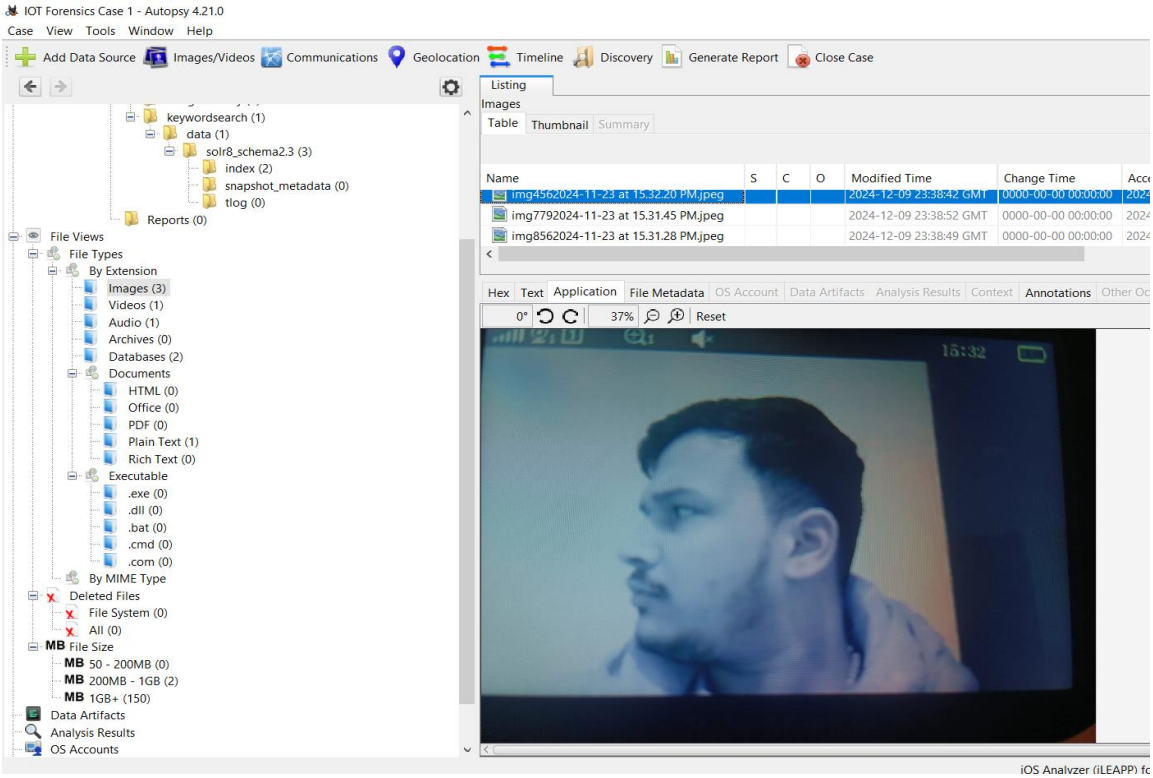

Figure 3: Retreived Image from Autopsy Forensic Analysis

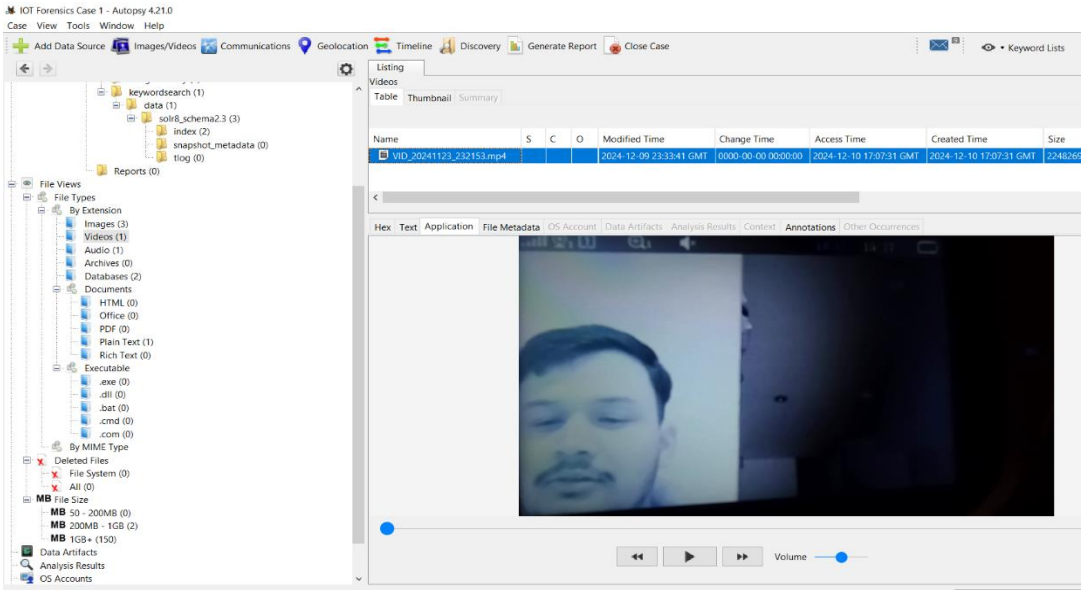

Figure 4; Retrieved Video File from Autopsy Forensic Analysis

5.2.3 Vulnerability Analysis and Penetration Testing:

Enumeration

In this phase a connection was established between the baby monitor and the WIFI Network. The scanning phase was executed using the Kali Linux Virtual Machine wherein the netdiscover command was used to first discover the IP address which was 192.168.155.131.

Scanning

After the IP address was identified, the scanning phase began by using Nmap to identify the ports and services that were running on the Camera. It was discovered that two ports 22 and 80 associated with the ssh and Http service were open.

Vulnerability Analysis and Exploitation

In this phase, we tested the IOT device across common vulnerabilities such as Broken Access Control, SQL Injection, Bruteforce attacks to identify any hash tables, login credentials. began by analyzing the open ports 22 and 80. While the camera utilized HTTP insisted of HTTPS we accessed the web interface of the camera. The web interface comprised of two fields, username, and password. In these username and password fields we tested input validation by executing inbound SQL Injection Query.

SELECT * FROM Users WHERE Username='1' OR '1' = '1' AND Password='1' OR '1' = '1'

However, after execution of this query we were unable to access any data pertaining to login credentials or hash tables.

Post this test, fuzzing was executed to identify any hidden files or directories. For fuzzing, the FFUF fuzzer was utilized. Upon execution of Fuzzing, it was identified that port 80 HTTP, stored a file “myfiles” which comprised of a private ssh key. The “myfiles” file comprised of a lot of encoded content. The encoded content was decoded using CyberChef an online

decoding tool which was inferred to be a Base 58 encrypted private ssh key. This file was vulnerable to brute force attack for which JohnTheRipper was used to obtain the ssh key. To execute a brute force attack, a wordlist was created that comprised of numerous combinations of usernames and passwords. Post brute forcing, the password "P@55word!" was identified as the password.

DDOS Attack was also simulated using the High Orbit Ion Cannon (HOIC) that is an opensource tool to execute DOS and DDOS Attacks. The DDOS Attack was executed to understand the behaviour of the IOT Device. To execute DDOS Attack, HOIC was installed onto our Windows 10 Host Machine. A key consideration here is that Windows flags HOIC to be Malware or file involving high security risk. As a result, the Windows Defender was turned off during installation. After installation, the ip address of the smart camera was entered in the format https:// 192.168.155.131 and the threads were set to 20. After execution of DDOS Attack it was observed that the Baby Monitor has a disrupted connection from the camera wherein the Baby Monitor could not detect the Smart Camera as shown in Figure 5.

Figure 5: Disruption of Services on Baby Monitor

5.3 Analysis of Findings:

The Findings of this study highlight the key vulnerabilities identified from this research through forensic analysis and penetration testing. The vulnerabilities identified are briefly described in the table below along with its potential impact and mitigation strategies.

Table 2: Vulnerability Analysis

Vulnerability Identified	Description	Impact	Mitigation Strategy
Weak SSH Credentials	The private SSH key was stored in a file named "myfiles" with base 58 encoding. Decoding revealed the password to be "P@55word"	Having weak SSH credentials can result in establishing an unauthorized ssh connection leading to compromise of the system	The SSH keys should be stored in secure key vaults using high encryption standards such as AES or DES
Unencrypted Local Storage	The IOT device has a specific slot for memory cards for storage. However, the	An attacker with remote access would easily be able to gain access to the stored footage. In	Use of cloud-based solutions for storage that contain inbuilt encryption standards

	camera still captured video files and images and stored it locally without encryption. The images and video files were retrieved by Autopsy.	addition, having a memory card for storage acts a single point of failure, wherein memory card stolen gives entire access to the video footage leading to privacy concerns	resulting in elimination of local storage and enhancing security for storage
Use of HTTP instead of HTTPS	The IOT device used HTTP instead of HTTPS for data transmission	HTTP has weak encryption, thus data transmitted can be intercepted compromising confidentiality and integrity	Use of secure protocols such as HTTPS that have secured encryption standards
DOS and DDOS Attack	The signal between the camera and the Monitor was disrupted by executing DDOS Attack through HOIC.	Disruption of services. The simulated attack was executed on a small scale. However, if simulated on a camera with similar security measures could result in greater impact	Implement cloud technologies for server-side use cases. Cloud technologies comprise of load balancers, thus mitigating the DDOS Attack
Weak Cryptographic Standards	The private SSH key was encrypted using a base 58.	Base 58 encoding could easily be decoded using an online decoded cyber-chef and then brute forced using JohnTheRipper	Implement strong cryptographic standards such as AES or RSA

6. Evaluation and Discussion:

The methodology designed comprised of Digital Forensics and Penetration Testing, was tailored specifically for the analysis of IOT Devices. The implemented methodology discovered critical vulnerabilities that could be exploited to execute high level of cyber-attacks. While executing firmware analysis, it was discovered that the device was using 2.4GHZ for WIFI transmission. 2.4GHz is inferior in terms of security as compared to modern WPA3 security standards. In this scenario, an attacker could easily execute a Man In The Middle Attack to intercept and modify the network packets during transmission. The process of packet interception and network traffic analysis was carried out using Wireshark. However, the results were not satisfactory as the packet capturing process faced significant technical errors. Attempts were made to resolve the errors by connecting an ethernet and execute network traffic analysis again but the results were the same.

The Digital Forensic Analysis carried out uncovered critical vulnerabilities highlighting out of scope behavior and weak storage mechanisms. The forensic toolkit used comprised of FTK Imager to create the logical image of the baby monitor while Autopsy was used for the analysis of the forensic image. Before executing Forensic analysis, the baby monitor was allowed to run

and capture audio in the environment. After creating the logical image, Autopsy was used wherein a case was created specifying the logical image as the data source for analysis. Upon analyzing the forensic image, it was discovered that the Baby Monitor recorded videos and audios and stored it locally in unencrypted format. However, the baby monitor only has a memory card slot for storage and does not reveal any other provisions for storage. This implies that that the Baby Monitor poses critical risks to privacy and confidentiality. In addition, the storage in unencrypted format raises considerations wherein an attacker can access and retrieve the footage if remote access is achieved. Multiple attempts were made to uncover any databases or associated hash tables. However, no information pertaining to databases or hash tables was retrieved. This expectation came from (Almazrouei *et al.*, 2023) wherein the researchers were able to retrieve login credentials from the database vava.db which was the database of the VAVA IP Security Camera.

The results retrieved from the Vulnerability Assessment and Penetration testing phase can be seen in Table 2. The baby monitor was found to be vulnerable to a series of attacks and also comprised of critical vulnerabilities that could be exploited. The baby monitor was scanned using the command nmap -sC -sV -O which highlights open ports, their versions and also the associated services running. Two ports were open, 22/SSH and 80 HTTP. The Baby Monitor used HTTP for communication which is an unencrypted communication protocol and can easily be intercepted using modern offensive security tools and techniques. In addition, while we were not able to retrieve any databases or hashes during the forensic process, in the Penetration Testing phase it was identified that SSH credentials were stored in a file named "myfiles" in a base 58 encoded format which was then decoded using cyber chef and Brute forced using JohnTheRipper. These experiments were carried out on a smaller scale considering the scope of the research. However, the findings discovered give a brief description of the security standards of the IOT Device. While Smart Cameras and Devices utilise cloud technologies for storage and retrieval of data, the baby monitor did not have any provisions associated for integration of cloud services. The absence of cloud services provided the opportunity to analyse the behaviour of the IOT Device in case of a DDOS Attack. The High Orbit Ion Cannon was used to execute the DDOS attack specifying the IP address and specifying the threads to 20. Upon execution of the DDOS Attack it was observed that the communication between the baby monitor and the camera was disrupted wherein the Camera was not detected on the monitor.

Discussion

In the research carried out by (Bhardwaj *et al.*, 2023) the researchers inferred that the firmware security is the most neglected fragment of IOT security. As a result, they proposed a twelve-step methodology to execute firmware analysis of IP cameras. The firmware level analysis uncovered a set of vulnerabilities wherein the SSL key of the camera was found in the root directory folder '/etc_ro' which were viewed suing the grep and cat command. The firm walker tool was used to analyse firmware by searching keywords such as usernames and passwords after which details about 'admin', 'root and 'password', 'passwd' were extracted from the cpoi-root/etc or folder of the Linux kernel. In our research a similar result was achieved wherein the password "P@55word" was retrieved by brute forcing the base 58 encoded SSH key using JohntheRipper. However, the results achieved in our research were derived from the penetration testing phase and not from the firmware analysis phase.

In the penetration testing carried out by (Almazrouei *et al.*, 2023) in Penetration Testing of VAVA security IOT Camera. The camera was secured with WPA-2 standards and used a mobile phone application VAVA Home for operational functionality. However, upon executing mobile phone forensics, it was discovered that VAVA stored the login credentials in a database called vava.db, while the username was stored in plaintext, the password was hashed using a MD5 Hashing Algorithm which was decrypted using tools such as JohnTheRipper and Hashcat. Further on, the network communication protocols were analysed to identify the ports and services running, wherein Telnet, FTP and SHH were the running protocols. Attempts were made to execute existing exploits for these ports using Metasploit after which it was found that found that vsftpd 2.0.8 (FTP) and sshd 2015.67 (SSH) were vulnerable to some attacks, but could not be successfully exploited. In our research a similar scenario was encountered wherein port 22/ssh was vulnerable and stored the password in "myfiles" file retrieved using the same tool JohnTheRipper. This implies that Smart Camera category of IOT Device store credentials which can be retrieved by means of penetration testing or forensic analysis.

The research besides identifying vulnerabilities also provides remediation and mitigation strategies for the identified vulnerabilities. Similar approach for remediation and mitigation strategies was encountered in the research carried out by (Kaur, 2024) wherein the researchers discussed remediation strategies for DDOS Attacks, Bruteforce Attacks and Firmware Vulnerabilities.

The novelty of the executed research lies in the findings of the forensic analysis wherein the captured video and audio files were retrieved. While the results encountered so far comprised of retrieving critical credentials, exploiting vulnerable ports, and remediating those vulnerabilities, none of the researchers were able to retrieve any audio footage, video footage captured by the Smart Cameras.

While we were successfully able to execute Forensic Analysis and Penetration Testing there were some key challenges faced during this research. First challenge encountered was unable to access the IOT Device via the USB cable because of Device Driver issues. Resolving this use was a challenge as it was difficult to analyse the root cause. However, after updating the device drivers and resetting the Baby Monitor, it could be detected. Second challenge faced was packet analysis. Wireshark was used to capture any packets and intercept traffic to analyse the network traffic to further on execute a Man in The Middle Attack. However, despite continuous captures, no data packets pertaining to the IOT device were captured. When port HTTP was discovered to be open and the web interface was accessed to execute a SQL Injection attack, despite the query execution no data or database information was retrieved resulting in an unsuccessful attempt for SQL Injection. This differed from the results achieved by (Almazrouei *et al.*, 2023) wherein the researcher was able to access file contents by exploiting the hardware.

7. Conclusion and Future Work:

The research executed in this study highlights the research question "What type of cyber-attacks can an IOT device such as Smart Cameras be susceptible to and what could be its mitigation strategies? further addressing the security concerns and the need to enhance the security of IOT Devices. For this purpose, a methodology was implemented integrating two domains Digital Forensics and Vulnerability Analysis and Penetration testing wherein

vulnerabilities were identified, analyzed, and mitigated enhancing the security of the Smart Cameras contributing to the IOT Ecosystem. The domain of IOT is growing rapidly with diverse application across various sectors including healthcare, Smart Homes, Agriculture and other critical sectors. However, due to this diverse and complex network the security of the IOT devices is often neglected resulting in high level cyber-attacks. The research highlights security vulnerabilities pertaining to, weak encryption standards, use of insecure communication protocols, firmware vulnerabilities and insecure storage. The analysis carried out against Dongguan Anhong ABM600 Baby Monitor uncovers critical vulnerabilities that can be exploited to execute high level of cyber-attacks in the real-world providing remediation and mitigation strategies to minimise the impact.

The Digital Forensic Analysis carried out using FTK Imager and Autopsy uncovered significant vulnerabilities pertaining to insecure data storage. The baby monitor has a dedicated slot for memory card for data storage. However, upon forensic analysis using Autopsy it was discovered that the baby monitor stored sensitive data such as video files and images without having any encryption standards associated. This raises considerable privacy concerns wherein an attacker if gained remote access to the baby monitor will be able to access the images and videos directly from the IOT Device storage. In addition, using a memory card for storage acts as a single point of failure wherein the forensic analysis highlighted the lack of security with regard to data storage as per the architecture of the device. As a result, it is imperative to ensure encryption standards for data storage.

The Vulnerability Analysis and Penetration testing uncovered considerable security risks that needs to be addressed. The first one being Weak SSH credential management wherein the ssh key was store inside a file “myfiles” using base 58 encoding. The decoding of this base 58 encryption was easily possible by using Code Chef, an online decoding tool. After decoding it brute force attack was executed using JohnTheRipper wherein it was discovered that a password “P@55word” was stored. Such weak credential management poses as critical vulnerabilities leading to system compromise. The second fining was use of insecure communication protocols wherein HTTP was used instead of HTTPS. Communication via HTTP can easily be intercepted as the communication is not encrypted. However, in this research we were unable to intercept or alter any packets or communication between the baby monitor. The third finding was, use of outdated WIFI Encryption technology where 2.4GHz was used without support of modern encryption protocols such as WPA3. The camera constantly communicates across the internet and diverse access points. In such a scenario having weak WIFI encryption technology poses significant threats such as remote access to the live footage of the camera.

In future this research can be carried forward by re-executing the forensic analysis. However, this time the Forensic Analysis can be executed using Magnet AXIOM which is a premium Digital Forensics Tool. The findings from Magnet AXIOM can be compared against the findings of FTK Imager and Autopsy wherein a comparative analysis can be carried out for Opensource tools against Paid Tools. In addition, the challenges faced in executing Man In The Middle Attack and SQL Injection can be studied to execute a successful execution of these attacks. In addition, IOT Devices particularly smart cameras are used across various purposes such as CCTV Surveillance, Security Cameras, and Baby Monitors. The footage captured by these devices are critical and pose to be critical sources of evidence in case of physical attacks such as robbery, theft, or hijacks. However, there is no provision associated in response to these

physical attacks. For this purpose, Artificial Intelligence and Machine Learning algorithms can be integrated along with the IOT Device to recognise any attacks such as robbery, theft hijacks or fire hazards and raise alerts accordingly. In addition, Artificial Intelligence and Machine Learning Algorithms can also be used to enhance the Digital Forensics Process to achieve more precise and accurate results.

Acknowledgement:

I would like to thank my project supervisor Professor Eugene McLaughlin for his unwavering support and guidance throughout the execution of the project. The weekly meetings were insightful highlighting the key factors and metrics to focus on for successful execution of this research. Professors' constant facilitation and feedback helped me overcome challenges I faced during Forensic Analysis for this research. In addition, I would also like to thank National College of Ireland for giving me the opportunity to undertake this research.

References:

Abura Samson (2024) 'Exploring security, performance and privacy in the internet of things: A comprehensive survey', *GSC Advanced Research and Reviews*, 21(1), pp. 280–319. Available at: https://doi.org/10.30574/gscarr.2024.21.1.0388.

Almazrouei, O. *et al.* (2023) 'Penetration Testing for IoT Security: The Case Study of a Wireless IP Security CAM', in *2023 IEEE 2nd International Conference on AI in Cybersecurity (ICAIC)*. IEEE, pp. 1–5. Available at: https://doi.org/10.1109/ICAIC57335.2023.10044176.

Bakhshi, T., Ghita, B. and Kuzminykh, I. (2024) 'A Review of IoT Firmware Vulnerabilities and Auditing Techniques', *Sensors*, 24(2), p. 708. Available at: https://doi.org/10.3390/s24020708.

Bhardwaj, A. *et al.* (2023) 'Forensic analysis and security assessment of IoT camera firmware for smart homes', *Egyptian Informatics Journal*, 24(4), p. 100409. Available at: https://doi.org/10.1016/j.eij.2023.100409.

Feng, X. *et al.* (2023) 'Detecting Vulnerability on IoT Device Firmware: A Survey', *IEEE/CAA Journal of Automatica Sinica*, 10(1), pp. 25–41. Available at: https://doi.org/10.1109/JAS.2022.105860.

Jaafar, A.G. *et al.* (2024) 'A Raise of Security Concern in IoT Devices: Measuring IoT Security Through Penetration Testing Framework', *International Journal of Advanced Computer Science and Applications*, 15(5). Available at: https://doi.org/10.14569/IJACSA.2024.0150568.

Kaur, K. *et al.* (2024) 'Unveiling the core of IoT: comprehensive review on data security challenges and mitigation strategies', *Frontiers in Computer Science*, 6. Available at: https://doi.org/10.3389/fcomp.2024.1420680.

Kim, K. *et al.* (2024) 'Cybersecurity and Forensic Analysis of IP-Cameras Used in Saudi Arabia', *Journal of Information Security and Cybercrimes Research*, 7(1), pp. 67–84. Available at: https://doi.org/10.26735/LLFQ4473.

Mahmood, H. *et al.* (2024) 'Comparative study of IoT forensic frameworks', *Forensic Science International: Digital Investigation*, 49, p. 301748. Available at: https://doi.org/10.1016/j.fsidi.2024.301748.

Misailov, A.Yu. *et al.* (2024) 'Enhancing Home Security with IoT Devices: A Vulnerability Analysis Using the IoT Security Test', *BIO Web of Conferences*, 86, p. 01084. Available at: https://doi.org/10.1051/bioconf/20248601084.

Nadir, I., Mahmood, H. and Asadullah, G. (2022) 'A taxonomy of IoT firmware security and principal firmware analysis techniques', *International Journal of Critical Infrastructure Protection*, 38, p. 100552. Available at: https://doi.org/10.1016/j.ijcip.2022.100552.

Sanmorino, A. *et al.* (2024) 'Enhancing IoT Security through an Artificial Neural Network Approach', *EAI Endorsed Transactions on Internet of Things*, 10. Available at: https://doi.org/10.4108/eetiot.5045.

Seifi, M. *et al.* (2023) 'How effective are residential CCTV systems: Evaluating the impact of natural versus mechanical surveillance on house break-ins and theft in hotspots of Penang Island, Malaysia', *Security Journal*, 36(1), pp. 49–81. Available at: https://doi.org/10.1057/s41284-022-00331-8.