Forensic Analysis Framework for Securing Consumer Internet of Things Devices: *Identifying Vulnerabilities and Improving Evidence Collection*

Student First and Last Name: Dawda Wally

Student ID: R2404D17931625

Course Title: UEL-CN-7000 Mental Wealth; Professional Life (Dissertation)

Date of Submission: 24th July 2025

Acknowledgements

I extend my deepest gratitude to my mother, **Kumba Dampha**, whose unwavering love, strength, and sacrifice have laid the foundation for all that I have accomplished. Her resilience and steadfast determination in the face of adversity have been a continual source of inspiration throughout my academic journey.

I also wish to express my heartfelt appreciation to my beloved wife, **Fatou Timbo**, whose optimism, understanding, and emotional support have been a constant source of strength. Her unwavering belief in me has been instrumental in helping me persevere throughout this journey.

I would also like to extend my gratitude to my special person, **Isatou Jagne,** whose support and continuous encouragement have been invaluable throughout this research. Her presence and belief in my abilities have significantly contributed to the successful completion of this study.

This work would not have been accomplished without the love, support, patience, and faith of the people above. I am deeply grateful to them.

Preface

The high rate of adoption of the Internet of Things (IoT) has been associated with great convenience for humanity, but has also come with high levels of complexity and security threats. Such devices as smart locks, IP cameras, or wearable sensors tend to contain sensitive data all the time but do not benefit much in terms of forensic preparedness. As I set out to undertake this research endeavour, I recognised that contemporary digital forensics techniques would hardly succeed in a direct encounter with the decentralised and behaviorally convoluted nature of consumer IoT landscapes.

This study was conceived as a result of the uncertainty around these security issues and the intention to work out effective remedies. The goal was to develop a people-oriented forensic framework that is not only compliant with the technological concepts of IoT products but also considers the actions of people and the established legal regulations. Using a mixed-methodology, the work incorporated both vulnerability mapping informed by the available sources of evidence and user behaviour surveys to develop a risk readiness focus, including major areas of security neglect, including the use of default passwords and firmware neglect.

One of the major outcomes of this study is a multi-layered framework comprising a Vulnerability Classification layer, a Forensic Procedural Readiness layer, and a User Awareness and Engagement layer. This framework primarily focuses on its practical applicability, which potentially sets it apart from many others. I have also put forward some sensible design artefacts, such as the legal compliance matrix, mobile interface mockups, which all help to reinforce the framework's practical applications within different security architecture. The study also brings a replicable, scalable, and legally-informed paradigm of forensic readiness, which has traditionally been a technical task, but needs to be presented as a socio-technical issue.

I believe this work can help to advance the emerging domain of IoT forensics and encourage more work to advance the security of our increasingly interconnected world.

Table of Contents

List of Tables

List of Figures

List of Abbreviations and Nomenclature

Abbreviation	Full Form
AI	Artificial Intelligence
API	Application Programming Interface
CCPA	California Consumer Privacy Act
CERT	Computer Emergency Response Team
CoAP	Constrained Application Protocol
CPSS	Cyber-Physical Systems Security
DSR	Design Science Research
DDoS	Distributed Denial of Service
DFA	Distributed Forensic Architecture
DNS	Domain Name System
ENISA	European Union Agency for Cybersecurity
FAIoT	Forensics-Aware Internet of Things

FTK	Forensic Tool Kit
GDPR	General Data Protection Regulation
HVAC	Heating, Ventilation, and Air Conditioning
HTTP	Hypertext Transfer Protocol
IoT	Internet of Things
IIoT	Industrial Internet of Things
JSON	JavaScript Object Notation
JTAG	Joint Test Action Group (debug interface)
MAC	Media Access Control
MQTT	Message Queuing Telemetry Transport
NFP	Network Foundation Protection
NIST	National Institute of Standards and Technology
OTA	Over-The-Air (firmware update)
OWASP	Open Worldwide Application Security Project

PIPEDA	Personal Information Protection and Electronic Documents Act
PRISMA	Preferred Reporting Items for Systematic Reviews and Meta-Analyses
RAM	Random Access Memory
SBOM	Software Bill of Materials
SDLC	Software Development Life Cycle
TLS	Transport Layer Security
UART	Universal Asynchronous Receiver-Transmitter
VLAN	Virtual Local Area Network
WORM	Write Once and Read Many
XML	Extensible Markup Language

Abstract

Consumer IoT devices continue to permeate globally, thus creating a new transformative digital environment where users' data can be illegally accessed by bad actors through vulenrabilities in connected devices, thereby contributing to security and forensic risks. Traditionally developed digital forensic solutions that are intended to be used in centralised computing environments prove to be incapable of handling such volatile and heterogeneous IoT vulnerabilities, especially within cloud computing environments. This study aims to explore and understand vulnerabilities in consumer IoT devices and how to improve evidence collection using a new forensic analysis framework.

The study design is based on a mixed-methods study that derives its foundation from Design Science Research (DSR). It combines a systematic literature review and user survey to collect relevant data for analysis and framework development. The survey reveals that the level of ignorance and preparedness about forensic practices among the users are on the rise. The systematic literature review indicates that device-level, firmware, network-level, and application-level vulnerabilities are common issues that need to be addressed. Results from the survey and systematic review are combined to formulate a layered forensic analysis framework that contains three layers: (1) a vulnerability classification and mapping layer, (2) procedural forensic readiness guidelines layer, and (3) a user engagement and literacy layer.

The introduced forensic analysis framework transforms the concept of forensic readiness to a socio-technical lens. It gives an effective strategy to improve incident response and digital evidence integrity of daily smart IoT environments. Finally, this study proposes the following recommendations: field verification of digital evidence collection and vulnerability detection mechanisms, using blockchain and AI in digital forensics, and localisation of awareness tools to apply to various demographics of users.

Keywords: Consumer IoT, digital forensics, forensic readiness, IoT vulnerabilities, behavioural security, user-centric framework, forensic analysis, digital evidence, security awareness, smart devices, forensic preparedness

Chapter 1: Introduction

1.1 Background of the Study

The Internet of Things represents one of the most transformative technological paradigms of the 21st century; an intricate web of interconnected devices that extends computational intelligence beyond traditional screens and into the physical world. IoT has become an inseparable part of the modern world. Its extensive application is not merely a trend but a global shift: as suggested by Statista, the number of devices enabled by the IoT should grow to more than 30.9 billion by 2022, and to more than 18.9 billion by 2025, which is a significant number in comparison to the past few decades, suggesting the scale and the pace at which the transition to the digital realm has proven to continue to move forward rapidly.

However, behind all these, something that is not visible on the surface is an uprising challenge: the unstable nature of security when it comes to consumer IoT environments. Unlike the system used at the enterprise level, consumer-oriented IoT devices are often completely or only remotely secured because of market competition, the rapid development cycle, and the lack of enforcement of regulations. As noted by Atlam, Walters, and Wills (2020), these devices commonly suffer from hardcoded credentials, outdated firmware, and unencrypted data transmissions, making them fertile grounds for exploitation by cybercriminals. IoT devices are made even more vulnerable by their ubiquitous nature, automation potential and real-time interaction.

Such an instance of security lapse obtains an even more sinister meaning when discussed within the confines of digital forensics. Contrary to conventional digital forensics, which is now entrenched in how to use static sources of data, like personal computers and centralised servers, IoT systems are not always legally compliant in terms of data storage and processing. A heterogeneous architecture is inherent in IoT, where there is a large variety of hardware and operating systems whose firmware tends to be proprietary and/or undocumented. Many devices operate with minimal memory, intermittent connectivity, and short-lived data retention

cycles—factors that complicate evidence collection, preservation, and analysis (Conti et al., 2018).

Moreover, it is quite difficult to implement forensic activities due to the decentralised and weak nature of the information generated by IoT devices. Logs may be written over in a matter of hours, be stored in volatile memory or pushed up to cloud servers with minimal local redundancy. Certain products use special proprietary protocols that can hardly be intercepted or decrypted unless the manufacturer fully cooperates. Even the identification of the existence and location of relevant information becomes a non-trivial task in many cases. According to Yaqoob et al. (2019), the lack of standardised tools and methodologies for IoT forensics leaves investigators with an inconsistent and often unreliable foundation for incident response and legal scrutiny.

The consequences of forensics unpreparedness are no longer hypothetical, as IoT infiltrates ever more high-stakes industries like healthcare, energy infrastructure, smart cities, and home security systems. The cost of forensics unpreparedness is, therefore, now imminent and potentially devastating for IoT consumers. For example, a hacked smart medical device or a hacked home surveillance system feed could have life-changing repercussions. Hence, forensic readiness, the capacity to collect, preserve, and analyse digital evidence in a legally defensible, technically sound way, is not only a technical necessity but a social need.

This research is positioned at the crossroads of security, forensic science, and human behaviour, as the forensic problems of IoT devices cannot be solved only through technical breakthroughs, but also through the understanding of users and their behaviour. As consumer IoT becomes an indivisible part of digital infrastructure, this study recommends the need to create a scalable, user-considerate forensic framework that is in line with the technological reality as well as legal anticipation.

1.2 Problem Statement

Although consumer IoT devices have been experiencing a booming market penetration and their massive integration in our lives, the field is left with a lack of standardised forensic methods that would be specific to such systems. The existing forensic tools, methods, and frameworks are not very useful when it comes to addressing the unique issues associated with IoT environments. Devices do not always have uniform logging, trusted communication protocols and standard data storage formats. Such inadequacies not only impair the process of vulnerability assessment but also the possibilities to obtain and maintain digital evidence after a security incident.

The lack of a unified framework of forensic analysis does not provide the consumers, investigators, and security professionals with unambiguous information on how to react to incidents related to IoT. This leads to disunity in practices, lower evidentiary integrity, and a higher possibility of missing vital information. Additionally, it is hard to prioritise risk mitigation measures unless one knows how the vulnerabilities are spread across the types of IoT devices.

1.3 Research Aims and Objectives

The primary objective of this study is to build a forensic analysis framework of consumer IoT devices. The framework can help to fill the gap between vulnerability assessment and forensic evidence gathering, which will allow investigators and security professionals to address the IoT-related incidents.

This study aims to achieve the following:

- To carry out a systematic literature review on resources that have been published on IoT security vulnerabilities and forensic approaches.
- To study a taxonomy of common vulnerabilities in consumer IoT devices by device type, technical domain and severity.
- To assess the current forensic practice and determine the strengths and weaknesses of the methods used in IoT.

- To develop a unified system integrating forensic preparedness, vulnerability categorisation and procedural suggestions on how to collect evidence.
- To set the stage for testing a new security framework with real-life case studies and written security incidents.

1.4 Research Question

To guide the direction of this research, the following research question is posed:

How can a standardised forensic analysis framework improve evidence collection and vulnerability detection in consumer IoT devices?

The question deals with the fundamental technical issue of combining forensic procedures with vulnerability analysis in the security landscape. Answering this question offers an opportunity to present the user perspective to know the behavioural determinants of forensic preparedness and security measures among the end-users in a real-life context.

Table 1: Research Objectives and Corresponding Questions

Research Objective	Research Direction
Examine forensic limitations in consumer IoT	What are the main forensic challenges in IoT environments?
Design a tailored forensic framework	How can a layered model improve evidence collection?

1.5 Significance of the Study

This study can be helpful within the digital forensics and cybersecurity domain. It also addresses key identified research gaps. The relevance of this study can be outlined in the following domains:

- **Forensic Science:** The research is proposing a new, methodical paradigm, which will be confined to the realities and constraints of IoT settings. This would enhance the preparation in digital forensics, integrity of evidence collection and standardisation of investigations.
- **Cybersecurity Practice:** The framework aids proactive management of risks and their recovery through categorisation, aligning the vulnerabilities with the forensic procedure in consumer devices.
- **User Education and Awareness:** These will be recommended based on the findings of the user perception survey on the means to enhance forensic readiness at the user level, such as secure placement of devices and backing up of data.
- **Policy and Standards:** The framework will guide the regulatory bodies and manufacturers on the best practices to put in place forensics-ready IoTs.
- **Academic Importance:** The study is an original empirical and theoretical underpinning of cybersecurity, digital forensics, and consumer IoT devices, which, thus far, have been of little scholarly interest.

1.6 Dissertation Structure Overview

The study is organised into the following chapters:

- **Chapter 1: Introduction** - Describes the background of the research, problem statement, aims, objectives, research question and the significance of the study.
- **Chapter 2: Literature Review** - a detailed exposition of what is happening in the field of IoT security and major research gaps and contributions.

- **Chapter 3: Methodology** - Describes the research design and how the researcher employs a systematic review, qualitative content analysis, and framework development strategy to answer the study's core research question.
- **Chapter 4: Findings** - Provides the outcomes of the conducted systematic literature review, user survey, and the evaluation of the proposed forensic methodology.
- **Chapter 5: Discussion** - Sets the stage for understanding the results of the study, evaluates the correctness of the suggested framework and addresses theoretical as well as practical implications.
- **Chapter 6: Conclusion and Recommendations** - Summarises the conclusions of the study and recommends future work and future policy guidelines.
- **References and Appendices** - Works out all the bibliographic references in APA 7th edition, along with supporting records, such as the IoT user survey.

Chapter 2: Literature Review

2.1 Introduction

The proliferation of IoT devices has transformed how individuals interact with digital systems in their everyday lives. However, this volatile increase also brings with it some serious security and forensics problems that need to be effectively addressed. The complexity surrounding the collation, storage and investigation of digital evidence poses a great deal of challenges, as it would in the traditional computing environment through the introduction of the IoT ecosystem into households, offices and other common places. The objective of this literature review is to point out the available academic, technical and policy-related relevant literature around the vulnerabilities of consumer IoT devices and the methodological weaknesses of the currently available forensic frameworks.

The chapter is structured around key thematic areas: IoT device vulnerabilities, digital forensic challenges specific to IoT, forensic readiness and best practices, user behaviour and its implications, and recent advances such as blockchain and artificial intelligence (AI) in digital forensics. Using such an approach helps to conceptually underpin the development of a forensic analysis framework that is subsequently presented in this dissertation.

2.2 IoT Vulnerabilities: Scope and Classification

The IoT ecosystem has a large number of security holes permeating through its entire stack. Security is one of the issues that is considered last by the manufacturer during the design and development of products because of the urgency inherent in the introduction of products into the market and keeping prices as low as possible (Bertino, 2020; Atlam et al., 2020; Ahmad et al., 2023). An outcome of such a trade-off is a generation of poor systems and devices, which are not resilient to the changing cyber threats. IoT vulnerabilities are typically segregated into three main categories encompassing the software level or application level, communication security level, network topology, as well as the hardware and firmware sectors.

2.2.1 Hardware and Firmware Vulnerabilities

Most of the IoT devices lack the required resources to perform advanced encryption, access control, and provide real-time status of the devices, which are the characteristics of a secure system (Conti et al., 2018; Deng et al., 2023). In addition, devices are more likely to be shipped with hardcoded credentials, accessible serial ports, and visible Joint Test Action Group (JTAG) or Universal Asynchronous Receiver-Transmitter (UART) connections that allow anything to be physically attacked and reverse-engineered (Acar et al., 2022).

The firmware vulnerabilities are especially perilous: they often persist regardless of a reboot or an update to the firmware. Such weakness can be exploited by attackers via the installation of rootkits or unauthorised access to the operating system level. The study conducted by Wang et al. (2021) revealed that over 50 per cent of the firmware images being analysed contained missing or outdated open-source components, with no update mechanism being present most of the time. It means that most IoT-making companies do not have secure software development life cycles (SDLCs)/software bill of materials (SBOMs) to monitor and inspect third-party dependencies (Morales et al., 2022).

The truth about the insecurity of embedded devices, however, was found to be a very bitter experience as the latest invasion of consumer routers or IP cameras has shown. As an illustration, Mirai and Mozi botnets have targeted the default logins and unpatched firmware to attack millions of gadgets in Distributed Denial of Service (DDoS) attacks (Sang et al., 2022). This encourages secure boots and firmware signing as one of the minimum defence requirements.

2.2.2 Communication and Network-Level Weaknesses

A lot of IoT communication protocols were developed to be efficient and to support low power transfer rather than be highly secure (Santos et al., 2019; Hamza et al., 2022). Message Queuing Telemetry Transport (MQTT), Constrained Application Protocol (CoAP) are also lightweight and have no built-in security unless the developers add it specifically. Messages in MQTT are plaintext by default and can be eavesdropped and replayed unless they are secured over

Transport Layer Security (TLS), which is typically missing because of hardware constraints on devices (Yaqoob et al., 2021).

One of the basic problems lies in the fact that the implementation of IoT networks is not often fragmented into different layers. Many devices are deployed on flat networks and are not subject to Virtual Local Area Network (VLAN) isolation, ensuring that once a single device is hacked, an attacker is able to navigate laterally to exploit other connected devices. This kind of lateral movement, which exploits the use of poorly secured smart lighting or Heating, Ventilation, and Air Conditioning (HVAC) systems, has already been recorded in a range of penetration testing demonstrations within enterprise security settings. It shows its capability of gaining an initial point of access into the networks of enterprise business (Alrawais et al., 2022).

Most IoT networks are susceptible to old and new vectors of IoT attacks regardless of inadequate dynamic IP filtering, lack of anomaly-based intrusion detection, or zero-trust in architecture. The absence of the integration of useful network monitoring and micro-segmentation will also make organisations vulnerable to multi-vector cyber threats because of these vulnerabilities.

2.2.3 Software and Application-Level Risks

The main cause of software vulnerability in IoT systems is poor coding and poor testing. The most common problems entail weak Application Programming Interfaces (APIs), absence of input sanitisation, lack of session management and poor authentication. The Top 10 IoT vulnerabilities (2022) provided by the Open World Wide Application Security Project (OWASP) state that APIs are regularly exposed with excessive rather than permissive access or no authentication, which allows unauthorised access to data and manipulation control.

In a recent study by Alshehri et al. (2023), more than 40 % of smart home applications did not apply simple security measures like storing credentials in an encrypted form or enabling session expiration on connected devices. Role-based access controls are not deployed in most interfaces, which makes them prone to privilege escalation and brute-force attacks (Zulkipli et al., 2018; Elmisery et al., 2023).

Moreover, the issue of increased concern about over-the-air (OTA) updates is on the rise. Although OTA brings ease of use, a malfunctioned implementation can also be used to send a malicious firmware or defeat integrity checks (Giaretta et al., 2022). It is common knowledge that developers tend to disregard the vulnerabilities of third-party libraries, and even a patched basic firmware on a device does not make it powerful enough to withstand advanced cyber-attacks.

Forensically, the described vulnerabilities also complicate post-incident investigation, as little logging and traceability are possible, and it is hard to attribute the identified vulnerability to potential actors, assess its impact, and mitigate it (Derdour et al., 2023).

Table 2: Summary of IoT Vulnerabilities by Layer

Layer	Example Vulnerabilities	Forensic Implication
Device	Hardcoded credentials, unprotected ports	Direct device access by an attacker
Firmware	Unsigned updates, outdated libraries	Tampered firmware logs
Network	Insecure protocols (e.g., MQTT), open ports	Man-in-the-middle attacks
Application	Weak authentication, exposed APIs	Credential leaks, log evasion

2.3 Forensic Challenges Unique to IoT

IoT forensics is not like other digital forensics due to the distributed, ephemeral and heterogeneous nature of IoT environments, which brings some unique challenges to scale. Unlike

in traditional systems, such as computers or mobile phones, where data may be fragmented, imaged and archived in a somewhat controlled environment, IoT systems are a network of low-resource devices, cloud, and edge nodes, and may frequently be real-time systems with little data retention and agency. All these features complicate evidence gathering, storage and analysis to a considerable degree (Perumal et al., 2015; Ullah et al., 2022).

2.3.1 Volatile and Distributed Evidence

The data on IoT devices dissipates and, therefore, presents a huge challenge to forensics. A significant part of the data is either held on volatile memory (e.g., Random Access Memory (RAM)) or is sent directly to distant cloud servers without passing through local storage. It is also volatile in the sense that any hitch in triggering the forensic processes may lead to the complete loss of vital information (Casey et al., 2020). To give an example, smart thermometers or wearable health-fitness devices can measure necessary information and store it briefly, but then delete it due to limited space.

This vulnerability of such information is the weakness in a chain of custody, which will be the most important aspect in making evidence. The authenticity and completeness of data are also doubtful due to a lack of standardised practices of logging within IoT environments. Event correlation between systems is challenging since forensic investigators could be dealing with incomplete, timestamp-disordered, or fragmented logs (Almalki et al., 2021). Also, timestamping schemes typically depend on largely asynchronised clocks on the devices (Sefidian et al., 2023).

2.3.2 Device Heterogeneity

The issue of the wide variety of hardware architectures, firmware releases, communications protocols and storage formats provides an insurmountable challenge to IoT forensic preparedness. The idea of Forensics-Aware IoT (FAIoT) was first introduced by Zawoad and Hasan (2015), whereby they required a transition toward proactive development of forensics as

opposed to reactive forensics. Yet, the adoption is low because manufacturers are not willing to trade performance or cost-efficiency in favour of forensic support (Sicari et al., 2021).

Moreover, IoT systems lack a framework for data acquisition. Reverse-engineering of the technology to determine the proprietary file systems or firmware architectures takes time, an aspect that investigators in many incidents have little to no choice, due to the nature of its legal complications. Because of this, Singh et al. (2022) point out that even identical (or at least, similar; e.g., two smart doorbells of different brands) may have completely different representations and formats of stored and transferred data, thus requiring a unique specific tool and/or technique.

Such diversity also restricts the use of current forensic tools, which mostly use commonly known operating systems (e.g. Windows, Linux, Android). They frequently fall short of recording and decoding important forensic artefacts through available toolkits, which lack support for lightweight or real-time operating systems, such as FreeRTOS or Zephyr, typical in IoT (Lopes et al., 2022).

2.3.3 Cloud and Legal Barriers

An essential component of IoT devices is cloud infrastructure since it stores data, processes information, and analyses the data. Where this is both scalable and manageable remotely, a complex jurisdiction and legal framework of forensic investigation are formed. Data can be located in several physical locations, each under different effective legal regimes, making access, admissibility, and compliance all more complex (Servida & Casey, 2019; Alenezi et al., 2023).

Forensic investigators have a high impediment in accessing logs or metadata when they attempt to access data from a cloud service provider. Access is usually slow, sensitive information is censored, or the refusal to cooperate altogether due to customer privacy or the lack of legal demands is also possible on the part of vendors. There is the possibility of corrupting forensic soundness even when they have been permitted access because there is no transparency concerning data manipulation and replication processes in the cloud (Taheri et al., 2022).

In addition, foreign privacy regulations, like the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA), are extremely restrictive about accessing, retaining, and transferring information, and this is particularly hard to deal with when it comes to gathering evidence across borders. To take one possible example, some of the data may be deleted even before an investigation starts under the principle of data minimisation enshrined in GDPR, data subject rights (such as the right to erasure) may be inconsistent with evidence preservation obligations (Koops & Leenes, 2020). These ambiguities on legal grounds can render the evidence collected inadmissible in a court of law or unusable by the prosecutors.

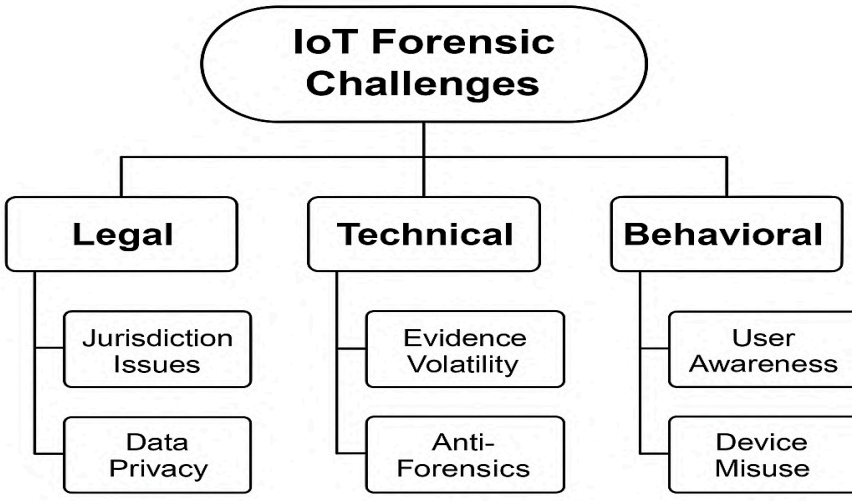

Figure 1: IoT Forensic Challenges Overview

2.4 Forensic Readiness and Best Practices

Forensic readiness refers to a proactive set of procedures, tools, and policies in such a way that, in case of a security breach, digital evidence could be collected, preserved and analysed efficiently. As opposed to reactive forensics, proactive forensics prioritises readiness, lower investigation cost, legal admissibility, and minimally disruptive operations (Ruan et al., 2021).

The peculiarities of the devices, considering IoT, should be considered in the framework of forensic readiness.

According to a Special Publication 800-213 of the National Institute of Standards and Technology (NIST), the pillars of IoT forensic readiness include secure and persistent logging, remote acquisition mechanisms, real-time alerting, and system recovery capabilities (NIST, 2021). This model lays emphasis on the development of the forensic capability into the lifecycle of IoT systems, such as systems design, operation and decommissioning.

On the same note, the European Union Agency of Cybersecurity (ENISA, 2020) has also mentioned forensic readiness as one of the strategic goals in IoT security. It includes such practical tips as:

- **Secure boot and firmware validation:** Ensures the integrity of the system from power-on and prevents tampering with system software.

- **Tamper-evident, timestamped logs:** Maintains non-repudiation and temporal correlation of events, vital for incident reconstruction.

- **Remote control interfaces:** Allow investigators or administrators to isolate compromised devices, extract volatile evidence, or trigger real-time incident responses.

However, despite these recommendations, they are not widely adopted by commercial IoT devices. Even basic logging facilities or the ability to record logs for only short periods are altogether lacking in consumer-grade machines in virtually all cases. Because a range of concerns competes against the willingness to incorporate strong forensic capabilities, vendors tend to avoid it (Bertino, 2020; Almutairi et al., 2022), but a variety of concerns competing with the desire to incorporate strong forensic capabilities can explain this behaviour of vendors (Bertino, 2020; Almutairi et al., 2022).

Moreover, the privacy-forensics trade-off is also coming to mind nowadays. To be prepared to log user actions and other patterns of behaviour, even for forensic purposes, may violate the data

protection principle that includes data minimisation under GDPR (Koops & Leenes, 2020). This confrontation puts the manufacturers in a dilemma of whether to take a chance of non-conformance with the forensic standards or to take a risk of violating the rights of the user.

Privacy-preserving forensic architectures have recently been suggested that emphasise collecting only metadata or anonymised logs except under a trigger condition (e.g., anomaly detection), in which case, evidence should be more deeply captured (Alenezi et al., 2023). Also, other new standards promote modular forensic preparedness, under which lightweight logging is handled by edge nodes, whereas more forensically worthy storage is available on companion apps or in cloud infrastructure (Khan et al., 2023).

The fact that the practical forensic preparedness of IoT environments must be technically plausible and legally sustainable is not only convenient but necessary (or, at least, authoritative).

2.5 Security Challenges in Consumer IoT Environments

Consumer IoT ecosystems are characterised by heterogeneity of devices, fragmentation of protocols and inadequate implementation of security measures. Most smart locks, cameras, appliances, and wearables tend to be delivered with little security, e.g., hardcoded credentials or outdated firmware and insecure connection-based communication protocols (Atlam, Walters, & Wills, 2020). This indicates a systemic problem of failure to implement the security-by-design principle due to market pressures (cost and decreased time-to-market introduction) placed on long-term resilience (Alrawais et al., 2021).

Insecure default settings, poor authentication, and physical hardening are some of the listed vulnerabilities by the OWASP IoT Top 10 (2022) that directly impact the forensic processes. Forensic investigators find it difficult to build the events or to prove the integrity of the data in instances in which there are no formal audit tracks and logging programs.

Stoyanova et al. (2020) suggest a layered vulnerability model that classifies the risks into the following layers: perception, network, and application. The latter classification is particularly desirable for forensic evaluation, as all stages must be tackled in distinctive ways regarding the

piece of evidence and substantiation. As an example, the tampering of the perception layer (e.g., manipulation of the sensors) needs a physical analysis, the attacks on the network layer (e.g., spoofing) would need the analysis of the packets, and attacks on the application layer (e.g., compromising an API) would need to consider APIs to be logged securely. Such stratified variations will direct the forensic readiness model that will be presented in this research.

2.6 Limitations of Current Forensic Techniques for IoT

The classical digital forensic techniques will not work with IoT. The methods of disk imaging, timeline inference, and memory forensics presuppose the presence of centralised storage and a unified file system, which is unlikely to be encountered in IoT (Conti et al., 2018). Instead, they encounter decentralised logs, proprietary firmware and data flows based on the cloud.

Critical logs can either be stored on volatile memory, lost after power-down or on cloud storage with encrypted information that requires vendor assistance to access (Perumal et al., 2015). In addition, some devices cannot run the forensic agent or integrity check due to a lack of computational performance and have to face constant threats with no ability to retrieve any trace of digital evidence in case of unauthorised access (Sefidian et al., 2023).

Another problem is its admissibility in law. Servida and Casey (2019) emphasise that there are no standard procedures related to the acquisition of IoT evidence, which causes a violation of the chain-of-custody and auditability. Genuine evidence can be taken as inadmissible in the court of law, unless there are validated tools and repeatable processes. The like constraints necessitate building of strict new forensic systems that are specific to IoT, which would be both technically possible and legally defensible.

2.7 Forensic Readiness and Standardisation Efforts

The necessity of forensic-ready IoT devices has already been understood by many organisations. Both NIST SP 800-213 (2021) and ENISA (2020) support the integration of forensic support into the architecture of the devices. It is advisable to have secure boot processes, tamper evidence, remote acquisition interfaces and access control models.

These standards, though critical, have not been applied consistently. According to Watson and Dehghantanha (2016), a major fundamental problem is that customers are not motivated, especially in cases of low-budget consumer markets, to make their vendors take security aspects seriously and invest in the costly task of applying it. One has to run into the issue of interoperability, too. Depending on the adoption of the standards, even in the cases of adherence, the implementation may be fragmented, and the portability of evidence can be minimised (Almutairi et al., 2022).

The result of some of the efforts carried out in this work is the availability of one forensic system that can work without any relation to the device architecture as well as the implantation peculiarities of the vendor, which will ensure functional as well as forensic viability of the same wide-range IoT ecosystems.

2.8 The Role of Cyber-Physical Systems Security (CPSS) Framework

Cyber-Physical Systems Security (CPSS) framework, which has been suggested by Sun et al. (2018), provides a comprehensive process of securing and analysing IoT ecosystems. It regards the system as a combination of a digital computation, physical processes and human actors. The integration may be crucial in the case of forensics when the sequence may be found within a software log, sensors and user activity.

The CPSS framework provides cross-modal analysis with the ability of the forensic examiner to compare the events in different modalities. It is worth mentioning that it renders the user a

dynamic factor by being a source of threat through misconfiguration or as an important part of a chain of evidence. Zawoad and Hasan (2015) also focus on the prominence of user-centred forensic intelligence, reasoning that forensic systems should be built to consider human error, including resetting the system or turning off the logging, which will unintentionally destroy the evidence.

In this study, the proposed forensic model is based on the CPSS framework, but the behavioural context would be linked to the technical artefacts to make the investigation more profound and accurate.

2.9 Behavioural and Human Factors in IoT Forensics

In spite of the fact that IoT forensics is a discipline that presupposes technological proficiency, the behaviour of users and their system recklessness will be the ticket to evidence retention and system protection. According to Bertino (2020) and Tawalbeh et al. (2020), most users do not select the option to update firmware, default credentials, or logging options, which are actions resulting in direct effects on the forensic preparedness of a system.

Also, when devices fail, the user may end up deleting some important evidence in the process of carrying out factory resets or deleting data on apps. Servida and Casey (2019) promote the inclusion of the elements of digital literacy in forensic readiness strategies. This will involve training users on the optimal ways of maintaining evidence as well as the hygiene of the devices.

It is against this background that this study integrates these suggestions by coming up with a dual-track readiness model, a model that is proposed to be embraced by both technical stakeholders (e.g., manufacturers, investigators) and end-users. The framework will also provide procedural guidelines that will help consumers keep their devices in a forensically sound state.

2.10 Comparative Analysis of Existing Forensic Frameworks

Even though several IoT forensic models have been proposed, they are still too broad or highly specific to a specific device. The famous models are represented by:

- **FAIoT (Zawoad & Hasan, 2015):** Presents forensic principles on the designing stage, but not on the operating stage.
- **Top-Down IoT Forensic Model (Perumal et al., 2015):** The evidence architecture gives precedence to OSI layers; however, it makes the assumption that a similar architecture is expected, which has never been observed in practice.
- **IoTDOTS (Rahman et al., 2018):** Provides a logging framework on smart homes, but its user compliance and ecosystem dependency make it hard to scale.

What is of more importance is that in these models, user behaviour is not considered, and only a couple consider legal interoperability among data protection regimes. This study will overcome such deficiencies by proposing a modular, integrated and law-based user-centred and flexible framework.

2.11 Advanced Approaches: Blockchain and AI in Forensic Processes

Some of the emergent technologies that are increasingly finding applications to solve IoT forensic challenges include blockchain and AI. Alenezi and Wills (2021) suggest the application of blockchain to a tamper-resistant, time-stamped log, which provides non-repudiation and traceability; the prerequisite that must be met to allow legal admissibility.

On the AI side, the light machine learning algorithms may identify the anomalies of the behaviour and automatically activate the evidence-gathering procedures (Tawalbeh et al., 2020). This would resolve the concern of transient information, as it would provide the storage of evidence in its first appearance.

It does not, however, come without disadvantages. Most IoT devices have low energy and computing resources and hence cannot implement complicated cryptographic or analytics schemes (Yaqoob et al., 2021). The proposed study, therefore, suggests the adoption of a modular integration process in which blockchain or AI modules are offloaded to the edge devices or gateway.

2.12 Identified Research Gaps

One can single out several gaps in the literature reviewed:

- The lack of integrated forensic systems/methods which integrate vulnerability classification, forensic preparedness, behavioural techniques and law.
- The forensic models popular today tend not to be interchangeable between the categories of devices due to hard-coded assumptions or limitations in the infrastructure.
- The properties of human behaviour and human error are not widely embraced in forensic design, yet they have a huge influence on evidence integrity.
- The absence of validation on real-world case studies is also conspicuous, hence decreasing the validity of the proposed theoretical definitions.

The identified gaps are addressed in the current research, which outlines and assesses a user-friendly, legally-informed, and architecture-agnostic forensics framework which can be validated in a consumer IoT case study.

Chapter 3: Methodology

3.1 Introduction

This chapter outlines the research design and methodological approach used to address the study's research question, which is:

Research Question: How can a standardised forensic analysis framework improve evidence collection and vulnerability detection in consumer IoT devices?

In order to answer this question in-depth, a mixed-methods research design was embraced. This was conducted on two major fronts: first, with a systematic literature review to locate and synthesise available forensic techniques and IoT vulnerabilities, and second, a quantitative survey to obtain primary data on user actions, awareness, and attitude towards forensic preparedness in IoT contexts.

3.2 Research Design

The study employs the Design Science Research (DSR) approach (Hevner et al., 2004; Peffers et al., 2007). DSR is appropriate to construct a viable framework, and it is planned in the following stages:

- Problem Identification
- Knowledge Acquisition using Systematic Review
- The Survey of User Contextual Insight
- Development of Artefact (Framework)
- Guidance-based validation and why real-world Use Cases are valuable

The topics discussed with the selected methodology are cyclic and evidence-based as they study intricate real-life issues such as forensic preparedness in consumer IoT devices.

Table 3: Method Selection Justification

Method	Justification
Systematic Review	To gather peer-reviewed insights on IoT forensics
User Survey	To understand real-world practices and gaps

3.3 Systematic Literature Review

3.3.1 Objectives

The systematic literature review was used in order to give an empirical basis regarding the categorisation of IoT vulnerabilities and the analysis of current forensic methods. This constitutes the background knowledge of the development of the framework.

3.3.2 Search Strategy and Databases

The PRISMA 2020 literature review guidelines were used (Page et al., 2021). The academic and technical databases that were searched are:

- IEEE Xplore
- Digital Library ACM
- ScienceDirect
- Google Scholar
- Repositories of ENISA and NIST

The keywords used included: IoT forensics, IoT vulnerabilities, forensic readiness, smart home security, digital forensic frameworks, vulnerability detection, legal compliance, etc.

3.3.3 Inclusion and Exclusion Criteria

Inclusion Criteria

The inclusion criteria were very elaborate in ensuring that all the sources that were selected were precisely in tandem with the scope and objectives of the present research. First, it was restricted to peer-reviewed journal articles and conference proceedings, technical reports and cybersecurity standards. This criterion made sure that the evidence was developed in regard to credible and verified sources and which is in line with the best practices in evidence-based research (Page et al., 2021).

Second, due to the time limitation, the review was limited to the literature published between 2015 and 2025. The rationale behind this approach is explained by the recent development of IoT technologies and the increasing interest of scholars in the field of digital forensics and security in the IoT realm (Yaqoob et al., 2019; Stoyanova et al., 2020). Because consumer electronics are changing quite rapidly, it is possible that older writings have not covered the existing weaknesses as well as the architectural paradigms and the forensic challenges that the present-day devices possess.

Third, it only captured literature that covered one or more of the following topics: (a) Forensic readiness in an IoT environment, (b) digital forensic methods and problems, (c) the vulnerabilities of consumer IoT devices, and (d) overall threats to cybersecurity in IoT implementations. Such topical orientation implied that selected pieces of work were directly applicable in the development of a forensic analysis framework of consumer IoT.

Finally, there was a preference for articles which discussed consumer-oriented IoT devices, e.g., smart home assistants, wearables, and personal health monitors, rather than industrial or enterprise systems. Such a distinction was necessary since the consumer hardware is unique in its limitations, including limited processing capabilities, low forensic awareness, and irregular user

behaviour, which cannot be compared to enterprise or critical infrastructure IoT systems (Bertino, 2020; Tawalbeh et al., 2020).

Exclusion Criteria

There were criteria of exclusion in order to have clarity, concentration, and academic integrity. First, the papers that deal only with any of the following: Industrial IoT (IIoT), smart manufacturing, and the creation of large-scale infrastructure systems were omitted. Though the same can be said about the forensic problems in these environments, they are significantly different in architecture, data handling, and legal control in comparison with consumer systems (Servida & Casey, 2019).

Second, the review did not take into consideration non-English publications. This was done so that there could be consistency in words and avoid the potential misinterpretation due to translation. Although this may induce bias in language selection, it can increase the reliability and accessibility of the interpretation and the process of analysis of the findings.

Third, papers that lacked an empirical foundation or a clear methodology were excluded. These included playbooks, abstract papers without application to reality and white papers written by vendors and not reviewed by peers. This was rationalised to focus on evidence-based results and research that help inform the scholarly debate with well-defined methods, data repositories, and approaches to analysis (Page et al., 2021; Perumal et al., 2015).

Application of the exclusion criteria assisted the review to discard information that would dilute the quality of analysis or would be out of scope regarding the focus on consumer IoT forensic preparedness. The process of systematic filtering was additionally backed by the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) framework, which offers guidelines for reporting transparent and reproducible literature reviews (Page et al., 2021).

3.3.4 Selection Process

After screening the titles and abstracts of papers, samples were selected, consisting of 58 articles out of the original sample of 143. The final 32 articles were selected to be studied in detail after a full-text search to define the themes based on relevance, methodological quality, and applicability of the papers to forensic analysis of consumer IoT.

3.3.5 Data Extraction and Analysis

To provide grouping and coding of the findings, a data extraction matrix was developed to code findings under the following categories:

- Categories of the IoT devices (e.g smart locks, cameras)
- Type of vulnerability (e.g. authentication, encryption, firmware)
- Forensic method (e.g. cloud, photo journey)
- Obstacles (e.g. data volatility, legal barriers)

This coding guides the framework's development in terms of the classification of vulnerability types.

3.4 User Survey Method

3.4.1 Purpose

The survey was aimed at obtaining empirical data about user practices, awareness, and challenges in the area of securing IoT devices. The survey attempts to complement the systematic literature review to answer the main research question of this study.

3.4.2 Survey Instrument Design

A structured questionnaire was created in order to investigate user behaviour, awareness and practices concerning the security and forensic preparedness of IoT devices. The questionnaire had 17 closed-ended and Likert-type questions that were categorised into five themes. This framework allowed the obtaining of quantitative data and preserving the conceptual consistency with the research goals.

3.4.2.1 Device Ownership and Usage

The initial part of the questionnaire was based on the types of IoT devices the respondents use, how often they use them, and the common use case scenarios. This gave a background understanding of the IoT environment surrounding user behaviour and attitudes. The insight into the ownership patterns also facilitated the selection of high-risk categories of devices and contributed to the shaping of the proposed forensic framework's applicability.

3.4.2.2 Security Behaviour

The second part involved the discussion of security practices of the respondents, including how regularly they would change default passwords, install firmware updates, and whether they applied two-factor authentication. The questions were very crucial in determining the practical usage of basic security hygiene, which closely affects forensic readiness and evidence integrity (Watson & Dehghantanha, 2016; Bertino, 2020).

3.4.2.3 Network Protection Methods

The third section focused more on firewalls, isolation of guest networks and intrusion detection at the network level of security controls. Because numerous IoT attacks appear or pass through

local networks, user-level network defence is closely associated with the capacity to identify, log and save electronic forensic clues (Conti et al., 2018).

3.4.2.4 Attitudes Toward Forensic Readiness and Responsibility

The fourth area assessed the level of exposure of users to the concepts of forensics and their tendencies to react to any events. The questions asked whether the respondents were aware of the actions that they should take following a security event (e.g. retention of logs or isolation of devices) and whether they felt users should bear some of the responsibility of evidence collection. This behavioural understanding was important in setting out a framework that will incorporate user education and involvement (Zawoad & Hasan, 2015; Tawalbeh et al., 2020).

3.4.2.5 Demographics and Cybersecurity Literacy

The closing section of the questionnaire gathered demographics data (e.g. age, educational degree) as well as the assessment of personal levels of digital literacy and familiarity with cybersecurity practices and courses. This allowed cross-tabulation of security behaviours and user profiles, and what the trends among end-users are. E.g. Do younger users tend towards forensic-friendly habits, or does digital literacy bring higher security on the devices?

3.4.3 Theoretical Basis

The theoretical implications of the questionnaire developed are based on the CPSS framework (Sun et al., 2018), which stresses the correlation of physical devices, cyber infrastructure and human users. Also, the studies that were conducted previously on both IoT user practices and digital forensic preparedness presented the relevance and validity of the design (Stoyanova et al., 2020; Yaqoob et al., 2019). Such a theoretical foundation ensured the survey was able to capture both the behavioural and technical domains of forensic readiness.

3.4.4 Sampling and Distribution

The questionnaire was created using Google Forms and sent out to participants on educational websites, internet discussion forums, and professional communities. Participation was voluntary and anonymous. Convenience sampling ensured a diverse range of user experiences.

3.4.5 Ethical Considerations

All participants signed an informed consent form. No personal identification data was collected, and the information gathered was kept safe and used only for this study. Ethical approval of the survey was done informally and according to the standard research ethical practices.

3.5 Justification for Using a Mixed-Method Approach

This study utilises a mixed-method study design that entails a systematic review of literature and a quantitative survey. This integration is motivated by the fact that the concept of forensic readiness in consumer IoT settings is quite multidimensional in nature. Effective digital forensics in such contexts requires an understanding of both technical factors (e.g., vulnerabilities, standards, forensic models) and human behaviours (e.g., user practices, awareness, and attitudes toward digital security). This approach allows for the design of a more holistic and practicable framework by synthesising knowledge in each sector.

By utilising literature on scholarly articles, standards on cybersecurity, and already established forensic paradigms, the review deduces appropriate current best practices, prevailing IoT vulnerabilities, estimation shortcomings, and developing tools. This process ensures that the proposed framework is grounded in validated knowledge and aligns with state-of-the-art research in cybersecurity and digital forensics (Page et al., 2021; Stoyanova et al., 2020). Also, this facilitates the credibility and replicability of the review in the sense that the review is facilitated through systematic and objective inclusion and exclusion criteria as stipulated by PRISMA.

To the same effect, the quantitative survey study is designed to record data on the actual user behaviour, security measures, and the degree of forensic preparedness. This data is crucial because much of the forensic viability of IoT devices depends not only on technical design, but also on how users configure, maintain, and interact with these systems (Tawalbeh et al., 2020; Watson & Dehghantanha, 2016).

In this case, a mixed-methods approach can help in triangulation since the findings obtained during the literature review and the survey can be used to confirm and complement one another. Triangulation enhances the validity of findings and alleviates the limits of biases caused by the application of only one method (Creswell & Plano Clark, 2018). To provide an example, the literature may provide an insight into the importance of safe logging and verification of firmware, whereas the survey findings would represent the fact that most users either do not know or are not observant enough to incorporate the practices into their routine.

On top of that, a combination of de facto qualitative and quantitative interpretations integrates the DSR approach to the creation of the forensic framework. DSR focuses on the theory-based, yet similarly practice-relevant artefact development in an iterative manner (Hevner et al., 2004; Peffers et al., 2007).

Chapter 4: Findings

4.1 Introduction

The chapter highlights and provides insight into the results presented by two mutually complementary sources of data: a systematic literature review and an organised quantitative survey. These results form the basis of the proposed forensic analysis framework, and they are organised based on themes that represent the overarching interest of this research: the vulnerability of consumer IoT devices, limitations of forensic approaches, preparedness, as well as the awareness of the end users. The results provide important lessons on the intersection of the technical issues and behavioural tendencies that contribute to the nature of the current forensic preparedness in the IoT ecosystem.

4.2 Insights from the Systematic Literature Review

Using the literature review performed following the PRISMA 2020 recommendations, this study made it possible to harmonise 32 publications: peer-reviewed journal articles, technical standards, and papers that were presented at conferences. It also revealed a few recurrent themes, the overall understanding of what a hodgepodge of consumer IoT security practices is.

4.2.1 Categories of Vulnerabilities

Many studies focused on the ongoing existence of serious vulnerabilities in consumer IoT devices. Both Conti et al. (2018) and Yaqoob et al. (2019) highlighted that vulnerabilities associated with authentication, especially the use of default credentials (unaltered or hardcoded), are highly popular. These problems are not mere remnants of omissions, but are designed in a way that neglects the security of onboarding processes and places the focus on low costs and users' convenience. Devices may be characterised by the absence of multi-factor authentication,

a low level of encryption, or the use of plaintext transmission of data over unsafe types of communication protocols (Hyper Text Transfer Protocol, MQTT, etc.).

The other theme was firmware vulnerabilities. A large number of devices lack support for over-the-air updates (OTA), or perform them in a non-encrypted and non-digitally signed way and can therefore be attacked using the supply chain or by abusing firmware-upgrading mechanisms. The risk is further exacerbated by the fact that such update mechanisms, upon their availability, are hardly ever used by the end-users.

Network-level vulnerabilities were no less widespread. The gadgets used do not provide encrypted communication, and therefore, they are prone to man-in-the-middle attacks. Additionally, consumer environments do not have network-level segmentation, which implies that a compromised device can serve as the foothold to lateral movement throughout the local network.

4.2.2 Forensic Limitations in Existing Methodologies

The conventional digital forensic tools do not work in most cases with IoT environments. Multiple sources, such as in a study by Watson and Dehghantanha (2016), pointed out that the ephemeral nature of IoT data, which is commonly stored in volatile memory or transferred to cloud services, poses considerable problems to the preservation of evidence. Also, the variation of devices and exclusive software platforms is another problem that complicates the creation of universal forensics instruments.

The other major conclusion is the reactive trend of the majority of forensic studies in the IoT scenario. Zawoad and Hasan (2015) condemned the current gears of post-incident investigation, stating the necessity of proactive forensic readiness efforts. Not many devices work with tamper-evident logging or safe event records; thus, in retrospectives, research might be impossible or challenging.

Jurisdictional and legal issues also became a burning concern. Servida and Casey (2019) highlighted the lawful ambiguity induced by cross-border data storage and, to a greater extent,

given the cloud-based IoT landscape. The issue of data ownership and controlling access to a device also interferes with forensic processes, particularly where multiple individuals share access to a device or smart-home system.

Such findings emphasise that a unified framework is necessary in that both technical restrictions and contextual realities need to be addressed, namely, user behaviour and jurisdictional restrictions.

4.3 Findings from the User Survey

The user survey yielded a total of 102 responses from individuals across diverse age segments, professional backgrounds, and educational qualifications. These responses provide essential insights into user behaviour and awareness levels that are potentially significant for forensic readiness in consumer IoT environments. The following section analyses the key demographic variables captured in the survey and contextualises their implications.

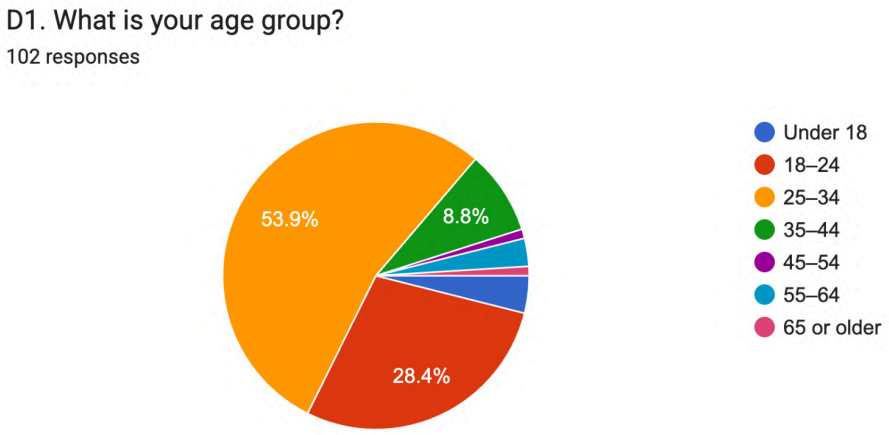

Figure D1: Age Distribution of Respondents

Most of the respondents (53.9%) are aged 25-34 years, as indicated in Figure D1, and 28.4 percent of the respondents are aged between 18-24 years. All these two groups together represent

more than 82 percent of the total sample, meaning that the base of participants is mainly young and Internet-savvy individuals. Another age group is between 35 and 44 years, which constituted 8.8 percent, and the rest, who are less than 18, between 45 and 54, between 55 and 64, and 65 years and older, constituted a small proportion of the responses.

Such age distribution indicates that most of the survey respondents are early-career professionals and students, as these groups are frequently very interested in the field of technology and digital services. Considering the fact that, in the context of consumer IoT, forensic readiness is directly related to the interaction with digital devices and platforms by users, the participation of younger representatives makes it particularly profitable, providing an insight into behavioural trends. The low ratio regarding older age groups, however, might be an indication of a shortcoming of intergenerational adoption or awareness of forensic best practices, which may be addressed in future outreach or policy making.

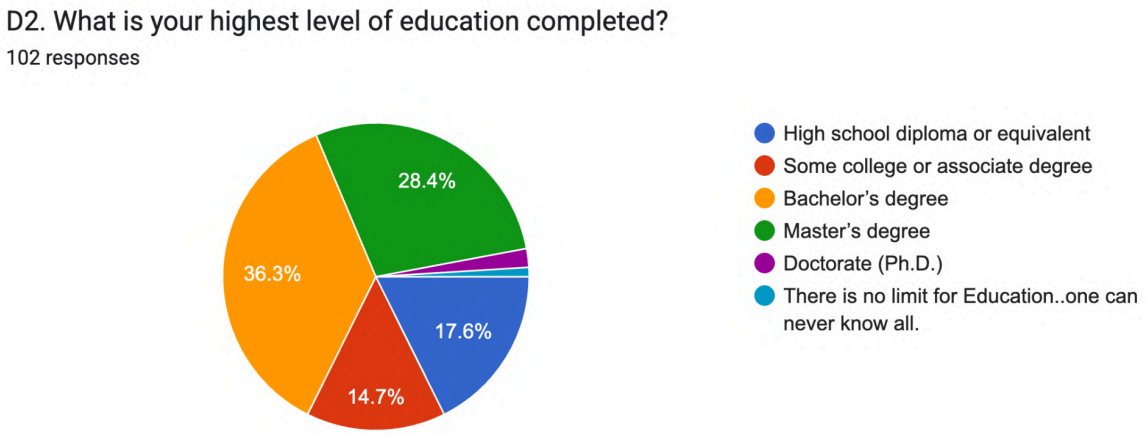

Figure D2: Educational Background of Respondents

Educational attainment of the respondents is shown in Figure D2. A large number (36.3%) of them reported having had some college education or an associate degree, and 28.4% had obtained a master. The percentage of members of the sample representing high school diploma holders and those with a bachelor's degree was 17.6% and 14.7%, respectively. A small group of them had a doctoral degree or other qualifications in the field of education.

The data shows a good education level among the survey participants, with the majority having undergone one form of post-graduate education or the other. This demographic parameter is especially expedient when interpreting the cognisance of digital security and forensic concepts among users. One can infer that the respondents have the mental ability to comprehend the main concepts involved in data protection and forensic traceability. Nonetheless, as discussed in sections below, the existence of a high formal level of education does not always translate into regular application of secure or forensic-conscious practices, thus highlighting the long gap between cognition and practice.

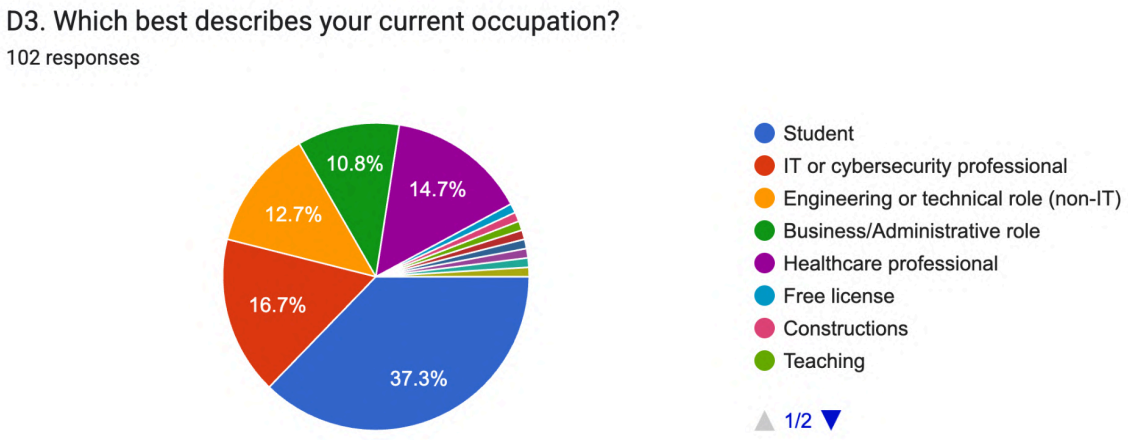

Figure D3: Occupational Background of Respondents

The most significant proportion of respondents are students (37.3%), as seen in Figure D3, followed by professionals who hold jobs in the IT or cybersecurity sector (16.7%). The engineering and technical professionals (non-IT) and the healthcare professionals amounted to 12.7% and 14.7%, respectively. Business and administration jobs were 10.8% and the rest of the occupations, like teaching, construction, and self-employed people, had a minimal contribution to the data.

Occupational forms give the age and education results additional support because they show clearly that the group of respondents is made up mostly of technically literate people or trainees. This percentage of IT and cybersecurity professionals is rather high and is especially important

to this study because they are the ones who can provide practical insight into the barriers to implementing and the readiness for forensics. However, even the inclusion of non-technical professionals provides the dataset with some balance, making it possible to comparatively analyse the differences in behaviour across domains.

4.3.1 Device Ownership and Usage Patterns

The survey indicated that there is a high penetration rate of consumer IoT devices by the respondents, smart speakers (40.20%), wearable (36.3%) and smart lighting systems (26.5%) being some of the most widely used consumer IoT devices. The variety of all device types indicates the dispersed environment of the IoT ecosystem as well as the necessity of any forensic framework to support as many functionalities and structures of devices as possible.

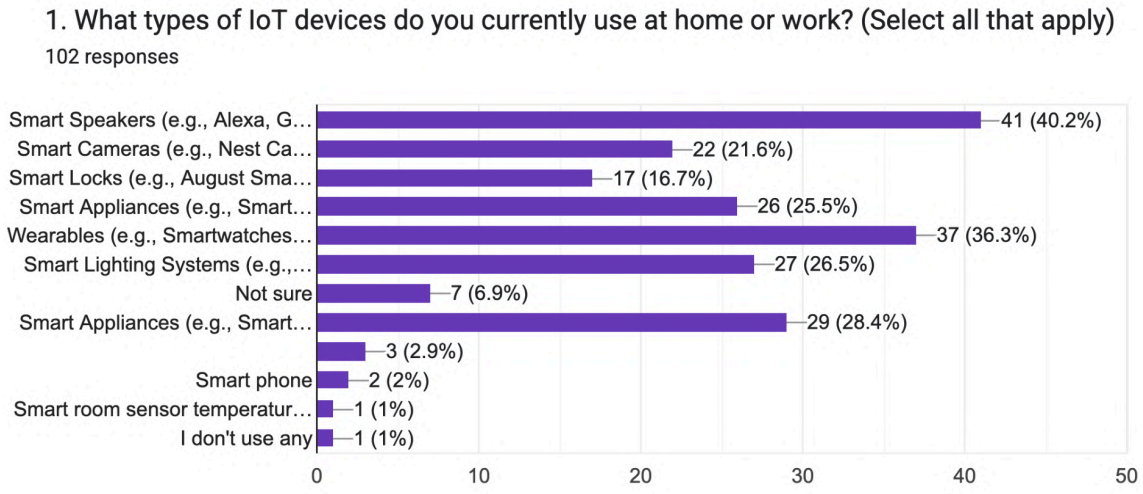

Figure S1: Device Ownership and Usage Patterns

4.3.2 Password Management and Credential Practices

Among the most terrifying discoveries is that of user credential practice. It was found that only 8.8 per cent of the respondents indicated that they fully customise usernames and passwords on their IoT devices. A considerable percentage (26.5) said that they had never done it, while some just did not recognise that such things were important, and others did not know how to do them. Such routines directly jeopardise the integrity of the device and point towards a major weak spot in attaining forensic readiness.

It has also been repeatedly said in the literature that default administrator credentials that have not been changed are usually one of the traits of a successful exploitation, especially in attacks with a large publicity like the Mirai botnet. Without altering default credentials, attackers can use poorly sophisticated tools to gain unauthorised access to the system. This necessarily has disastrous implications regarding the security of devices as well as the forensic sufficiency of the evidence that these devices carry or convey.

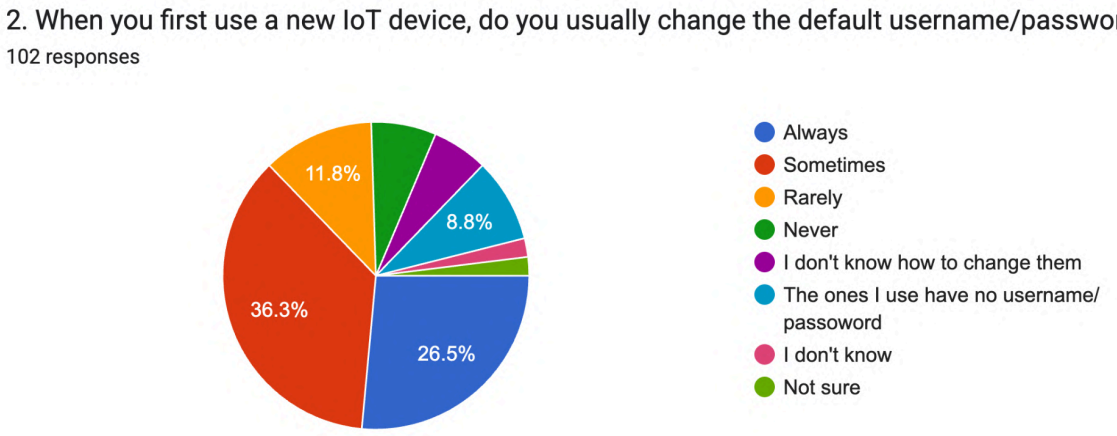

Figure S2: Password Management and Credential Practices

4.3.3 Firmware and Software Maintenance

Firmware updates are crucial to patching the known vulnerability and making sure that the mechanisms of forensic logging work. Nevertheless, the survey showed that this way only 8.8 of the users actively use updates at the time when they are released. Disturbingly, 44.1 percent acknowledged still having never updated their devices. Those behaviours have major impacts in that they would leave weak vulnerabilities that compromised devices have reliable or full forensic artefacts and might even permit the attackers to obfuscate their tracks using already known exploits.

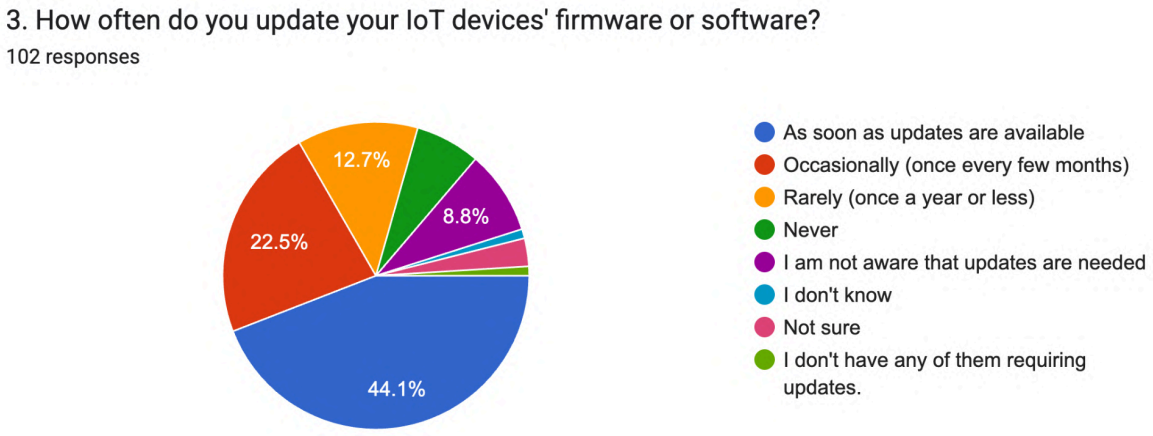

Figure S3: Firmware and Software Maintenance

4.3.4 Network Security Measures

Even though most of the users (59.8%) stated that they used strong Wi-Fi passwords, less than 18 percent were taking more stringent measures like router updates or network isolation. In this study, around 16.7 percent of participants did not take any specific steps to secure their IoT devices, and this shows a shortage of a layered defence approach at the network level. This grows the attack vectors and the complexity of isolating machines that have been compromised, being part of a forensic investigation.

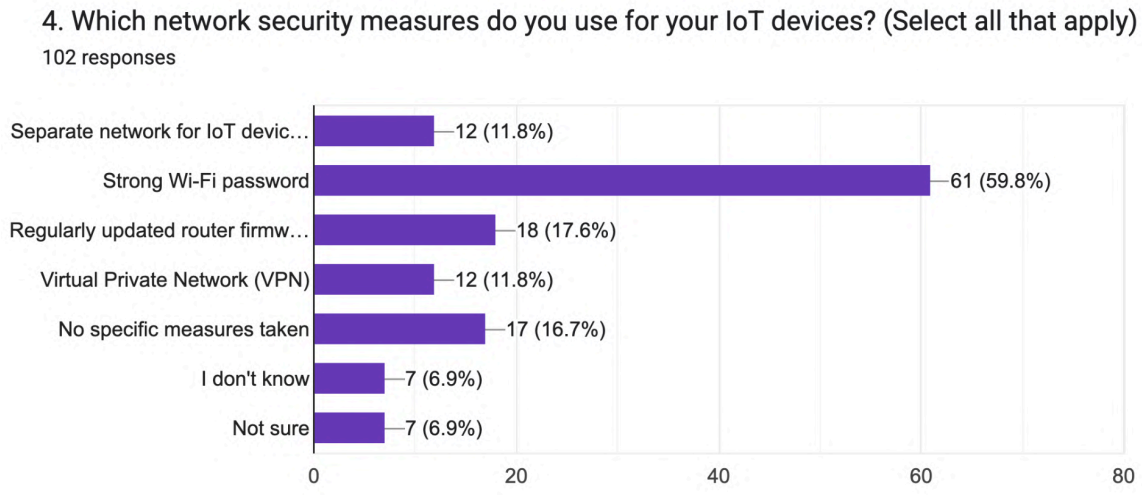

Figure S4: Network Security Measures

4.3.5 Forensic Awareness and Readiness

The most important conclusion of the survey is possibly connected to the level of forensic awareness. Less than 20 percent of participants stated that they would be aware of how to conserve data or devices in a way that could be understood by a forensic examination. Almost one-fourth never thought about the problem, and a very large percentage was not sure at all what to do in case of a security incident (27.5%).

These facts are a powerful argument in favour of incorporating user guidance in the suggested forensic structure. In the absence of user collaboration, key information can be deleted, devices reinstalled, or logs are overwritten, which means forensic examination can be rendered useless.

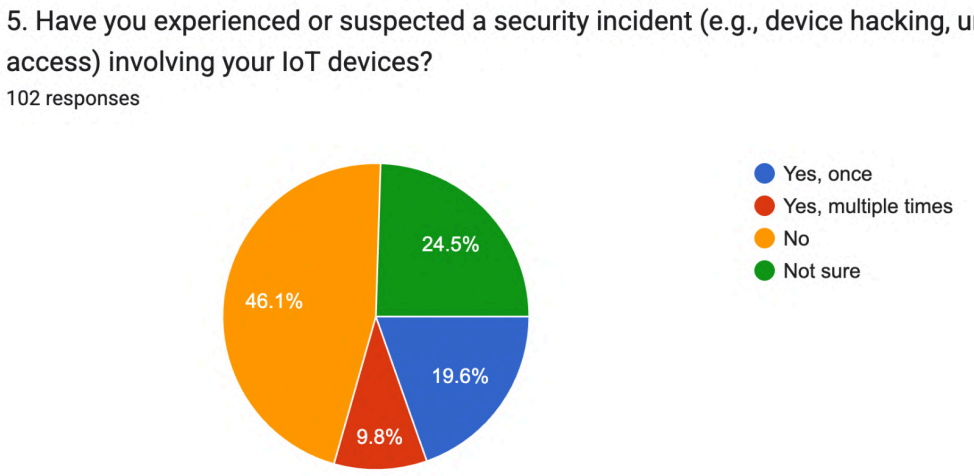

Figure S5: Forensic Awareness and Readiness

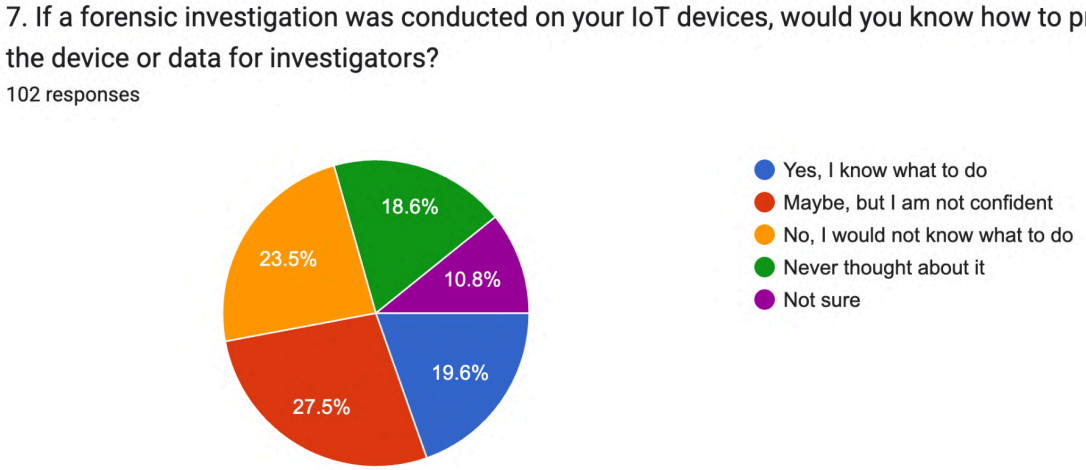

Figure S6: Attitudes Toward Best Practices

4.3.6 Attitudes Toward Best Practices

Although the amount of forensic awareness is not huge, the survey has opened a possible intervention potential. Over 50 percent (56.9 percent) of the respondents said that they would not

oppose taking up forensic best practices in case such best practices were available publicly and were easy. This observation is quite consistent with the objectives of the study and explains why this framework should include user-level procedural components.

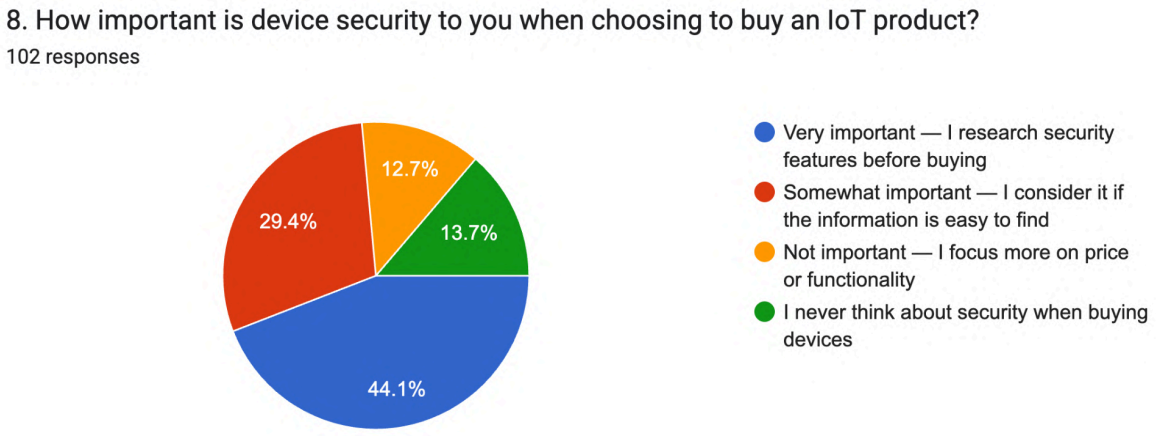

Figure S7: Willingness to Adopt Forensic Best Practices

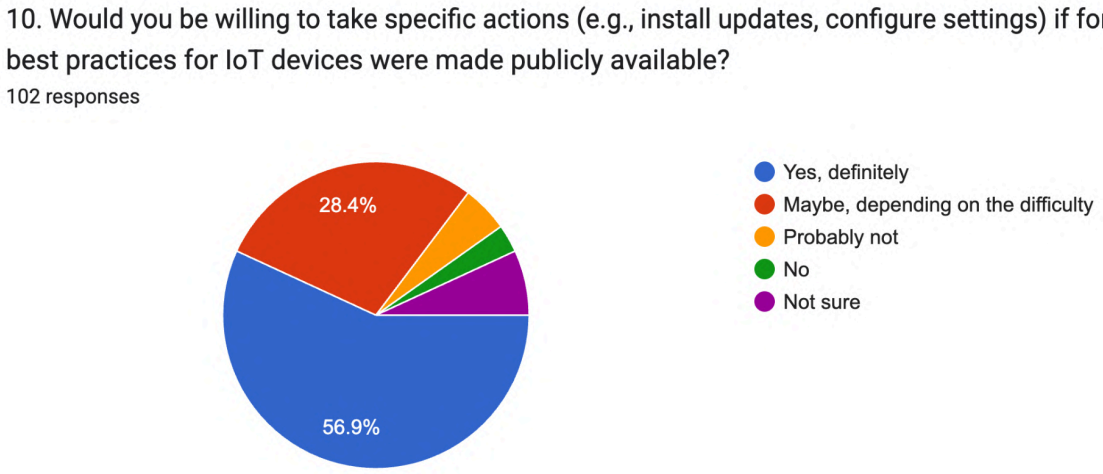

Figure S8: Perceived Importance of IoT Security

Table 4: Key Survey Results Summary

Survey Topic	Most Common Response	% of Respondents
Firmware updates	Never update	44.1%
Default credentials	Never changed	26.5%
Awareness of forensic steps	Don't know what to do after an incident	27.5%

Chapter 5: Framework Development

5.1 Introduction

Based on the information obtained using the systematic literature review and user survey results, the current chapter discusses the derivation of an effective forensic analysis framework in the consumer IoT setting. The framework looks to solve the reality of evidence gathering, forensic preparedness and exposure identification in heterogeneous and usually unrelated IoT landscapes. Moreover, it addresses user-friendly approaches in stemming awareness levels and technical literacy, which happens to be the lowest among end-users.

The chapter consists of the following parts: the theoretical background of the framework, an extensive description of the framework's elements, real-life situations of the application of the framework, and the strategy of the framework's operationalisation and validation. All of the sections are made to guarantee the scalability, flexibility, and performance of the framework in different consumer IoT ecosystems.

5.2 Theoretical and Methodological Foundation

The framework is developed according to the principles of the Design Science Research (DSR) as explained by Hevner et al. (2004), Peffers et al. (2007). DSR aims at building artefacts which address identified real-world problems. The methodology stresses cyclic design, individual care to stakeholders, and rigorous validation. In that respect, the framework of forensic analysis is conceptualised as a functional artefact that can mitigate all technical, as well as human-oriented concerns within consumer IoT forensics.

The model is also guided by the framework postulated for CPSS (Sun et al., 2018) that provides a comprehensive perspective through which IoT ecosystems can be analysed. CPSS underscores the interactions of human users, the embedded devices, and the cyber-physical environments and tends to focus on both the technical infrastructure and forensic strategies and human behavioural

forensic strategies due to their importance. The multidimensional process helps to ensure that the framework is not only centred on the post-incident response but also aimed at creating proactive systems that can carry out forensic preparedness.

5.3 Overview of the Forensic Analysis Framework Architecture

The forensic analysis framework is composed of **three interdependent layers**:

1. **Vulnerability Classification and Mapping Layer**
2. **Forensic Readiness and Procedural Guidance Layer**
3. **User Awareness and Engagement Layer**

Table 5. Framework Summary Table

Framework Component	Key Features	Purpose
1. Vulnerability Classification Layer	Categorises vulnerabilities across device, firmware, network, and application layers	Helps investigators map vulnerabilities to specific forensic artefacts and risks
2. Forensic Readiness & Procedures	Includes pre- and post-incident actions: device inventory, secure logging, evidence acquisition	Ensures standardisation, legal admissibility, and integrity of digital evidence

3. User Awareness & Engagement Layer	Offers user manuals, incident action cards, and microlearning modules	Empowers non-technical users to adopt best practices and preserve evidence effectively

These layers offer a strong, end-to-end remedy to developing backbone forensic capability in IoT consumer environments. The framework has been organized on these three domains, thus making it to balance up systemic preparedness and participation of the users.

5.4 Vulnerability Classification and Mapping Layer

This base layer gives a systematic taxonomy for IoT vulnerabilities to categorise them. It is based on OWASP IoT Top 10 (2022), Yaqoob et al. (2019) and results of the literature review. The taxonomy levels are:

5.4.1 Device-Level Vulnerabilities

Such vulnerabilities are a result of physical and hardware weaknesses. These may include hardcoded credentials that come to the firmware, an unsecured debug port (e.g. UART and JTAG), and not implementing secure boot gateways. Lack of secure boot makes devices vulnerable to low-level firmware attacks that may compromise the integrity of such devices since their start-up. These vulnerabilities can possibly exist throughout the device lifecycle and are hard to identify or put right without aggressive physical evaluation, and thus form a platform of high risk in forensic investigation.

5.4.2 Firmware-Level Vulnerabilities

Vulnerabilities of the firmware can be associated with the operating system within the device. Some of the most common vulnerabilities are the absence of cryptographic signing in firmware updates, the absence of secure boot loaders, and a lack of use of general libraries that are more current or unpatched. Such vulnerabilities have been able to place attackers in a position to push malicious code, change the logging behaviour or turn off forensics capabilities altogether. This is a very important layer of the taxonomy, as the forensic investigators must ensure that there is integrity of firmware before making use of the log data or the internal timestamps as a portion of admissible evidence.

5.4.3 Network-Level Vulnerabilities

A lot of the IoT equipment connects to insecure networks, i.e. plain Hypertext Transfer Protocol (HTTP) or even obsolete wireless protocols. They can equally open ports that they do not need to or are not well segmented from other devices in the network. As an example, a smart light bulb can be accessed by the same subnet as a smart lock or camera. Such devices may be compromised and unleashed to undergo lateral attacks. Forensically, these flaws make it easier to attribute and correlate logs. The acquisition activity at this level should take into consideration network traffic dumps, port scans, and DNS logs to minimise the reconstruction of the attack vector.

5.4.4 Application-Level Vulnerabilities

Examples of application-level vulnerability are insecure mobile applications, open APIs, weak session management and the absence of access controls. The result of these issues is usually credential leaks, privilege escalations, and data exfiltration through exposed endpoints. This layer of forensics should contain the API call logs analysis, observation of the application behaviour and the endpoint detection mechanisms. The user practices are also a factor that

overlaps tremendously with this domain, because using weak passwords or giving too many privileges may allow application-level exploitation.

5.5 Forensic Readiness and Procedural Guidance Layer

The second layer of the framework provides full guidance on the procedural roadmap that can be incorporated either before or after a security breach. It contains a gradual development to reinforce the overall forensic posture.

5.5.1 Pre-Incident Readiness

Device Inventory Management: Having an up-to-date inventory of all the IoT devices and corresponding metadata, IP addresses, Media Access Control (MAC) addresses, the version of firmware, and network affiliations is an essential starting point for forensic accountability. Through this catalogue, investigators can narrow down the possible targets and define their evidence-gathering strategy promptly.

Secure Logging: The devices need to be set up in a manner such that the logs created when an incident occurs are dated, signed and sent to be stored in a secure, remote location. Local logs can be encrypted and replicated in cloud archives in harmonised formats, e.g., JavaScript Object Notation (JSON), Extensible Markup Language (XML), that are more effortless to decipher.

Firmware Integrity Validation: It is recommended to use firmware integrity checks based on a hash by checking a periodic value of known-good values provided by vendors. This is done to guarantee that device behaviour and logs have not been tampered with due to firmware that has been altered.

Network Monitoring: On the network end, lightweight intrusion detection devices like Snort or Zeek may be placed at gateway devices and used to monitor variations in the network traffic. Snapshots or log preservation procedures need to be set off through alerts.

5.5.2 Post-Incident Response Protocol

Detection and Quarantine: When a dangerous behaviour is detected, the affected device must be initially quarantined logically to inhibit the additional invasion or manipulation of the information within a network. This can be done through Virtual Local Area Network (VLAN) reassignment or by the use of MAC address filtering.

Evidence Acquisition:

> **Volatile Data:** Retrieved through the (Random Access Memory) RAM with the help of physical or JTAG methods.
>
> **Saved Data:** Is composed of logs, configuration information and file system snapshots. These extractions can be done with tools such as Forensic Tool Kit (FTK) Imager or Binwalk.

Chain of Custody Management: The involvement of each person accessing the evidence should be documented, including the tool, time, and individuals involved. Such recording is mandatory when it comes to preserving evidentiary integrity in a court.

Preservation and Reporting: Forensic reports on device metadata and timelines of the incident on incidents should be provided. The data must be stored using a write-once medium, e.g. Write Once and Read Many (WORM) disk or forensic containers such as AFF4, to avoid manipulation.

This operational layer operationalises best practices and develops repeatable processes that increase forensic soundness and admissibility in the courts.

5.6 User Awareness and Engagement Layer

Visual mockup and interface prototypes of the suggested educational tools and companion applications are provided in chapter 6 under the sub-heading 6.8.6 to elucidate implementation routes to better the comprehension of usability. Realising that forensic preparedness cannot only

be limited to technical means, the framework incorporates a special layer that centres on user training, behavioural conditioning, and user-friendly instructions.

5.6.1 Forensic Literacy Tools

Basic awareness of the impact of user activities on the integrity of a device and the viability of the evidence is often lacking among end-users. The model gives an idea of downloadable user manuals according to the type of device being used. Such tutorials will have visual cues to:

- Change the default password
- Plan software changes in hardware
- Investigate and translate the security caution tube

They also clarify the consequences of factory resets, power cycling, and incorrect cell-phone settings from a forensic perspective.

5.6.2 Incident Action Cards

These quick-reference aids are available in the form of a checklist that a user can read as soon as a suspicious activity is detected. These cards convey information that discourages activities which could trash up evidence (unplugging devices, reinstalling apps, etc) and instead encourage little or no interference until a professional investigation is set in achievable mode. Such cards are either paper (e.g., in the packaging of products) or electronic (e.g., in application interfaces).

5.6.3 Educational Modules

The framework will make it possible to promote the usage of modular microlearning content, which can be sent through apps, QR-codes, and onboarding emails. Topics include:

- Overview of digital forensics

- Typical threats and indicators of the IoT Compromise
- Ideal security measures when working in home networks

The modules shall close the knowledge gap and develop a culture of security awareness among non-expert users, therefore enhancing the success of the other layers of the framework.

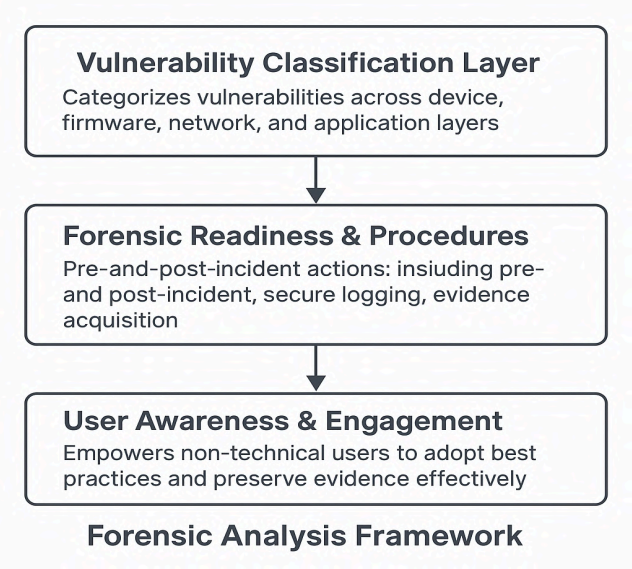

Figure 2. Forensic Analysis Framework

5.7 Real-World Application Scenarios

Some of the imaginary yet quite realistic scenarios are described to understand how the framework works in practical conditions:

5.7.1 Smart Camera Compromise

In the given case, one of the users complains about unauthorised access to their smart camera. With the framework, the threat is put on an isolated machine, export the cloud backups of logs, and look out for incidents of unauthorised access. The firmware on the device is checked through

a hash comparison. The router displayed network logs that indicated a significant increase in outbound connections, indicating a possible command and control type of communication. An investigator can connect the attacked logs with the known attack signatures and point to the breach to credential stuffing through third-party data leak.

5.7.2 Smart Lock Intrusion

One of the residents discovers that his or her smart lock was opened when he or she was not present at home. The steps of responding to this entail the extraction of Bluetooth access logs, confirmation of the API interaction timestamp, and examining the activity logs within the mobile app. The forensic investigation reveals that a former tenant has not been denied entry because he/she has not been forgotten when setting up the app sharing permissions, which shows a usual usability-forensics trade-off in smart access systems.

5.7.3 Baby Monitor Hijacking

The baby monitor reports some strange voices from a family. Computer logs are retrieved, and the Domain Name System (DNS) cache is examined to determine the origins of connections. It was found that the device was communicating with IP addresses which have been found to belong to a botnet. Firmware scan makes an appearance that the patch level is old, and the report of the forensic analysis is handed to the vendor to organise a concerted release and future fixes.

The presented examples illustrate the flexibility of the framework to different types of devices, compromise situations, and the scope of user interaction.

5.8 Operationalisation and Implementation Pathways

The framework needs to be embedded in the existing ecosystems to become effective:

- From the manufacturer's standpoint, they can place forensic readiness templates into device setup wizards or companion mobile applications.
- It is possible to integrate the framework into user awareness programs through Cybersecurity Training Programs.
- The procedural guidelines can be incorporated into standardised Law Enforcement and Computer Emergency Response Team (CERT) tools of incident response.

The structure has been modular in its design, where stakeholders have the flexibility to implement modules as resources are made available and as the technical skills of the implementers are adequate.

5.9 Validation Strategy

The conceptual validation can be carried out based on:

- **Scenario Analysis:** Using the framework for typical IoT Incidents
- **Triangulation:** This is done by making sure the components of the framework dovetail with gaps in existing literature and the behaviour of resultant users.
- **Peer review:** Requiring the opinion of specialists on the rough draft (future iterations are going to have it)

To be validated further, the framework may be tested in smart home labs or implemented in tabletop incident simulations to determine effectiveness.

Table 6: Mapping Vulnerabilities to Evidence Types

Vulnerability	Artefact to Collect
Default credentials	Login history, config files
Unencrypted traffic	Network capture logs
API exposure	API call logs, access tokens

Chapter 6: Discussion

6.1 Introduction

The present chapter critically discusses the developed forensics analysis framework that has been hypothetically designed in Chapter 5. It analyses its broader academic and practical picture within IoT forensics and forensic science. The discussion restates the main research question that informed the study, and assesses the contributions of the framework alongside the availability of existing models. Emphasis is put on the framework's aim to find a balance between the technical soundness and the inclusivity of use when approaching the design of digital forensics, which is frequently disregarded. In this chapter, the author also addresses ethical, legal, and practical concerns introduced by forensic readiness implementation in consumer IoT systems.

6.2 Addressing the Research Question

Research Question: How can a standardised forensic analysis framework improve evidence collection and vulnerability detection in consumer IoT devices?

The recommended framework supports the process of gathering evidence in several ways. First, it presents a comprehensive vulnerability classification framework between device, firmware, network, and application, thus allowing the forensic investigator to methodically discover possible avenues of attack and their evidence sources. The taxonomy is a generalised structure that applies to different devices, unlike ad-hoc investigations that only apply to a specific device due to expertise on the device.

Second, the framework goes ahead and proposes procedural guidelines consistent with international best practices (e.g., NIST SP 800-213), making forensic processes consistent and integrity-oriented. Most of the forensics failures have been based on the partial documentation of the chain of custody or destruction and the unsuitable processing of volatile data. The framework reduces the possibility of compromised evidence by integrating effective practices (like secure

logging, evidence triaging, and integrity verification) into the pre- and post-incident workflows process.

Third, the fact that real-world scenarios are also considered proves that the framework can be used in a broad spectrum of incidents, including unauthorised access to smart locks and hacked baby monitors. Such scenarios bear amplification of their utility, particularly in settings where resource limitations and the inexperience of users are prevalent.

Lastly, the layered structure of the framework allows it to scale up, making its module-by-module adoption convenient. An organisation with lower levels of forensic maturity can start with the foundation level of process and then progress to more advanced practices such as auto logging and anomaly identification.

The user survey revealed disturbing trends: many of the users fail to change proposed credentials and do not update their devices' firmware as frequently as they should, and also do not possess any knowledge about forensic preservation concepts. Nevertheless, more than half of the surveyed persons stated that they would be willing to implement best practices in case they were available and simple to apply.

The survey gave birth to a serious revelation, which has strongly contributed to the user awareness layer of the proposed framework. End-users are usually passive in the traditional models of forensics. The assumption is refuted in this work, and it introduces a new participatory style in which users are provided with both the knowledge and tools to retain any possible evidence. Knowledge modules, incident action cards and configuration checklists close the gap between the technical requirements and user behaviour.

In addition, through its integration with CPSS theory, the framework also aligns with the view of the users as an important element of the forensic ecosystem. These activities, networks, and even a lack of knowledge define the digital footprints. Therefore, forensic preparedness should begin not only through hardening of devices but also through user empowerment.

6.3 Contributions to Knowledge and Practice

6.3.1 Theoretical Contributions

This study provides contributions to the scholarly debate on digital forensics and cybersecurity. It advances the CPSS model in that it uses the framework within the area of forensic readiness. The framework shows that digital forensics cannot be merely reduced to technical work, but should also include a socio-technical practice of involving the end-users, the legal system, and digitally connected devices.

Also, through the use of a DSR approach, the work can be considered an example of how evidence-based artefact development may be applied in cybersecurity. It extends the studies by Peffers et al. (2007) and implements them in a fairly unexplored field: IoT forensics in the consumer context.

6.3.2 Practical Contributions

Practically, the framework can be applied as a toolset for forensic investigators and even manufacturers of such devices. The taxonomy and the procedural guidelines can guide the forensic investigators so that they can invoke them in their evidence-gathering process. The framework allows manufacturers to design devices that will facilitate forensic readiness, including secure logging or built-in indications to remind the user to change credentials. Users, in their turn, can employ the literacy tools, as well as action cards, to stay prepared at a minimum level.

Modularity of the framework will also enable it to be able to adapt to the advancements in technologies as well. When something more like AI-based detection components or blockchain-based logs is introduced, the entire structure does not necessarily need to change to accommodate those.

6.4 Comparison with Existing Forensic Models

Upon comparison with the existing frameworks like FAIoT (Zawoad & Hasan, 2015) and the top-down forensic approach (Perumal et al., 2015), the framework that is proposed helps to provide several improvements.

The ideas of FAIoT include the establishment of forensic features into the very design of devices. Although this is theoretically sound, it lacks information on how they can be implemented practically. Although the model designed by Perumal is systematic, it looks at the forensic readiness as a reporter-based (top-down), investigator-driven activity without considering the variety of consumer device context and consumer behaviours.

The proposed framework, on the other hand, highlights bottom-up readiness. It begins with the user and moves upwards, such that even non-experts could have something to contribute to the forensic process. It has a layered structure; vulnerability classification, procedural guidance and user education that have filled the gaps existing in the earlier models.

Additionally, the presence of scenario-based validation creates a practical background, which is lacking in most conceptual frameworks. It not only displays what ought to be done but also how this might turn out in practical environments.

Table 7: Framework Comparison with Existing Models

Model	Scope	User Role	Strengths	Limitations
FAIoT	Device-level	Passive	Forensic-by-design	No user education component
Perumal's Top-Down	Layer-based	Investigator-centric	Structured approach	Inflexible to device diversity

Proposed Framework	End-to-end	Inclusive	Modular, user-focused, practical	Needs field validation

6.5 Ethical, Legal, and Privacy Considerations

The balance between investigative depth and user privacy connotations constitutes one of the under-discussed areas in IoT forensics. A lot, if not all, of IoT devices, gather sensitive information, including voice recordings, health records, or geo-location information. Such collection and analysis of information as a forensic measure attracts ethical issues on consent, data minimisation, and admissibility of the information in a court of law.

Certain known issues can be addressed through the framework, albeit with a suggestion of not enabling full logging where possible, and to insist that users need to give consent during forensic investigations. Jurisdictional environments such as the General Data Protection Regulation (GDPR) are complex and have complicated facets that need consideration. To use an illustrative example, forensic logging may interfere with the right to be forgotten, implying a need to implement dynamic retention policies that strike the right balance between evidentiary value and privacy requirements.

Ethically, the framework acknowledges that there is a possible forensic overreach. Investigative tools are prone to be abused: without demarcation, they will be redistributed to surveillance, or they will infringe the principle of proportionality. The aspects of ethical guidance should therefore be taught during the training, and the forensic tools ought to have an audit trail aspect to make them accountable.

6.6 Limitations of the Framework

Despite its strengths, the framework is not devoid of limitations. To begin with, it has not been empirically verified in real life/forensic investigations. Although scenario-based validation helps gain some experience, the field implementation must be carried out to determine the usability and adaptability within real-world constraints.

Second, the framework is now targeted at consumer-grade IoT devices. It is unlikely to be transferred directly to industrial or mission-critical IoT systems, whose operation needs to be based on different architectures and in varied regulatory environments.

Third, the user cooperation, an innovation in itself, presupposes the level of digital literacy that is not necessarily always present. Although the framework attempts to close this gap using some educational tools, it requires additional empirical studies to determine how effective those tools are.

6.7 Opportunities for Future Research and Enhancement

Subsequent studies may find an answer to the shortcomings of the existing framework by adopting it in pilot schemes or smart home testbeds. It would allow one to evaluate its influence on the results of forensic studies in a controlled environment.

The introduction of more sophisticated technologies, including tamper-evident logs provided by blockchain or on-the-fly anomaly detection provided by AI, can provide the ground on which such innovations can be introduced. These technologies have the potential to automate forensics, achieve better accuracy and may offer little to no reliance on human skills.

Lastly, culturally modified modules may be incorporated in future versions of the framework that will capture the different legal and behavioural standards across regions. This would make it more applicable and relevant across various domains.

6.8 Recommendations

In light of the findings and implications of the present study, this study provides a series of recommendations that are aimed at leading/guiding future studies, technological development, and policy documents on IoT forensics. These recommendations are divided into strategic areas that include implementation, technological improvement, user empowerment, and possible future research directions.

6.8.1 Implementation and Validation

- **Pilot Deployments in the Real World:** The given forensic framework can be piloted either in natural or semi-controlled settings, e.g., smart home laboratory, university test-bed, or municipal IoT initiative. Such testbeds will facilitate assessments on the feasibility of use, the usability of operation, and evidentiary accuracy via real-life conditions.
- **Sector-Specific Adaptation:** Although the current study targeted consumer-grade equipment, the model can be extended to cover the areas of industrial IoT, smart healthcare, and vehicle networks. The pressures in each vertical are the introduction of special constraints (e.g., regulatory, latency and data sensitivity), which have not been borne out in the forensic protocols.
- **Regulation Harmonisation and Certification Routes:** It is also necessary to optimise the framework according to the European guidelines on security and privacy standards, on which ENISA, NIST, and ISO/IEC 30141 have published official guidelines. Such long-term prospects must incorporate formalising the existing bits of the framework into certifiable guidelines of IoT forensic readiness.

6.8.2 Technological Enhancements

- **Blockchain:** Blockchain technology can be researched to realise leak-proof and unchangeable histories of actions with devices. This would eliminate forensic traceability and data integrity even where there is an adversarial environment (Alenezi & Wills, 2021).
- **Threat and anomaly detection:** The small machine learning models must be installed in IoT gateways or edge nodes, where they can monitor patterns of behaviour, detect anomalous behaviour, and result in automatic forensic data retention (Tawalbeh et al., 2020).
- **Distributed Forensic Architecture (DFA):** The forensic workload must be allocated throughout a layered framework, which includes edge, fog, and cloud, to reduce the computation tasks conducted in restricted devices. This method will make it scalable and will not overload the endpoints.

6.8.3 User Engagement and Literacy

- **The Competence in Companion Tools:** Mobile applications and web-based platforms ought to be created to orient the consumer to incident detection, response, and preservation of evidence. Such aids ought to incorporate visual logs, alert systems and paperless forms of reporting.
- **Local and participatory Awareness Programs:** Educational content also has to be made flexible in terms of different digital literacy levels and cultural environments. Certain consideration must be paid to the vulnerable groups of users, who may include children, the elderly, and non-native speakers, to stimulate inclusive forensic preparedness.
- **Network Foundation Protection (NFP) Gamification of IoT-Hygiene:** To cultivate a habit of repeated activity, these measures of cyber hygiene must be gamed, by the use of reward programs, badges and active learning sessions that promote positive forensic behaviour when using a device in everyday life.

6.8.4 Future Research Directions

- **Data Sovereignty and Lawful Jurisdiction Research:** The developed framework is to be analysed according to various local regulations [e.g., GDPR, California Consumer Privacy Act (CCPA), ePrivacy Directive] to make sure that the recommendations do not merely possess technical expediency but are legally binding in all jurisdictions.
- **Progressive evolution in Volatile evidence capture:** Fundamental research in this direction should include live memory capture techniques and discard just-in-time forensic imagers, which translate the ephemeral information on the Internet of Things devices, especially in volatile or transient data situations.
- **Open Research and Development Ecosystem:** An open-source repository ought to be created to incorporate open-source forensic tools, modular frameworks, case study documentation, configuration templates and seek group development in the arena.

6.8.5 Legal and Regional Adaptability

- To operate the forensic structure within the global framework, there must be a solution to the variation in jurisdiction when it comes to the protective measures affecting data and evidence collection procedures. The use of consumer IoT devices in a cross-border setting is more and more common, with the disparity between the right to privacy, the consent standard, and data admissibility standards being a major factor that can affect forensic work significantly.

In this respect, a table summarising the compliance matrix has been developed (see Table 6.1) that helps forensic practitioners with vital legal considerations regarding the various regions when dealing with evidence. This table presents the general norms outlined in log retention, which require a consent provision, access privileges, and admissibility as evidence through some of the most popular frameworks.

Table 8: Summary of Forensic Compliance Considerations by Region

Region	Law/Framework	Log Retention	Consent Requirement	Data Access Rules
European Union	GDPR	Max 6 months	Explicit (Art. 6)	User and processor limits
United States of America (California)	CCPA	Undefined	Opt-out mechanism	Accessible upon request
Canada	Personal Information Protection and Electronic Documents Act (PIPEDA)	"As necessary"	Informed consent	User-requested disclosure
Global (IoT Trust Mark)	Various	Varies	Transparent by design	Manufacturer-managed access

6.8.6 Usability and Visualisation Enhancements

- **Visual Mockups of Companion Tools Design:** To make the user engagement layer of the framework paralleled with the practical applicability and accessibility, a visual prototype (e.g., a wireframe or the mock of a mobile interface) of such tools as an incident action card, a mobile forensic assistant app, and a device hygiene checklist interface should be created. Such tools are very important to guide non-technical users in case of security incidents and encourage daily forensic hygiene processes.

The visual mockups ought to present user-friendly spaces and clear guides, progress warnings (e.g., secure and dangerous settings), and simple routes of interaction that will accommodate either active preparedness and active evidence-gathering. Instead of having them buried in

technical manuals, these tools ought to be functional and straightforward in their use, as well as interesting to look at, to have high rates of adoption.

These mockups can serve multiple purposes:

- They can be taken as a guide by the developers in implementing User experience/User interface features in line with forensic objectives.
- They can be used in awareness programs by educators or trainers and even in any onboarding modules.
- They can be used to audit the availability of features of forensic readiness oriented to the user at certification or product review time by the policymakers and security auditors.

When such visuals are added to the forensic framework, they strengthen its relevance, build an understanding, and make multi-stakeholders interested in the involvement in forensic preparedness as a common task.

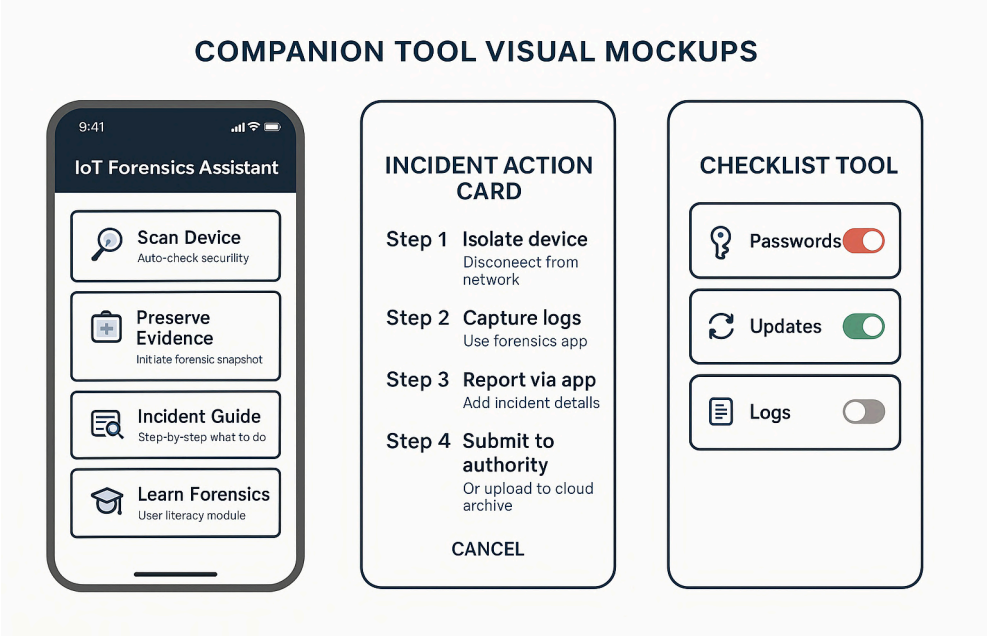

Figure 3. Mockup screens of the IoT Forensics Assistant app.

Left: Main dashboard for initiating scans, evidence capture, and literacy modules.
Centre: Step-by-step incident response action card.
Right: Simplified checklist for IoT security hygiene with visual status indicators.

Chapter 7: Conclusion

This study aimed to explore the forensic weaknesses of consumer IoT technologies and elaborate on a forensics analysis framework that enhances technical forensic practices and involves an understanding of user behaviours in the preservation of digital evidence. The study seeks to understand whether to enhance forensic systems by adopting a standardised framework and how to involve users in the forensic preparedness. A multidimensional answer to the ever-changing complexities of the consumer IoT ecosystem has been provided.

The study initially conducted a thorough literature review based on state-of-the-art methods through a mixed-methods approach to identify vulnerabilities in IoT devices and to scrutinise the unsafe reality of consumer IoT environments. Findings showed that popular devices are often delivered with a programmed firmware, insecure communications, hardcoded passwords, and weak, changing logs (Bertino, 2020; OWASP, 2022). This predisposes them to unauthorised use by malicious actors, and evidence collection and post-incident analysis is often challenging.

The user survey also added support to the systemic disconnection between forensic awareness and the function of devices. The majority of participants lack knowledge about simple measures that can be taken to ensure safe cybersecurity best practices, including updating firmware or changing the default passwords, although many of them showed readiness to change their approach in case they had the necessary expert support. This discovery not only highlighted a fatal lack of forensic models but also points to a total lack of user agency.

To this end, the study presented a layered forensics analysis framework. These layers are:

- A vulnerability detection framework is classified into hardware, network and application.
- A procedural plan of readiness, provided to regulate actions of proactive and reactive forensics.
- A user interface level with the introduction of educational capabilities, checklists of incidents and literacy episodes.

The framework is modularly constructed and able to perform across multiple device sets and stages of forensic maturity.

Notably, the framework changes the definition of forensic readiness as a socio-technical construct, which requires the cooperation of users, investigators, and designers. The study is effective in putting a case on the need to incorporate legal, behavioural, and technical aspects in any research and development on forensic science by injecting forensic concepts into both machine architecture and human interaction.

Although the framework is conceptually strong and supported with evidence, its application in the real-life forensic environment is an essential line of its development. Moreover, the consumer IoT focus implies a high potential for development in other aspects of the digital realm in other industries and market niches, such as healthcare or automotive systems.

In conclusion, this study provides a primary roadmap to a future where digital forensics of consumer IoT is more trustworthy, user-friendly and proactive to the security conditions of ubiquitous computing. It requires a transition toward a forensics-by-design approach instead of ad-hoc and reactive incident response methods, thereby setting the stage for a scalable, verifiable, and empowered forensic framework in the age of digital interconnectedness.

References

Acar, A., Fereidooni, H., Abera, T., Conti, M., & Sadeghi, A. R. (2022). Things not forgotten: A comprehensive study of security and privacy issues in the firmware of smart devices. ACM Computing Surveys, 55(3), 1–36. https://doi.org/10.1145/3475730

Ahmad, M., Baig, Z. A., & Dutta, M. (2023). An assessment of security challenges in consumer IoT ecosystems: A survey and taxonomy. Journal of Network and Computer Applications, 209, 103560. https://doi.org/10.1016/j.jnca.2022.103560

Alenezi, A., & Wills, G. (2021). Enhancing IoT forensic readiness using blockchain: Opportunities and challenges. Forensic Science International: Digital Investigation, 36, 301102. https://doi.org/10.1016/j.fsidi.2021.301102

Alenezi, M., & Wills, G. (2021). Blockchain-based logging framework for Internet of Things forensic readiness. Future Internet, 13(2), 38. https://doi.org/10.3390/fi13020038

Alenezi, A., Al-Rashid, A., & Alghamdi, T. (2023). Cross-border forensic challenges in IoT cloud environments: Legal and technical perspectives. Sensors, 23(3), 1260. https://doi.org/10.3390/s23031260

Almalki, A., Gritzalis, D., & Alhaidari, F. (2021). Challenges in evidence collection and chain-of-custody management for IoT forensics. IEEE Access, 9, 162217–162231. https://doi.org/10.1109/ACCESS.2021.3135098

Almutairi, H., Khan, M. K., & Malik, S. (2022). Forensic readiness for consumer IoT: Opportunities, challenges, and best practices. Future Generation Computer Systems, 128, 328–343. https://doi.org/10.1016/j.future.2021.10.013

Alrawais, A., Alhothaily, A., Hu, C., & Cheng, X. (2021). Security and privacy issues in the Internet of Things: A survey. IEEE Internet of Things Journal, 8(7), 5410–5428. https://doi.org/10.1109/JIOT.2020.3013369

Atlam, H. F., Walters, R. J., & Wills, G. B. (2020). Internet of Things security, privacy, and forensic issues: A review of recent advances and future perspectives. IEEE Access, 8, 117952–117975. https://doi.org/10.1109/ACCESS.2020.3004940

Atlam, H. F., Walters, R. J., & Wills, G. B. (2020). Internet of Things: State-of-the-art, challenges, applications, and open issues. International Journal of Intelligent Computing and Cybernetics, 13(2), 233–244. https://doi.org/10.1108/IJICC-09-2019-0116

Bertino, E. (2020). Data security and privacy: Concepts, approaches, and research directions. Foundations and Trends® in Privacy and Security, 3(1–2), 1–112. https://doi.org/10.1561/3300000016

Bertino, E. (2020). Data security and privacy in the IoT. Computer, 53(9), 86–89. https://doi.org/10.1109/MC.2020.2992716

Casey, E., Ferraro, M., & Nguyen, L. (2020). Investigation and attribution of IoT evidence in the age of cloud computing. Digital Investigation, 32, 200902. https://doi.org/10.1016/j.diin.2020.200902

Conti, M., Dehghantanha, A., Franke, K., & Watson, S. (2018). Internet of Things security and forensics: Challenges and opportunities. Future Generation Computer Systems, 78, 544–546. https://doi.org/10.1016/j.future.2017.07.060

Deng, H., Wang, H., & Zhou, X. (2023). Lightweight cryptography for IoT: Survey and challenges. IEEE Internet of Things Journal, 10(1), 719–734. https://doi.org/10.1109/JIOT.2022.3176941

Elmisery, A. M., Rho, S., & Abdulaziz, A. (2023). Security and access control in smart environments: Current status and future directions. Sensors, 23(2), 897. https://doi.org/10.3390/s23020897

ENISA. (2020). Good practices for the security of IoT. European Union Agency for Cybersecurity. https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot

ENISA. (2020). Guidelines for securing the Internet of Things. European Union Agency for Cybersecurity. https://www.enisa.europa.eu/publications/guidelines-for-securing-the-internet-of-things

Giaretta, A., De Caro, A., & Lanzone, M. (2022). Secure over-the-air updates in resource-constrained IoT environments. Security and Privacy, 5(3), e173. https://doi.org/10.1002/spy2.173

Hamza, A., El-Medany, W., & Almalki, F. A. (2022). A comprehensive review of communication protocols in IoT: Challenges and solutions. Wireless Networks, 28, 2033–2052. https://doi.org/10.1007/s11276-021-02869-2

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. MIS Quarterly, 28(1), 75–105. https://doi.org/10.2307/25148625

Ho, A. T. S., & Li, S. (2015). Handbook of Digital Forensics of Multimedia Data and Devices. Wiley.

Khan, R., Khan, S. U., Zaheer, R., & Khan, S. (2023). Modular forensic logging frameworks for heterogeneous IoT environments. Computer Standards & Interfaces, 86, 103657. https://doi.org/10.1016/j.csi.2022.103657

Koops, B. J., & Leenes, R. (2020). Privacy regulation cannot be hardcoded: A critical comment on the "privacy by design" provision in data protection law. International Review of Law, Computers & Technology, 34(2), 122–138. https://doi.org/10.1080/13600869.2020.1732936

Lopes, L. A., Ferreira, M., & Silva, L. (2022). IoT forensic tools: A comparative study. Computers & Security, 118, 102735. https://doi.org/10.1016/j.cose.2022.102735

NIST. (2021). IoT Device Cybersecurity Guidance for the Federal Government (SP 800-213). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-213

Nieto, A., Rios, R., & Lopez, J. (2018). Digital witness and privacy in IoT: An Anonymous witnessing approach. In 2018 IEEE International Conference on Future IoT Technologies (pp. 1–6). IEEE. https://doi.org/10.1109/FIOT.2018.8325613

OWASP. (2022). OWASP Internet of Things Project. https://owasp.org/www-project-internet-of-things/

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., ... & Moher, D. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. BMJ, 372, n71. https://doi.org/10.1136/bmj.n71

Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A design science research methodology for information systems research. Journal of Management Information Systems, 24(3), 45–77. https://doi.org/10.2753/MIS0742-1222240302

Perumal, S., Norwawi, N. M., & Raman, V. (2015). Internet of Things (IoT) digital forensic investigation model: Top-down forensic approach methodology. In 2015, Fifth International Conference on Digital Information Processing and Communications (ICDIPC) (pp. 19–23). IEEE. https://doi.org/10.1109/ICDIPC.2015.7323012

Rahman, A., Carbunar, B., & Rishe, N. (2018). IoTDots: A forensic framework for smart environments. Proceedings of the 15th ACM Conference on Security and Privacy in Wireless and Mobile Networks, 235–246. https://doi.org/10.1145/3212480.3212494

Ruan, K., Huebner, E., & Carthy, J. (2021). Advancing forensic readiness: A theoretical framework for proactive digital investigation capability. Journal of Digital Forensics, Security and Law, 16(1), 2–19. https://doi.org/10.15394/jdfsl.2021.1693

Sang, Y., Lei, Y., & Liu, L. (2022). Survey of recent botnets targeting IoT: Attacks, detection, and mitigation. Computer Networks, 206, 108785. https://doi.org/10.1016/j.comnet.2021.108785

Santos, J., Macedo, R., & Bernardino, J. (2019). Security mechanisms in the MQTT protocol: A survey. Proceedings of the International Conference on Information Technology & Systems, 121–131. https://doi.org/10.1007/978-3-030-35962-1_13

Sefidian, A., Rezazadeh, J., & Farahbakhsh, R. (2023). Time synchronisation challenges in IoT forensics. Journal of Information Security and Applications, 70, 103295. https://doi.org/10.1016/j.jisa.2022.103295

Servida, A., & Casey, E. (2019). A framework for trustworthy IoT forensics. Digital Investigation, 28, S109–S117. https://doi.org/10.1016/j.diin.2019.01.016

Sicari, S., Rizzardi, A., & Cappiello, C. (2021). Towards forensic-ready IoT: A privacy-oriented architecture for smart homes. Sensors, 21(17), 5759. https://doi.org/10.3390/s21175759

Singh, R., Jain, V., & Goel, S. (2022). Comparative analysis of file systems and forensic challenges in IoT. Journal of Digital Forensics, Security and Law, 17(1), 1–15. https://doi.org/10.15394/jdfsl.2022.1872

Statista. (2022). Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025. https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/

Stoyanova, M., Nikoloudakis, Y., Panagiotakis, S., Pallis, E., & Markakis, E. K. (2020). A survey on the Internet of Things (IoT) forensics: Challenges, approaches, and open issues. IEEE Communications Surveys & Tutorials, 22(2), 1191–1221. https://doi.org/10.1109/COMST.2020.2973311

Sun, M., Tang, Y., Fu, S., & Zhang, M. (2018). A universal cyber-physical systems framework: Specification, modelling, verification. In 2018 IEEE International Conference on Smart Cloud (SmartCloud) (pp. 133–138). IEEE. https://doi.org/10.1109/SmartCloud.2018.00030

Tawalbeh, L. A., Muheidat, F., Tawalbeh, M., & Quwaider, M. (2020). IoT privacy and security: Challenges and solutions. Applied Sciences, 10(12), 4102. https://doi.org/10.3390/app10124102

Ullah, I., Mehmood, M., & Habib, M. A. (2022). IoT forensics: A comprehensive review of recent developments and future directions. Journal of Network and Computer Applications, 201, 103313. https://doi.org/10.1016/j.jnca.2022.103313

Watson, S., & Dehghantanha, A. (2016). Digital forensics: The missing piece of the Internet of Things promise. Computer Fraud & Security, 2016(6), 5–8. https://doi.org/10.1016/S1361-3723(16)30056-4

Yaqoob, I., Hashem, I. A. T., Ahmed, A., Kazmi, S. A., & Hong, C. S. (2019). Internet of things forensics: Recent advances, taxonomy, requirements, and open challenges. Future Generation Computer Systems, 92, 265–275. https://doi.org/10.1016/j.future.2018.09.058

Zawoad, S., & Hasan, R. (2015). FAIoT: Towards building a forensics-aware ecosystem for the Internet of Things. In 2015 IEEE International Conference on Services Computing (pp. 279–284). IEEE. https://doi.org/10.1109/SCC.2015.47

Zulkipli, N. H. N., Alenezi, A., & Wills, G. B. (2018). IoT forensic: Bridging the challenges in digital forensics and the Internet of Things. In the 2nd International Conference on Internet of Things, Big Data and Security (pp. 315–324). https://doi.org/10.5220/0006684103150324

Appendix

Link to survey questions and responses