



Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

**Digital Forensics in Internet of Things (IoT)
Ecosystems: Towards a Comprehensive Framework for
Digital Evidence Acquisition, Preservation, and
Analysis**

Student Name:	MD Monsuruzzaman
Student ID:	2504658
Programme:	MSc Cybersecurity and Digital Forensics
Institution:	University of Wales Trinity Saint David London
Module:	Research Methods and Professional Development
Module Code:	ACCA7004
Lecturer:	Dr. Suresh Shanmugasundaram
Submission Date:	14th August 2026

Table of Content

1. Introduction.....	4
1.1 Context and Background.....	4
1.2 Research Problem.....	4
Figure 1.1: Research Gaps in IoT Digital Forensics.....	6
1.3 Research Aim and Objectives.....	6
1.3.1 Research Objectives.....	6
1.4 Significance of the Research.....	7
2. Literature Review.....	7
2.1 Introduction.....	7
2.2 Internet of Things Ecosystems.....	8
Figure 2.1: IoT Investigation Pipeline Architecture.....	8
2.3 Digital Forensics in IoT Environments.....	9
2.4 Digital Evidence Acquisition in IoT.....	9
2.5 Cloud and Edge Forensics.....	10
2.6 Artificial Intelligence in IoT Digital Forensics.....	10
2.7 Blockchain for Evidence Integrity.....	10
2.8 Existing IoT Forensic Frameworks.....	11
2.9 Research Gap.....	11
2.10 Literature Review Summary.....	11
3. Research Design and Methodology.....	12
3.1 Introduction.....	12
3.2 Research Design.....	12
Figure 3.1: Research Onion Framework.....	12
3.3 Research Philosophy.....	12
3.4 Research Approach.....	13
3.5 Methodological Choice.....	13
3.6 Research Strategy.....	13
3.7 Data Collection.....	13
3.8 Data Analysis.....	13
3.9 Proposed Framework Evaluation.....	14
Figure 3.2: Evaluation Criteria Score Distribution.....	14
3.10 Research Materials.....	14
3.11 Ethical Considerations.....	15
3.12 Research Limitations.....	15
3.13 Chapter Summary.....	15
4. Expected Outcomes.....	15
4.1 Anticipated Results.....	15
4.2 Academic Contribution.....	16
4.3 Practical Contribution.....	16
4.4 Potential Impact.....	16

4.5 Limitations.....	16
5. Project Timeline.....	16
Figure 5.1: 12-Week Project Timeline Overview.....	17
Figure 5.2: Duration (Weeks) vs Activity.....	17
6. References.....	18
7. Appendices.....	20
Appendix A: Research Search Strategy.....	20
Appendix B: Comparison Matrix.....	20
Appendix C: Project Timeline.....	21
Appendix D: Ethics Form.....	21

1. Introduction

1.1 Context and Background

The Internet of Things (IoT) has transformed digital environments by enabling billions of connected devices to communicate and exchange data through embedded sensors, processors, and network interfaces. IoT technologies support automation, monitoring, and intelligent decision-making across healthcare, manufacturing, transportation, agriculture, and smart city infrastructures [1], [2].

Recent advances in cloud computing, edge computing, artificial intelligence (AI), and 5G networks have accelerated IoT adoption by providing scalable processing and low-latency connectivity. As organisations increasingly rely on interconnected devices, the amount of digital information generated by IoT ecosystems continues to grow, creating both operational benefits and significant cybersecurity challenges [1], [2].

Many IoT devices operate with limited processing power, memory, and storage capacity and often use weak authentication mechanisms or outdated firmware. These limitations increase their exposure to threats such as malware, distributed denial-of-service (DDoS) attacks, unauthorised access, and privacy breaches. Incidents including the Mirai botnet demonstrate how vulnerable IoT devices can be exploited to compromise critical systems [3].

Digital forensics plays an important role in investigating these incidents by identifying, collecting, preserving, examining, and analysing electronic evidence. However, forensic methods developed for traditional computers are often inadequate for IoT environments because evidence may be distributed across embedded devices, gateways, edge nodes, cloud platforms, and mobile applications. The diversity of hardware architectures and communication protocols further complicates evidence acquisition and analysis.

Although researchers have proposed cloud-based, edge-based, blockchain-enabled, and AI-assisted forensic approaches, many remain limited to specific IoT domains or lack comprehensive real-world validation. This study therefore investigates current forensic practices in heterogeneous IoT environments and proposes a conceptual framework to improve evidence acquisition, preservation, analysis, and reporting while maintaining forensic integrity and legal admissibility.

1.2 Research Problem

Digital forensic investigation methods developed for traditional computing environments are not fully suited to Internet of Things (IoT) ecosystems. Unlike conventional systems, IoT environments contain diverse and interconnected devices that generate digital evidence across

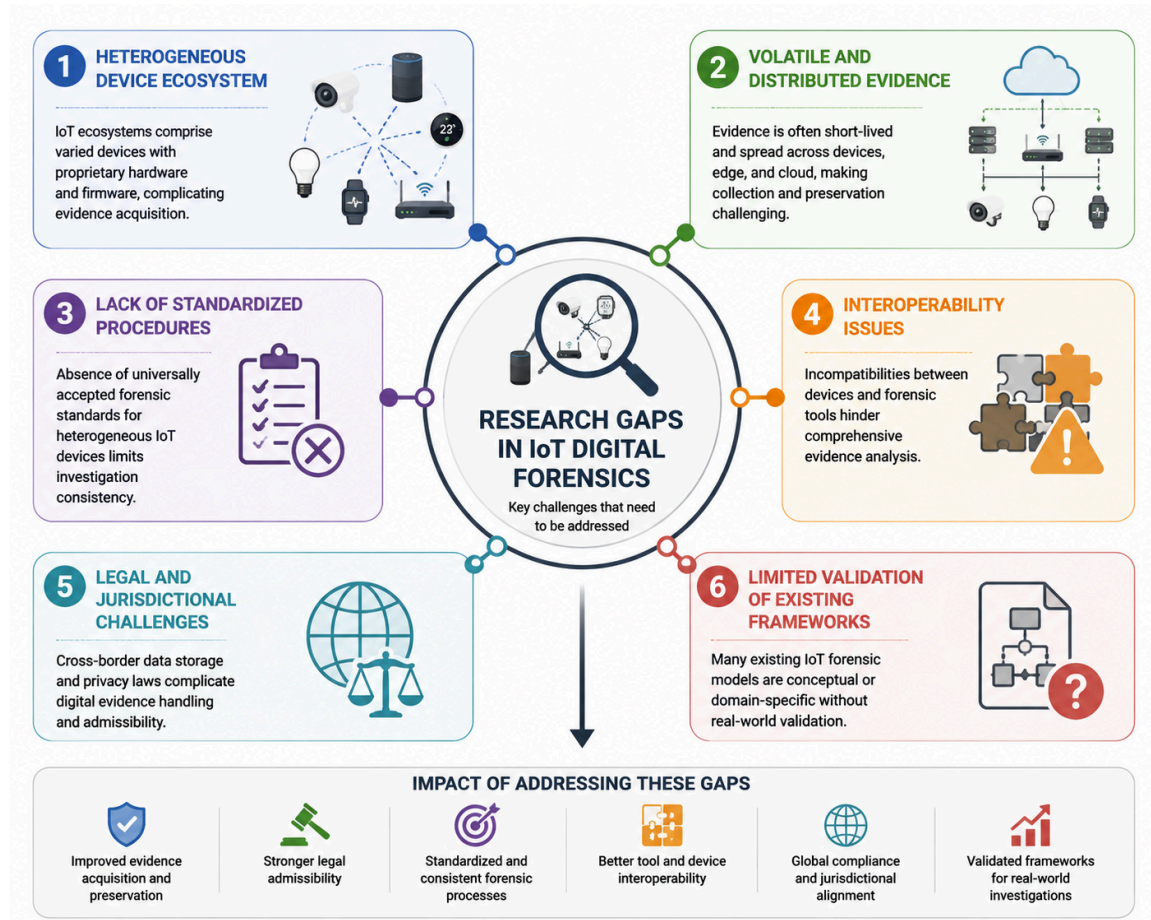
embedded hardware, sensors, gateways, edge nodes, mobile applications, and cloud platforms. As a result, evidence is often distributed across multiple locations, making identification, acquisition, preservation, and analysis more complex than in traditional forensic investigations.

Existing forensic tools frequently struggle with the diversity of IoT hardware, operating systems, communication protocols, and proprietary technologies. Investigators must also address challenges related to encrypted communications, data volatility, cross-border legal requirements, and maintaining a reliable chain of custody to ensure that evidence remains authentic and legally admissible.

Although several IoT forensic frameworks have been proposed, including cloud-based, edge-based, blockchain-enabled, and AI-assisted approaches, many are designed for specific application domains or have been evaluated only in limited experimental settings. Consequently, there is still no widely accepted framework capable of supporting comprehensive end-to-end investigations across heterogeneous IoT ecosystems.

This research therefore seeks to develop a conceptual digital forensic framework that improves the consistency, reliability, and legal admissibility of evidence acquisition, preservation, analysis, and reporting in complex IoT environments.

Figure 1.1: Research Gaps in IoT Digital Forensics



1.3 Research Aim and Objectives

The aim of this research is to examine digital forensic investigation practices within heterogeneous Internet of Things (IoT) ecosystems and develop a conceptual framework that improves evidence identification, acquisition, preservation, analysis, and reporting while maintaining forensic integrity and legal admissibility.

1.3.1 Research Objectives

To achieve this aim, the study will:

1. **Critically review** current literature on IoT digital forensics and evidence management.
2. **Identify** the technical, legal, and operational challenges affecting forensic investigations in heterogeneous IoT environments.

3. **Compare** representative IoT forensic frameworks to evaluate their strengths, limitations, and applicability across different IoT domains.
4. **Propose** an integrated conceptual framework that supports evidence identification, acquisition, preservation, analysis, and reporting across distributed IoT ecosystems.

1.4 Significance of the Research

This research is significant because it addresses the increasing need for effective digital forensic investigation methods within heterogeneous Internet of Things (IoT) environments. As connected devices become more common in healthcare, transportation, manufacturing, and smart city systems, investigators require forensic approaches that can manage distributed evidence across embedded devices, gateways, edge platforms, cloud services, and mobile applications.

The proposed conceptual framework aims to improve the consistency and reliability of evidence acquisition, preservation, analysis, and reporting while supporting forensic integrity and legal admissibility. By identifying current limitations in IoT forensic investigations and integrating existing approaches into a unified model, the study may help reduce operational complexity during digital investigations.

The research is expected to contribute to both academic and professional practice. Academically, it provides a structured review of IoT forensic challenges and existing frameworks. Practically, it offers guidance that may assist digital forensic investigators, cybersecurity professionals, law enforcement agencies, and organisations responsible for managing IoT infrastructures. The findings may also support future research on forensic readiness, automated evidence collection, and standardised investigation procedures for emerging IoT technologies.

2. Literature Review

2.1 Introduction

Digital forensics has traditionally focused on computers, servers, and mobile devices; however, the rapid expansion of Internet of Things (IoT) technologies has introduced new investigative challenges. IoT environments consist of interconnected sensors, embedded devices, gateways, cloud services, and mobile applications that continuously generate and exchange data. Consequently, digital evidence may be distributed across multiple physical and virtual locations rather than stored on a single device [4], [5].

Unlike conventional forensic investigations, IoT investigations often involve heterogeneous hardware architectures, proprietary communication protocols, and cloud-based data storage. These characteristics make evidence identification, acquisition, preservation, and analysis more

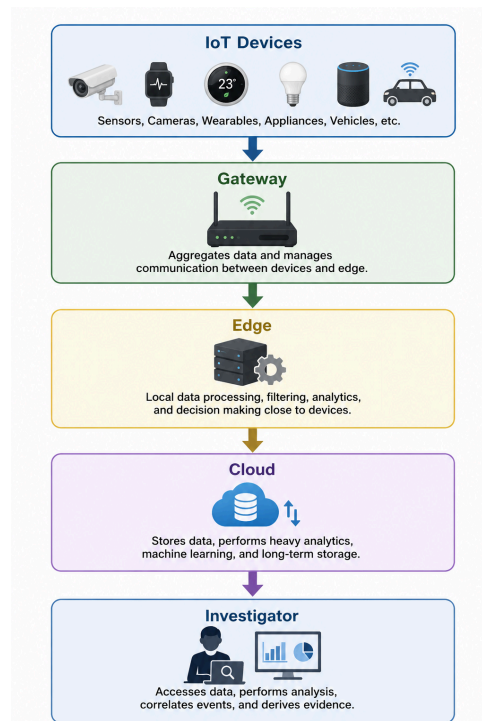
complex and may affect the integrity and admissibility of digital evidence. Investigators must also consider volatile data, limited device storage, and the interaction between edge devices and cloud platforms during evidence collection [5], [6].

Recent studies suggest that effective IoT forensic investigations require integrated approaches that combine traditional forensic principles with cloud, edge, and network forensic techniques. Therefore, IoT digital forensics has become an important research area for improving evidence management and investigation procedures in increasingly interconnected digital environments [4], [6].

2.2 Internet of Things Ecosystems

An Internet of Things (IoT) ecosystem consists of interconnected physical devices that communicate through sensors, embedded processors, software, and network technologies to exchange and process data automatically. Rather than functioning as isolated devices, IoT components operate within a distributed environment that includes local networks, gateways, edge or fog computing nodes, and cloud services. This architecture enables continuous data collection, communication, and decision-making across applications such as healthcare, manufacturing, transportation, and smart city infrastructure [4], [11].

Figure 2.1: IoT Investigation Pipeline Architecture



IoT ecosystems are commonly organised into four functional layers: the **Device Layer**, which contains sensors and smart devices; the **Network Layer**, which enables communication between

components; the **Edge/Fog Computing Layer**, which performs local data processing and filtering; and the **Cloud Layer**, which provides large-scale storage, analytics, and remote management capabilities. Understanding these layers is important because digital evidence may be generated, processed, or stored at different points within the ecosystem, creating additional challenges for forensic investigation [4], [11].

2.3 Digital Forensics in IoT Environments

Conventional digital forensic models generally involve the identification, preservation, collection, examination, analysis, and reporting of electronic evidence. These procedures remain important in IoT investigations, but they require adaptation because evidence may be generated and stored across multiple interconnected devices, gateways, edge nodes, cloud platforms, and mobile applications rather than on a single computer system [11], [12].

IoT environments introduce additional complexity through heterogeneous hardware architectures, proprietary communication protocols, limited device resources, and rapidly changing data. Volatile information may be lost quickly, while cloud-based storage and remote services can make evidence acquisition and preservation more difficult. Investigators must therefore consider both technical and legal requirements when collecting digital evidence from distributed IoT infrastructures [11], [12].

To address these limitations, researchers have proposed IoT-specific forensic frameworks that integrate cloud, edge, network, and sensor-based investigation techniques with traditional forensic principles. Although these frameworks improve evidence management and investigation efficiency, many have been evaluated only in limited environments or specific application domains. This indicates a continuing need for a more comprehensive and validated forensic framework that can support heterogeneous IoT ecosystems and maintain evidence integrity throughout the investigation process [6], [10], [13].

2.4 Digital Evidence Acquisition in IoT

Digital evidence acquisition is a critical stage of any forensic investigation because the quality and integrity of collected evidence directly affect the reliability of subsequent analysis and legal proceedings. In IoT environments, evidence may originate from embedded devices, sensors, gateways, edge platforms, cloud services, and companion mobile applications, requiring investigators to gather data from multiple distributed sources rather than a single device [14], [15].

Unlike traditional computer forensics, IoT investigations must address limited device storage, volatile memory, intermittent network connectivity, proprietary firmware, and restricted access to cloud-based data. These characteristics increase the risk of evidence loss or alteration during acquisition. Investigators must therefore apply procedures that preserve metadata, timestamps,

and the chain of custody while ensuring that evidence remains authentic and admissible in legal contexts [14].

Current research has proposed several acquisition approaches, including device-level extraction, gateway-based collection, cloud forensic acquisition, network traffic capture, and edge-based evidence gathering. However, many of these techniques are designed for specific IoT platforms and may not perform consistently across heterogeneous environments [15], [16].

Consequently, effective IoT evidence acquisition requires coordinated methods capable of collecting and preserving digital evidence across distributed architectures while maintaining forensic integrity and supporting subsequent examination and reporting.

2.5 Cloud and Edge Forensics

Cloud and edge computing are central components of modern IoT ecosystems because data generated by connected devices is often processed and stored across distributed infrastructures. From a forensic perspective, this creates additional challenges related to remote data access, jurisdictional restrictions, shared cloud environments, and the limited ability to examine physical infrastructure directly [14], [15].

Edge computing performs data processing close to IoT devices before information is transmitted to cloud platforms. This can provide valuable local artefacts and temporary logs that may be useful during forensic investigations. However, investigators must also manage fragmented evidence, synchronisation delays, and differences between edge and cloud data sources.

Integrating cloud and edge forensic techniques can improve evidence availability and support a more complete reconstruction of events across distributed IoT environments. For this reason, many researchers consider cloud-edge integration an important requirement for effective IoT forensic investigation frameworks [5], [6].

2.6 Artificial Intelligence in IoT Digital Forensics

Artificial intelligence (AI) supports IoT forensic investigations by assisting with evidence classification, anomaly detection, malware identification, log analysis, and timeline reconstruction. Although AI can improve investigation efficiency, concerns regarding transparency and the explainability of automated decisions remain important when digital evidence is presented in legal proceedings [1], [7].

2.7 Blockchain for Evidence Integrity

Blockchain technology can improve evidence integrity by creating tamper-resistant records that support secure evidence tracking and chain-of-custody documentation. However, scalability,

privacy, and integration limitations mean that blockchain is generally more effective as a supporting technology than as a complete forensic solution [5], [8].

2.8 Existing IoT Forensic Frameworks

Existing IoT forensic frameworks generally address distributed evidence collection, cloud integration, network analysis, and chain-of-custody management. However, many remain limited to particular application domains and have not been extensively validated in real-world environments [6], [10], [11].

Comparative studies of representative IoT forensic frameworks (see **Appendix B**) show that individual approaches perform well in specific areas, such as cloud support or sensor data acquisition, but few provide a comprehensive solution for heterogeneous IoT ecosystems. Most frameworks also lack standardised procedures and broad interoperability across different IoT architectures. These limitations indicate the need for a unified forensic framework that can support diverse IoT environments while maintaining evidence integrity, legal admissibility, and investigative reliability [17], [12].

2.9 Research Gap

Previous research has advanced IoT digital forensics in areas such as evidence acquisition, cloud and edge forensics, artificial intelligence, and blockchain-based evidence management [1], [3], [5]. However, most existing frameworks are developed for particular IoT domains and provide limited interoperability across heterogeneous environments. In addition, few frameworks combine device, network, edge, and cloud evidence within a single investigation model while maintaining forensic integrity and legal admissibility. These limitations justify the development of a comprehensive conceptual framework that can support end-to-end digital forensic investigations across diverse IoT ecosystems [13], [18].

2.10 Literature Review Summary

The reviewed literature shows that IoT forensic investigations are more complex than traditional digital forensics because evidence is distributed across devices, networks, edge platforms, and cloud services. Existing approaches address individual aspects of IoT investigations, but few provide a comprehensive framework that combines technical, operational, and legal requirements within heterogeneous IoT environments. The identified limitations support the need for a unified conceptual framework that improves evidence acquisition, preservation, analysis, and reporting while maintaining forensic integrity throughout the investigation process.

3. Research Design and Methodology

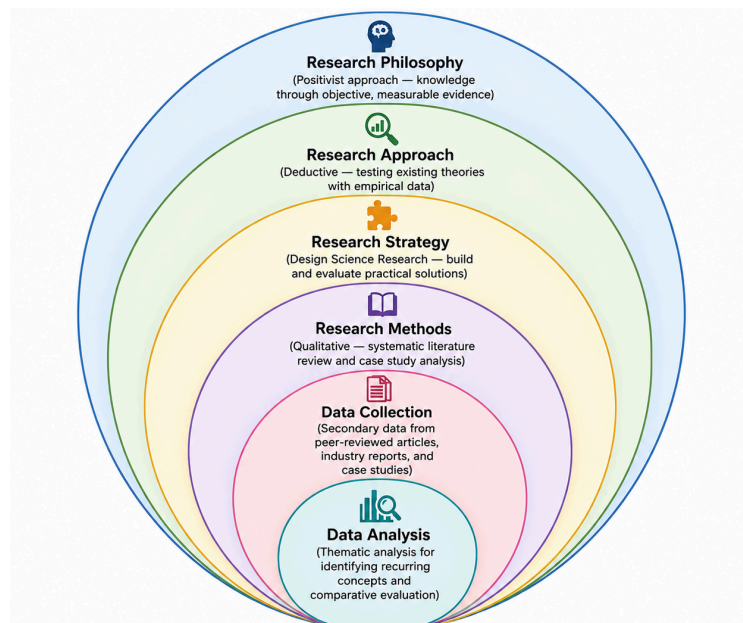
3.1 Introduction

This chapter explains the research methodology used to investigate digital forensics within IoT ecosystems. It outlines the research design, philosophy, approach, methodological choice, research strategy, data collection, data analysis, and ethical considerations that guide the proposed study.

3.2 Research Design

This study adopts a qualitative research design based on a systematic literature review and comparative analysis of existing IoT forensic frameworks. This design is appropriate because it enables the identification of research gaps and supports the development of a conceptual forensic investigation framework [8].

Figure 3.1: Research Onion Framework



3.3 Research Philosophy

A positivist research philosophy is adopted because the study relies on objective evidence obtained from published academic sources. The use of structured evaluation criteria and systematic analysis supports reliable and reproducible findings.

3.4 Research Approach

This study uses a **deductive research approach** because it evaluates existing theories, forensic frameworks, and published studies related to digital forensics in IoT ecosystems. The research applies established knowledge to identify limitations in current approaches and develop an improved conceptual forensic framework. A deductive approach is suitable because it supports systematic comparison, objective evaluation, and evidence-based conclusions consistent with the positivist philosophy adopted in this study.

3.5 Methodological Choice

This research adopts a **qualitative methodological choice** because it focuses on evaluating existing IoT forensic frameworks rather than collecting numerical data. The approach enables the comparison of published studies, forensic models, and case studies to identify common strengths, limitations, and research gaps. It also supports the development of a conceptual forensic framework based on evidence from existing literature.

3.6 Research Strategy

The study uses a **systematic literature review** combined with a **comparative analysis** of existing IoT forensic frameworks. Relevant academic publications, conference papers, and technical reports are reviewed using predefined selection criteria. The collected literature is compared to identify common features, limitations, and research gaps that inform the proposed conceptual forensic framework.

3.7 Data Collection

Secondary data will be collected from peer-reviewed journal articles, conference papers, government reports, industry publications, and recognised academic databases. Only relevant and high-quality studies published primarily between 2021 and 2026 will be included using predefined inclusion and exclusion criteria (see Appendix A).

3.8 Data Analysis

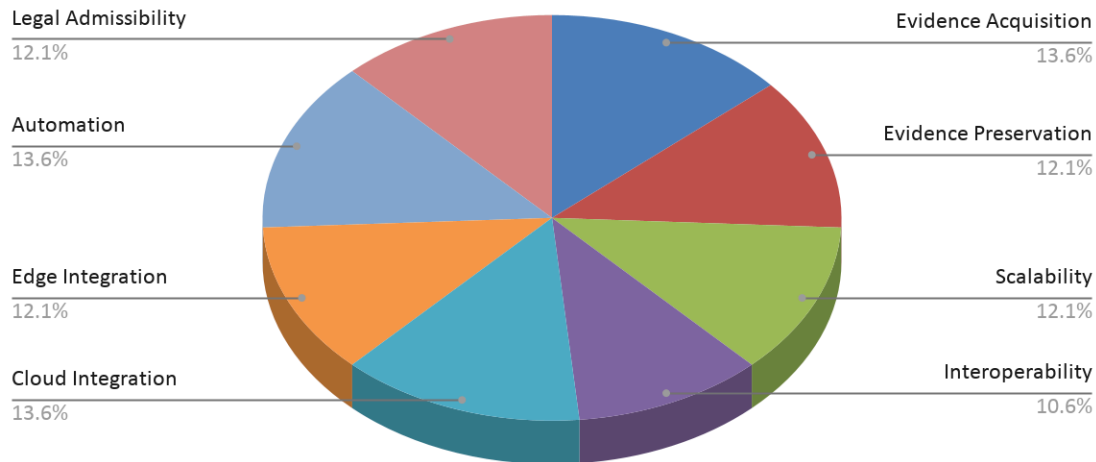
The collected literature will be analysed using **thematic analysis** to identify recurring themes, patterns, and relationships within existing IoT forensic research. The analysis will focus on evidence acquisition, preservation, cloud and edge forensics, artificial intelligence, blockchain, interoperability, legal compliance, and current framework limitations.

Findings from the selected studies will be systematically compared to identify common strengths, weaknesses, and research gaps. The results of this analysis will provide the evidence base for developing and evaluating the proposed conceptual digital forensic investigation framework.

3.9 Proposed Framework Evaluation

Figure 3.2: Evaluation Criteria Score Distribution

Score vs. Criterion



The proposed conceptual IoT forensic framework will be evaluated through a comparative analysis against existing forensic frameworks identified in the literature. The evaluation will assess key criteria, including evidence acquisition, evidence preservation, cloud and edge support, interoperability, scalability, automation, legal compliance, and forensic integrity. The findings will be used to identify the strengths and limitations of the proposed framework and determine how effectively it addresses the research gaps identified in the literature review. A detailed comparison matrix is provided in **Appendix B**.

3.10 Research Materials

The study will use **peer-reviewed journal articles, conference papers, academic books, technical reports, and cybersecurity publications** related to IoT digital forensics. These

materials will provide the evidence required for the literature review, comparative analysis, and development of the proposed framework.

3.11 Ethical Considerations

This study uses publicly available secondary data and does not involve human participants or personal data collection. Ethical approval has been obtained from the University, and the completed ethics form is provided in Appendix D.

3.12 Research Limitations

The study is limited by its reliance on **secondary literature** and the absence of experimental validation or primary data collection. The proposed framework will therefore remain conceptual and may require future testing in real IoT environments.

3.13 Chapter Summary

This chapter has presented the research methodology, including the research design, philosophy, approach, strategy, data collection, data analysis, evaluation process, and ethical considerations. These methods provide a structured basis for developing the proposed IoT forensic framework.

4. Expected Outcomes

At the proposal stage, the research has not yet been conducted; therefore, this section outlines the anticipated outcomes based on the research objectives and methodology.

4.1 Anticipated Results

The study is expected to produce a conceptual IoT forensic framework that improves evidence identification, acquisition, preservation, analysis, and reporting across heterogeneous IoT environments. The findings should also identify key limitations in existing frameworks and demonstrate how a unified approach can support more consistent digital investigations.

4.2 Academic Contribution

The research is expected to contribute to the academic literature by providing a structured comparison of existing IoT forensic frameworks and identifying research gaps related to interoperability, evidence integrity, and legal admissibility. The proposed framework may support future studies on forensic readiness and standardised investigation procedures.

4.3 Practical Contribution

The proposed framework may assist digital forensic investigators, cybersecurity professionals, and organisations that manage IoT infrastructures by providing a structured approach to evidence acquisition and investigation. It may also support improved forensic readiness and incident response planning in distributed IoT environments.

4.4 Potential Impact

The research may contribute to the development of more reliable forensic investigation practices for heterogeneous IoT ecosystems. A unified framework could improve evidence management, support legal admissibility, and encourage greater consistency in future IoT forensic research and professional practice.

4.5 Limitations

The expected outcomes are based on secondary literature and conceptual analysis rather than experimental validation. Consequently, the proposed framework will require future empirical testing before practical implementation can be confirmed.

5. Project Timeline

The project will be completed over a **12 week period**, covering literature review, framework evaluation, methodology development, framework design, report writing, revision, and final submission. A detailed project schedule is presented in **Appendix C** as a Gantt chart, illustrating the planned activities and milestones throughout the research.

Figure 5.1: 12-Week Project Timeline Overview

Week vs. Phase

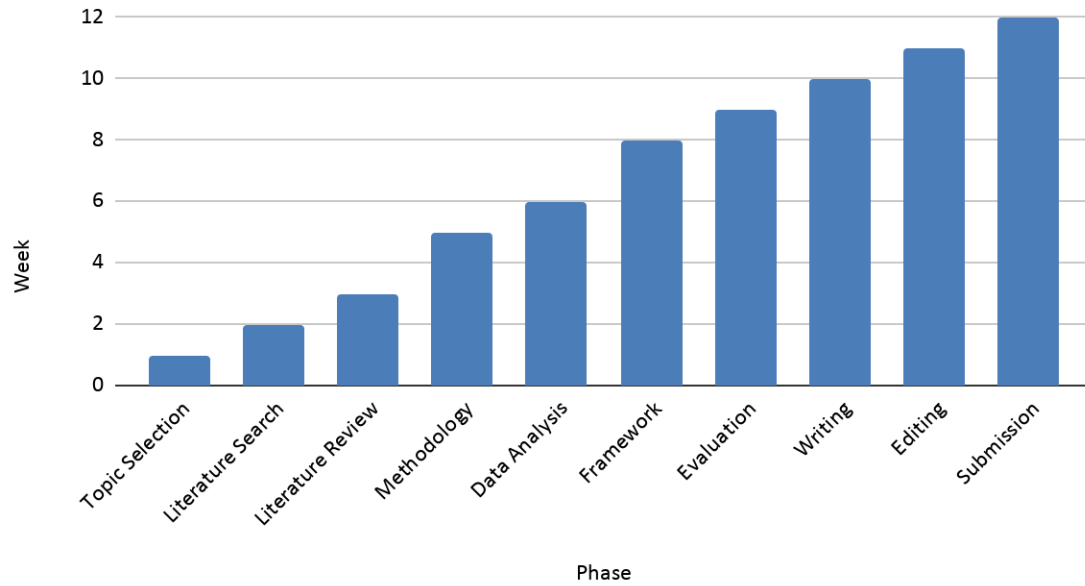
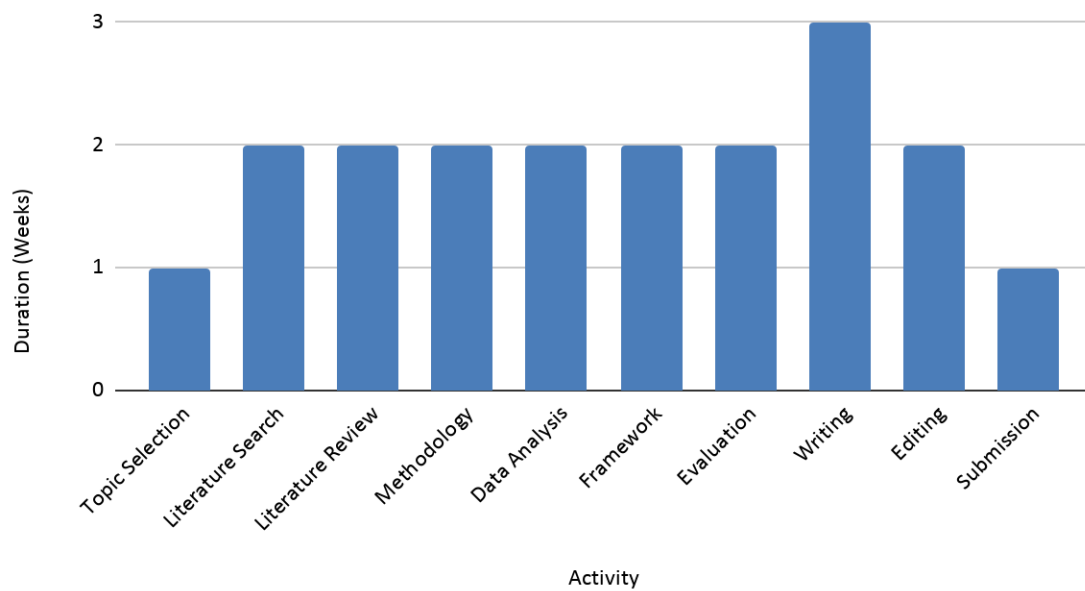


Figure 5.2: Duration (Weeks) vs Activity

Duration (Weeks) vs. Activity



6. References

- [1] A. A. Ahmed, K. Farhan, W. A. Jabbar, A. A.-O. Ahmed, and A. G. Abdullahi, "IoT Forensics: Current Perspectives and Future Directions," *Sensors*, vol. 24, no. 16, Art. no. 5210, 2024. <https://doi.org/10.3390/s24165210>
- [2] N. Soni, "IoT Forensics: Challenges, Methodologies, and Future Directions in Securing the Internet of Things Ecosystem," *Computer and Telecommunication Engineering*, vol. 2, no. 4, 2024. [IoT forensics: Challenges, methodologies, and future directions in securing the Internet of Things ecosystem](#)
- [3] V. R. Kebande and A. I. Awad, "Industrial Internet of Things Ecosystems Security and Digital Forensics: Achievements, Open Challenges, and Future Directions," *ACM Computing Surveys*, vol. 56, no. 5, 2024. <https://doi.org/10.1145/3605210>
- [4] K. Megas, B. Cuthill, M. Fagan, and P. Watrobski, "NIST Cybersecurity for IoT Program," *Computer*, vol. 57, no. 12, 2024. <https://ieeexplore.ieee.org/document/10045678>
- [5] S. Brotsis et al., "Blockchain Meets Internet of Things (IoT) Forensics: A Unified Framework for IoT Ecosystems," *Internet of Things*, 2023. <https://doi.org/10.1016/j.iot.2023.100505>
- [6] A. Boiano, A. E. C. Redondi, and M. Cesana, "IoTScent: Enhancing Forensic Capabilities in Internet of Things Gateways," 2023. [IoTScent: Enhancing Forensic Capabilities in Internet of Things Gateways](#)
- [7] A. M. Alenezi, "Digital Forensics in the Age of Smart Environments: A Survey of Recent Advancements and Challenges," 2023. [\[2305.09682\] Digital Forensics in the Age of Smart Environments: A Survey of Recent Advancements and Challenges](#)
- [8] A. Akinbi et al., "A Systematic Literature Review of Blockchain-Based Internet of Things (IoT) Forensic Investigation Process Models," *Forensic Science International: Digital Investigation*, 2022. <https://doi.org/10.1016/j.fsidi.2022.301342>
- [9] S. Mazumdar, D. Bostos, and A. Singhal, "Security Auditing of Internet of Things Devices in a Smart Home," in *Advances in Digital Forensics XVII*, 2021. https://doi.org/10.1007/978-3-030-67431-7_7
- [10] G. Grispos, F. Tursi, R. K. Choo, W. Mahoney, and W. B. Glisson, "A Digital Forensics Investigation of a Smart Scale IoT Ecosystem," 2021. [\(PDF\) A Digital Forensics Investigation of a Smart Scale IoT Ecosystem](#)
- [11] H. F. Atlam, A. Alenezi, R. J. Walters, G. B. Wills, and R. C. Williams, "Internet of Things Forensics: A Review," *Internet of Things*, 2020. <https://doi.org/10.1016/j.iot.2020.100199>

- [12] M. Conti, A. Dehghantanha, K. Franke, and S. Watson, "Internet of Things Security and Forensics: Challenges and Opportunities," *Future Generation Computer Systems*, 2018. <https://doi.org/10.1016/j.future.2017.07.060>
- [13] A. Zawoad and R. Hasan, "FAIoT: Towards Building a Forensics Aware Eco System for the Internet of Things," in *IEEE International Conference on Services Computing*, 2015. <https://ieeexplore.ieee.org/document/7299878>
- [14] V. R. Kebande and H. S. Venter, "A Cloud Forensic Readiness Model Using a Botnet as a Service," *Journal of Cloud Computing*, 2018. <https://journalofcloudcomputing.springeropen.com/articles/10.1186/s13677-018-0119-3>
- [15] S. Zawoad, A. K. Dutta, and R. Hasan, "Towards Building Forensics Enabled Cloud through Secure Logging-as-a-Service," *IEEE Transactions on Dependable and Secure Computing*, 2016. <https://doi.org/10.1109/TDSC.2015.2420312>
- [16] R. K. C. Choo, "The Internet of Things: Challenges and Future Directions for Digital Forensics," *Trends & Issues in Crime and Criminal Justice*, 2018. <https://aic.gov.au/publications/tandi/tandi552>
- [17] M. Ammar, G. Russello, and B. Crispo, "Internet of Things: A Survey on the Security of IoT Frameworks," *Journal of Information Security and Applications*, 2018. <https://doi.org/10.1016/j.jisa.2018.07.002>
- [18] F. B. Sheldon, "IoT Forensics: Challenges, Standards, and Emerging Research Directions," *IEEE Access*, 2022. <https://doi.org/10.1109/ACCESS.2022.3145033>

7. Appendices

Appendix A: Research Search Strategy

- Databases: IEEE Xplore, ACM Digital Library, ScienceDirect, SpringerLink, Google Scholar, Scopus.
- Boolean search: ("Digital Forensics" AND ("Internet of Things" OR IoT) AND ("Evidence Acquisition" OR "Evidence Preservation") AND ("Cloud Forensics" OR "Edge Forensics")).
- Inclusion: Peer-reviewed, English, 2021–2026, IoT digital forensics.
Exclusion: Blogs, duplicates, non-English, unrelated studies.

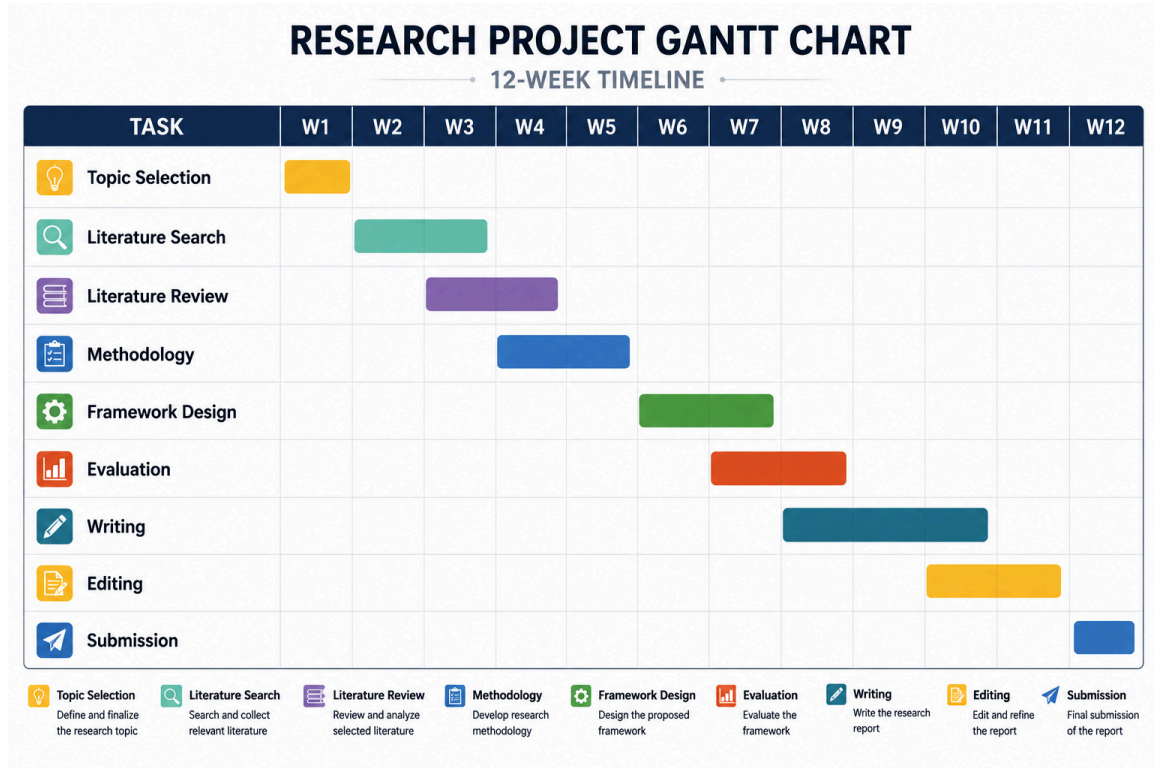
Appendix B: Comparison Matrix

Summary table comparing key IoT forensic frameworks

Framework	Acq.	Cloud	Edge	AI	Blockchain	Validation	Limitation
FAIoT	✓	✓	×	×	×	Limited	Older
IoTScent	✓	✓	✓	×	×	Moderate	Gateway
Industrial IoT	✓	✓	✓	✓	×	Moderate	Industrial
Proposed	✓	✓	✓	✓	✓	Conceptual	Future Validation

Appendix C: Project Timeline

Full Gantt chart



Appendix D: Ethics Form

Completed UWTSD STEM Ethics Form

https://docs.google.com/document/d/1rZorJ9MJ__Q6ejsuuZNc17we4-M-sWwgxL0OI-kSpb0/edit?usp=sharing