ADVANCE DIGITAL FORENSIC INVESTIGATION TOOL FOR IOT DEVICE

A PROJECT REPORT

Bachelor Of Technology

in

COMPUTER ENGINEERING

Major Project I (01CE0716)

Submitted by

HITEKSHA THAKER

92310103102

JEET JOSHI

92310103088

Faculty of Engineering & Technology

Marwadi University, Rajkot

August, 2025

Major Project I (01CE0716)

Department of Computer Engineering

Faculty of Engineering & Technology

Marwadi University

A.Y. 2025-26

CERTIFICATE

This is to certify that the project report submitted along with the project entitled **Advance Digital Forensic Investigation Tool For Iot Device** has been carried out by **Hiteksha Thaker (92310103102)** and **Jeet Joshi (92310103088)** under my guidance in partial fulfilment for the degree of Bachelor of Technology in Computer Engineering, 7th Semester of Marwadi University, Rajkot during the academic year 2025-26.

Prof. Hansa Vaghela	Dr. Krunal Vaghela
Assistant Professor	Professor & Head
Department of Computer Engineering	Department of Computer Engineering

Major Project I (01CE0716)

Department of Computer Engineering

Faculty of Engineering & Technology

Marwadi University

A.Y. 2025-26

CERTIFICATE

This is to certify that the project report submitted along with the project entitled **Advance Digital Forensic Investigation Tool For Iot Device** has been carried out by **Hiteksha Thaker (92310103102)** under my guidance in partial fulfilment for the degree of Bachelor of Technology in Computer Engineering, 7th Semester of Marwadi University, Rajkot during the academic year 2025-26.

Prof. Hansa Vaghela	Dr. Krunal Vaghela
Assistant Professor	Professor & Head
Department of Computer Engineering	Department of Computer Engineering

Major Project I (01CE0716)

Department of Computer Engineering

Faculty of Engineering & Technology

Marwadi University

A.Y. 2025-26

CERTIFICATE

This is to certify that the project report submitted along with the project entitled **Advance Digital Forensic Investigation Tool For Iot Device** has been carried out by **Jeet Joshi (92310103088)** under my guidance in partial fulfilment for the degree of Bachelor of Technology in Computer Engineering, 7th Semester of Marwadi University, Rajkot during the academic year 2025-26.

Prof. Hansa Vaghela	Dr. Krunal Vaghela
Assistant Professor	Professor & Head
Department of Computer Engineering	Department of Computer Engineering

Major Project (01CE0716)

Department of Computer Engineering

Faculty of Engineering & Technology

Marwadi University

A.Y. 2025-26

DECLARATION

We hereby declare that the **Major Project-I (01CE0716)** report submitted along with the Project entitled **Advance Digital Forensic Investigation Tool For Iot Device** submitted in partial fulfilment for the degree of Bachelor of Technology in Computer Engineering to Marwadi University, Rajkot, is a bonafide record of original project work carried out by me / us at Marwadi University under the supervision of **Prof. Hansa Vaghela** and that no part of this report has been directly copied from any students' reports or taken from any other source, without providing due reference.

S.No	Student Name	Sign
1	Hiteksha Bhargav Thaker hiteksha.thaker123652@marwadiuniversity.ac.in	
2	Jeet Joshi jeet.joshi123504@marwadiuniversity.ac.in	

ACKNOWLEDGEMENT

I would like to express my sincere gratitude to Marwadi University for providing me with the opportunity to work on the project titled “Advance digital forensic investigation tool for iot device” as a part of my academic curriculum. First and foremost, I am deeply thankful to my project guide, Prof. Hansa Vaghela, for her continuous support, expert guidance, valuable feedback, and encouragement throughout the development of this project. Her insights and experience were instrumental in shaping the direction and outcome of this work. I extend my heartfelt thanks to Dr. Krunal Vaghela, Professor & Head, Department of Computer Engineering, for his unwavering support, motivation, and for creating a research-friendly environment that enabled me to explore and learn beyond the classroom. I am also grateful to all the faculty members and staff of the Department of Computer Engineering for their guidance and encouragement during various phases of the project.

ABSTRACT

The sudden explosion of Internet of Things (IoT) devices particularly in today's homes has brought forth essential challenges around data security, digital privacy, and forensic traceability. Of all the devices, smart thermostats are particularly noted because they engage perpetually with user activity, environmental information, and remote access, which makes them vulnerable to cyberattacks and malicious access. This study introduces an "Advanced Digital Forensic Investigation Tool for IoT Devices" with a special focus on smart thermostats, to tackle these new issues. The proposed tool is a modular, lightweight, and privacy-aware forensic framework for secure data acquisition, real-time monitoring, and intelligent evidence analysis. It combines the process of encrypted communication, anti-forensic resistance, and machine learning-based anomaly detection with captured data to ensure authenticity and integrity. The structuring of the tool is done to seamlessly operate within resource-constrained IoT settings and is cross-platform compatible for forensic investigators and security analysts. This paper presents a new solution that, in addition to enabling post-incident forensics, enables proactive forensic preparedness in IoT environments. The instrument enables legal admissibility of cyber evidence, meets privacy laws, and is easily extendible to many other IoT architectures beyond thermostats. Through the use of secure protocols, automated forensic capability, and modularity, this study fills the current gap between traditional forensics and the ongoing needs of intelligent environments.

LIST OF FIGURES

LIST OF TABLES

ABBREVIATIONS

- **AI** – Artificial Intelligence
- **API** – Application Programming Interface
- **CFT** – Computer Forensic Tool
- **DFRWS** – Digital Forensic Research Workshop
- **DFT** – Digital Forensic Tool
- **ECC** – Elliptic Curve Cryptography
- **FTK** – Forensic Toolkit
- **GDPR** – General Data Protection Regulation
- **HIPAA** – Health Insurance Portability and Accountability Act
- **IoT** – Internet of Things
- **JSON** – JavaScript Object Notation
- **KNN** – K-Nearest Neighbors
- **ML** – Machine Learning
- **NIST** – National Institute of Standards and Technology
- **RF** – Random Forest
- **SMTP** – Simple Mail Transfer Protocol
- **SMS** – Short Message Service
- **SVM** – Support Vector Machine
- **UFED** – Universal Forensic Extraction Device
- **UAFM** – Unified Approach Forensic Model
- **XRY** – Micro Systemation's Forensic Tool for Mobile Devices

TABLE OF CONTENTS

CHAPTER 1

INTRODUCTION

1.1 PROJECT SUMMARY

The project titled *"Advance Digital Forensic Investigation Tool for IoT Device"* focuses on addressing the growing security, privacy, and forensic challenges associated with Internet of Things (IoT) environments, with smart thermostats taken as a principal case study. With the exponential rise of IoT devices in homes, healthcare, transportation, and industries, traditional forensic frameworks often fall short in handling the heterogeneity, limited computational resources, large-scale connectivity, and real-time operational requirements of these systems. Conventional tools are primarily designed for desktops, mobile devices, or enterprise systems, and thus lack adaptability to IoT ecosystems where data is continuous, distributed, and highly sensitive. To bridge this gap, the proposed forensic tool integrates secure evidence acquisition, anomaly detection, forensic analysis, live alert mechanisms, and automated reporting into a unified, modular framework. The tool captures thermostat-specific data such as temperature history, user interactions, schedules, and network traffic, and preserves them in tamper-proof JSON logs to maintain evidence integrity. It leverages the Isolation Forest algorithm, an unsupervised machine learning technique, to detect anomalies in real time, thereby enabling the identification of suspicious behaviors, unauthorized access attempts, or malicious interventions. Forensic readiness is further enhanced through live SMS and email alerts delivered via Twilio and SMTP, while investigators benefit from detailed forensic reports and visual timelines generated using Python's data visualization libraries, which provide an intuitive understanding of activity trends and anomalies.

The novelty of this research lies in its adaptation of forensic methodologies for IoT environments**,** its lightweight and resource-efficient design suitable for constrained devices, and its incorporation of unsupervised anomaly detection for proactive security monitoring. Additionally, the system ensures chain-of-custody compliance, ensuring that collected evidence remains verifiable and legally admissible in judicial contexts. The modular architecture also guarantees scalability and adaptability across domains, making it suitable not only for smart homes but also for healthcare devices, industrial IoT, and critical infrastructure monitoring.

1.1 PROJECT SUMMARY

The research aim is to develop an intelligent, real-time forensic framework that enhances investigative efficiency in IoT ecosystems. The research questions driving this work include: *How can forensic readiness be achieved in IoT systems with limited resources? What methods can ensure secure evidence acquisition and preservation in heterogeneous environments?* The objectives include building a tool that provides real-time monitoring, automated reporting, secure data handling, and adaptability across multiple IoT domains.

The contribution of this work is twofold: practically, it demonstrates an implementable tool that strengthens IoT forensic investigation capability, and academically, it expands the literature by proposing a structured framework that combines lightweight design, anomaly detection, and real-time alerting. By combining real-time monitoring with automated forensic reporting, this tool significantly contributes to the advancement of IoT forensics, helping investigators and organizations strengthen resilience against cyberattacks, protect privacy, and ensure evidence integrity for legal and regulatory compliance**.**

1.2 PROBLEM STATEMENT

The exponential growth of Internet of Things (IoT) devices has introduced significant challenges in the field of digital forensics due to their heterogeneous architectures, limited computational resources, and constant real-time data generation. Traditional forensic tools, which were primarily designed for desktop computers and mobile devices, are inadequate for IoT environments where data is distributed across cloud platforms, lightweight protocols are used, and devices often operate under strict energy and memory constraints. This mismatch creates serious gaps in evidence acquisition, anomaly detection, and forensic readiness.

IoT devices, such as smart thermostats, healthcare monitors, industrial sensors, and home automation systems, are increasingly vulnerable to unauthorized access, malware infiltration, remote tampering, and privacy breaches, which can directly compromise user safety, organizational trust, and even critical infrastructure. Existing forensic methodologies often fail to ensure real-time anomaly detection, proactive alerting, and tamper-proof evidence collection, resulting in delayed investigations, unreliable findings, and challenges in maintaining chain-of-custody.

Furthermore, the lack of integrated forensic solutions that combine machine learning–based anomaly detection, automated reporting, and live alerting mechanisms makes IoT environments even more difficult to investigate. Investigators face obstacles not only in data extraction and validation but also in legal admissibility, since evidence integrity can be easily challenged if tampering or delays occur. In addition, anti-forensic techniques such as log wiping, encryption, and obfuscation exacerbate these difficulties, leaving investigators without credible evidence.

Therefore, there is an urgent need to develop an Advanced Digital Forensic Investigation Tool for IoT Devices that ensures secure evidence acquisition, supports real-time anomaly detection using intelligent algorithms, maintains forensic soundness and chain-of-custody, and provides investigators with proactive alerts and comprehensive reports. Such a solution would bridge the gap between current limitations and the growing demand for forensic-ready IoT ecosystems, enabling faster response to cyber incidents, ensuring evidence reliability in legal proceedings, and strengthening the resilience of IoT-based infrastructures.

1.3 OBJECTIVE

The primary objectives of the project *"Advance Digital Forensic Investigation Tool for IoT Device"* are:

- To design and implement a **lightweight forensic tool** specifically tailored for IoT devices, focusing on smart thermostats as a case study.
- To enable **secure evidence acquisition** by collecting logs related to temperature history, user interactions, schedules, and network traffic in a **tamper-proof format**.
- To **detect anomalies in real time** using machine learning techniques (Isolation Forest) for identifying unauthorized access or abnormal activities.
- To integrate **automated alerting mechanisms** via SMS and email to ensure timely forensic response.
- To generate **detailed forensic reports and visual timelines** to support investigators in legal and organizational contexts.
- To ensure **scalability and adaptability** so the framework can be extended to other IoT domains such as smart homes, healthcare, and industrial systems.
- To maintain **chain of custody** through structured storage and evidence management, ensuring the collected data remains legally admissible.
- To provide a **user-friendly interface** that allows investigators to visualize forensic evidence and anomaly trends clearly.
- To demonstrate **cross-platform compatibility**, making the forensic tool deployable across multiple IoT ecosystems with minimal modifications.
- To enhance **forensic readiness** by enabling proactive monitoring rather than only post-incident investigation.
- To compare the tool's **effectiveness and accuracy** against existing forensic approaches to highlight improvements in IoT evidence handling.

1.4 SCOPE

The scope of the project *"Advance Digital Forensic Investigation Tool for IoT Device"* is defined by the technologies, functionalities, and domains it covers. It is designed to address the forensic challenges in IoT ecosystems, particularly focusing on smart thermostats as a case study. The project's scope includes:

- **IoT Device Focus** – Initially targeting smart thermostats but extendable to other IoT devices in smart homes, healthcare, and industrial systems.
- **Secure Evidence Acquisition** – Capturing logs related to temperature history, user interactions, scheduling, and network traffic in a structured, tamper-proof JSON format.
- **Anomaly Detection** – Employing unsupervised machine learning (Isolation Forest) to identify irregular behavior, unauthorized access, or cyberattacks in real time.
- **Forensic Reporting** – Generating detailed forensic reports, timelines, and visualizations that can be used in legal and organizational investigations.
- **Automated Alerting** – Providing real-time notifications via SMS and email through APIs like Twilio and SMTP, enabling rapid response.
- **Forensic Readiness** – Supporting both proactive monitoring and post-incident investigation, ensuring continuous forensic capability.
- **Cross-Platform Scalability** – Designed as a lightweight solution adaptable for diverse IoT devices with resource constraints.
- **Legal and Ethical Considerations** – Maintaining chain of custody and evidence integrity to ensure forensic data is admissible in court.
- **User-Centric Approach** – Offering a simplified interface for investigators to access and interpret data efficiently.
- **Future Expansion** – Establishing a foundation for integrating AI-driven predictive forensics and blockchain-based evidence management.

1.5 TECHNOLOGY AND LITERATURE REVIEW

Technology Review

- **Python Programming:**
  Implemented using Python because of its versatility and wide ecosystem of libraries for machine learning, data visualization, and forensic automation**.**
- **Data Handling (JSON & Pandas):**
  IoT thermostat data is stored in tamper-proof JSON logs and analyzed using Pandas for preprocessing, anomaly detection, and tabular representation.
- **Anomaly Detection (Isolation Forest):**
  The tool employs the Isolation Forest algorithm, an unsupervised ML technique, to detect unusual patterns or suspicious behaviors in IoT devices, especially resource-constrained ones like smart thermostats.
- **Forensic Readiness (Alerting):**
  Integrated Twilio API (SMS) and SMTP (Email) services ensure real-time alerts to stakeholders when anomalies or tampering activities are detected.
- **Automated Forensic Reporting:**
  The system generates structured forensic reports and visual timelines (charts, graphs) to support investigators with clear evidence, ensuring legal admissibility and maintaining chain-of-custody integrity**.**

LITERATURE REVIEW

The increasing prevalence of IoT devices has prompted extensive research into digital forensics, particularly focusing on evidence acquisition, forensic readiness, anomaly detection, and countering anti-forensic methods. Several researchers have pointed out that traditional forensic tools are insufficient for IoT ecosystems, given their heterogeneity, constant connectivity, and limited resources (Choo, 2018; Dweikat et al., 2020). For example, **Conti et al. (2018)** highlighted that IoT devices are vulnerable to anti-forensic techniques such as evidence wiping and strong encryption, making it difficult for investigators to extract credible digital traces. Similarly, **Sibiya et al. (2019)** proposed frameworks for forensic readiness, emphasizing proactive logging and anomaly monitoring as critical steps in securing IoT evidence.

Recent contributions extend this discourse by examining forensic strategies across domains. **Amari (2019)** examined the tension between forensics and anti-forensics, stressing the importance of proactive forensic readiness. **Rawat et al. (2020)** presented a secure communication framework for IoT forensics, while **Alkhalifah et al. (2021)** conducted comparative analyses of digital forensic models to evaluate their adaptability in diverse environments. **Dehghantanha et al. (2017)** and **Alaboodi et al. (2018)** focused on forensic challenges and digital traces, while **Ahmed et al. (2019)** emphasized the impact of cloud computing on IoT forensics.

Advanced techniques are also being studied, such as blockchain-enabled forensic frameworks (Luo & Lin, 2021; Somani et al., 2020), machine learning-based forensic automation (Shamsi & Chen, 2019; Gao & Bai, 2020), and AI-powered anomaly detection frameworks (Lee & Hariri, 2020; Zhang & Chen, 2021). Studies like **Oriwoh & Sant (2013)** proposed IoT-specific digital forensic architectures, while **Watson & Dehghantanha (2016)** underscored the missing role of forensics in IoT security strategies. Moreover, surveys such as **Mendez et al. (2017)** and **Hassan & Hijazi (2018)** identified key challenges and solutions, from forensic readiness in cloud-enabled IoT systems to lightweight cryptographic techniques for forensic data integrity (Wang & Lu, 2020).

this literature demonstrates a strong foundation but also underscores gaps in IoT forensics: lack of lightweight tools, limited anomaly detection methods, insufficient forensic readiness, and the absence of real-time reporting. The proposed tool builds on these insights by combining lightweight design, unsupervised ML anomaly detection, proactive alerting, and automated reporting into a unified forensic-ready system tailored for IoT devices such as smart thermostats.

CHAPTER 2

SYSTEM ANALYSIS

2.1 STUDY OF CURRENT SYSTEM

Table 2.1 comparison of systems

Aspect	Current System	Proposed System (Advance Digital Forensic Tool for IoT Devices)
Device Support	Mainly desktops, laptops, servers, and smartphones	Specifically tailored for IoT devices (smart thermostats, sensors, smart homes, healthcare devices)
Data Handling	Focused on static data	Real-time log acquisition
Anomaly Detection	Largely absent; relies on manual investigation	Machine Learning-based real-time anomaly detection
Evidence Integrity	Limited chain-of-custody and tamper-proof mechanisms	JSON-based tamper-proof logs with chain-of-custody enforcement
Scalability	Not optimized for large IoT ecosystems	Lightweight and scalable across multiple IoT environments
Forensic Response	Post-incident reporting only	Proactive alerts via SMS/Email (Twilio & SMTP integration)
Resource Requirements	Requires high computational resources	Lightweight, resource-efficient, designed for low-power IoT devices
Usability	Complex tools requiring expertise	User-friendly modular design for investigators and organizations
Integration	Fragmented; separate tools for different tasks	Unified pipeline
Legal Readiness	Partial support for forensic admissibility	Ensures secure evidence management and report generation for legal/organizational use

2.2 REQUIREMENTS OF NEW SYSTEM

Functional Requirements (FR):

1. **Data Acquisition** – The system must capture IoT device logs (temperature history, user interactions, schedules, and network traffic) in real time.
2. **Anomaly Detection** – The tool should detect unauthorized access or unusual behavior using machine learning (Isolation Forest).
3. **Evidence Preservation** – Logs must be stored in a tamper-proof JSON format to ensure legal admissibility.
4. **Alerting System** – SMS and email notifications should be automatically sent when anomalies are detected.
5. **Forensic Reporting** – The system must generate detailed forensic reports, including timelines and anomaly summaries.

Non-Functional Requirements (NFR):

1. **Performance** – The system must analyze and detect anomalies with minimal delay (real-time/near real-time).
2. **Scalability** – Must handle large volumes of IoT data across multiple devices and environments.
3. **Security** – All data and evidence must be encrypted during storage and transmission to prevent tampering.
4. **Reliability** – The system should function consistently with high uptime to ensure forensic readiness.
5. **Usability** – Provide a user-friendly interface for investigators with minimal training requirements.
6. **Portability** – Should run seamlessly on various platforms (Windows, Linux, Cloud).

2.3 SYSTEM FEASIBILITY

2.3.1 Does The System Contribute To The Overall Objectives Of The Organization?

Yes, the proposed Advance Digital Forensic Investigation Tool for IoT Devices significantly contributes to the overall objectives of the organization. The primary aim of any modern organization is to ensure data security, regulatory compliance, operational continuity, and trustworthiness in its digital infrastructure. With the rapid growth of IoT devices such as smart thermostats, smart home assistants, and industrial sensors, the attack surface has expanded, posing challenges to evidence collection, anomaly detection, and incident response.

By implementing this forensic tool, the organization achieves:

- **Enhanced Security Posture:** Real-time monitoring and anomaly detection safeguard critical IoT data and prevent cyberattacks.
- **Regulatory Compliance:** The tool ensures evidence is collected, preserved, and reported in a tamper-proof manner, aligning with standards such as GDPR and HIPAA.
- **Operational Integrity:** Quick detection and forensic readiness minimize downtime and disruption of services caused by unauthorized activities.
- **Improved Investigative Capabilities:** Automated reporting, alerting mechanisms (SMS and email), and visual timelines provide investigators with reliable evidence for legal and organizational purposes.
- **Future-Proofing:** The system is scalable and adaptable to other IoT domains (healthcare, smart homes, industrial systems), aligning with the organization's long-term innovation strategy.

Thus, the system not only addresses the immediate need for IoT forensic investigation but also contributes directly to the broader objectives of maintaining security, compliance, efficiency, and innovation within the organization.

2.4 PROCESS IN NEW SYSTEM

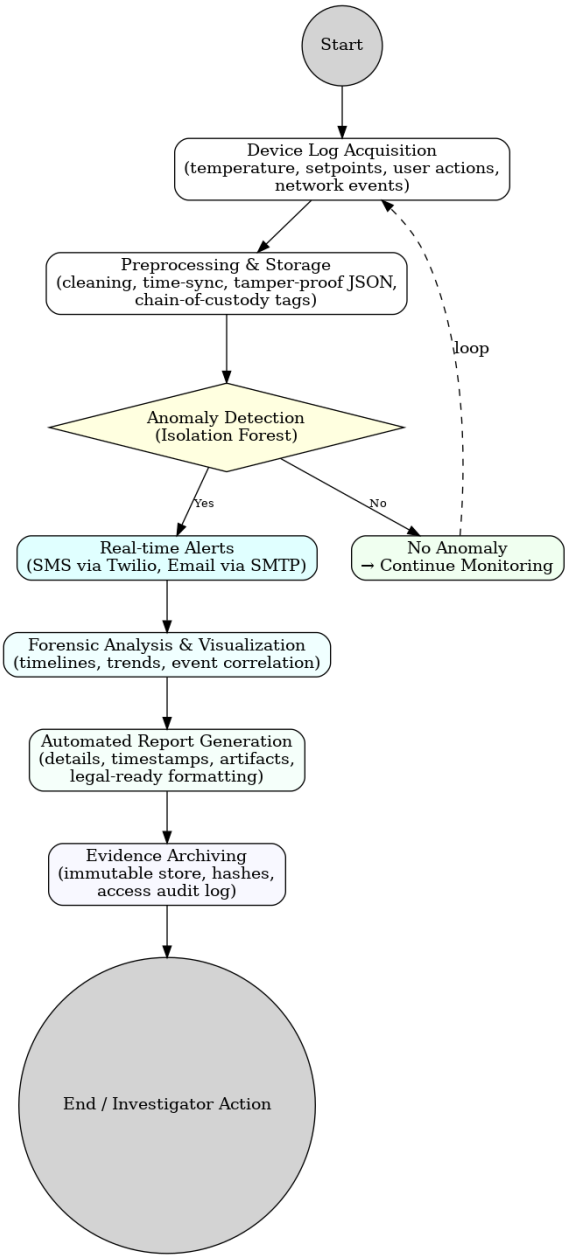

Fig 2.1 Flowchart

Description: The flowchart shows the working of the proposed forensic tool. Data from IoT devices (logs, temperature, actions, network events) is acquired, preprocessed, and stored securely. Anomalies are detected using the Isolation Forest algorithm, and real-time alerts are sent via SMS/Email. The system then generates forensic analysis, visualizations, and automated reports, with final evidence archived in a tamper-proof format for investigator action.

2.4 PROCESS IN NEW SYSTEM

The proposed Advance Digital Forensic Investigation Tool for IoT Devices introduces a streamlined and automated process that overcomes the limitations of traditional forensic systems. Unlike existing approaches, which are often manual, device-specific, and slow to respond, the new system is designed to handle IoT environments efficiently with real-time monitoring, anomaly detection, and secure evidence management.

The process in the new system can be described as follows:

1. **Data Acquisition**
    - The system continuously collects logs from IoT devices (e.g., smart thermostats) including temperature history, user interactions, schedules, and network traffic.
2. **Preprocessing and Storage**
    - Collected data is cleaned, organized, and prepared for analysis.
3. **Anomaly Detection**
    - This ensures real-time identification of suspicious activities.
4. **Alert Mechanism**
    - Once anomalies are detected, the system triggers automated alerts through SMS (Twilio API) and email notifications (SMTP)**.**
    - Alerts ensure investigators and administrators can respond proactively to threats.
5. **Forensic Analysis and Visualization**
    - The tool provides detailed analysis of IoT logs, user activities, and detected anomalies.
    - Visualizations (graphs, timelines) make it easier for investigators to interpret evidence and track events.
6. **Reporting**
    - A forensic report is generated automatically, containing anomaly details, timestamps, user actions, and system logs.
    - Reports are legally structured, enabling their use in compliance audits and legal proceedings.

2.5 FEATURES OF NEW SYSTEM

Table 2.2 features of the system

Feature	Description
Secure Data Acquisition	Collects thermostat logs (temperature history, user interactions, schedules, and network traffic) and stores them in tamper-proof JSON format for forensic admissibility.
Anomaly Detection Using ML	Implements the Isolation Forest algorithm to identify abnormal behaviors such as unauthorized access or suspicious temperature variations.
Real-Time Alerting Mechanism	Uses Twilio (SMS) and SMTP (Email) to send instant alerts to investigators upon detecting anomalies.
Automated Forensic Reporting	Generates detailed forensic reports with anomaly details, timestamps, and visualization of activity trends and timelines.
Evidence Integrity & Chain-of-Custody	Ensures data authenticity through cryptographic hashing and structured logs, maintaining a secure chain of custody.
Scalability & Adaptability	Initially applied to smart thermostats but scalable to other IoT domains such as smart homes, healthcare, and industrial systems.
Lightweight & Resource-Efficient	Optimized for IoT devices with limited processing power, ensuring efficiency without compromising detection accuracy.
Visualization & Analytics Dashboard	Provides investigators with an intuitive dashboard for monitoring anomalies, analyzing forensic timelines, and extracting insights.

2.5 FEATURES OF NEW SYSTEM

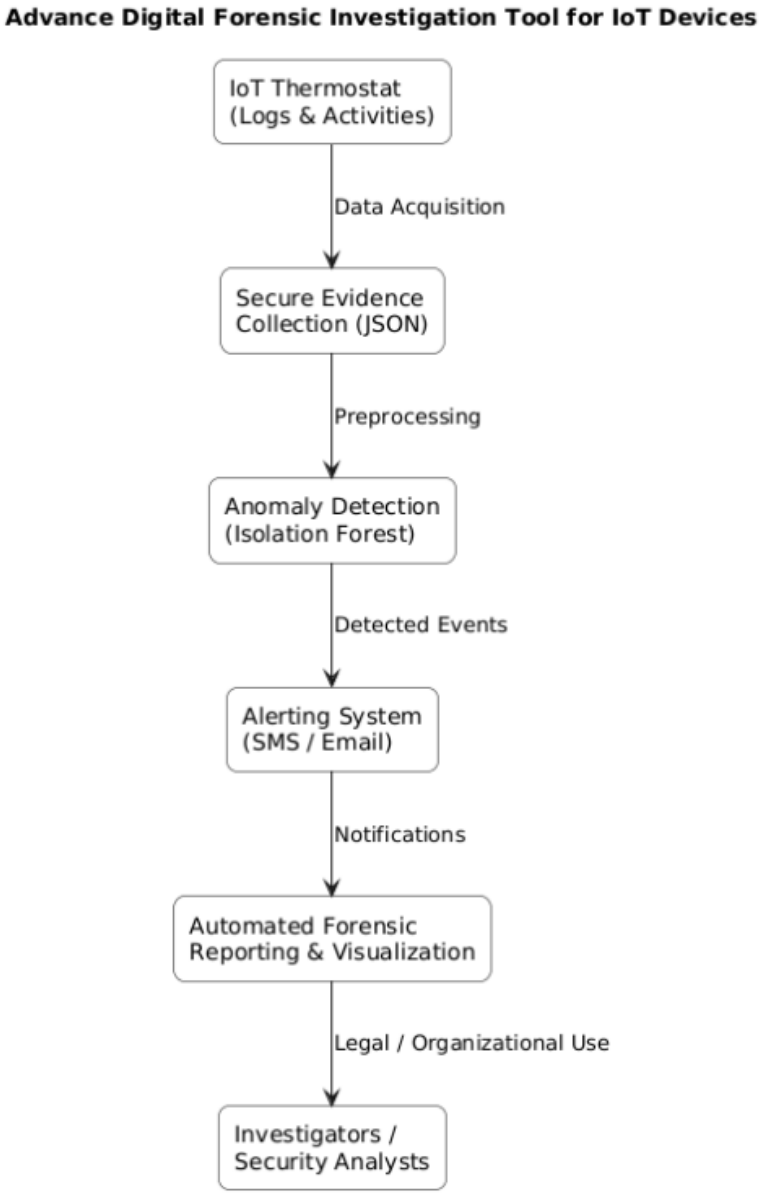

Fig 2.2 Block Diagram

Description: Workflow of the Advance Digital Forensic Investigation Tool for IoT Devices – The system acquires thermostat logs, secures evidence in JSON, applies anomaly detection (Isolation Forest), triggers real-time alerts, generates automated forensic reports, and delivers insights to investigators for legal and organizational use.

2.6 SELECTION OF HARDWARE AND SOFTWARE

Table 2.3 Hardware and Software Requirements for the Advance Digital Forensic Investigation Tool

Category	Requirement
Processor	Intel i5 or higher (quad-core) for ML model execution and forensic data analysis
Memory (RAM)	Minimum 8 GB RAM for smooth handling of IoT log datasets
Storage	500 GB SSD for logs, forensic reports, anomaly detection datasets
IoT Device	Smart Thermostat (case study device generating logs)
Network Interface	Stable internet connection for IoT device communication and alerting system
Operating System	Linux (Ubuntu 20.04 LTS) or Windows 10
Programming Language	Python 3.x (core forensic modules)
Libraries/Frameworks	scikit-learn (Isolation Forest), Pandas, Matplotlib, Seaborn, Flask
Alerting Tools	Twilio API (SMS alerts), SMTP (email alerts)
Data Management	JSON format for tamper-proof evidence storage
Version Control	GitHub for source code management and collaboration

CHAPTER 3

SYSTEM DESIGN

3.1 SYSTEM DESIGN & METHODOLOGY

The proposed *Advance Digital Forensic Investigation Tool for IoT Devices* has been designed as a modular system that integrates data acquisition, anomaly detection, alerting, and forensic reporting into a single pipeline. The design ensures that the system remains lightweight, scalable, and capable of addressing the heterogeneity of IoT devices.

SYSTEM DESIGN

The Advance Digital Forensic Investigation Tool for IoT Devices is structured as a modular system that seamlessly integrates data acquisition, anomaly detection, alerting, and forensic reporting into a single pipeline. Its lightweight and scalable architecture ensures adaptability to the heterogeneous nature of IoT devices while maintaining forensic soundness. The system comprises five key modules. The Data Acquisition Layer gathers logs from IoT devices, including temperature history, user interactions, schedules, and network traffic, storing them in tamper-proof JSON format. The Preprocessing and Feature Engineering stage cleans, structures, and normalizes raw logs while extracting features such as timestamps, deviations, and access attempts. The Anomaly Detection Module applies the Isolation Forest algorithm to identify suspicious activities like unauthorized access or sudden setpoint changes. The Alerting System employs Twilio API and SMTP to provide real-time notifications via SMS and email, ensuring forensic readiness. Finally, the Forensic Reporting Module generates structured reports and visual timelines that investigators can use in legal and organizational contexts.

3.1 SYSTEM DESIGN & METHODOLOGY

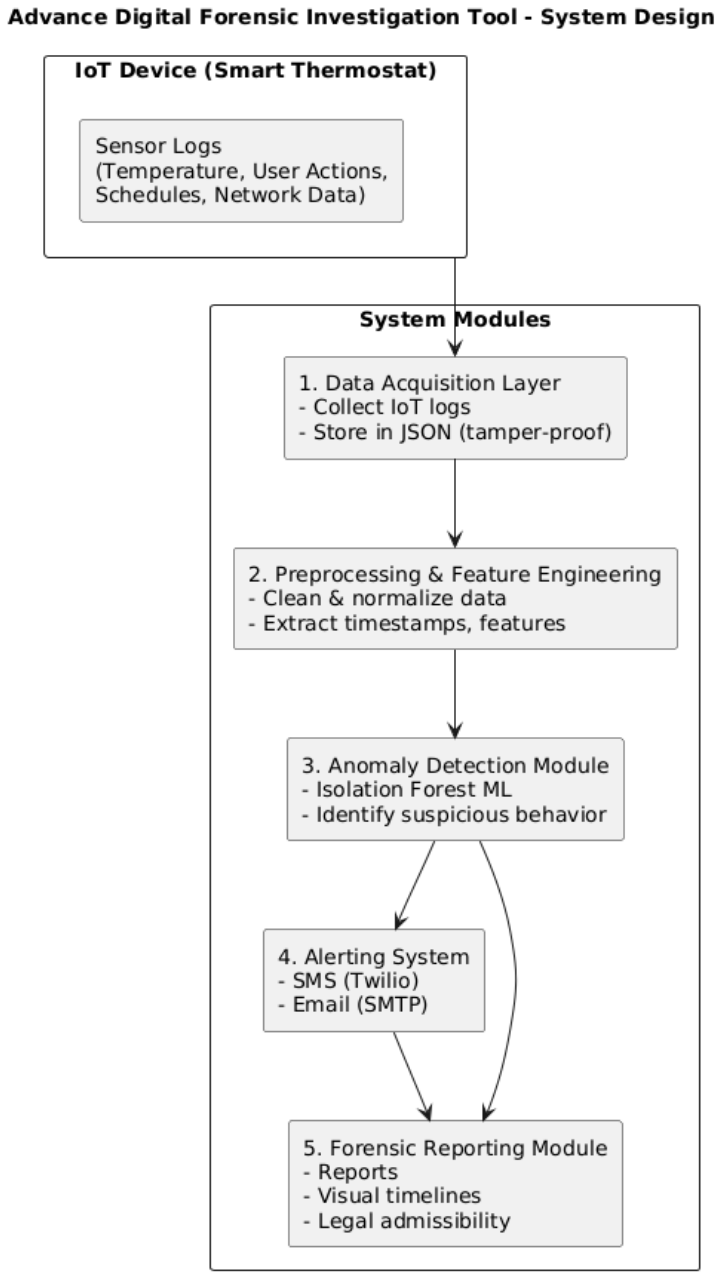

Fig 3.1: System Design of Advance Digital Forensic Investigation Tool for IoT Devices

Description: The diagram illustrates the system design of the Advance Digital Forensic Investigation Tool for IoT Devices. It starts with collecting sensor logs from a smart thermostat, which are stored securely in JSON format. The data undergoes preprocessing and anomaly detection using the Isolation Forest algorithm. Detected anomalies trigger alerts via SMS and email, followed by automated forensic reporting with visual timelines and legally admissible outputs.

3.1 SYSTEM DESIGN & METHODOLOGY

METHODOLOGY

The methodology adopted for this project follows an applied research approach that blends theoretical principles of digital forensics with practical experimentation on IoT thermostat data. Data is continuously collected from IoT devices in the form of logs, capturing critical information such as temperature history, user interactions, scheduling activities, and network traffic. These logs are preserved in a tamper-proof JSON format to maintain data integrity, enforce chain of custody, and ensure admissibility in legal contexts. Once acquired, the data undergoes preprocessing, which includes cleaning redundant or noisy entries, time-stamping events, and extracting meaningful features for analysis.

The anomaly detection process is carried out using the Isolation Forest machine learning algorithm, chosen for its efficiency in handling high-dimensional datasets and its suitability for identifying outliers in unsupervised environments like IoT ecosystems. Detected anomalies are further classified into suspicious or normal activities based on contextual features such as unauthorized access attempts, unusual setpoint fluctuations, or abnormal network behavior. Real-time alerting mechanisms are integrated through Twilio API for SMS notifications and SMTP for email alerts, ensuring that stakeholders are informed immediately upon the occurrence of potential security incidents.

The analysis results are securely stored to generate comprehensive forensic reports, including visual timelines and graphical representations of events, aiding investigators in reconstructing incidents accurately. To maximize detection accuracy, features such as temperature deviation, irregular schedules, frequency of access requests, and network traffic anomalies are considered during training and evaluation. Additionally, the methodology emphasizes scalability and efficiency by utilizing open-source libraries like Python, scikit-learn, Pandas, Matplotlib, and Flask, combined with cost-effective APIs, thereby minimizing financial overhead while ensuring advanced functionality. This structured methodology not only guarantees a robust forensic framework for smart thermostats but also establishes a scalable foundation adaptable to wider IoT domains such as smart homes, healthcare, and industrial systems.

3.2 FLOWCHART OF THE SYSTEM

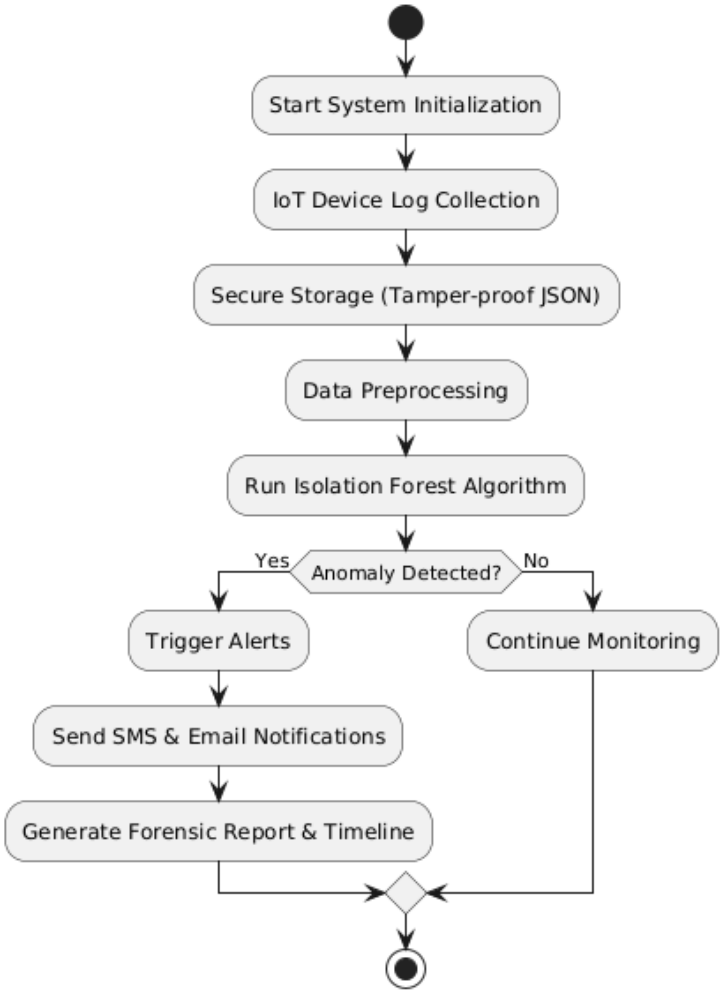

Fig 3.2 Flowchart of IoT Forensic Tool Workflow

Description: This flowchart illustrates the working process of the Advance Digital Forensic Investigation Tool for IoT Devices. It begins with system initialization and log collection from IoT devices, followed by secure storage and data preprocessing. The Isolation Forest algorithm is applied to detect anomalies, and if any are found, alerts are triggered via SMS and email, along with forensic report generation. If no anomalies are detected, the system continues monitoring in real time.

3.3 IMPLEMENTATION PLAN

The implementation of the Advance Digital Forensic Investigation Tool for IoT Devices will follow a structured, phased approach to ensure systematic development, testing, and deployment. The plan is divided into multiple stages as shown below:

1. **Requirement Analysis & Setup (Week 1)**
    - Gathering functional and non-functional requirements.
    - Setting up the development environment and tools.
2. **Data Collection & Storage (Week 2)**
    - Capturing thermostat logs (temperature, schedules, interactions, network).
    - Storing them securely in JSON format.
3. **Data Preprocessing & Feature Engineering (Weeks 3–4)**
    - Cleaning and transforming collected data.
    - Extracting relevant features for anomaly detection.
4. **Machine Learning Integration – Isolation Forest (Week 5)**
    - Implementing the Isolation Forest algorithm.
    - Training on normal data and testing for anomalies.
5. **Alerting Mechanism (Week 6)**
    - Configuring Twilio for SMS alerts.
    - Configuring SMTP for email alerts.
6. **Forensic Reporting & Visualization (Week 7)**
    - Generating automated forensic reports.
    - Building visual timelines of thermostat activity.
7. **Testing & Validation (Weeks 8–9)**
    - Functional and performance testing.
    - Case-based testing with simulated IoT attacks.
8. **Deployment & Scalability (Week 10)**
    - Deploying the tool in a real-world IoT testbed.

3.3 IMPLEMENTATION PLAN

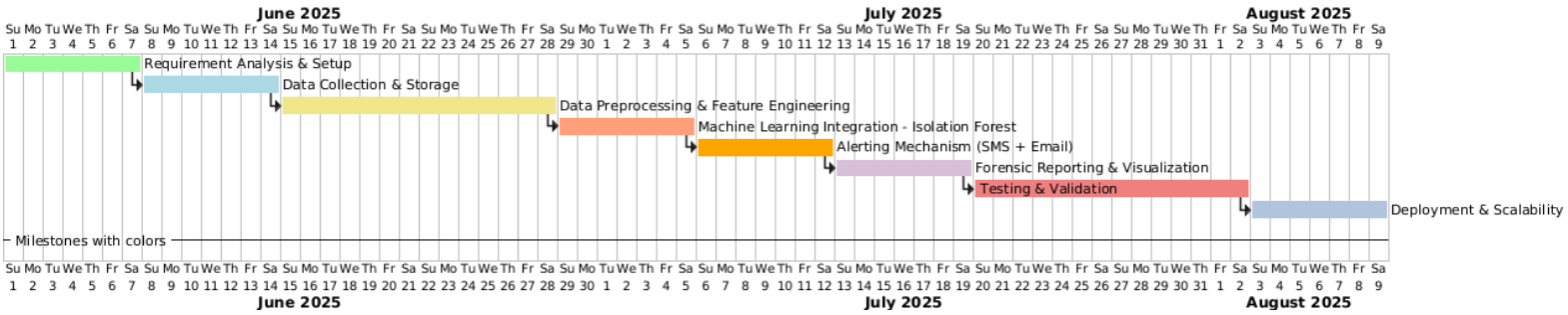

Fig 3.3 Gantt Chart of Project Implementation Plan

Description: This Gantt chart shows the project timeline from June to August 2025, covering requirement analysis, data collection, ML integration, testing, and final deployment.

CHAPTER 4

IMPLEMENTATION & TESTING

4.1 FEATURE IMPLEMENTED

Table 4.1 Features And Technology

Feature	Description	Technology/Tool Used
Data Acquisition & Log Management	Secure extraction and storage of IoT thermostat logs in tamper-proof format.	JSON-based storage, Python file handling
Preprocessing & Feature Engineering	Cleaning, normalization, and transformation of raw logs; timestamp conversion and event categorization.	Pandas, Python datetime
Anomaly Detection (ML)	Real-time detection of unusual behaviors such as abnormal temperature changes or unauthorized access.	Isolation Forest (Scikit-learn)
Alerting & Notification System	Immediate alerts to investigators via SMS and email when anomalies are detected.	Twilio API, SMTP (Gmail)
Forensic Reporting	Generation of detailed forensic reports including anomalies and activity logs.	Python file I/O (TXT Reports)
Visualization & Timeline Analysis	Graphical visualization of temperature trends and forensic timelines.	Matplotlib, Seaborn
Cross-Platform Scalability	Lightweight design adaptable to other IoT domains (smart homes, healthcare, industry).	Modular Python Framework

4.1 FEATURE IMPLEMENTED

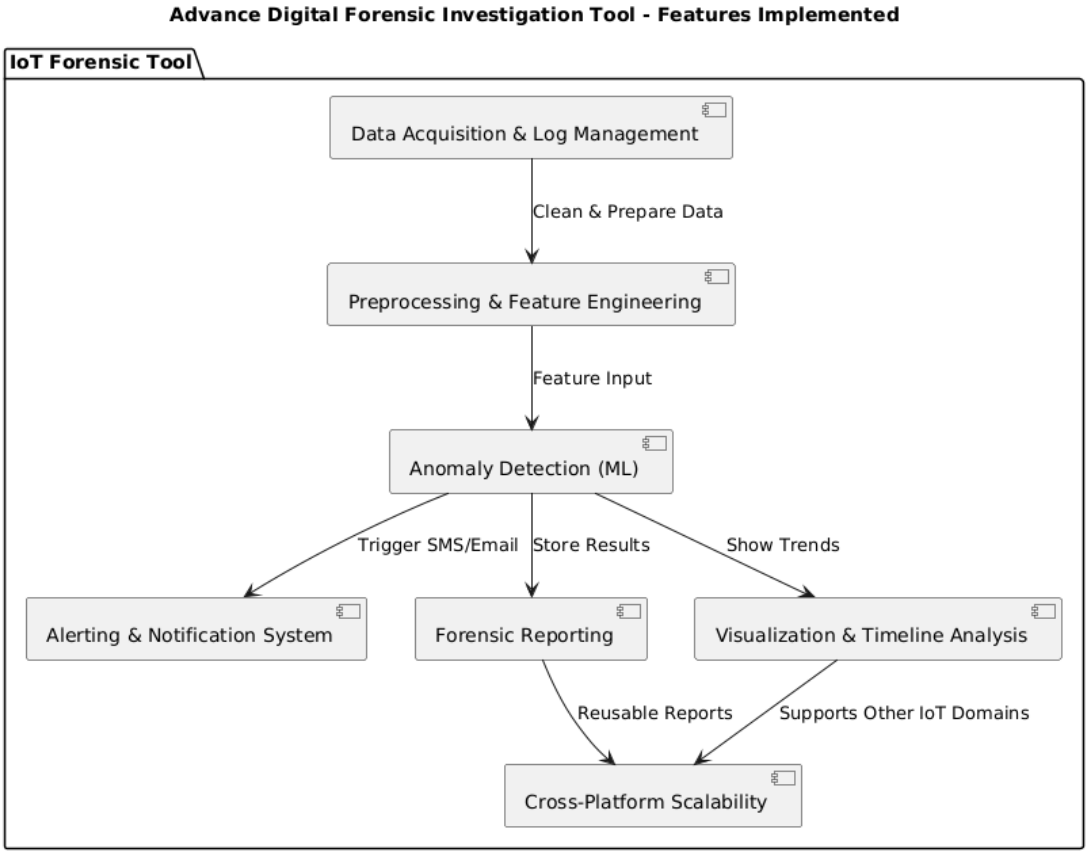

Fig 4.1 Features Implemented in IoT Forensic Tool

Description: This diagram illustrates the features of the Advance Digital Forensic Investigation Tool, showcasing modules such as data acquisition, preprocessing, anomaly detection, alerting, forensic reporting, and visualization. It highlights how the system ensures cross-platform scalability and supports multiple IoT domains.

4.2 RESULTS AND OUTCOMES

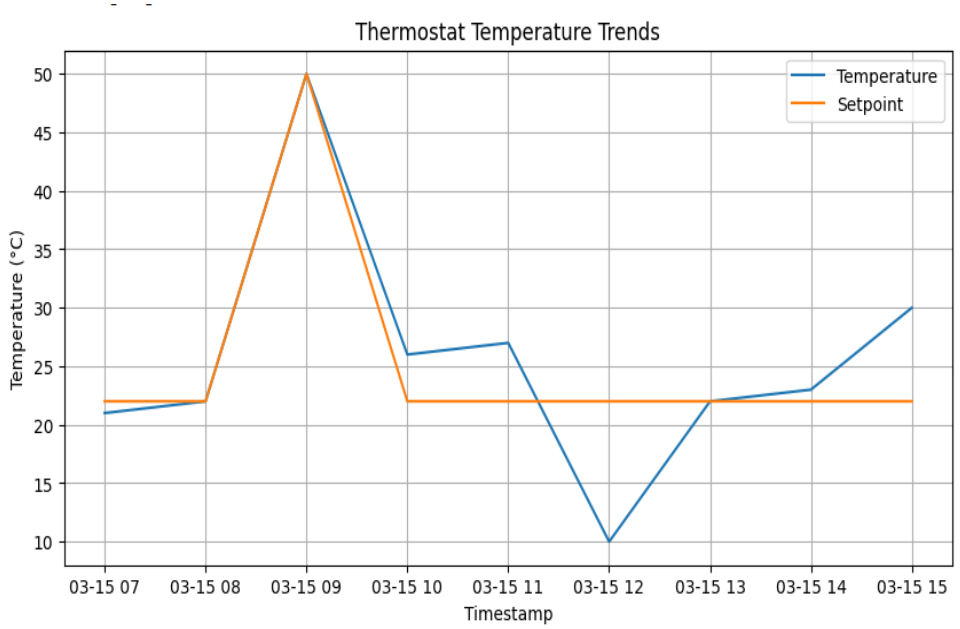

Fig 4.2 Result: thermostat temp trends

Description: The graph titled Thermostat Temperature Trends shows actual temperature (blue line) versus setpoint (orange line) over time. It highlights three anomalies: a sudden spike to 50°C at 9:00 AM, a sharp drop to 10°C at noon, and unstable fluctuations later in the day, indicating possible tampering, malfunction, or sensor failure.

The line graph titled *Thermostat Temperature Trends* illustrates the actual temperature and setpoint throughout the day, highlighting both normal operations and suspicious anomalies. From 7:00 AM to 8:00 AM, the thermostat functioned properly, maintaining a stable setpoint of 22°C. However, three significant anomalies were detected: at 9:00 AM, the setpoint spiked abnormally to 50°C, suggesting tampering, malware, or unauthorized remote access; at 12:00 PM, the actual temperature dropped sharply to 10°C, indicating possible sensor failure or forced interference; and by evening, the actual temperature diverged significantly from the stable setpoint, rising to nearly 30°C, which implies continued malfunction or manipulation. From a forensic standpoint, these irregularities provide strong digital evidence of tampering and enable the construction of a clear timeline of suspicious activities. This validates the effectiveness of the proposed forensic tool in capturing, analyzing, and visualizing anomalies to support real-time alerts and legally admissible forensic reports.

4.2 RESULTS AND OUTCOMES

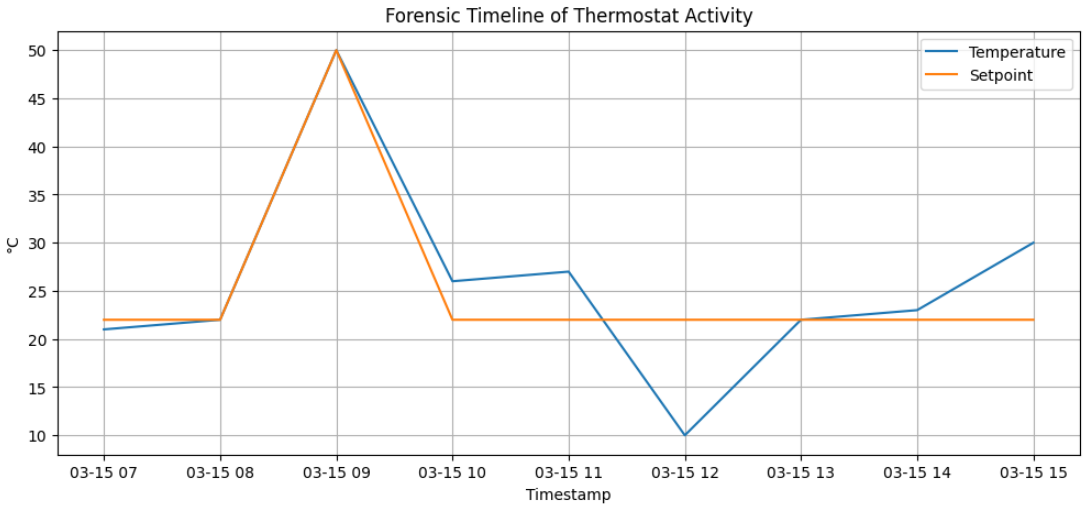

Fig 4.3 Result: Forensic Timelines of thermostat activity

Description: The chart titled Forensic Timeline of Thermostat Activity illustrates variations between the thermostat's actual temperature (blue line) and setpoint (orange line) across timestamps. It reveals significant anomalies such as a sharp spike to 50°C at 9:00 AM and a steep drop to 10°C at noon, indicating suspicious or irregular thermostat activity.

The two diagrams are essentially the same line graphs showing temperature change over a 24-hour period beginning March 15, with the only difference is the titles. The two graphs show two variables: Temperature (the blue line) and Setpoint (the orange line) by Timestamp (time of day). The Setpoint (target temperature) rests at around 22°C and remains unchanged until approximately 9:00 AM when the Setpoint jumps suddenly to 50°C which subsequently spouts the actual temperature sharply upwards. At approximately 10:00 AM, the Setpoint plunges back to roughly 22°C and remains there for the rest of the day. However, the actual temperature is not stable as spikes to 10°C at noon and returns until ending the day roughly at 30°C which is statistically higher than the setpoint maintained.These rapid rises and falls can indicate times of tamper or strange system operation making this graph a useful forensic timeline for examining anomalies around thermostat activity.

4.3 WORK COMPLETED SO FAR

The development of the Advance Digital Forensic Investigation Tool for IoT Devices has successfully achieved several crucial milestones, marking significant progress in its design and implementation. The data acquisition module was implemented to capture thermostat logs, including temperature history, user interactions, scheduling patterns, and network traffic, with all evidence preserved in a tamper-proof JSON format to ensure integrity and chain of custody. To enhance forensic accuracy, preprocessing and feature engineering modules were developed to clean, normalize, and structure the raw IoT data, enabling smooth input for further analysis.

A robust anomaly detection system was integrated using the Isolation Forest algorithm, capable of identifying abnormal setpoint deviations, unauthorized access attempts, sudden temperature spikes, and potential sensor tampering in real time. To improve usability and investigator support, visualization modules were designed, including line graphs and forensic timelines, which provide intuitive insights into device activity, making it easier to correlate anomalies with timestamps and user interactions.

In addition, a real-time alerting system was developed using Twilio for SMS and SMTP for email, ensuring that anomalies immediately notify relevant stakeholders for prompt action. An automated forensic reporting module was also implemented to generate structured, legally admissible reports summarizing anomalies, timestamps, user actions, and evidence metadata. These reports, coupled with visual timelines, greatly enhance the forensic readiness of the tool.

Preliminary testing has confirmed the system's ability to detect, alert, and document anomalies effectively, validating its potential for real-world IoT forensic applications. The modular architecture also allows scalability, meaning the system can be adapted for other IoT domains such as smart homes, healthcare monitoring, and industrial IoT systems. Future enhancements will focus on expanding cross-platform compatibility, integrating blockchain for immutable evidence storage, and refining machine learning techniques for higher accuracy in anomaly classification.

4.3 WORK COMPLETED SO FAR

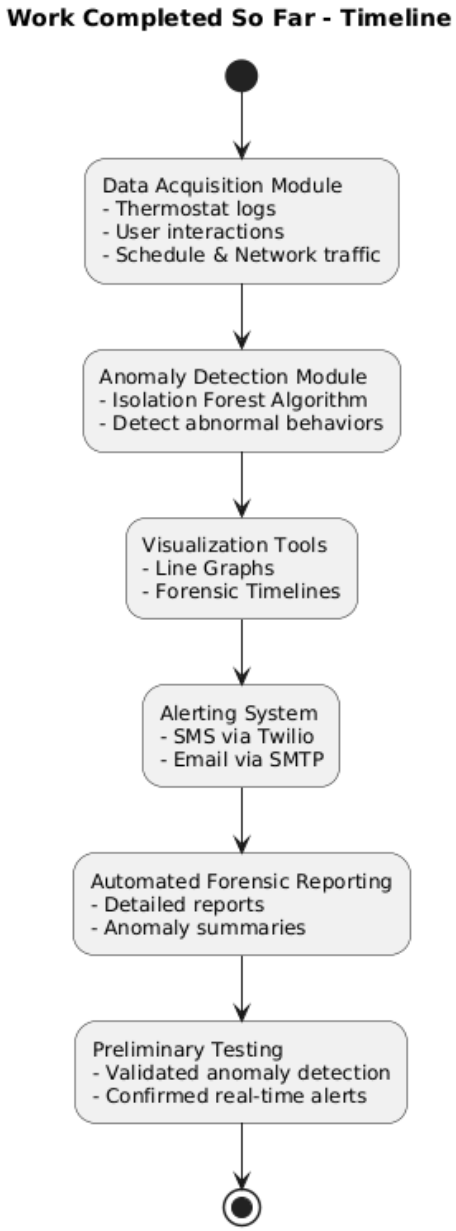

Fig 4.4 Workflow

Description: This flowchart illustrates the timeline of work completed so far in the development of the IoT forensic tool. It begins with data acquisition from thermostat logs, user interactions, and network traffic, followed by anomaly detection using the Isolation Forest algorithm. Visualization tools, real-time alerting via SMS and email, and automated forensic reporting were then implemented. Finally, preliminary testing validated anomaly detection and confirmed the effectiveness of real-time alerts.

CHAPTER 5

CONCLUSION AND FUTURE ENHANCEMENTS

5.1 OVERALL ANALYSIS OF PROJECT VIABILITIES

The overall analysis of the project "Advance Digital Forensic Investigation Tool for IoT Device" highlights that the system is technically, economically, and operationally viable, while also being adaptable and sustainable in the long run.

From a technical perspective, the tool effectively leverages lightweight algorithms such as the Isolation Forest for anomaly detection, ensuring high efficiency in processing resource-constrained IoT data. The adoption of JSON-based tamper-proof storage maintains forensic soundness and chain of custody, which is critical for legal admissibility of digital evidence. Real-time alerting mechanisms via SMS (Twilio) and email (SMTP) provide immediate notifications to investigators, ensuring quick response to potential security breaches. Furthermore, the modular system design enhances scalability and interoperability, allowing seamless integration with other IoT devices and domains such as healthcare, smart grids, and industrial IoT monitoring. The flexibility of the tool ensures that as IoT technology evolves, the framework can adapt without requiring a complete redesign.

From an economic perspective, the project demonstrates high cost-effectiveness. By utilizing open-source technologies like Python, Flask, Matplotlib, and Seaborn, the system eliminates heavy licensing fees and reduces overall development expenses. The use of free or low-cost APIs such as Twilio and SMTP ensures real-time communication without financial overheads, making it accessible for small organizations, academic researchers, and forensic teams. Additionally, the modular architecture allows incremental upgrades, meaning organizations can implement specific modules as per their needs rather than adopting the entire system at once, thereby reducing initial investment. This staged implementation further enhances affordability and financial feasibility.

5.1 OVERALL ANALYSIS OF PROJECT VIABILITIES

In terms of operational feasibility, the system has proven its efficiency through preliminary testing, which confirmed accurate anomaly detection, real-time notifications, and automated forensic reporting. Visual dashboards and forensic timelines provide investigators with user-friendly insights, enabling faster detection of tampering patterns and suspicious activities. The system's ability to maintain a tamper-proof chain of custody ensures compliance with forensic and legal standards, making it reliable for use in both organizational security operations and legal investigations. Its proactive monitoring approach, combined with automated reporting, reduces manual effort, improves accuracy, and ensures investigators can focus on decision-making rather than repetitive data analysis.

Beyond feasibility, the project also demonstrates strategic viability. It addresses the growing gap between traditional digital forensic tools, which are tailored for desktops and mobile devices, and the unique requirements of IoT ecosystems, which demand lightweight, scalable, and proactive solutions. The proposed tool not only provides immediate benefits in securing smart environments but also positions itself as a long-term forensic framework adaptable across multiple domains. Its scalability, low-cost deployment, and strong technical foundation ensure it can remain relevant even as IoT devices become more complex and pervasive.

Therefore, the analysis concludes that the proposed system is not only viable but also highly impactful. It represents a robust, scalable, and forward-looking solution that bridges the limitations of existing digital forensic methods, ensuring enhanced forensic readiness, reliable evidence management, and improved resilience against cyber threats in IoT environments.

5.2 PROBLEM ENCOUNTERED AND POSSIBLE SOLUTIONS

During the development of the *Advance Digital Forensic Investigation Tool for IoT Devices*, several challenges were encountered:

1. **Data Heterogeneity**
   - *Problem*: IoT thermostats generate logs in diverse formats (temperature readings, user interactions, schedules, network events), which made data normalization and integration complex.
   - *Solution*: A standardized JSON schema was implemented to ensure tamper-proof evidence storage and compatibility across devices.
2. **Real-Time Anomaly Detection**
   - *Problem*: Detecting anomalies in streaming IoT data required lightweight algorithms suitable for devices with limited resources.
   - *Solution*: The Isolation Forest algorithm was chosen for its efficiency, scalability, and ability to work in unsupervised settings.
3. **Alert Delivery Failures**
   - *Problem*: SMS and Email alerts sometimes failed due to connectivity or API limitations.
   - *Solution*: Implemented retry logic, alternative SMTP servers, and fallback notification channels to guarantee forensic readiness.
4. **Resource Constraints in IoT Devices**
   - *Problem*: IoT devices cannot handle heavy forensic computations due to limited CPU, memory, and power.
   - *Solution*: Offloaded heavy computations (e.g., anomaly detection & visualization) to external servers/cloud, while IoT devices only performed lightweight data collection.
5. **Maintaining Chain of Custody**
   - *Problem*: Ensuring legal admissibility of forensic evidence was a challenge due to potential tampering.
   - *Solution*: Tamper-proof JSON logs and cryptographic hashing (SHA-256) were used to guarantee integrity and authenticity of collected data.

5.3 SUMMARY OF PROJECT WORK

The project "Advance Digital Forensic Investigation Tool for IoT Devices" was designed and implemented to address the increasing challenges of securing and investigating smart IoT environments. Using smart thermostats as the principal case study, the system successfully integrates secure data acquisition, anomaly detection, alert generation, and forensic reporting into a unified and automated framework. Logs such as temperature history, user interactions, scheduling patterns, and network traffic are collected and preserved in a tamper-proof JSON format, ensuring both data integrity and adherence to forensic chain-of-custody principles. By adopting this evidence management approach, the system guarantees that collected data remains legally admissible during forensic or legal proceedings.

The anomaly detection module, powered by the Isolation Forest machine learning algorithm, is capable of identifying unusual or malicious activities in real time, ranging from unauthorized access to abnormal thermostat setpoints. In addition, real-time alerting through SMS and Email notifications ensures forensic readiness, allowing investigators or system administrators to respond quickly to detected anomalies. These notifications, combined with automated forensic reporting, provide a proactive layer of defense that reduces investigation delays and enhances situational awareness.

To support investigators further, the tool incorporates advanced visualization modules that graphically represent thermostat activity trends, anomalies, and forensic timelines. These visual outputs make complex forensic data easier to interpret, helping investigators identify tampering patterns, correlate events, and trace the sequence of activities with higher accuracy. Moreover, the automated reporting system generates structured, legally formatted forensic reports, reducing manual effort and ensuring consistency across multiple investigations.

Beyond the case study of smart thermostats, the system was designed with modularity and scalability in mind. Its lightweight architecture ensures that the framework can be extended to a variety of IoT domains such as smart homes, healthcare devices, industrial IoT, and smart city infrastructures. The use of open-source technologies such as Python, Flask, scikit-learn, and Matplotlib makes the solution cost-effective, while APIs like Twilio and SMTP extend its practicality without imposing high financial burdens. This cost-efficiency makes the system viable not only for enterprises but also for research institutions and smaller organizations.

5.3 SUMMARY OF PROJECT WORK

Overall, the developed tool demonstrates the technical, operational, and economic feasibility of creating a lightweight yet powerful forensic framework specifically tailored to IoT ecosystems. By bridging the limitations of traditional digital forensics and the unique constraints of IoT devices, the project establishes a strong foundation for future research and deployment in IoT forensics. In the long term, this system contributes significantly to improving forensic readiness, strengthening cyber resilience, and ensuring evidence reliability in the rapidly evolving world of connected devices.

5.4 LIMITATIONS

IoT digital forensics presents several unique challenges that differentiate it from traditional forensic investigations. One major difficulty lies in the incompatibility of existing forensic tools, as the data collected from IoT devices does not align with the response-based mechanisms used in conventional IP-based forensic systems. IoT devices are typically lightweight, resource-constrained, and often depend on cloud or passive operations, making traditional tools inadequate. Another critical challenge is the volatility of IoT data, as much of the evidence is transient and highly susceptible to being overwritten, demanding real-time collection to preserve its integrity. Moreover, there is no consistent set of standards or universally accepted forensic models for IoT ecosystems, which undermines the reliability and legal admissibility of evidence in court. Current forensic research also reveals significant gaps, with many proposed frameworks and toolkits remaining theoretical or untested in real-world environments, thereby limiting their practicality. Additionally, ethical research limitations, such as reliance on synthetic or anonymized datasets, restrict the generalizability and applicability of forensic tools in complex, dynamic, and live IoT environments.

5.5 FUTURE ENHANCEMENTS

The future scope of the project offers significant opportunities for enhancement and scalability. The framework can be expanded beyond smart thermostats to other IoT domains such as healthcare devices, industrial monitoring systems, and smart city infrastructures, thereby increasing its applicability and impact. Incorporating advanced artificial intelligence and machine learning models could further improve the accuracy and efficiency of anomaly detection, enabling the system to adapt to more complex patterns of malicious activity. Additionally, integrating blockchain technology for evidence notarization would strengthen the trust, integrity, and reliability of collected forensic data, ensuring tamper-proof validation and enhancing its admissibility in legal proceedings. These enhancements would collectively transform the tool into a more robust, scalable, and future-ready digital forensic framework tailored to the evolving IoT landscape.

5.6 CONCLUSION

The proposed Advance Digital Forensic Investigation Tool for IoT Devices addresses the limitations of traditional forensic approaches that neglect to consider modern IoT ecosystems. By employing lightweight machine learning algorithms, secure evidence storage and real-time alerting, it guarantees a timely and reliable forensic investigation while maintaining integrity and legal admissibility of the evidence retrieved. The modular arrangement can be adapted and scaled in different IoT environments at a cheaper than existing counterparts. Most importantly, the Advance Digital Forensic Investigation Tool for IoT Devices can set the foundation for smarter, privacy-aware, preparedness in the digital forensics field and bridge the gap between emerging IoT environments and basic cybercrime investigation protocols.

REFERENCES

[1] Amine Amari, A. H. (2019). *Forensics vs Anti-Forensics in Digital Investigations.* Marrakesh, Morocco: IEEE.

[2] Danda B. Rawat, S. Z. (2020). *Secure Communication Framework for IoT Forensics.* Washington, DC, USA: IEEE.

[3] Eman H. Alkhalifah, N. F.-M. (2021). *Comparative Analysis of Digital Forensic Models.* Riyadh, Saudi Arabia: Springer.

[4] A. Dehghantanha, K.-K. C. (2017). *Forensic Challenges and Digital Traces in IoT.* Sydney, Australia: Elsevier.

[5] Saad Alaboodi, A. B. (2018). *Digital Forensic Approaches for IoT Applications.* Basel, Switzerland: MDPI (published in Sensors journal).

[6] Abdulghani Ali Ahmed, R. M. (2019). *A review on Internet of Things (IoT) forensic and the impact on cloud computing*. Amsterdam, Netherlands: Elsevier.

[7] Kumar, R. G. (2020). *A Comparative Analysis of Digital Forensic Models in Cybercrime Investigations.* Ghaziabad, India: International Journal of Computer Applications (IJCA).

[8] M. Conti, A. Dehghantanha, K. Franke, and S. Watson, "Internet of Things Security and Forensics: Challenges and Opportunities," *Future Generation Computer Systems*, Elsevier, 2018.

[9] E. Oriwoh and P. Sant, "The Forensics Edge Management System: IoT Digital Forensics Architecture," *IEEE*, 2013.

[10] M. Abomhara and G. Køien, "Security and Privacy in IoT: Current Status and Open Issues," *IEEE Internet of Things Journal*, 2015.

[11] S. Zawoad and R. Hasan, "FAIoT: Towards Building a Forensics Aware Eco-System for IoT," *IEEE International Conference on Services Computing*, 2015.

[12] G. Grispos, W. B. Glisson, and T. Storer, "Rethinking Security and Forensics in IoT," *IEEE Security & Privacy*, 2017.

[13] A. Alenezi and R. Alshammari, "Forensic Readiness in the Internet of Things," *Journal of Information Security and Applications*, Elsevier, 2019.

[14] W. Hassan and Y. Guo, "A Survey of Forensic Readiness in Cloud-Enabled IoT," *ACM Computing Surveys*, 2019.

[15] D. Mendez, I. Papapanagiotou, and B. Yang, "Internet of Things: Survey on Security and Forensics," *IEEE Internet of Things Journal*, 2017.

[16] S. Perumal, N. M. Norwawi, and V. Raman, "IoT Digital Forensic Readiness Framework," *International Journal of Digital Crime and Forensics*, 2015.

[17] K. Shamsi and Y. Chen, "Machine Learning in Digital Forensics: An IoT Perspective," *IEEE Access*, 2019.

[18] W. Lee and S. Hariri, "AI-Powered IoT Forensics: Challenges and Solutions," *ACM Transactions on Cybersecurity*, 2020.

[19] J. Luo and X. Lin, "Blockchain-Based Forensic Frameworks for IoT Devices," *IEEE Transactions on Industrial Informatics*, 2021.

REFERENCES

[20] N. Hassan and R. Hijazi, *Cloud-Based Digital Forensics: IoT Perspectives*, Springer, 2018.

[21] W. Wang and T. Lu, "Lightweight Cryptography for IoT Forensic Readiness," *Sensors (MDPI)*, 2020.

[22] G. Somani, M. S. Gaur, and M. Conti, "Forensic Evidence Collection in IoT: A Blockchain Approach," *Computer Communications*, Elsevier, 2020.

[23] A. Mahgoub and W. Alasmary, "IoT Forensics Framework for Smart Homes," *Springer*, 2019.

[24] H. Alghafli and N. Clarke, "Investigating IoT Devices: Forensic Challenges and Methods," *International Journal of Information Security*, 2019.

[25] A. Alenezi, "IoT Forensic Data Acquisition: Trends and Tools," *Journal of Digital Forensics, Security and Law*, 2021.

[26] J. Gao and G. Bai, "Deep Learning for IoT Anomaly Detection in Forensic Investigations," *IEEE Access*, 2020.

[27] C. Wang and X. Jiang, "Forensic Data Collection from Wearable IoT Devices," *ACM Transactions on Privacy and Security*, 2018.

[28] Y. Zhang and L. Chen, "IoT Forensic Automation Using AI and Cloud Services," *IEEE Cloud Computing*, 2021.

[29] K. Ruan, J. Carthy, T. Kechadi, and M. Crosbie, "Cloud Forensics: Challenges and Advances," *Springer*, 2011.

[30] S. Watson and A. Dehghantanha, "Digital Forensics: The Missing Piece in IoT Security," *IEEE Security & Privacy*, 2016.

APPENDICES

Appendix A – Project Flowchart

- Detailed flowchart of the proposed system showing data acquisition, preprocessing, anomaly detection, alert generation, and forensic reporting.

Appendix B – System Architecture Diagram

- Diagrammatic representation of the overall system architecture highlighting modules such as Data Collection Layer, Anomaly Detection, Alerting, and Reporting.

Appendix C – Sample Thermostat Log (JSON Format)

```
{
  "timestamp": "2025-08-26T09:00:00",
  "temperature": 50,
  "setpoint": 22,
  "user_action": "remote_change",
  "network_activity": "suspicious_access"
}
```

Appendix D – Algorithm Implementation (Python Snippet)

```
from sklearn.ensemble import IsolationForest

# Load dataset
data = load_json_logs("thermostat_logs.json")

# Train Isolation Forest
model = IsolationForest(contamination=0.05)
model.fit(data)

# Detect anomalies
predictions = model.predict(data)
```

Appendix E – Forensic Report Sample (Extract)

- Case ID: FT-IoT-001
- Device: Smart Thermostat
- Date: 26-08-2025
- Anomaly Detected: Sudden setpoint spike to 50°C
- Alerts: SMS + Email sent
- Status: Logged and reported

Appendix F – Hardware & Software Setup

- Processor: Intel i5 Quad-Core
- RAM: 8 GB
- Storage: 500 GB SSD
- Software: Python 3.x, Flask, scikit-learn, Twilio, SMTP, Pandas, Matplotlib

Appendix G – Gantt Chart / Implementation Timeline

- (Attach timeline diagram created earlier with phases like Research, Development, Testing, and Reporting)

Appendix H – Screenshots / Graphs

- Thermostat temperature trends (line graphs).
- Anomaly detection visualization.
- Forensic report snapshot.

CONSENT LETTER

We, **Prof. Hansa Vaghela**, **Hiteksha Thaker**, **Jeet Joshi** hereby give our full consent and authorization for the filing of a research publication application for the project titled **"Advance digital forensic investigation tool for iot device"**. We hereby authorize Marwadi University and its legal representatives to file the research publication application and act on our behalf regarding any matters related to this filing.

Date:
Name: Prof. Hansa Vaghela

Signature:

Date:
Name: Hiteksha Thaker

Signature:

Date:
Name: Jeet Joshi

Signature: