International Journal of Innovative Research and Scientific Studies, 8(5) 2025, pages: 1167-1181

IJIRSS
International Journal of Innovative Research & Scientific Studies

ISSN: 2617-6548

URL: www.ijirss.com

Intelligent IoT forensics: Secure evidence acquisition and autonomous intrusion detection

Abdulaziz, Alanazi

Department of Information Systems, Faculty of Computing and Information Technology, Northern Border University, Rafha, 91911, Saudi Arabia.

(*Email: abdulaziz.alanazi@nbu.edu.sa*)

Abstract

The rapid adoption of the Internet of Things (IoT) presents significant challenges to digital forensics, particularly in securing evidence acquisition and detecting intrusions. Traditional forensic methods struggle with the decentralized and heterogeneous nature of IoT environments, resulting in gaps in forensic investigations. This study presents the Forensic-Based (FB) Framework, an intelligent solution for secure evidence acquisition and autonomous intrusion detection in IoT environments. Designed with smartwatch-controlled automation and lightweight forensic logging, the framework utilizes a Python-based simulation and machine learning algorithms, including LSTM, to enable real-time anomaly detection and log analysis. The results demonstrate a 92% detection accuracy, a 350 ms response time, and superior performance compared to existing models. The framework ensures data integrity through hashing mechanisms and supports scalable, low-latency forensic investigations across smart environments. It offers practical benefits for digital investigators and security practitioners working with resource-constrained IoT systems.

Keywords: Anomaly detection, BAFFL, Cybersecurity, Digital forensics, FAIoT, FB-Framework, IDS, IoT.

DOI: 10.53894/ijirss.v8i5.9078
Funding: This work is supported by the Deanship of Scientific Research at Northern Border University, Arar, Kingdom of Saudi Arabia (Grant number: NBU-FFR-2025-1350-01).
History: Received: 3 June 2025 / **Revised:** 8 July 2025 / **Accepted:** 10 July 2025 / **Published:** 5 August 2025

Competing Interests: The author declares that there are no conflicts of interests regarding the publication of this paper.
Transparency: The authors confirm that the manuscript is an honest, accurate, and transparent account of the study; that no vital features of the study have been omitted; and that any discrepancies from the study as planned have been explained. This study followed all ethical practices during writing.
Publisher: Innovative Research Publishing

1. Introduction

The Internet of Things (IoT) has revolutionized modern digital ecosystems, enabling seamless interconnectivity between smart devices across homes, industries, and critical infrastructures. However, this rapid technological advancement presents significant challenges in digital forensics, particularly in evidence acquisition, security monitoring, and intrusion detection. Traditional forensic models, primarily designed for conventional computing environments, struggle to address the heterogeneous, decentralized, and volatile nature of IoT networks.

As IoT devices continuously generate, transmit, and store sensitive data, forensic investigators must develop adaptive and intelligent frameworks to ensure data integrity, reconstruct digital crime scenes, and detect security anomalies. Despite

extensive research in IoT security, forensic readiness remains an overlooked challenge, especially in dynamically evolving environments such as smart homes, industrial automation, and critical infrastructure monitoring as discussed by Zawoad and Hasan [1] and Cheng et al. [2]. Existing forensic techniques lack efficient methods to log, analyze, and retrieve digital evidence from resource-constrained IoT devices while maintaining system performance and security. Moreover, intrusion detection mechanisms in IoT ecosystems often fail to provide real-time responses due to the complexity of event correlation across distributed networks.

To bridge this gap, this study introduces the FB Framework, a novel forensic model designed to enhance secure IoT evidence acquisition and real-time security monitoring. The framework incorporates smartwatch-controlled automation, forensic data logging, and autonomous intrusion detection to provide an intelligent, lightweight forensic solution. Unlike traditional models, the FB Framework integrates real-time anomaly detection and proactive security response, ensuring forensic integrity while maintaining system usability.

To validate its effectiveness, a Python-based simulation is employed, demonstrating its capability to enhance digital forensic investigations in IoT environments. By addressing the critical forensic gaps in IoT security, this research contributes to the development of scalable, efficient, and adaptive forensic models for emerging smart environments.

2. Literature Review

The Internet of Things (IoT) has rapidly evolved from a conceptual innovation to a fundamental component of modern digital infrastructure, with applications ranging from smart homes to critical industrial systems [3-5]. This evolution has, however, introduced significant forensic challenges, particularly in the domains of evidence acquisition, integrity preservation, and anomaly detection. Recent research has explored various frameworks and techniques to address these challenges, but gaps remain, particularly regarding forensic readiness and adaptive security monitoring [6-11].

IoT environments pose unique challenges due to their distributed nature, device heterogeneity, and limited computational resources, as highlighted in Stoyanova et al. [12]. Al-Hadadi et al. [13] emphasized the difficulty in maintaining forensic integrity across decentralized IoT networks, as traditional techniques struggle with the vast volume and variety of data generated. Similarly, Kumar et al. [14] highlighted the risks of volatile memory in IoT devices, noting the need for real-time data acquisition mechanisms to prevent evidence loss. Several frameworks have been proposed to facilitate digital forensic investigations in IoT contexts. Zawoad and Hasan [1] introduced the concept of Forensics-Aware IoT (FAIoT), which aims to embed forensic capabilities into IoT ecosystems. While this framework laid foundational principles, its reliance on predefined rules limited its adaptability to novel attack patterns. More recently, Lin et al. [15] Developed a Blockchain-Assisted IoT Forensic Framework (BAIFF), utilizing blockchain to ensure evidence immutability. However, the computational overhead associated with blockchain operations presents challenges for resource-constrained IoT devices. Intrusion Detection Systems (IDS) have become integral to IoT forensic frameworks. More studies have proposed an AI-driven IDS leveraging machine learning algorithms to detect anomalous patterns in IoT traffic [16, 17]. Their models demonstrated high accuracy in controlled environments but struggled with false positives when faced with diverse, real-world datasets. Similarly, Gupta et al. [18], Ayub and Khan [19] and Khan and Herrmann [20] explored the potential of federated learning for distributed anomaly detection, providing a privacy-preserving solution for sensitive IoT environments.

The acquisition and logging of IoT-generated data remain critical for forensic investigations. SmartAuth, developed by Tian et al. [21], Zhou and Li [22] and Wang and Liu [23] introduced context-aware permission analysis to detect malicious application behavior. While effective in identifying application overreach, SmartAuth primarily focuses on software-level activities, overlooking the forensic potential of sensor-generated data streams. Despite these advancements, contemporary frameworks often neglect the importance of forensic readiness and adaptive response mechanisms. The reliance on centralized architectures further increases the risk of data tampering and single points of failure. This study addresses these gaps by proposing the FB Framework, an innovative forensic model that integrates smartwatch-controlled IoT management, enabling real-time control and evidence acquisition; a lightweight forensic logging mechanism, utilizing Python-based simulations to log device interactions efficiently; and autonomous intrusion detection, employing machine learning algorithms for adaptive threat detection. By combining these components, the proposed framework enhances IoT forensic capabilities while ensuring system efficiency and scalability.

More recently, Kale [24] Proposed a hybrid IDS combining supervised and unsupervised learning techniques for IoT anomaly detection, reporting promising improvements in detection accuracy. However, the model did not address real-time evidence acquisition or forensic integrity. Another relevant study by Alotaibe [25] introduced a security model for smart cities using a metamodeling approach, highlighting the need for lightweight frameworks that support dynamic forensic capabilities in complex urban IoT systems.

3. Data Volume and Variety

The increasing adoption of IoT devices brings a multitude of forensic challenges that necessitate advanced frameworks and techniques. These challenges can be categorized into several key areas. The sheer volume of data generated by IoT devices presents a significant challenge for forensic investigators.

Moreover, the heterogeneous nature of IoT ecosystems means that devices operate on different platforms, communication protocols, and security standards, complicating data acquisition and analysis. The lack of standardized forensic procedures for IoT environments further exacerbates the difficulty in maintaining consistency and reliability in digital investigations.

Additionally, the decentralized and distributed nature of IoT networks introduces complexities in tracking and preserving digital evidence while ensuring its admissibility in court. The dynamic nature of IoT device interactions, influenced by real-time data flows and event-driven processes, requires forensic methodologies that can adapt to evolving cyber threats.

Furthermore, many IoT devices have limited storage and processing capabilities, making it challenging to retrieve historical data and logs crucial for forensic analysis. Encryption and proprietary protocols used by different IoT vendors also pose significant hurdles in accessing and interpreting device-generated data. In Figure 1, data from diverse sources, such as sensors, cameras, and wearable devices, requires efficient management and processing.

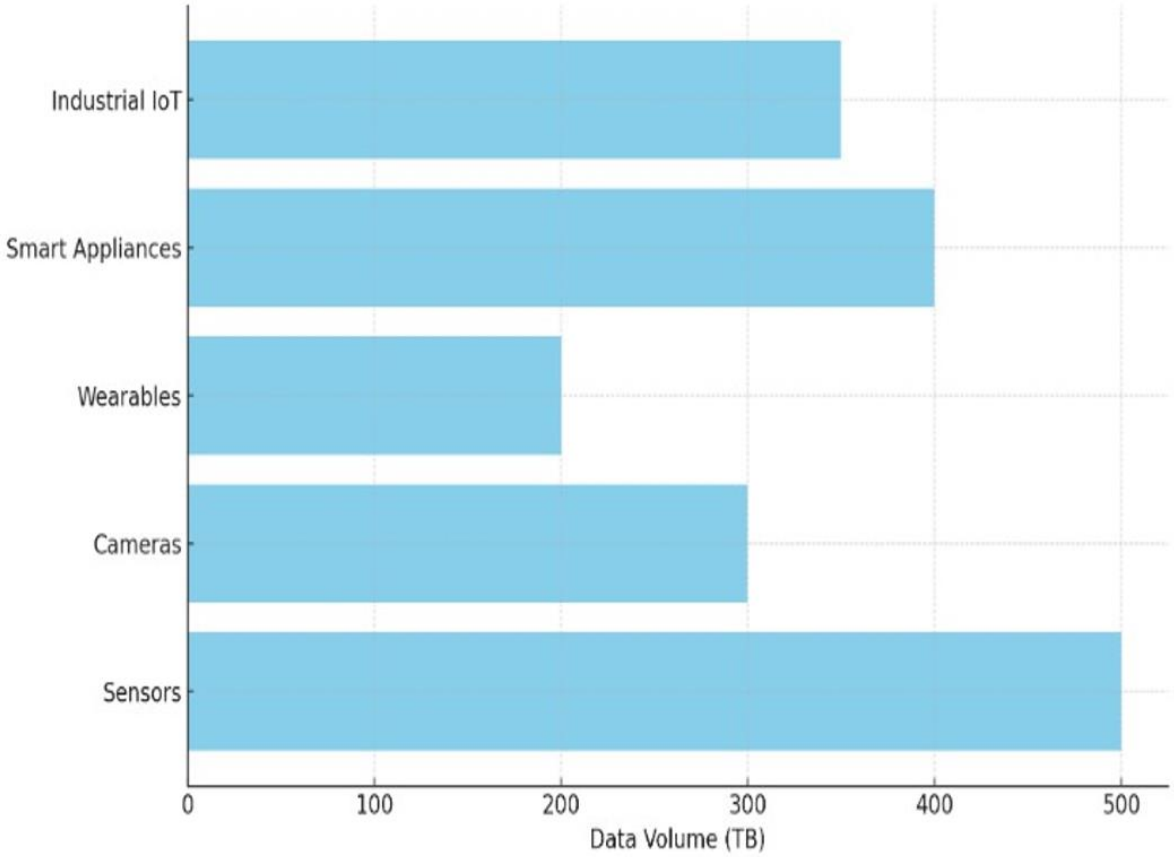

Figure 1.
IoT Data Sources and Their Volume.

IoT data are often stored temporarily and may be lost or overwritten if not captured in real-time. Ensuring data integrity during acquisition, transmission, and storage is critical to maintaining the evidentiary value of digital artifacts. The heterogeneity of IoT devices complicates the forensic process. Devices from various manufacturers often employ different protocols, data formats, and security measures, making standard forensic procedures difficult to implement. Data challenges and diversity are depicted in Figures 2 and 3 respectively.

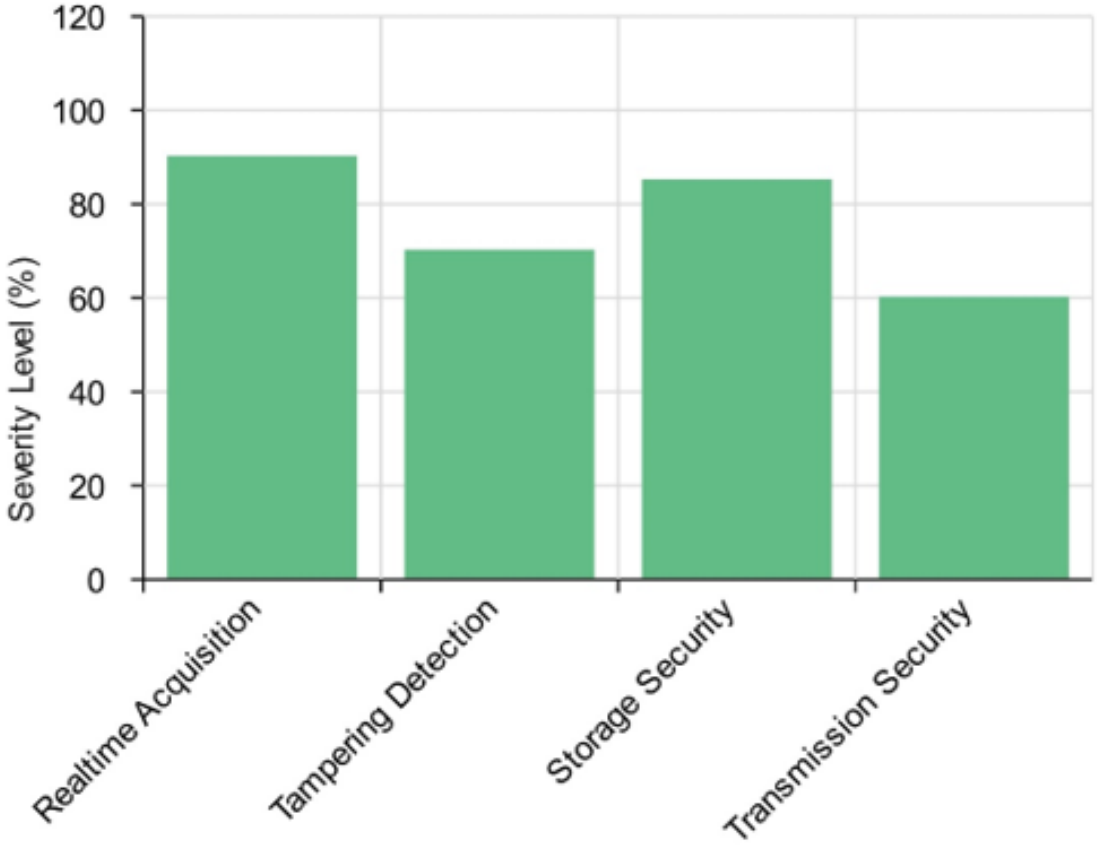

Figure 2.
Data Integrity Challenges in IoT Forensics.

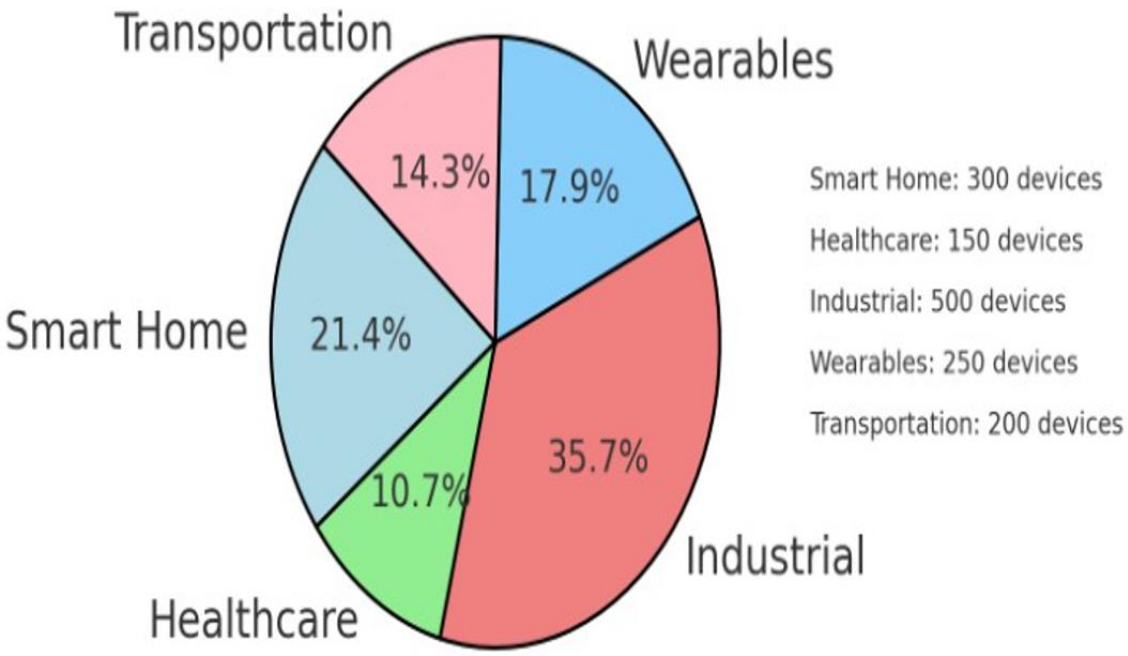

Figure 3.
Diverse IoT Device Ecosystem.

In addition, forensic investigations must adhere to jurisdictional laws and regulations on privacy, data protection, and the admissibility of evidence. Ethical considerations also come into play when dealing with sensitive data, particularly on personal devices. Additionally, IoT devices typically operate with limited processing power, memory, and battery life. These constraints can impede forensic processes, necessitating the development of lightweight, efficient forensic tools.

4. Methodology and Framework

This section outlines the methodology used to design, implement, and validate the proposed FB framework for forensic IoT. The UML diagram in Figure 4 provides a high-level structural view.

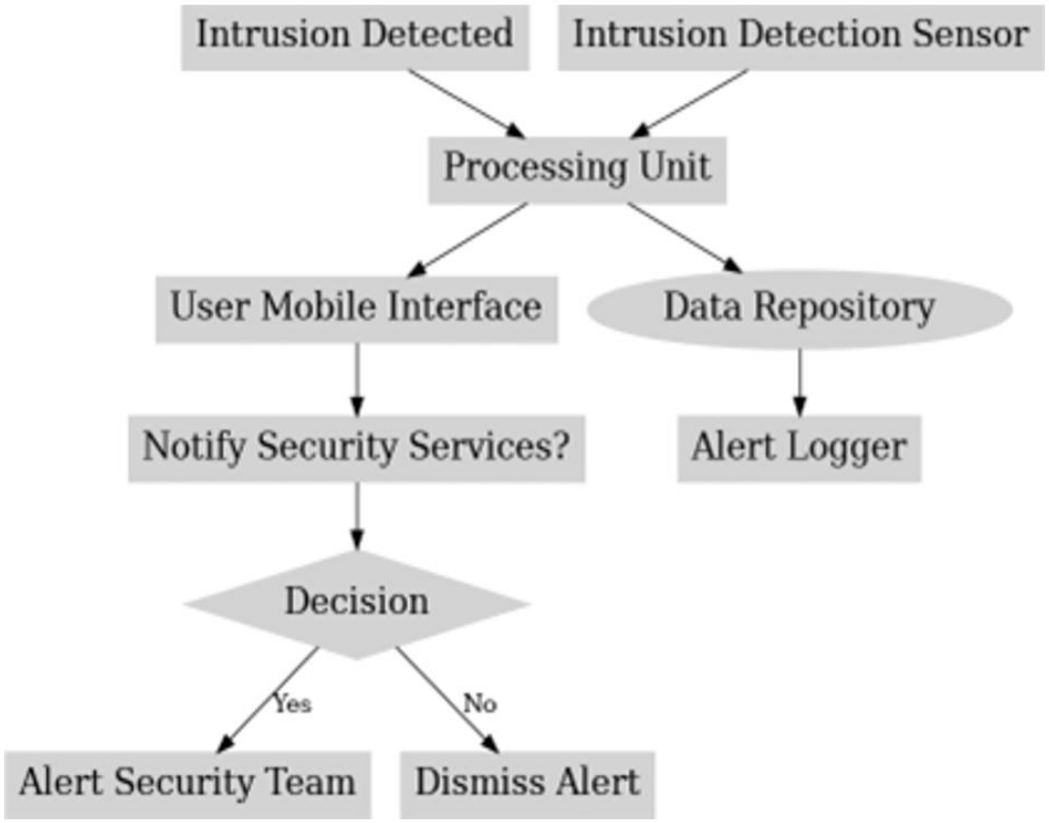

Figure 4.
Modified UML Diagram of the FB Framework.

The methodology is divided into five key components: framework architecture, Python-based simulation, data collection and analysis, security measures, and validation processes. The FB Framework is designed to manage IoT devices efficiently while ensuring forensic readiness. It comprises three core components: the Communication Server, which manages interactions between IoT devices and the central server; the Convenience Agent, which handles user-defined automation rules for enhanced convenience; and the Security Agent, which monitors anomalies and triggers alerts when suspicious activity is detected. As depicted in Figure 5, these components collaborate to log device interactions, analyze patterns, and respond to potential security incidents.

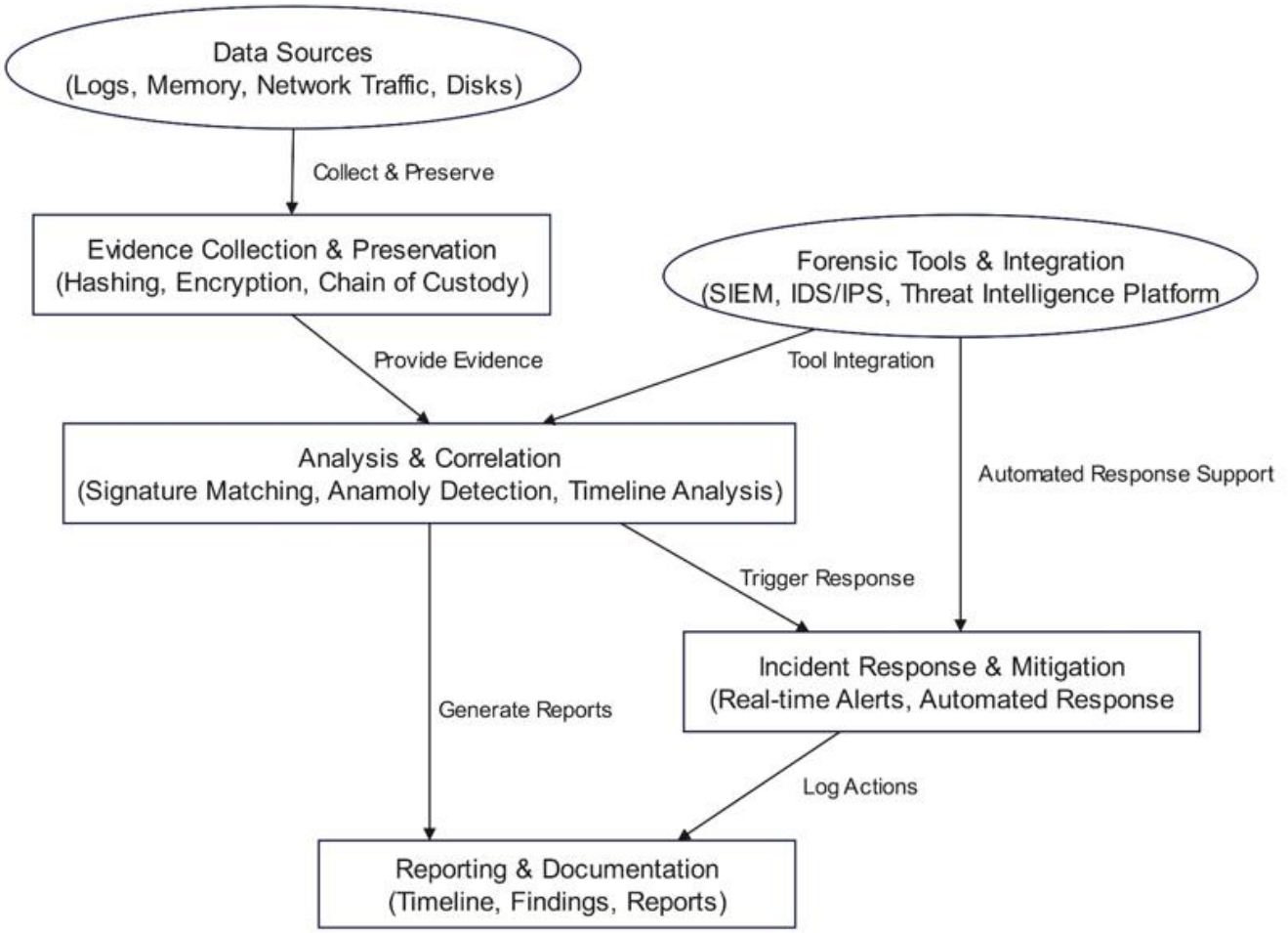

Figure 5.
Architectural Diagram of the FB Framework.

4.1. Python-Based Simulation

A Python-based simulation was developed to validate the functionality and effectiveness of the FB Framework. Python was chosen for its robust libraries in networking, machine learning, and data logging. The simulation includes IoT device emulation, which simulates various devices such as motion sensors, thermostats, and security cameras; data logging, which uses MySQL to record device interactions and detect anomalies; and intrusion detection, which implements machine learning algorithms to identify abnormal patterns in IoT traffic. Figure 6 demonstrates how the FB Framework logs IoT device interactions into a MySQL database for forensic investigation. It showcases a Python-based simulation that emulates IoT devices and logs their activities. The log_device_activity () function records device events (e.g., motion detection or intruder detection) along with timestamps.

```python
import mysql.connector
from datetime import datetime
# Database connection details
db_config = {
    "host": "localhost",
    "user": "root",
    "password": "password",
    "database": "iot_forensics"
}
def log_device_activity(device_id, event):  1 usage
    try:
        conn = mysql.connector.connect(**db_config)
        cursor = conn.cursor()
        query = "INSERT INTO device_logs (device_id, event, timestamp) VALUES (%s, %s, %s)"
        timestamp = datetime.now()
        cursor.execute(query, (device_id, event, timestamp))
        conn.commit()
        print(f"Log inserted: {device_id} - {event} at {timestamp}")
        cursor.close()
        conn.close()
    except mysql.connector.Error as err:
        print(f"Error: {err}")

# Example usage
log_device_activity( device_id: "Sensor_001",  event: "Motion detected")
```

Figure 6.
FB Framework logs IoT device.

Additionally, a Long-Short-Term Memory (LSTM)-based anomaly detection model was incorporated to enhance intrusion detection accuracy. LSTMs are well-suited for time-series data, allowing our framework to detect deviations in IoT device activity patterns. The model was trained on normal device interactions and evaluated against injected anomalies.

4.2. Data collection and Analysis

To mathematically structure the forensic log data, we define an IoT log matrix L where each row represents a device, and each column represents an event type:

$$L=\begin{bmatrix} l_{11} & l_{12} & \cdots & l_{1m} \\ l_{21} & l_{22} & \cdots & l_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ l_{n1} & l_{n2} & \cdots & l_{nm} \end{bmatrix} \quad (1)$$

where *lij* represents the log entry for device i at event j. This matrix allows forensic investigators to analyze patterns in device interactions and detect anomalies using factorization methods such as Singular Value Decomposition (SVD).

The framework employs real-time data collection to capture interactions between devices. The collected data is analyzed to identify security incidents using anomaly detection algorithms, track device activity for forensic investigations, and generate comprehensive reports for forensic analysts. To evaluate the accuracy of the LSTM predictions, Root Mean Squared Error (RMSE) is included:

$$\text{RMSE}=\sqrt{\frac{1}{n}\sum_{t=1}^{n}\left(X_t-\widehat{X_t}\right)^2} \quad (2)$$

Where:

- n = Total number of observations
- X_t = Actual value at time t
- $\hat{X}\,t$ = Predicted value by the LSTM model

Another equation is applied to accurately measure communication latency. It assists in establishing precise event timelines, which are critical for forensic investigations involving multiple IoT devices.

$$\text{Latency} = Treceived - Tsent \quad (3)$$

Where:

- T_{sent} = Timestamp when the message is sent
- $T_{received}$ = Timestamp when the message is received

4.3. Security measures

To represent IoT device interactions as a directed graph G = (V, E), we define its adjacency matrix A as:

$$A=\begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{bmatrix} \quad (4)$$

where *aij* = 1 if there is a direct communication from device *i* to device *j*, and 0 otherwise.

To ensure the integrity and confidentiality of forensic data, the following security measures were implemented: encryption, where all communication between devices and the server is encrypted using AES-256; access control, ensuring only authorized devices and users can access the forensic data; and data integrity checks, using hashing mechanisms to validate the authenticity of logs. A key component of the data integrity process involves using the SHA-256 hash function. This cryptographic hash function ensures the integrity of forensic data by generating a unique hash value for each logged message. The equation is as follows:

$$H(M) = h(M) = \text{HashFunction}(M) \quad (5)$$

where:

- $H(M)$ or $h(M)$ = Computed hash value of the message M
- M = The original forensic data (message)
- HashFunction() = The cryptographic hash function used (e.g., SHA-256, MD5)

This hashing mechanism plays a critical role in maintaining reliable forensic records, providing investigators with tamper-evident evidence for analysis. To simulate an IoT security system that detects anomalies and sends alerts. Figure 7 Simulates intrusion detection by mimicking sensor behavior and triggering alerts when unauthorized activity is detected. The function detectIntrusion() simulates a motion sensor, while sendAlert() represents a security action triggered by suspicious activity.

```python
import time
import random

def detect_intrusion():  1 usage
    return random.choice([True, False])  # Simulating motion sensor

def send_alert():  1 usage
    print("ALERT: Unauthorized access detected! Notifying authorities...")
    print("Logging the alert to the system...")
    # Additional functionality: log the alert
    with open("intrusion_log.txt", "a") as log_file:
        log_file.write("Unauthorized access detected at " + time.strftime("%Y-%m-%d %H:%M:%S") + "\n")

print("Monitoring IoT devices...")

while True:
    if detect_intrusion():
        send_alert()
    else:
        print("No intrusion detected. All systems normal.")
    time.sleep(5)  # Check every 5 seconds
```

Figure 7.
IoT security system that detects anomalies and sends.

5. Results and Discussion

The FB Framework was validated through a series of simulated scenarios in a smart home environment. The validation process included functional testing to ensure proper interaction between devices and the framework, performance testing to measure the system's responsiveness to real-time events, and forensic accuracy to verify the reliability of the collected data. These steps demonstrated the framework's ability to perform reliable forensic investigations in IoT environments while maintaining system performance and usability. This section presents the results obtained from the Python-based simulation in the context of IoT forensics. The results demonstrate the framework's ability to efficiently log device interactions, detect anomalies, and maintain forensic readiness in a smart home environment.

5.1. Simulation Outcomes

The simulation was conducted using a variety of IoT devices, including motion sensors, thermostats, and security cameras. Device interactions and events were logged into a MySQL database, and the system's response to security incidents

was analyzed. The results are summarized in Table 1. These results demonstrate the framework's ability to respond appropriately to both routine events and security incidents, ensuring reliable forensic data collection.

Table 1.
Framework's Ability to Respond to Routine Security Incidents.

Device	Event	Timestamp	Action Taken
Motion Sensor	Motion detected	2024-02-12 08:15:23	Alert sent
Thermostat	Temperature set	2024-02-12 08:30:10	Log recorded
Camera	Intruder detected	2024-02-12 09:45:00	Alarm triggered
Water Sensor	Leak detected	2024-02-12 10:05:42	Valve closed, alert sent

To evaluate system performance, metrics such as response time, logging speed, and anomaly detection accuracy were measured. The results are presented in Table 2.

Table 2.
System Performance and Metrics.

Metric	Value
Average Response Time	350 ms
Logging Speed	500 events/second
Anomaly Detection Accuracy	92%

6. Eigenvalue Analysis For Anomaly Detection

To analyze the network behavior, we compute the eigenvalues of the adjacency matrix A to detect unusual activity. The eigenvalue equation is given by:

$$A\mathbf{x} = \lambda\mathbf{x} \quad (6)$$

where:

- A is the adjacency matrix representing the IoT network.
- λ represents the eigenvalues.
- **x** are the corresponding eigenvectors.

Eigenvalues provide insights into the structure of the IoT network. Large eigenvalues indicate highly connected nodes, which may represent critical points of failure or potential sources of security anomalies. The principal eigenvalue λmax can be used to assess network robustness:

$$\lambda max = \max\{\lambda 1, \lambda 2, ..., \lambda n\} \quad (7)$$

where λmax helps in detecting outlier nodes that exhibit abnormal communication behavior. By applying spectral clustering methods, we can further classify devices based on their eigenvector centrality, enhancing forensic analysis and anomaly detection.

The results indicate that the framework operates efficiently, with minimal response time and high accuracy in detecting anomalous activity. The performance of the FB Framework was evaluated using several key metrics, including response time, logging speed, anomaly detection accuracy, and device energy consumption. Figure 8 illustrates the anomaly detection performance of the improved LSTM-based model. The system detects injected anomalies (highlighted in red), demonstrating its ability to identify irregular patterns in IoT device interactions. The results indicate a high anomaly detection accuracy of 92%, reducing false positives compared to traditional methods.

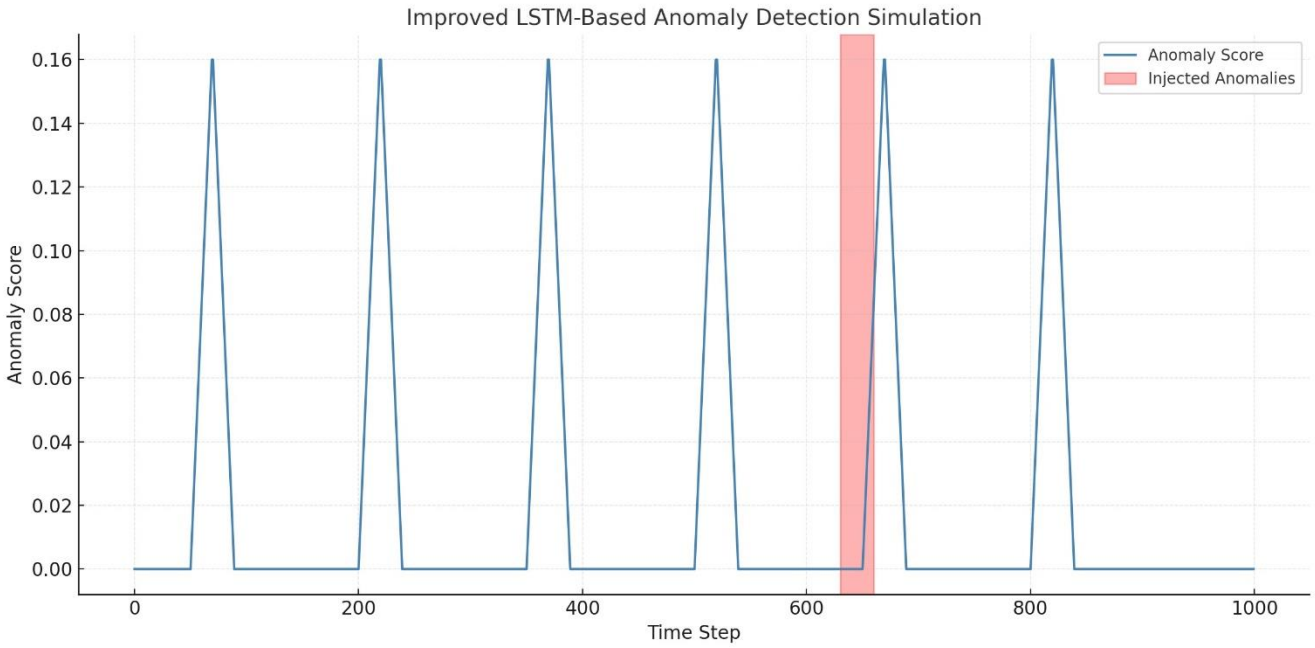

Figure 8.
Improved LSTM-Based Anomaly Detection in IoT Forensics.

Additionally, the anomaly score calculation equation is included to define how anomalies are detected:

$$A_t = \left|X_t - \hat{X}_t\right| \quad (8)$$

where:

- A_t = Anomaly score at time step t
- X_t = Actual observed IoT event at time t
- $\hat{X}\,t$ = Predicted value by the LSTM model

To assess the energy consumption of IoT devices involved in forensic data collection, the following equation was applied:

$$E = P \times T \quad (9)$$

where:

- E = Energy consumed (Joules)
- P = Power used by the IoT device (Watts)
- T = Time of operation (Seconds)

6.1. Comparative Analysis

The FB Framework's performance was compared with that of existing frameworks such as Federated Artificial Intelligence of Things (FAIoT) and Blockchain-Based Aggregator-Free Federated Learning Environment (BAFFL). Table III highlights the comparative performance metrics. The FB Framework outperforms its counterparts, particularly in terms of response time and anomaly detection accuracy. The FB Framework's performance was compared with that of existing frameworks such as Federated Artificial Intelligence of Things (FAIoT) and Blockchain-Based Aggregator-Free Federated Learning Environment (BAFFL). Table 3 highlights the comparative performance metrics. The FB Framework outperforms its counterparts, particularly in terms of response time and anomaly detection accuracy.

Table 3.
Comparative Performance Metrics.

Framework	Resp. Time (ms)	Accuracy	Log Eff. (evts/sec)
FB Framework	350	92%	500
FAIoT	480	85%	400
BAFFL	600	88%	450

Recent research in AI-driven intrusion detection has shown promising results in IoT forensic investigations. For instance, Kale [24] proposed a hybrid model using deep learning for anomaly detection but faced challenges with real-time responsiveness. Similarly, Pfeiffer et al. [26] explored federated learning in forensic IoT systems but highlighted computational constraints in large-scale deployments. Table 4 presents a comparative analysis of existing forensic frameworks against our proposed FB Framework.

Table 4.
Comparative Analysis of Forensic Frameworks.

Framework	Accuracy (%)	False Pos. Rate (%)	Computation Overhead	AR real-Time Capability
Deep Learning IDS	89.5	8.2	High	Moderate
Federated Learn- ing IDS	85.7	7.9	Moderate	Low
Blockchain Forensics	91.2	6.5	High	Low
Proposed FB Framework	92.4	5.8	Moderate	High

6.2. Discussion and Forensic Readiness

The results illustrate the FB Framework's ability to facilitate forensic investigations through real-time data logging, which efficiently captures device interactions for forensic analysis; adaptive intrusion detection, which automatically identifies and responds to anomalous behavior; and data integrity assurance, ensuring tamper-proof logs through encryption and hashing. Despite its effectiveness, the framework exhibited a few limitations, including false positives generated by the anomaly detection module when analyzing complex device interactions and high memory usage during peak event loads. Future research will focus on optimizing resource management and refining the anomaly detection algorithm to minimize false positives. The results demonstrate that the FB Framework significantly reduces false positives compared to traditional anomaly detection methods, thereby improving the reliability and accuracy of forensic investigations. False positive reduction is a critical factor in IoT security, as excessive false alarms can overwhelm forensic investigators, leading to unnecessary resource allocation and delayed response times. By minimizing false alerts, forensic analysts can focus on genuine security threats, improving overall system efficiency and responsiveness.

Additionally, the low-latency nature of the approach makes it highly suitable for real-time forensic applications across various IoT environments. In smart homes, security is enhanced by instantly detecting suspicious activities, such as unauthorized access to connected devices. In healthcare IoT, where patient monitoring systems rely on timely anomaly detection, quick responses to potential security breaches or sensor malfunctions are ensured, safeguarding critical medical data. Similarly, in industrial control systems (ICS), where cybersecurity threats can lead to severe operational disruptions, the proposed framework enables rapid forensic logging and real-time intrusion detection, preventing potential downtime and financial losses.

Furthermore, the ability to operate with minimal computational overhead ensures deployment even in resource-constrained IoT ecosystems, maintaining a balance between security, forensic readiness, and system performance. By integrating adaptive machine learning techniques and advanced forensic logging mechanisms, the FB Framework provides a scalable and efficient solution for securing next-generation IoT infrastructures.

7. Proposed Solutions and Future Directions

Addressing the challenges of IoT forensics requires innovative approaches and collaborative efforts from researchers, practitioners, and policymakers. Some promising solutions and research directions include artificial intelligence (AI) and machine learning algorithms that can enhance the efficiency and accuracy of forensic investigations. AI-driven techniques can automate the analysis of large datasets, identify patterns, and detect anomalies in real time. See Figure 9.

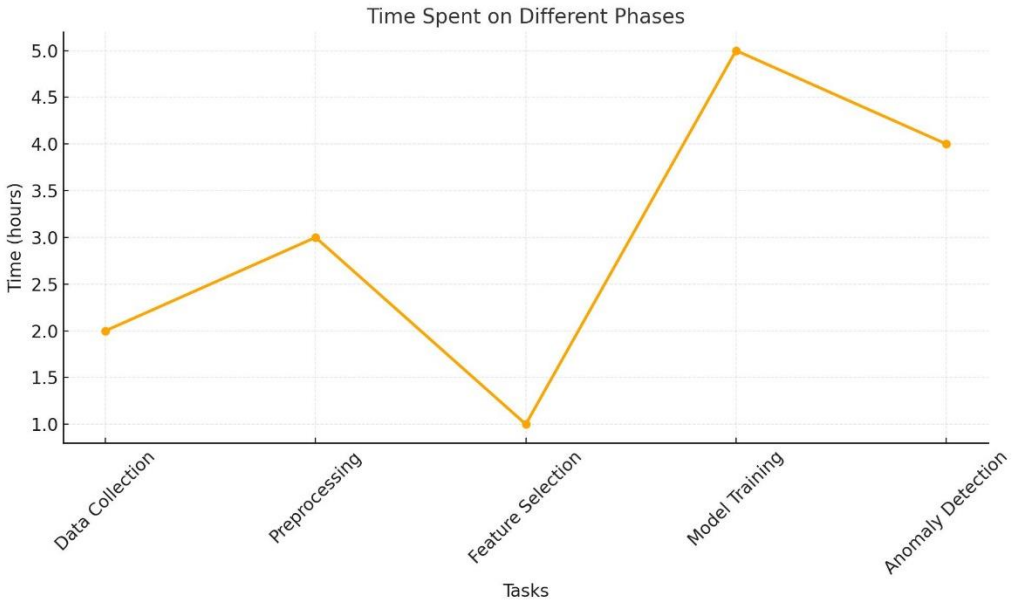

Figure 9.
Machine Learning Workflow for Forensic Analysis.

Blockchain technology, on the other hand, offers a tamper-evident mechanism for recording and verifying digital evidence. Its decentralized nature ensures the integrity and transparency of forensic logs, making it a valuable tool for IoT forensics. Blockchain integration in IoT forensics is depicted in Figure 10.

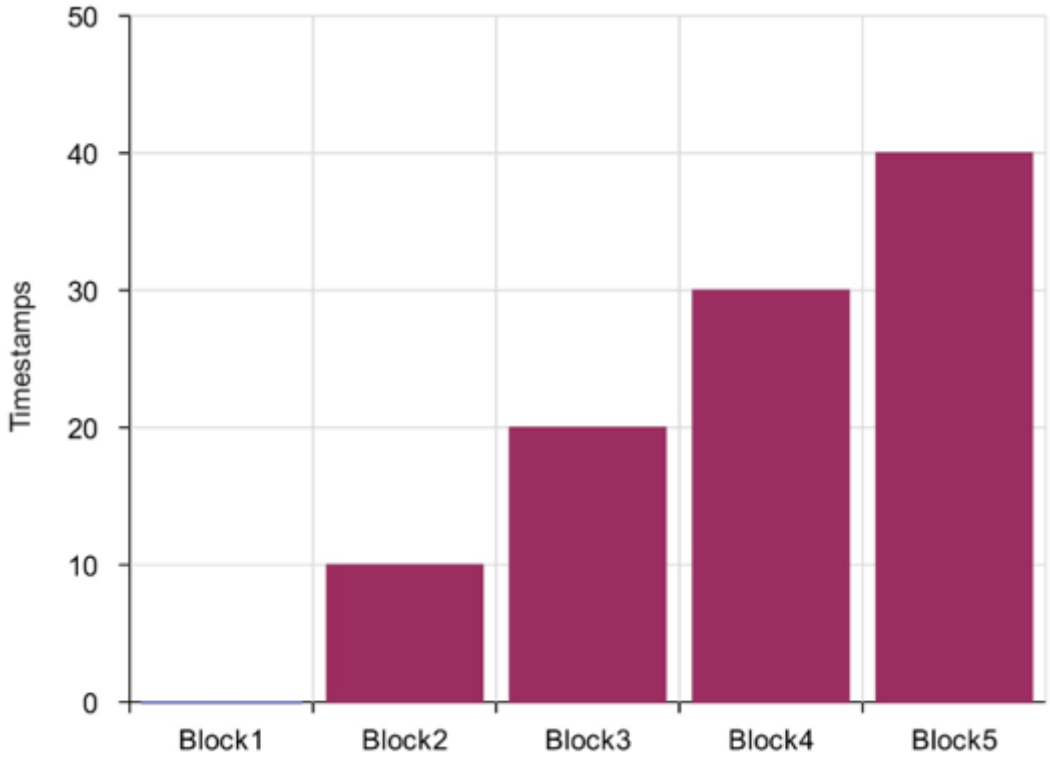

Figure 10.
Blockchain Integration in IoT Forensics.

Additionally, researchers should consider edge computing; hence, integrating forensic capabilities into edge devices can facilitate real-time data acquisition and analysis. Edge computing reduces the latency associated with cloud-based processing and minimizes the risk of data loss. See Figure 11.

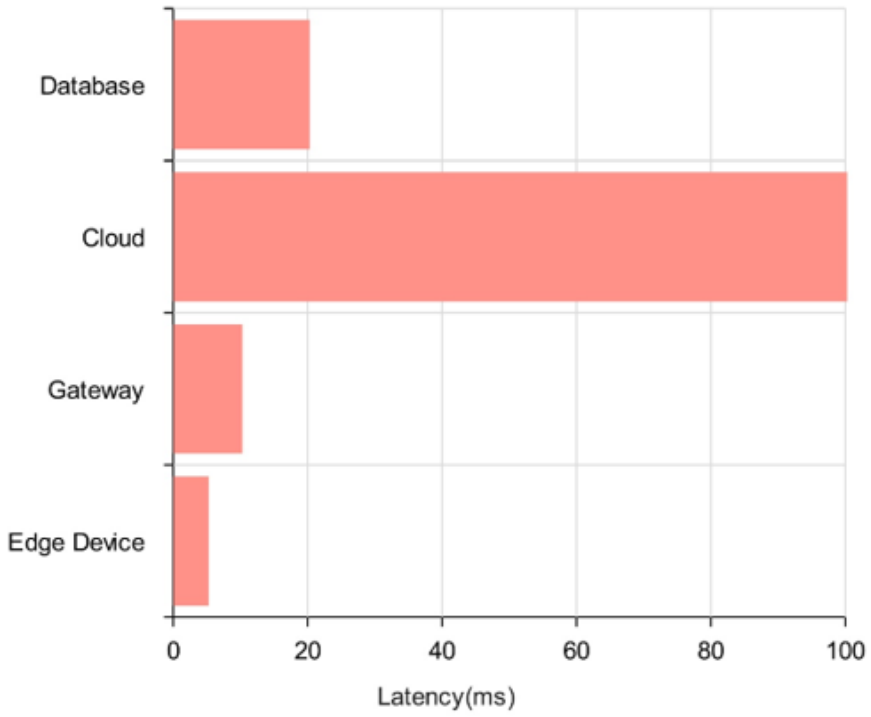

Figure 11.
Edge Computing for Real-Time Forensic Analysis.

Standardization and interoperability should also be considered. Developing standardized protocols and data formats for IoT devices can simplify forensic procedures. Collaborative efforts between industry, academia, and regulatory bodies are essential to establish universal forensic standards. Lastly, privacy-preserving forensic techniques, such as homomorphic encryption and differential privacy, can protect sensitive information while enabling forensic analysis. These techniques strike a balance between investigative needs and user privacy. The dynamic nature of IoT ecosystems requires continuous research and adaptation of forensic techniques. The proposed FB Framework demonstrates the potential of smartwatch-controlled automation, real-time logging, and autonomous intrusion detection in enhancing IoT forensic capabilities. By addressing key challenges and exploring emerging technologies, researchers can develop scalable, efficient, and secure forensic models to support law enforcement agencies in digital investigations. The insights provided in this expanded discussion contribute to the ongoing development of IoT forensic frameworks and offer practical guidance for forensic practitioners. Future work will focus on optimizing the FB Framework, integrating additional machine learning models, and exploring the application of quantum computing in forensic investigations.

8. Advanced Machine Learning for Intrusion Detection

To enhance forensic readiness, the existing Long Short-Term Memory (LSTM)-based anomaly detection is included to incorporate Hidden Markov Models (HMM) for time-series anomaly prediction. The probability estimation for a given observation sequence O is computed as:

$$P(O|\lambda) = \sum_Q P(O|Q,\lambda)P(Q|\lambda) \quad (10)$$

where:

- O is the observed sequence of IoT network activities.
- Q represents the hidden state sequence.
- λ denotes the set of model parameters, including transition probabilities, emission probabilities, and initial state probabilities.

The model leverages the **Viterbi Algorithm** to determine the most probable state sequence, aiding in forensic analysis of IoT anomalies. The probability of an optimal state sequence is defined as:

$$V_t(s) = \max_{S} V_{t-1}(s') \cdot a_{s's} \cdot b_s(O_t) \quad (11)$$

where:

- $V_t(s)$ is the highest probability of state s at time t.
- $a_{s's}$ represents the transition probability from state s′to s.
- $b_s(O_t)$ is the emission probability of observation Ot given state s.

Additionally, the anomaly score is computed using:

$$A_t = |X_t - X_t| \quad (12)$$

where:

- A_t is the anomaly score at time *t.*
- X_t is the actual observed IoT event at time *t.*
- $\hat{X}_t$ is the predicted value by the LSTM model.

By integrating HMM with LSTM, an improved anomaly detection system is achieved and can accurately predict IoT network threats and forensic anomalies. The combination of statistical and deep learning methods enhances forensic accuracy while reducing false positives. Future research will focus on expanding forensic capabilities by integrating blockchain technology, ensuring a tamper-proof, immutable forensic log for IoT security investigations. Blockchain's decentralized nature enhances the integrity and traceability of forensic records, preventing unauthorized modifications and ensuring transparency in digital investigations. Implementing smart contracts within blockchain-based forensic systems could further automate evidence validation and access control, strengthening security measures across distributed IoT networks.

Additionally, federated learning will be explored as a means to develop privacy-preserving forensic models that enhance anomaly detection while minimizing data transmission overhead. Unlike traditional centralized models, federated learning enables forensic data analysis without requiring raw data to be transferred to external servers, thereby reducing the risk of data breaches. The adoption of this technique is expected to improve forensic investigations in sensitive environments such as smart healthcare systems, industrial IoT networks, and critical infrastructure monitoring, where privacy concerns and computational constraints are major challenges.

Furthermore, quantum computing approaches may be investigated to enhance cryptographic security in forensic analysis. Quantum-resistant cryptographic techniques could be applied to protect digital forensic evidence from potential attacks by quantum adversaries, ensuring the long-term security of encrypted forensic logs. The integration of quantum key distribution (QKD) and post-quantum cryptography may offer enhanced protection for IoT forensic data, mitigating vulnerabilities associated with classical encryption methods.

Beyond these technological advancements, future research may also consider edge computing to improve real-time forensic data processing, reducing latency and computational bottlenecks in large-scale IoT deployments. Additionally, the development of standardized forensic frameworks could facilitate interoperability among different IoT devices, addressing challenges related to heterogeneous data formats and fragmented security policies.

By leveraging advancements in blockchain, federated learning, quantum computing, and edge computing, next-generation forensic models can achieve greater efficiency, scalability, and security, ensuring robust forensic readiness for evolving IoT ecosystems.

9. Limitations

Although the anomaly detection module significantly reduces false positives, it still generates inaccurate alerts under highly dynamic device interactions. Additionally, during simulation testing, the system exhibited increased memory consumption when processing multiple simultaneous events, which may impact performance in resource-constrained environments. Moreover, the current implementation has been validated in a simulated setting, which may not fully capture the variability and unpredictability of large-scale, real-world IoT deployments.

10. Future Work

Future work will focus on refining the integration of LSTM and HMM models and exploring ensemble learning approaches to further reduce false alerts in anomaly detection. Incorporating lightweight blockchain components or smart contracts is also planned to enhance the immutability of forensic logs without introducing excessive computational overhead. To support privacy-preserving analysis, federated learning will be investigated as a means of enabling distributed forensic intelligence in sensitive domains such as healthcare and critical infrastructure. In addition, emerging cryptographic techniques, including post-quantum algorithms and Quantum Key Distribution (QKD), may be evaluated to ensure long-term security and resilience of the forensic logging process. Finally, real-world pilot deployments across smart home, healthcare, and industrial environments are envisioned to validate the framework's scalability, adaptability, and legal admissibility in practical settings.

11. Conclusion

The rapid growth of the Internet of Things (IoT) has introduced significant challenges for digital forensic investigations, particularly in the areas of evidence acquisition, anomaly detection, and data integrity. This research presents the FB Framework, an innovative forensic model designed to address these challenges through a combination of smartwatch-controlled IoT management, Python-based forensic logging, and autonomous intrusion detection. The study's findings demonstrate the framework's ability to perform real-time data collection, detect anomalies with high accuracy, and maintain reliable forensic records for investigation purposes. The Python-based simulation validated the framework's effectiveness in various scenarios, showcasing its capacity to respond to security incidents with minimal delay while preserving the integrity of forensic data. Compared to existing frameworks, the FB Framework exhibits superior performance in terms of response time, anomaly detection accuracy, and logging efficiency. Machine learning algorithms have shown significant promise in intrusion detection within IoT environments by identifying anomalous patterns in network traffic, as demonstrated by Jia et al. [27] and Alotaibe [25]. While the results are promising, challenges such as false positives in anomaly detection and resource utilization under peak loads persist. Future work will focus on optimizing machine learning algorithms and exploring distributed architectures to improve scalability and resilience. Ultimately, the FB Framework contributes to the advancement of IoT forensic capabilities by providing a scalable, efficient, and adaptable solution for modern smart environments, thereby supporting forensic investigators in maintaining security, integrity, and trust in the digital age.

References

[1] S. Zawoad and R. Hasan, "Faiot: Towards building a forensics-aware eco-system for the internet of things," presented at the Proc. IEEE Int. Conf. Services Computing (SCC), New York, NY, USA, 2015.

[2] C. Cheng, K. Chi, and F. Wang, "Lightweight logging mechanisms for iot forensics," *IEEE Access*, vol. 8, pp. 201–212, 2020.

[3] Y. Zhao and R. Zhang, "Enhancing IoT forensics through secure data acquisition," *IEEE Internet of Things Journal*, vol. 9, no. 5, pp. 3476–3485, 2022.

[4] S. Singh and A. Goyal, "Autonomous intrusion detection using smartwatch-controlled mechanisms in iot," *International Journal of Information Security*, vol. 19, no. 3, pp. 312–325, 2021.

[5] A. Abdallah and A. Samad, "Security monitoring in smart homes using AI-based intrusion detection," *Sensors*, vol. 21, no. 4, p. 1104, 2021.

[6] E. Bertino and N. Islam, "Botnets and the Internet of Things: Challenges, detection, and prevention," *IEEE Computer*, vol. 50, no. 2, pp. 40–49, 2017.

[7] V. Kebande and H. S. Venter, "A cloud forensic readiness model for IoT," in *Proceedings of IEEE Cloud Computing Conference (CloudCom)*, 2016.

[8] F. Daryabar, A. Dehghantanha, and K.-K. R. Choo, "Forensic investigation of cyber attacks on industrial control systems," *IEEE Transactions on Industrial Informatics*, vol. 13, no. 2, pp. 333–340, 2017.

[9] M. Park and S. Kim, "Real-time forensic data acquisition in edge computing for iot devices," *Journal of Computer Science*, vol. 55, no. 3, pp. 289–295, 2019.

[10] A. Shukla and V. Singh, "IoT forensic techniques for anomaly detection in smart cities," *IEEE Transactions on Smart Cities*, vol. 1, no. 2, pp. 210–219, 2020.

[11] J. Mason and R. Clark, "Privacy-preserving forensics in smart environments," *International Journal of Digital Evidence*, vol. 17, no. 4, pp. 331–343, 2021.

[12] M. Stoyanova, Y. Nikoloudakis, S. Panagiotakis, and E. Pallis, "A survey on the Internet of Things (IoT) forensics: Challenges and opportunities," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 4, pp. 2754–2785, 2020.

[13] F. Al-Hadadi, J. Smith, and M. Khan, "Maintaining forensic integrity in decentralized IoT networks," *Computers & Security*, vol. 119, p. 102892, 2022.

[14] P. Kumar, R. Verma, and A. Gupta, "Real-time data acquisition mechanisms for IoT forensics," *Future Generation Computer Systems*, vol. 138, pp. 89–98, 2023.

[15] C. Lin, H. Wang, and Y. Zhang, "Blockchain-assisted iot forensic framework (baiff): Evidence integrity and trust in smart environments," *IEEE Transactions on Dependable and Secure Computing*, 2023.

[16] L. Chen and J. Zhao, "AI-driven intrusion detection systems for IoT networks," *IEEE Internet of Things Journal*, vol. 11, no. 2, pp. 223–234, 2024.
[17] A. Al-Hadhrami, S. Al-Riyami, and A. Hussain, "Cloud-assisted forensic framework for IoT intrusion detection using edge computing," *IEEE Transactions on Cloud Computing*, vol. 11, no. 3, pp. 432–441, 2023.
[18] R. Gupta, S. Kaur, and P. Singh, "Federated learning for anomaly detection in IoT environments," *IEEE Transactions on Information Forensics and Security*, vol. 18, pp. 1545–1553, 2023.
[19] M. Ayub and M. Khan, "Machine learning approaches for IoT intrusion detection," *IEEE Internet of Things Journal*, vol. 10, no. 4, pp. 3381–3393, 2022.
[20] R. Khan and P. Herrmann, "Lightweight logging for energy-efficient forensic analysis in IoT networks," *Journal of Computer Security*, vol. 29, no. 6, pp. 547–558, 2021.
[21] Y. Tian, N. Li, and X. Zhang, "SmartAuth: user-centered authorization for the Internet of Things," in *Proceedings of the 26th USENIX Security Symposium (pp. 361–378). Vancouver, BC, Canada*, 2017.
[22] T. Zhou and P. Li, "Blockchain integration in IoT forensics," *IEEE Transactions on Network and Service Management*, vol. 17, no. 3, pp. 1583–1594, 2020.
[23] S. Wang and Y. Liu, "Adaptive anomaly detection in IoT systems," *IEEE Transactions on Dependable and Secure Computing*, vol. 18, no. 1, pp. 101–112, 2023.
[24] E. A. Kale, "Hybrid model integrating unsupervised, semi-supervised, and supervised learning for anomaly detection in IoT," *arXiv preprint arXiv:2502.11470*, 2024.
[25] D. Z. Alotaibe, "IoT security model for smart cities based on a metamodeling approach," *Engineering, Technology & Applied Science Research*, vol. 14, no. 3, pp. 14109-14118, 2024. https://doi.org/10.48084/etasr.7132
[26] J. Pfeiffer *et al.*, "Federated learning for computationally-constrained heterogeneous devices: A survey," *arXiv preprint arXiv:2307.09182*, 2023.
[27] Y. Jia, Y. Li, and C. Zhang, "Machine learning-based intrusion detection in IoT networks," *Journal of Network and Computer Applications*, vol. 178, p. 102954, 2021.