The state of IoT forensics: Trends, challenges, and future research directions

Salmon Oliech Owidi[1]
Elyjoy Muthoni Micheni[2]
Lilian Ronoh Cherotich[3]

[1*]salmonowidi@gmail.com

[1,2]Tom Mboya University (TMU), [3]Kaimosi Friends University (KAFU), [1,2,3]Kenya

https://doi.org/10.51867/ajernet.7.2.109

ABSTRACT

The Internet of Things (IoT) has experienced exponential growth across healthcare, agriculture, transportation, and manufacturing sectors, with the number of connected devices projected to reach 29 billion by 2030, simultaneously creating new avenues for cybercriminal activities and unprecedented challenges for digital forensic investigators. This paper provides a comprehensive analysis of the current state of IoT forensics, examining the specialized techniques, tools, and methodologies required to extract, analyze, and preserve digital evidence from IoT devices. Through a qualitative synthesis of 29 recent peer-reviewed studies, key impediments to effective IoT forensic investigations uncovered by this review include device diversity, the absence of uniform technical standards, restrictions in device resources, the ephemeral character of data, and unresolved legal and ethical dimensions surrounding privacy and multi-jurisdictional evidence handling. A concrete finding from this review is that only 3 of the 29 examined studies reported any form of empirical validation in real-world IoT environments. This reveals that most existing IoT forensic frameworks remain theoretical rather than applied, with significant gaps in evidence collection and pre-processing methodologies. This paper acknowledges that its recommendations similarly lack empirical validation, reflecting a broader field-wide challenge rather than a limitation unique to any single study. Nevertheless, this paper recommends the development of standardized forensic frameworks incorporating artificial intelligence and blockchain technologies, mandatory forensic readiness in IoT device design, and enhanced cross-disciplinary collaboration between computer scientists, legal experts, and law enforcement agencies.

Keywords: Cybercrime Investigation, Digital Forensics, Evidence Collection, IoT Forensics, IoT Security

I. INTRODUCTION

The Internet of Things (IoT) represents a network of interconnected devices embedded with electronics, software, sensors, and connectivity capabilities that enable data sharing and automated communication across diverse industries (Atzori et al., 2010). From smart home appliances and wearable health monitors to industrial control systems and autonomous vehicles, IoT devices have become pervasive in modern society. However, this proliferation has introduced significant security vulnerabilities, as many IoT devices lack robust protection mechanisms, standardized security protocols, and firmware update capabilities (Nadir et al., 2022; Gupta et al., 2015).

The expanding use of IoT devices in criminal activities has created an urgent demand for IoT forensics. Consider the 2016 Mirai botnet attack: over 600,000 compromised IoT devices (primarily cameras and routers) were used to launch a record 620 Gbps DDoS attack against DNS provider Dyn (Antonakakis et al., 2017; Kolias et al., 2017). When forensic investigators attempted to trace the attack, they encountered severe practical obstacles most devices had no local storage, logs were overwritten within hours, and evidence resided transiently across cloud servers in multiple jurisdictions (Chernyshev et al., 2018; Ahmed et al., 2024). Such real-world incidents expose the gap between theoretical forensic frameworks and applied investigative capabilities. IoT forensics is a specialized discipline within digital forensics focused on the identification, collection, analysis, and preservation of digital evidence from IoT devices for legal proceedings or incident response (Conti et al., 2018). Unlike traditional digital forensics, IoT forensics must contend with unique challenges including limited device processing power, diverse data formats, volatile memory, cloud-dependent architectures, and the absence of universal forensic methodologies (Chernyshev et al., 2018).

Despite growing research interest in IoT forensics, the field remains nascent and fragmented. Existing literature reveals persistent gaps between theoretical frameworks and practical applications, inadequate attention to procedural and ethical issues, and a lack of standardized tools and protocols (Ahmed et al., 2024; Stoyanova et al., 2020). This paper aims to address these gaps by providing a systematic review of the state of IoT forensics, analyzing current trends, identifying critical challenges, and proposing future research directions.

1.1 Research Objective

To systematically review the state of IoT forensics, analyzing current trends, identifying critical challenges, and proposing future research directions.

II. LITERATURE REVIEW

2.1 Foundational Concepts in IoT Forensics

IoT forensics integrates techniques from traditional digital forensics, network forensics, and cloud forensics to address IoT-related crimes (Oriwoh et al., 2013). The forensic investigation process typically involves several critical phases: seizure and protection of IoT devices, extraction of volatile and non-volatile data, analysis of device data and network communications, event reconstruction, and presentation of findings (Harbawi & Varol, 2017). Unlike conventional digital forensics, IoT investigations often require multiple iterations of these processes as new evidence sources emerge during examination (Kyei et al., 2012).

The complexity of IoT systems arises from their heterogeneous nature devices operate on different operating systems, utilize varied storage systems, employ diverse data formats, and communicate through multiple network protocols (Kouahla et al., 2021). This diversity complicates the development of universal forensic procedures and makes it difficult to replicate and compare results across different devices (Ahmed et al., 2024).

2.2 Existing Review Studies and Their Limitations

Several comprehensive reviews have attempted to survey the IoT forensics landscape. Hou et al. (2019) introduced a three-dimensional framework incorporating temporal, spatial, and technical dimensions to standardize digital investigations in IoT contexts. While valuable, their analysis lacked critical assessment of strengths and weaknesses in reviewed studies. Atlam et al. (2020) examined IoT forensics with emphasis on artificial intelligence integration, discussing opportunities and open research directions, but provided only general discussions of challenges without in-depth critical analysis of individual studies.

Nadir et al. (2022) focused specifically on IoT firmware security, offering an updated assessment of vulnerabilities and solutions, but notably omitted auditing of hardware and network connectivity protocols. Studiawan et al. (2019) surveyed forensic investigation techniques for operating system logs, yet their proposed approaches were not primarily designed for IoT environments, raising questions about applicability and necessary adaptations.

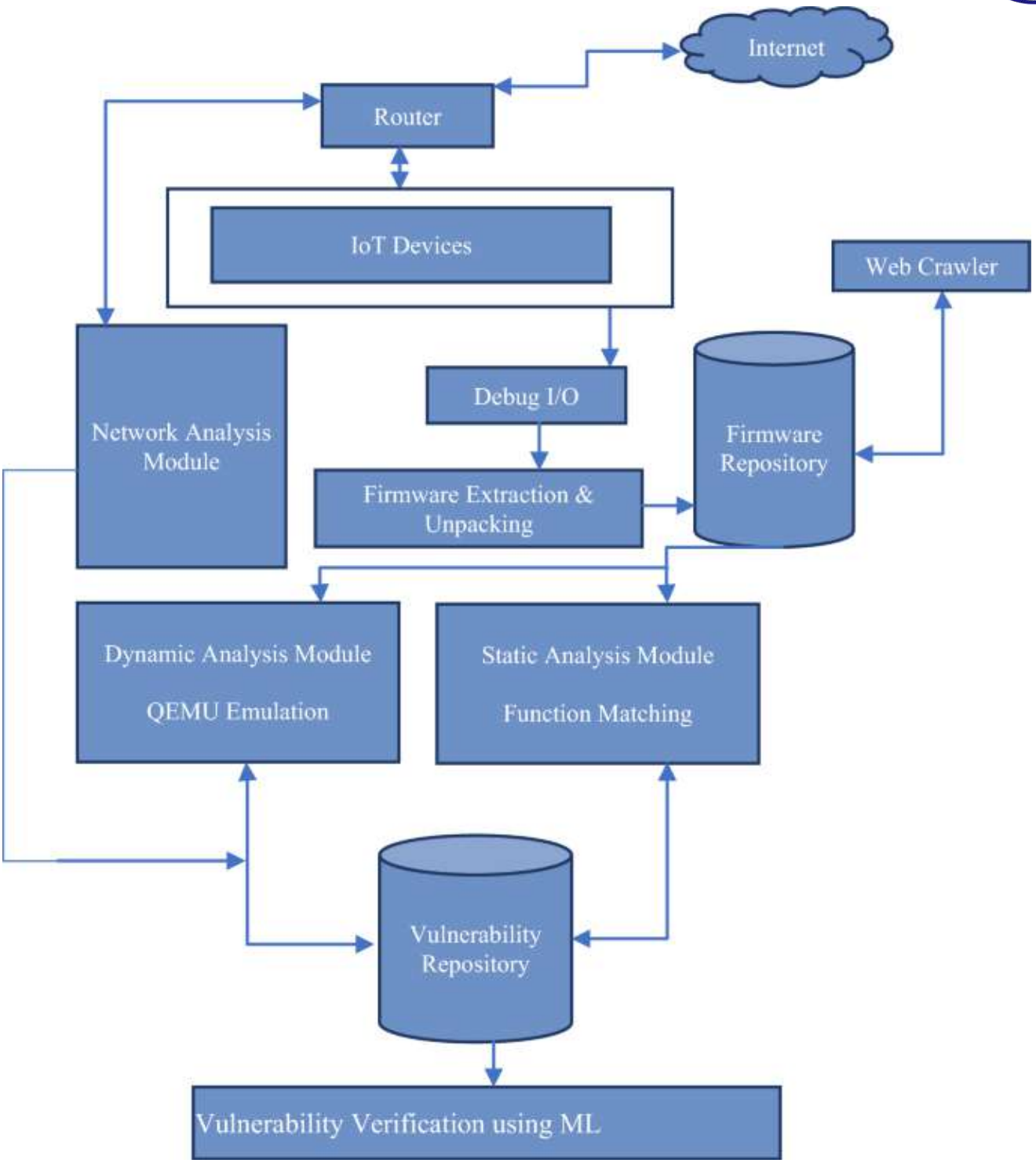

Figure 1

IoT & Embedded Device Firmware Security: Architecture, Extraction Techniques, and Vulnerability Analysis Frameworks

The architecture illustrated in the diagram represents a foundational model for IoT forensic investigation and vulnerability analysis, capturing the interplay between device-level data, network traffic, and firmware integrity. In the context of this study, it demonstrates how forensic processes can be enhanced through automation and intelligent analysis. The model integrates modules for network monitoring, firmware extraction, and dynamic/static analysis, each contributing to the identification and validation of digital evidence within IoT ecosystems. As Ahmed et al. (2024) emphasize, the complexity of IoT environments demands scalable frameworks capable of handling heterogeneous data sources and counter-forensic techniques. By incorporating machine learning for vulnerability verification, this architecture exemplifies the emerging trend toward AI-driven IoT forensics, offering a pathway to improve evidence reliability, investigative efficiency, and forensic readiness in future IoT systems.

Table 1

Comparative Analysis of Prior IoT Forensics Studies: Contributions and Weaknesses

Module	Function	Relevance to IoT Forensics
IoT Devices & Router	Capture data and connect to the Internet.	Represents the entry point for forensic evidence collection, where device logs, sensor data, and communication traces originate.
Network Analysis Module	Monitors traffic and identify anomalies.	Supports forensic investigation by detecting suspicious patterns, intrusion attempts, or data exfiltration routes.
Firmware Extraction & Unpacking	Retrieves device firmware for analysis.	Critical for identifying embedded vulnerabilities and reconstructing attack vectors, a major challenge noted in Ahmed et al. (2024).
Static & Dynamic Analysis Modules	Static analysis inspects code; dynamic analysis emulates execution (QEMU).	These parallel processes reveal both latent and active threats, addressing the need for hybrid forensic techniques in IoT environments.
Firmware Repository & Web Crawler	Collects and updates firmware samples.	Enables large-scale comparative analysis and supports forensic readiness by maintaining reference datasets.
Vulnerability Repository	Stores discovered flaws and exploits.	Acts as a forensic evidence database, facilitating cross-case correlation and trend analysis.
Vulnerability Verification using ML	Applies machine learning to validate and classify vulnerabilities.	Demonstrates the emerging role of AI in IoT forensics, automating detection and improving accuracy in evidence interpretation.

Most significantly, a systematic literature review by Lutta et al. (2021) concluded that most existing studies remain theoretical rather than applied, identifying this as a fundamental research gap. Similarly, Ahmed et al. (2024) noted that despite numerous proposed frameworks, none adequately address the full range of data types, applications, or jurisdictional requirements that may be involved in real-world forensic inquiries.

2.2.1 Tool Validation Gap

Few standardized testing techniques exist to evaluate the reliability and accuracy of IoT forensic tools and methodologies (Ahmed et al., 2024). Existing tools such as Cellebrite UFED, XRY, Autopsy, Magnet AXIOM, Wireshark, and Splunk primarily designed for mobile, computer, or network forensics are frequently adapted to IoT contexts without rigorous validation. Kaushik et al. (2024) rated Cellebrite and XRY 5/5 for mobile forensics but noted limited IoT-specific validation; Magnet AXIOM received 4/5 for usability and integration across computer, mobile, and limited IoT contexts. Validation studies have been attempted, including Shin et al. (2024) who validated a forensic methodology on Samsung SmartThings, Aqara, and Hikvision cameras, and Rizvi et al. (2024) who achieved >99.6% accuracy on the CICIoT2023 dataset using an AI-driven forensic framework on Raspberry Pi devices.

Table 2

Existing Tools used in validation

Tool Category	Specific Tools	Validation Status
Mobile/Device Forensics	Cellebrite UFED, XRY	Rated 5/5 for mobile; limited IoT-specific validation (Kaushik et al., 2024)
Open-Source Forensics	Autopsy, FTK	Validation ongoing (Fairbanks et al., 2024)
Commercial Multi-Platform	Magnet AXIOM	Rated 4/5 usability/integration; IoT validation limited (Kaushik et al., 2024)
Network Traffic Analysis	Wireshark, tcpdump	5/5 for accuracy; IoT network layer applicable
Log Analytics	Splunk, ELK Stack	5/5 scalability; not forensics-native

However, critical validation gaps persist: no standardized testing methodology exists across these tools, comparative validation on identical IoT device sets is rare, and most studies report accuracy without measuring false positive/negative rates relevant to court admissibility. The absence of shared benchmark datasets for IoT forensics analogous to DFRWS scenarios for traditional forensics remains a fundamental obstacle to rigorous tool validation.

2.3 Iot Forensic Layers

The IoT forensic architecture can be conceptualized as three interconnected layers, each presenting distinct evidence sources and investigative challenges (Ahmed et al., 2024; Alenezi et al., 2019).

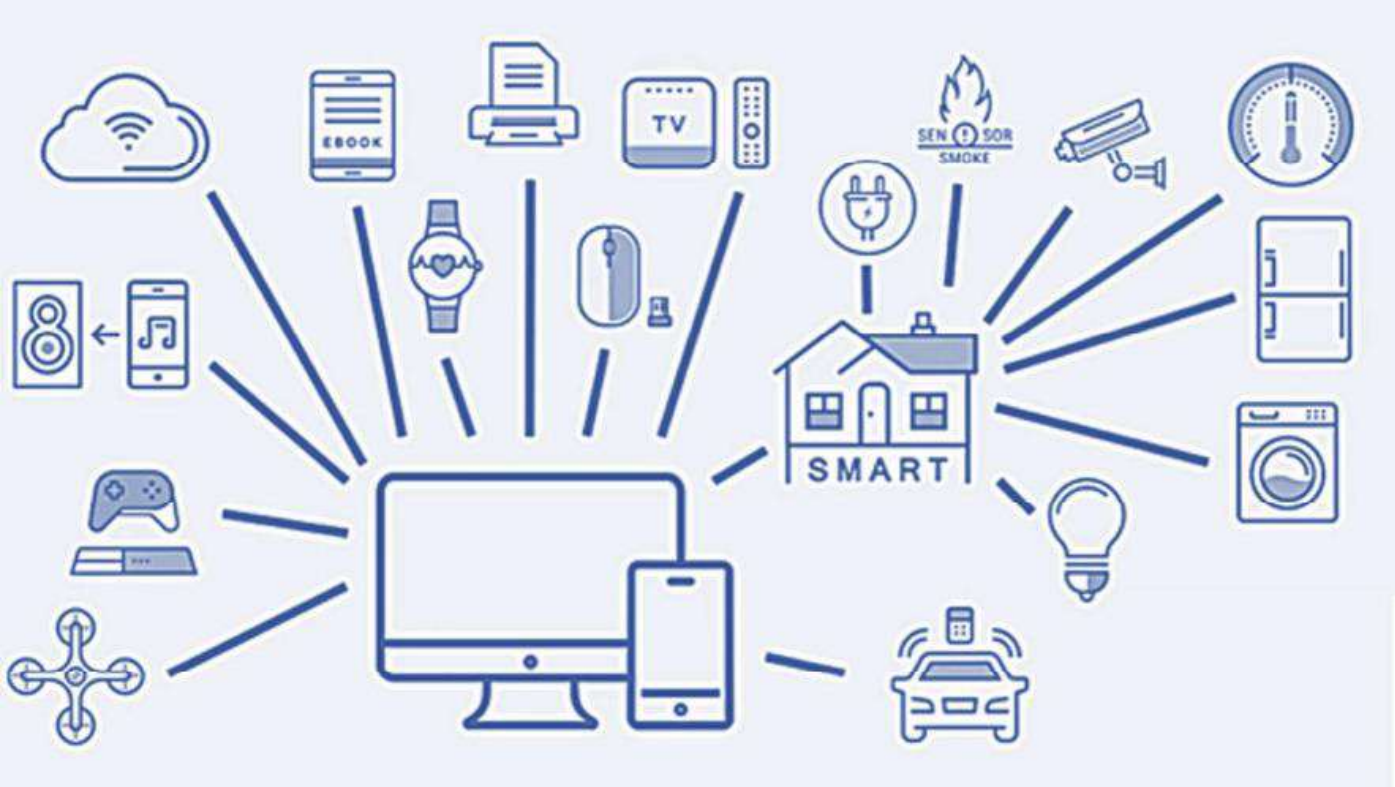

Figure 2
Internet of Things Connected Anytime Anywhere with Anchor Device.

The Internet of Things (IoT) represents a vast and intricate ecosystem where sensors, smart devices, and embedded systems interact continuously through diverse communication channels and data infrastructures. This interconnected framework, spanning RFID networks, Wi-Fi, mobile, and wired systems, creates both opportunities and complexities for digital investigations. While IoT enhances automation and intelligent data processing, it simultaneously introduces forensic challenges due to the exponential growth of connected devices and the dynamic nature of data exchange (Harbawi & Varol, 2017). The widespread adoption of cloud services and virtualization further complicates evidence acquisition, as transient data and distributed architectures often obscure digital traces. Consequently, traditional forensic approaches may prove inadequate for analyzing volatile IoT environments, underscoring the need for adaptive, forensic-ready models capable of addressing the evolving landscape of IoT-related crimes. IoT exist into the following layers;

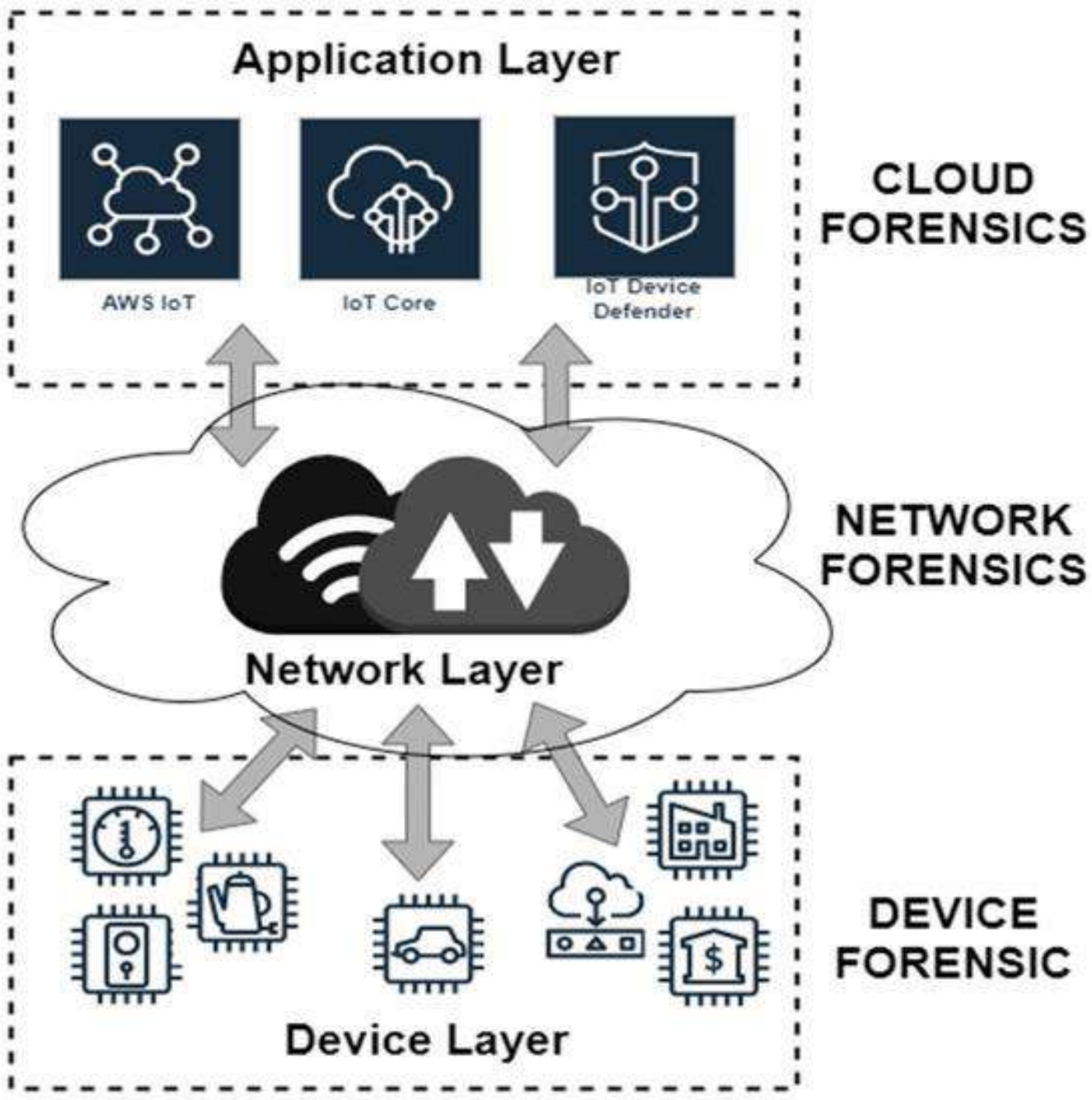

Figure 3
Forensic Layers

2.3.1 Device Layer Forensics

The device layer encompasses the physical IoT devices themselves, including CCTV cameras, medical implants, smart home appliances, networked vehicles, and unmanned aerial vehicles. Evidence may be acquired from local device memory, including audio recordings, images, videos, log files, user behavior data, sensor readings, heart rate data, configuration data, telemetry data, and device state information. However, the absence of universal forensic methods for this layer remains a significant obstacle, as different devices employ proprietary storage formats and encryption mechanisms (Ahmed et al., 2024).

Acquisition techniques at the device layer range from minimally invasive methods to more destructive approaches. Minimally invasive techniques include Joint Test Action Group (JTAG) interfaces, In-System Programming (ISP), and Universal Asynchronous Receiver-Transmitter (UART) connections, which can enable full physical acquisition of onboard memory without permanently altering the device (Scientific Working Group on Digital Evidence [SWGDE], 2024). When these methods are unavailable or insufficient, chip-off analysis the physical removal of a memory chip from the device circuitry may be necessary, though this technique risks data loss or damage to the original evidence due to the heat exposure required during the removal process (Kumar, 2024). Emerging alternatives such as in-circuit memory analysis offer non-destructive data acquisition directly from microchip-level components, preserving

device operability while maintaining forensic soundness (Kumar, 2024). The choice of acquisition method depends critically on device type, storage architecture, and the evidentiary requirements of the investigation.

Beyond the devices themselves, forensic examiners should also consider evidentiary sources connected to IoT devices. Companion applications installed on smartphones or computers such as those used to configure smart home devices or monitor fitness trackers often contain residual data, cached communications, and configuration logs that can be recovered using traditional forensic tools (SWGDE, 2024). Additionally, third-party cloud services integrated with IoT devices (e.g., media content providers for smart speakers, monitoring services for smart sensors) may independently store data that complements or duplicates manufacturer-held evidence, sometimes with different retention policies or legal access requirements (SWGDE, 2024). Real-world casework has demonstrated the evidentiary value of this layer: data extracted from a victim's Fitbit device was successfully used to establish time of death and contradict witness accounts in multiple homicide investigations (Lorenz et al., 2026). These examples underscore that device layer forensics requires a holistic approach encompassing not only the target device but also its associated digital ecosystem.

2.3.2 Network Layer Forensics

The network layer comprises the various networks connecting IoT devices to each other and to the internet, including Personal Area Networks (PANs), Body Area Networks (BANs), Wide Area Networks (WANs), Home Area Networks (HANs), and Local Area Networks (LANs). Leveraging the logging and auditing capabilities of these networks can yield legally admissible evidence to trace users within the IoT ecosystem. Network forensic analysis examines traffic patterns, communication records, and device interactions to reconstruct events and identify anomalous behavior (Stoyanova et al., 2020; Ahmed et al., 2024).

2.3.3 Cloud Layer Forensics

Due to the storage and computational constraints of IoT devices, most IoT ecosystems rely on cloud computing for data storage and processing. The cloud layer stores client-centric artefacts and relevant data including authentication logs, access records, system logs, database transactions, and application logs (Alenezi et al., 2019). Major cloud platforms introduce specific forensic challenges. AWS IoT Core, for example, stores device data across region-specific buckets with varying legal access requirements, and its default logging retention periods are often too short for criminal investigations (Ahmed et al., 2024). Azure IoT Hub presents difficulties in reconstructing device-to-cloud message flows because telemetry data is frequently encrypted end-to-end and deleted after predefined time windows. Google Cloud IoT Core (discontinued in 2023 but still operational in legacy deployments) compounds these issues by distributing evidence across multiple proprietary services including Pub/Sub, Cloud Functions, and BigQuery, each with independent logging and access controls.

Beyond platform-specific obstacles, extracting evidence from cloud environments presents universal challenges related to data jurisdiction (evidence may reside on servers in countries with differing legal frameworks), service provider cooperation (providers may delay or refuse access without proper legal process, which can take months across international boundaries), and the volatile nature of cloud-stored data (logs and temporary storage may be purged automatically within hours or days) (Alenezi et al., 2019; Ahmed et al., 2024).

2.4 Gaps in Existing Research

Based on the reviewed literature, several critical gaps emerged: Methodological Gap: There is a scarcity of empirically validated, practical forensic frameworks designed for large-scale IoT environments (Ahmed et al., 2024; Lutta et al., 2021). Standardization Gap: The absence of universal standards for IoT forensic procedures, evidence formats, and tool validation impedes cross-jurisdictional investigations and courtroom admissibility (Stoyanova et al., 2020). Privacy and Legal Gap: Existing models inadequately address privacy protection, user consent, and multi-jurisdictional legal requirements throughout the forensic process (Le et al., 2018; Ahmed et al., 2024). Forensic Readiness Gap: Most IoT devices are designed without consideration for forensic preparedness, lacking logging capabilities, secure evidence preservation mechanisms, and tamper-resistant features (Alenezi et al., 2019). Tool Validation Gap: Few standardized testing techniques exist to evaluate the reliability and accuracy of IoT forensic tools and methodologies (Ahmed et al., 2024).

III. METHODOLOGY

This study employed a systematic literature review methodology to assess the current state of IoT forensics, synthesize existing knowledge, identify research gaps, and propose future directions, consistent with best practices for evidence synthesis in digital forensics (Lutta et al., 2021). The review was guided by four primary research questions: what are the main trends and emerging techniques in IoT forensics; what critical technological, procedural, legal, and ethical challenges confront investigators; what limitations exist in current frameworks and methodologies; and what future research directions are needed to advance the field from theoretical models to practical applications.

A systematic search was conducted across five major academic databases IEEE Xplore, ScienceDirect, SpringerLink, ACM Digital Library, and MDPI using a Boolean search string combining terms such as "*IoT forensics," "Internet of Things forensics," "digital forensics," "challenges," "frameworks," "evidence collection," "AI," "machine learning," "blockchain," "cloud forensics," and "network forensics."* Forward and backward snowballing was also applied to reference lists of seminal papers (e.g., Atzori et al., 2010; Conti et al., 2018) and key review studies (e.g., Ahmed et al., 2024; Stoyanova et al., 2020) to ensure comprehensive coverage.

Inclusion criteria required peer-reviewed journal articles, conference proceedings, and authoritative book chapters published in English between 2010 and 2024, focusing on IoT-specific forensic challenges, frameworks, tools, or case studies. Exclusion criteria eliminated sources lacking any peer-review mechanism (e.g., blog posts, white papers, preprints), studies limited to general digital forensics without IoT specificity, and articles not available in full text. Peer-reviewed conference proceedings were retained given their significant contributions to this rapidly evolving field. Following duplicate removal and title, abstract, and full-text screening, 29 core studies were selected for in-depth analysis, including the 25 cited references plus four foundational works.

A standardized data extraction form captured bibliometric information, research focus, proposed framework features, identified challenges, limitations (particularly theoretical versus applied status), and proposed future directions. Thematic synthesis was then employed, using iterative coding to identify recurring patterns that were grouped into five thematic categories presented in the findings: artificial intelligence applications, network architecture and frameworks, blockchain-based solutions, cutting-edge techniques (electromagnetic side-channel analysis, operating system logs, audiovisual biometrics), and procedural, legal, and ethical challenges. The systematic criteria adopted is as per the diagram below. Comparative analysis of frameworks was summarized in tabular form, and a critical assessment was made of gaps between theoretical proposals and empirical validation, as highlighted by Lutta et al. (2021) and Ahmed et al. (2024).

IV. FINDINGS & DISCUSSION

4.1 Artificial Intelligence in IoT Forensics

4.1.1 Current State and Applications

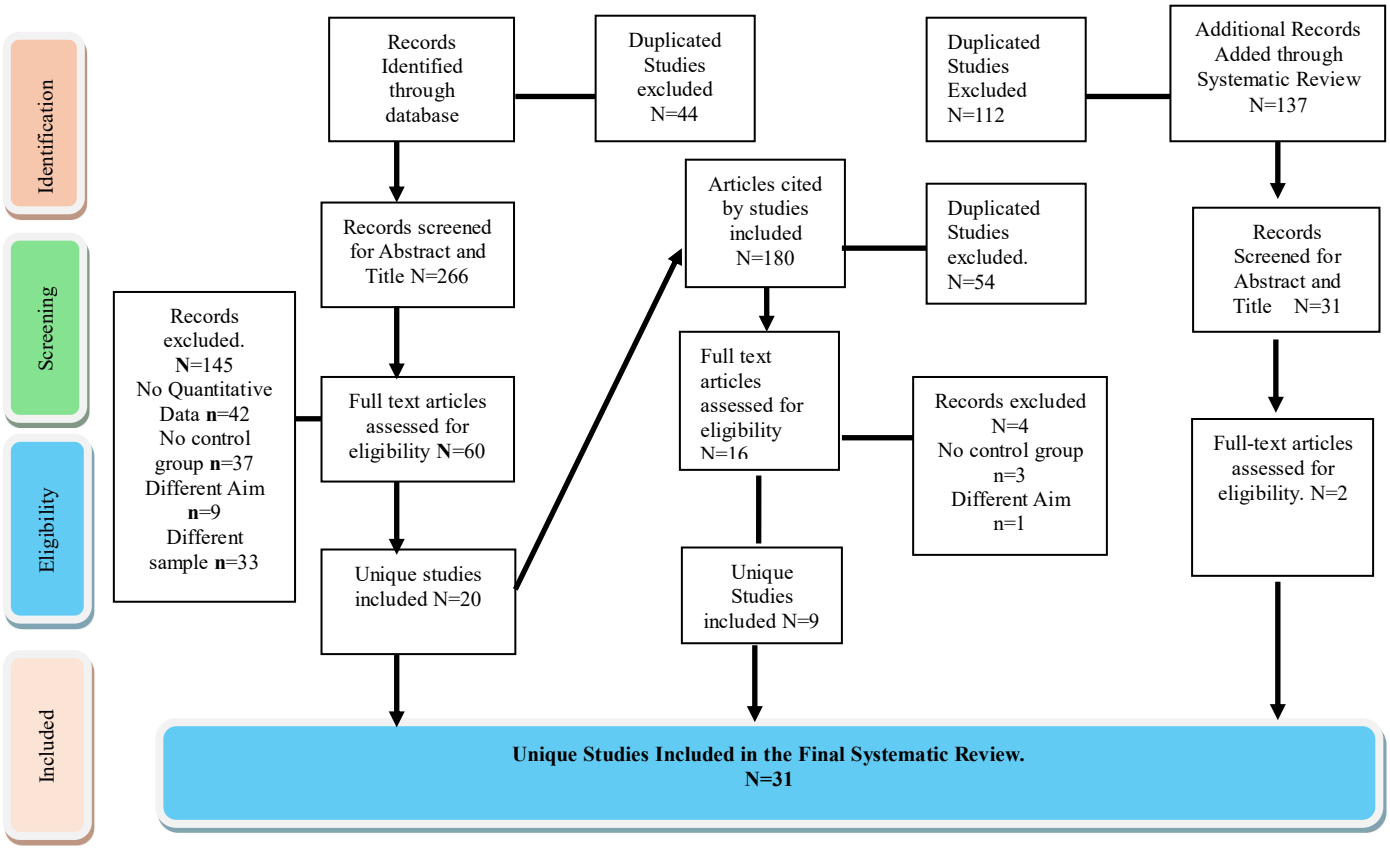

Figure 4
Systematic Literature Review - Flowchart

Artificial intelligence (AI) and machine learning (ML) techniques have emerged as promising tools for addressing IoT forensic challenges, particularly for handling the vast volumes of heterogeneous data generated by IoT devices. Atlam et al. (2020) provided a comprehensive examination of AI's role in IoT forensics, emphasizing its necessity for successful forensic investigations in complex IoT environments. AI applications include automated evidence identification, anomaly detection in network traffic, device fingerprinting, and predictive analytics for attack vector identification.

Yadav et al. (2020) developed systematic frameworks for categorizing IoT device fingerprinting mechanisms, enabling more reliable device identification during investigations. Similarly, Yousefnezhad et al. (2021) demonstrated automated IoT device identification based on full packet information using real-time network traffic analysis, achieving high accuracy rates in controlled environments a significant limitation, as performance in noisy, real-world conditions with previously unseen device types remains unvalidated.

4.1.2 Challenges and Limitations

Despite these advances, significant challenges remain. Almohlis et al. (2021) identified critical requirements that IoT forensic process models must address, noting that most AI-based approaches lack proper calibration, verification, and independent replication fundamental requirements for court-admissible digital evidence. Additionally, AI models trained on specific IoT ecosystems may not generalize to diverse device types or configurations. Ahmed et al. (2024) concluded that further research is needed to establish frameworks capable of successfully handling the vast volumes of data produced by heterogeneous IoT devices while maintaining forensic soundness.

Beyond generalization concerns, AI-based forensic systems face specific technical vulnerabilities that investigators must understand. Deep learning models commonly used in IoT forensics are susceptible to adversarial attacks, including poisoning attacks during training and inference attacks during testing, which can compromise the integrity of forensic evidence (Ding et al., 2024). These vulnerabilities are particularly concerning in legal contexts where evidence integrity must be proven beyond reasonable doubt. Furthermore, most existing AI forensic solutions have been validated using synthetic or laboratory-generated datasets rather than real-world IoT incident data, raising questions about their operational effectiveness under authentic forensic conditions (Qureshi et al., 2024). The absence of standardized, publicly available IoT forensic datasets comparable to those in traditional digital forensics (e.g., DFRWS datasets) compounds this validation problem. Another critical limitation is the computational overhead of AI-based forensic analysis on resource-constrained IoT edge devices, which may preclude real-time forensic readiness in many deployment scenarios (Rizal et al., 2025).

4.1.3 Future Directions

Future research should focus on developing AI-based forensic investigation frameworks specifically designed for smart home environments, where multiple heterogeneous devices generate interconnected evidence streams. Additionally, the integration of explainable AI (XAI) techniques may help address the "black box" problem that currently undermines courtroom admissibility of AI-derived evidence. The legal principle that forensic evidence must be interpretable by human stakeholders is not merely technical but constitutional in many jurisdictions, as black box AI systems have been shown to perform predictably worse in criminal justice settings compared to interpretable alternatives (Garrett & Rudin, 2023).

Several promising directions warrant investigation. First, lightweight AI models specifically optimized for resource-constrained IoT edge devices could enable forensic readiness without compromising device performance; privacy-preserving BERT variants and lightweight models like GEADD have demonstrated potential for real-time forensic applications in constrained IoT and Industrial IoT (IIoT) environments (Da Silva De Queiroz, 2025). Second, automated forensic readiness frameworks that combine AI with ISO/IEC 27043 standards could serve as early warning systems capable of detecting, collecting, and analyzing various types of IoT attacks automatically while maintaining evidentiary integrity (Rizal et al., 2025). Third, systematic validation methodologies using diverse, real-world IoT forensic datasets are urgently needed, as current research lacks comprehensive IoT-specific datasets that reflect the complexity of actual forensic scenarios (Qureshi et al., 2024). Finally, interdisciplinary approaches combining deep learning with traditional forensic methods may yield more robust solutions for malware detection and forensic analysis in heterogeneous IoT ecosystems (Qureshi et al., 2024).

4.2.1 Zone-Based Architectures

Le et al. (2018) proposed a blockchain-based IoT forensic framework (BIFF) that divides IoT networks into three zones; internal, middleware, and external, applying triaging concepts to the forensic investigation model. According to the researchers, this architecture is suitable for internal incident responders. However, Ahmed et al. (2024) critically noted that the model excludes IoT devices and applications from the investigation scope, operating exclusively at the network layer and failing to address user privacy concerns or provide mechanisms to protect user identification in collected data.

Subsequent research has attempted to address these limitations through multi-blockchain architectures. A multi-blockchain model proposed for forensic investigations of IoT devices on distributed networks leverages different blockchains optimized for distinct aspects of the forensic process, including data integrity verification, evidence logging, and chain of custody management (Rizal et al., 2025). Experimental results demonstrate that such multi-blockchain approaches significantly enhance reliability, accuracy, and efficiency compared to single-blockchain or non-blockchain methods, particularly in distributed network environments where evidence may be fragmented across multiple jurisdictions (Rizal et al., 2025). More recent innovations include IoTP4Chain, a system that leverages programmable data plane technology to collect, identify, aggregate, and filter IoT forensic data based on a taxonomy of preprocessing functions before storing evidence on a blockchain, thereby addressing scalability bottlenecks that have historically limited blockchain adoption in IoT forensics (Susin et.al, 2024).

4.2.2 Process Model Requirements

Stoyanova et al. (2020) conducted a comprehensive review of digital forensic process models specific to IoT contexts, defining requirements that IoT forensic process models must fulfill to be applicable to IoT organizations. Their analysis of existing cloud forensic process models against identified requirements revealed significant gaps in standardizing cloud forensics. The study emphasized that public organizations and legal authorities must recognize that IoT forensics still trails behind other established areas of digital forensics, demanding further funding and research.

Contemporary process models have evolved to address these gaps. An enhanced digital forensic model specifically designed for IoT environments takes a comprehensive approach spanning the entire investigation process from establishing Standard Operating Procedures (SOPs) during pre-investigation to archival of evidence on secure backup servers during post-investigation (Rao, 2024). This model addresses critical existing challenges, including the need for consistent methods to regularly update databases encompassing device types, manufacturers, and communication protocols a problem that has historically impeded IoT forensic investigations (Rao, 2024). Furthermore, standardized frameworks such as ISO/IEC 27043 have been adapted specifically for IoT forensic readiness, providing structured approaches that combine technical forensic processes with legal and procedural considerations (Rizal et al., 2025).

4.2.3 Systematic Literature Review Findings

Lutta et al. (2021) conducted a systematic literature review of IoT forensic advancements, focusing on data recovery and acquisition, file systems, and data analysis techniques. Their critical finding that most existing studies remain theoretical rather than applied represents a fundamental challenge requiring realistic, implementable solutions. The review concluded that intelligent and efficient tools that are scientifically validated are necessary to guide digital investigations in complex IoT environments.

A more recent systematic review of deep learning solutions for malware detection and forensic analysis in IoT (Qureshi et al., 2024) organized the literature into four distinct categories: IoT Security, Malware Forensics, Deep Learning, and Anti-Forensics. This review identified several persistent research gaps that extend beyond those noted by Lutta et al. (2021), including: (1) the need for comprehensive IoT-specific datasets that reflect real-world forensic conditions; (2) the integration of interdisciplinary methods combining computer science, law, and criminal justice; (3) scalable real-time detection solutions capable of operating on resource-constrained devices; and (4) advanced countermeasures against anti-forensic techniques that criminals increasingly employ to conceal IoT-related criminal activities (Qureshi et al., 2024) . The review further emphasized that the primary issue remains the complexity of IoT malware and the fundamental limitations of current forensic methodologies, calling for a robust methodological framework to guide future research toward more effective security solutions.

4.3.1 Capabilities and Implementations

Blockchain technology has attracted significant attention for IoT forensic applications due to its inherent capabilities for ensuring chain of custody, privacy, integrity, provenance, traceability, and evidence verification throughout the investigation process (Akinbi et al., 2022). Most proposed models are based on permissioned blockchains, though the same architectures could theoretically be applied to permissionless blockchains such as Bitcoin, Ethereum, Algorand, Avalanche, and Polkadot. Akinbi et al. (2022) conducted a systematic literature review of blockchain-based IoT forensic investigation process models, evaluating the effectiveness of various proposed models and proof-of-concept prototypes based on outcomes and performance metrics. The evaluation identified several concerns and unsolved issues, including scalability limitations, transaction costs, and integration challenges with existing forensic workflows.

Recent innovations have advanced beyond single-blockchain architectures. The IoTP4Chain system addresses the fundamental scalability challenge of blockchain-based IoT forensics by moving preprocessing functions to the programmable data plane, enabling efficient data collection, aggregation, and filtering before blockchain storage (Susin et.al, 2024). This approach allows forensic investigators to handle the exponential growth of IoT data without creating

blockchain bottlenecks. Additionally, multi-blockchain models have been proposed for distributed IoT networks, where evidence may be scattered across numerous devices, cloud services, and jurisdictions. In such environments, each blockchain within the model is optimized for a different aspect of the forensic process separate chains for data integrity verification, evidence logging, chain of custody management, and access control thereby improving both security and operational efficiency (Susin et.al, 2024).

4.4 Critical Gaps

Ahmed et al. (2024) identified a noticeable absence of descriptive studies on blockchain-based IoT forensic models, noting that most models remain theoretical due to the lack of prototypes established to indicate their practical applications. Unlike the evidence collection weaknesses highlighted in other categories, blockchain-based approaches face distinct challenges related to practical deployment, including the computational overhead of blockchain operations on resource-constrained IoT devices and the need for empirical security assessments.

Beyond blockchain-specific gaps, broader critical gaps persist across the IoT forensics landscape. Qureshi et al. (2024) identified the absence of comprehensive IoT-specific forensic datasets as a primary obstacle to progress, noting that researchers cannot rigorously validate tools or compare methodologies without standardized, publicly available data. Additionally, the integration of anti-forensic countermeasures remains severely underdeveloped; as criminals employ increasingly sophisticated methods to circumvent forensic techniques including data obfuscation, encryption, and remote wiping forensic methodologies must evolve correspondingly (Qureshi et al., 2024). The lack of scalable real-time detection solutions for large-scale IoT deployments represents another critical gap, particularly as IoT networks continue to expand at compound annual growth rates exceeding 24% (Susin et.al, 2024). Finally, the persistent divide between technical forensic research and legal evidentiary requirements remains unbridged; while AI and blockchain solutions show technical promise, their courtroom admissibility has not been systematically evaluated against the legal standards that vary across jurisdictions (Garrett & Rudin, 2023).

4.5 Future Research Needs

Future research should conduct empirical examinations of the security aspects of current blockchain-based IoT forensic investigation models, including quantitative performance evaluations and real-world deployment studies. Additionally, researchers should explore hybrid models that combine blockchain with other technologies such as AI and edge computing to address current limitations.

4.6 Cutting-Edge and Emerging Techniques

4.6.1 Electromagnetic Side-Channel Analysis

Sayakkara et al. (2019) provided a comprehensive survey of electromagnetic (EM) side-channel analysis for enhancing digital forensic investigations of IoT devices. EM side-channel analysis utilizes unintentional electromagnetic emissions to monitor computer activity and data processing without requiring physical changes to the target device making it particularly suitable for forensic applications where evidence integrity is paramount.

The authors examined various EM side-channel attack methodologies, selecting those with potential for IoT device evaluation scenarios. While EM side-channel analysis has demonstrated effectiveness as a *"door opener"* for cryptographically secured data storage and communication, its application in digital forensics remains in its infancy. The technology requires court-admissible, forensically sound processing protocols before it can significantly impact the industry and expedite stalled investigations involving secure IoT devices (Sayakkara et al., 2019; Ahmed et al., 2024).

4.6.2 Operating System Log Forensics

Studiawan et al. (2019) conducted a thorough analysis of forensic investigation techniques for operating system logs, constructing a taxonomy based on generic investigation methods including event log recovery, event correlation, event reconstruction, and visualization. Their review of publicly available datasets used in OS log forensic research revealed a primary challenge: insufficient utilization of shared datasets, which impedes the evaluation and comparison of proposed solutions for efficiency.

Susin et.al (2024) addressed legal, privacy, and cloud security issues, providing an overview of both historical and contemporary theoretical frameworks in digital forensics. Notably, the author highlighted the importance of proactive forensic readiness initiatives and widely recognized standards, concluding that attackers continue to employ increasingly intricate methods to circumvent forensic techniques, necessitating sophisticated countermeasures.

4.6.3 Audiovisual Biometric Forensics for Smart Cities

Ross et al. (2020) explored cutting-edge digital forensic techniques for audiovisual biometric data applicable to smart city applications. Smart cities comprise networks of interconnected IoT devices that must communicate with each other and with humans, with biometric authentication serving to protect human-machine interactions. However, ensuring security and privacy when dealing with biometric data presents unique challenges. The study examined existing digital

image, audio, and video-based forensic approaches applied to biometric data, with particular focus on challenges posed by deepfake audios and videos an emerging threat requiring continuous methodological adaptation.

Recent work by Malik et al. (2024) demonstrated federated learning-based deepfake detection for smart city IoT networks, achieving high accuracy while preserving citizen privacy. Similarly, Sharma and Gupta (2025) proposed multi-modal forensic methods combining image, video, and metadata analysis to detect manipulation in Internet of Multimedia Things (IoMT) systems. However, Rao and Krishnan (2024) caution that current legal frameworks for CCTV surveillance are inadequate for AI-driven biometric identification systems deployed in public spaces.

4.7 Procedural, Legal, and Ethical Challenges

4.7.1 Procedural Problems

Beyond technological challenges, Ahmed et al. (2024) identified significant procedural problems related to preparedness, reporting, and presentation. Many organizations lack forensic readiness plans, leaving them unprepared to preserve evidence when security incidents occur. The absence of standardized reporting formats complicates evidence presentation across different jurisdictions. Additionally, the multi-iterative nature of IoT investigations increases the volume of data requiring analysis, creating resource-intensive burdens, particularly in large-scale investigations involving hundreds or thousands of devices (Ahmed et al., 2024; Harbawi & Varol, 2017).

4.7.2 Legal and Jurisdictional Issues

Multiple jurisdictions present particular challenges for IoT forensics, as data may be stored on clouds located in different countries, devices may be manufactured in one jurisdiction, owned in another, and the crime may occur across national boundaries (Surange & Khatri, 2021). Each jurisdiction may have different requirements for evidence admissibility, data privacy, and law enforcement authority. Alenezi et al. (2019) acknowledged the difficulty of incorporating various jurisdictional requirements but suggested considering commonalities across frameworks to simplify and improve the process.

4.7.3 Ethical and Privacy Concerns

Privacy requirements for IoT forensics include transparency (consumers must be informed about forensic analysis techniques, policies, and practices applied to their data), data access (consumers must have access to their data throughout the investigation), accountability (investigators must adhere to privacy regulations), information security (collected personal data must be protected against unauthorized access, loss, or alteration), and compliance (auditing tools must ensure the investigation process adheres to privacy standards) (Le et al., 2018; Ahmed et al., 2024).

Zia et al. (2017) emphasized that much information gathered from IoT devices may be deemed personal by device owners, and IoT architectures may collect location information without explicit user consent. These ethical considerations must be balanced against evidentiary needs a tension that remains inadequately addressed in current frameworks.

4.8 Discussion

4.8.1 Interpretation of Findings

The findings of this review reveal that IoT forensics remains an emerging field characterized by significant gaps between theoretical frameworks and practical applications. While researchers have proposed numerous models incorporating AI, blockchain, and cutting-edge techniques, few have been empirically validated in real-world IoT environments. This disconnect between theory and practice represents the most critical obstacle to advancing the field (Lutta et al., 2021; Ahmed et al., 2024).

The challenges identified span technological, procedural, legal, and ethical domains, suggesting that solutions require interdisciplinary collaboration. Technological challenges device heterogeneity, resource constraints, and lack of standardization may be partially addressed through AI and blockchain integration, but these technologies introduce their own complexities. Procedural challenges around forensic preparedness and reporting require organizational and policy interventions. Legal and ethical challenges demand engagement with legal scholars, policymakers, and privacy advocates.

4.8.2 Implications for Research and Practice

For researchers, the findings indicate several priority areas: (1) development of empirically validated forensic frameworks tested in real-world IoT environments; (2) creation of standardized testing methodologies for forensic tools; (3) investigation of privacy-preserving forensic techniques; and (4) exploration of AI-driven automation for evidence identification and analysis.

For practitioners and law enforcement, the findings underscore the importance of forensic readiness planning and the need for continuous training as IoT technologies evolve. Organizations should implement real-time logging, volatile data processing capabilities, and support for diverse hardware and file systems (Ahmed et al., 2024). Law

enforcement agencies should develop protocols for multi-jurisdictional IoT evidence handling and establish partnerships with cloud service providers.

For IoT manufacturers and policymakers, the findings argue for mandatory forensic readiness requirements in IoT device design. Nadir et al. (2022) noted that many IoT devices contain outdated, poorly written code with potential exploits and lack mechanisms for updating firmware. Regulatory frameworks should require minimum security and logging standards, similar to data protection requirements in GDPR.

V. CONCLUSION & RECOMMENDATIONS

5.1 Conclusion

This paper has provided a comprehensive analysis of the state of IoT forensics, examining current trends, critical challenges, and future research directions through systematic review of recent literature, particularly the 2024 survey by Ahmed and colleagues. IoT forensics differs fundamentally from traditional digital forensics due to the unique characteristics of IoT devices limited processing power, device heterogeneity, diverse network architectures, cloud dependency, and the convergence of virtual and physical environments.

The findings reveal that although numerous theoretical frameworks have been proposed, significant gaps remain between research and practical application. Critical challenges cluster around five domains: evidence collection and pre-processing (exacerbated by counter-analysis techniques and cross-device data gathering difficulties), procedural problems (particularly preparedness and reporting), legal and jurisdictional complexities, ethical and privacy concerns, and the absence of standardized testing methodologies for forensic tools.

Key technological approaches including artificial intelligence for automated analysis, blockchain for chain-of-custody preservation, and emerging techniques such as electromagnetic side-channel analysis for cryptographically secured devices show promise but require further empirical validation and standardization. The systematic literature review concluded that most existing studies remain theoretical, a finding that reinforces the urgent need for applied, implementable solutions.

Moving forward, the IoT forensics community must prioritize the development of empirically validated frameworks, mandatory forensic readiness in device design, standardized testing methodologies, and privacy-preserving investigative techniques. Interdisciplinary collaboration between computer scientists, legal experts, law enforcement agencies, and IoT manufacturers will be essential to address the multi-faceted challenges identified. As IoT devices continue to proliferate across every domain of human activity, from healthcare to transportation to criminal enterprises, the importance of robust, reliable, and legally sound IoT forensic capabilities will only increase. The time for theoretical proposals has passed; the field now requires practical, validated solutions capable of withstanding legal scrutiny and operational demands.

5.2 Recommendations

Based on the systematic review of 29 studies and the identified gaps in IoT forensics literature, this paper offers the following recommendations. Researchers should prioritize empirically validated frameworks tested in real-world IoT environments beyond laboratory settings, develop explainable AI systems to address courtroom admissibility concerns, and create standardized benchmark datasets analogous to DFRWS for traditional forensics. IoT manufacturers must incorporate forensic readiness by design, including built-in logging capabilities, secure evidence preservation, and tamper-resistant features, while policymakers should introduce regulatory requirements for minimum security and logging standards similar to GDPR but tailored to forensic preparedness. Law enforcement agencies need internal protocols for multi-jurisdictional IoT evidence handling and formal partnerships with major cloud providers (AWS, Azure, Google Cloud) to expedite evidence access. Finally, the research community should establish standardized testing methodologies for IoT forensic tools, conduct empirical performance assessments of blockchain-based models in production environments, and develop privacy-preserving techniques that balance evidentiary needs with user rights.

Declaration of Interest

The authors declare that they do not have any known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Funding Declaration

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

REFERENCES

Ahmed, A. A., Al-Bakri, K., Al-Othman, A., Gara, A. G., & Abdullah, W. A. (2024). A state-of-the-art review of IoT forensics: Challenges, techniques, and future directions. *Sensors*, *24(*16), 5210.

Akinbi, A., MacDermott, A., & Ismael, A. M. (2022). A systematic literature review of blockchain-based Internet of Things (IoT) forensic investigation process models. *Forensic Science International: Digital Investigation*, *42*, 301470.

Alenezi, A., Atlam, H., Alsagri, R., Alassafi, M., & Wills, G. (2019). IoT forensics: A state-of-the-art review, challenges and future directions. In *Proceedings of the 4th International Conference on Complexity, Future Information Systems and Risk (COMPLEXIS 2019)* (pp. 106-115). Crete, Greece.

Almohlis, N., Alashjaee, A. M., & Haney, M. (2021). Requirements for IoT forensic models: A review. In K. Daimi, H. R. Arabnia, L. Deligiannidis, M. S. Hwang, & F. G. Tinetti (Eds.), *Advances in Security, Networks, and Internet of Things* (pp. 123-138). Springer.

Antonakakis, M., April, T., Bailey, M., Bernhard, M., Bursztein, E., Cochran, J., ... & Yegneswaran, V. (2017). Understanding the Mirai botnet. In *Proceedings of the 26th USENIX Security Symposium* **(**pp. 1093-1110).

Atlam, H. F., Hemdan, E. E.-D., Alenezi, A., Alassafi, M. O., & Wills, G. B. (2020). Internet of Things forensics: A review. *Internet of Things*, *11*, 100220.

Atzori, L., Iera, A., & Morabito, G. (2010). The internet of things: A survey. *Computer Networks*, *54*(15), 2787-2805.

Chernyshev, M., Zeadally, S., Baig, Z., & Woodward, A. (2018). Internet of things forensics: The need, process models, and open issues. *IT Professional*, *20*(3), 40-49.

Conti, M., Dehghantanha, A., Franke, K., & Watson, S. (2018). Internet of Things security and forensics: Challenges and opportunities. *Future Generation Computer Systems*, *78,* 544-546.

Da Silva De Queiroz, H. J. (2025). Explainable AI in high-stakes forensic decision-making. In *AI in Digital Forensics and Cybercrime Investigation* (pp. 245-278). IGI Global.

Ding, W., Abdel-Basset, M., Ali, A. M., & Moustafa, N. (2024). A survey of intelligent multimedia forensics for internet of things communications: Approaches, strategies, perspectives, and challenges for a sustainable future. *Engineering Applications of Artificial Intelligence*, *136,* 109234.

Fairbanks**,** J., Arifin, M. M., Afreen, S., & Curtis, A. (2024). Survey and analysis of IoT operating systems: A comparative study on the effectiveness and acquisition time of open-source digital forensics tools. *ArXiv Preprint:2407.01474*.

Garrett, B. L., & Rudin, C. (2023). Interpretable algorithmic forensics. *Proceedings of the National Academy of Sciences*, *120*(41), e2301842120.

Gupta, J., Nayyar, A., & Gupta, P. (2015). Security and privacy issues in internet of things (IoT). *International Journal of Research in Computer Science, 2*(4), 18-22.

Harbawi, M., & Varol, A. (2017). An improved digital evidence acquisition model for the Internet of Things forensic I: A theoretical framework. In *Proceedings of the 2017 5th International Symposium on Digital Forensic and Security (ISDFS)* (pp. 1-6). Tirgu Mures, Romania.

Hou, J., Li, Y., Yu, J., & Shi, W. (2019). A survey on digital forensics in Internet of Things. *IEEE Internet of Things Journal*, *7*(1), 1-15.

Kaushik, K., Bhardwaj, A., & Dahiya, S. (2024). Unique taxonomy and review of new age smart home IoT forensics tools. *Recent Advances in Computer Science and Communications*, *19*(2). 1-19. DOI: https://doi.org/10.2174/0126662558335096241012163610

Kolias, C., Kambourakis, G., Stavrou, A., & Voas, J. (2017). DDoS in the IoT: Mirai and other botnets. *Computer***,** *50*(7), 80-84.

Kouahla, Z., Benrazek, A. E., Ferrag, M. A., Farou, B., Seridi, H., Kurulay, M., Anjum, A., & Asheralieva, A. (2021). A survey on big IoT data indexing: Potential solutions, recent advancements, and open issues. *Future Internet*, *14*(1), 19.

Kumar, V. S. (2024). *In-circuit forensic analysis of IoT memory modules* (Doctoral dissertation). Edith Cowan University. https://doi.org/10.25958/3rrf-j702

Kyei, K., Zavarsky, P., Lindskog, D., & Ruhl, R. (2013). A review and comparative study of digital forensic investigation models. In *Proceedings of the Digital Forensics and Cyber Crime: 4th International Conference, ICDF2C 2012* (pp. 314-327). Lafayette, IN: Springer.

Le, D.-P., Meng, H., Su, L., Yeo, S. L., & Thing, V. (2018). BIFF: A blockchain-based IoT forensics framework with identity privacy. In *Proceedings of the TENCON 2018-2018 IEEE Region 10 Conference* (pp. 1234-1239). Jeju, Republic of Korea.

Lorenz, S., Stinehour, S., & Chennamaneni, A. (2026). A case study on the use of Amazon visual ID facial recognition metadata in investigation. *Forensic Science International: Digital Investigation*, *46,* 301700.

Lutta, P., Sedky, M., Hassan, M., Jayawickrama, U., & Bakhtari Bastaki, B. (2021). The complexity of internet of things forensics: A state-of-the-art review. *Forensic Science International: Digital Investigation*, *38*, 301210.

Malik, A., Khan, S., & Lee, J. (2024). Federated deepfake detection for smart city IoT networks. *IEEE Internet of Things Journal*, *11*(8), 13456-13468.

Nadir, I., Mahmood, H., & Asadullah, G. (2022). A taxonomy of IoT firmware security and principal firmware analysis techniques. *International Journal of Critical Infrastructure Protection*, *37*, 100552.

Oriwoh, E., Jazani, D., Epiphaniou, G., & Sant, P. (2013). Internet of things forensics: Challenges and approaches. In *Proceedings of the 9th IEEE International Conference on Collaborative Computing: Networking, Applications and Worksharing* (pp. 608-615). Austin, TX.

Qureshi, S. U., He, J., Tunio, S., Zhu, N., Nazir, A., Wajahat, A., Ullah, F., & Wadud, A. (2024). Systematic review of deep learning solutions for malware detection and forensic analysis in IoT. *Journal of King Saud University - Computer and Information Sciences*, *36*(8), 102164.

Rao Gudlur, V. V. (2024). Enhanced digital forensic model for securing the Internet of Things. *2024 IEEE 14th Symposium on Computer Applications & Industrial Electronics (ISCAIE)*, 5-9. DOI: 10.1109/ISCAIE61308.2024.10576479

Rao, P., & Krishnan, S. (2024). AI biometric surveillance in public spaces: Legal and ethical challenges. *Computer Law & Security Review*, *52*, 106015.

Rizal, R., Selamat, S. R., Mas'ud, M. Z., & Widiyasono, N. (2025). Enhanced readiness forensic framework for the complexity of Internet of Things (IoT) investigation based on artificial intelligence. *Journal of Advanced Research in Applied Sciences and Engineering Technology*, *50*(1), 121-135.

Rizvi, S., Scanlon, M., McGibney, J., & Sheppard, J. (2024). Pushing network forensic readiness to the edge: A resource constrained artificial intelligence-based methodology. 2024 *Cyber Research Conference - Ireland (Cyber-RCI)*, 1-8. IEEE.

Ross, A., Banerjee, S., & Chowdhury, A. (2020). Security in smart cities: A brief review of digital forensic schemes for biometric data. *Pattern Recognition Letters*, *138*, 346-354.

Sayakkara, A., Le-Khac, N.-A., & Scanlon, M. (2019). A survey of electromagnetic side-channel attacks and discussion on their case-progressing potential for digital forensics. *Digital Investigation*, *29*, 43-54.

Sharma, R., & Gupta, V. (2025). Multi-modal forensic analysis for Internet of Multimedia Things. *Forensic Science International: Digital Investigation*, *52,* 301800.

Shin, D-H., Han, S-J., Kim, Y-B., & Euom, I-C. (2024). Research on digital forensics analyzing heterogeneous Internet of Things incident investigations. *Applied Sciences*, *14*(3), 1128.

Stoyanova, M., Nikoloudakis, Y., Panagiotakis, S., Pallis, E., & Markakis, E. K. (2020). A survey on the internet of things (IoT) forensics: Challenges, approaches, and open issues. *IEEE Communications Surveys & Tutorials*, *22*(2), 1191-1221.

Studiawan, H., Sohel, F., & Payne, C. (2019). A survey on forensic investigation of operating system logs. *Digital Investigation*, *29*, 1-20.

Surange, G., & Khatri, P. (2021). IoT Forensics: A review on current trends, approaches and foreseen challenges. In *Proceedings of the 2021 8th International Conference on Computing for Sustainable Global Development (INDIACom)* (pp. 909-913). New Delhi, India.

Susin, R. P., Parizotto, R., Gaspary, L. P., & Schaeffer-Filho, A. E (2024). IoTP4Chain: Leveraging programmable data plane for efficient IoT forensics using blockchain. *2024 IEEE Latin-American Conference on Communications.*

SWGDE. (2024). Best Practices for Internet of Things Seizure and Analysis (23-F-003-1.0). *Scientific Working Group on Digital Evidence* (pp77-79)

Yadav, P., Feraudo, A., Arief, B., Shahandashti, S. F., & Vassilakis, V. G. (2020). Position paper: A systematic framework for categorising IoT device fingerprinting mechanisms. In *Proceedings of the 2nd International Workshop on Challenges in Artificial Intelligence and Machine Learning for Internet of Things* (pp. 62-68). New York, NY: Association for Computing Machinery.

Yousefnezhad, N., Malhi, A., & Framling, K. (2021). Automated IoT device identification based on full packet information using real-time network traffic. *Sensors*, *21*(8), 2660.

Zia, T., Liu, P., & Han, W. (2017). Application-specific digital forensics investigative model in internet of things (IoT). In *Proceedings of the 12th International Conference on Availability, Reliability and Security* (pp. 1-7). Reggio Calabria, Italy: Association for Computing Machinery.

APPENDICES

Appendix A

Summary of Key IoT Forensic Frameworks

Framework/Model	Key Features	Limitations	Source
3D IoT Forensics Framework	Temporal, spatial, technical dimensions	Lacks critical analysis of weaknesses	Hou et al. (2019)
BIFF (Blockchain IoT Forensics)	Three-zone architecture, identity privacy	Excludes devices/applications from scope	Le et al. (2018)
FALoT	Forensics aware ecosystem	Theoretical, not empirically validated	Zawoad & Hasan (2015)
IoT Forensic Process Model	Requirements-based approach	Gaps in standardization	Stoyanova et al. (2020)

Appendix B

Categorization of IoT Forensic Challenges

Challenge Category	Specific Challenges	Priority Level
Technological	Device heterogeneity, resource constraints, data volatility, lack of standardization	High
Procedural	Lack of forensic readiness, inadequate reporting formats, multiple investigation iterations	High
Legal	Multi-jurisdictional evidence, varying admissibility requirements, cloud data sovereignty	Medium
Ethical	User privacy, informed consent, data access rights	Medium
Methodological	Absence of standardized testing, insufficient tool validation, theory-practice gap	High

Appendix C

Future Research Priorities Matrix

Research Area	Short-term (1-2 years)	Medium-term (3-5 years)	Long-term (5+ years)
AI in IoT Forensics	Explainable AI models	Automated evidence correlation	Predictive forensic analytics
Blockchain Integration	Permissioned blockchain pilots	Hybrid blockchain-cloud models	Interoperable forensic blockchains
EM Side-Channel	Protocol standardization	Court-admissible processing methods	Automated EM forensic tools
Forensic Readiness	Design guidelines	Manufacturer certification programs	Regulatory requirements
Multi-Jurisdictional	Framework harmonization	International cooperation protocols	Global forensic standards