Journal of Artificial Intelligence and Computing (JAIC)
ISSN (e): 3005-3358
Volume: 4, Number: 1, Pages: 19 - 27, Year: 2026

IoT Forensics and Current Landscape and Future Trajectories: A Survey

Kamran Ahmad and Irshad Ahmed
Department of Information Security, University of Management and Technology, Lahore, Pakistan
Corresponding Author: Kamran Ahmad (Email: kamahed3201@gmail.com)

Received: 12/02/2026, Revised: 23/05/2026, Accepted: 15/06/2026

***Abstract*—Internet of Things (IoT) forensics focuses on detecting security incidents, collecting evidence, and analyzing digital traces in IoT environments. Unlike traditional digital forensics, it faces challenges due to limited device processing power, storage, and connectivity. This paper reviews the current state of IoT forensics through a qualitative analysis of existing literature. It identifies key challenges such as evidence acquisition, data preprocessing, anti-forensic techniques, and cloud-based data recovery. The study also discusses forensic readiness, documentation, privacy, and evidence presentation. The findings highlight the need for reliable forensic mechanisms and provide directions for future research in IoT forensic investigations.**

Keywords: Evidence, Digital Investigations, Cybercrime, Forensics, IoT Security, IoT Privacy, Forensic Readiness, Artificial Intelligence

I. Introduction

The Internet of Things (IoT) enables data exchange and communication through interconnected objects embedded with electronics, software, sensors, and network connectivity. It supports collaboration across sectors such as manufacturing, transportation, healthcare, and agriculture. However, to fully realise IoT's potential and ensure data privacy and security, challenges such as weak protection, lack of standardisation, compatibility issues, and hacking risks must be addressed. The growing use of IoT devices in society, including their involvement in criminal activities, has also increased the need for IoT forensics and proper handling of digital evidence in legal proceedings [1].

IoT forensics refers to the extraction, analysis, and preservation of digital evidence from IoT devices for incident response, criminal investigations, and legal processes. It supports evidence extraction, network communication analysis, forensic tool development, device diversity management, evidence reliability, and standardization of forensic procedures. It also helps investigators identify the origin, nature, and scope of security breaches involving connected devices.

IoT forensics supports legal and investigative processes by ensuring that data collected from IoT devices remains valid, reliable, and intact for use as evidence in court. The process involves securing the device, extracting volatile and non-volatile data, analyzing device artefacts and network interactions, and presenting the findings. However, variations in IoT data formats, storage systems, and operating systems make evidence extraction challenging. Network traffic and communication logs are also analyzed to understand device activity and interactions.

Examining the operating system or firmware version of an IoT device is useful for identifying known vulnerabilities and possible exploits. By using vulnerability databases and OS-identification tools, investigators can better understand device weaknesses and reconstruct security incidents. However, many IoT devices lack reliable firmware update mechanisms and may contain outdated or insecure code, increasing the risk of exploitation [2]. IoT forensic research also remains challenging due to device heterogeneity, inconsistent data formats, limited interoperability, dynamic device behavior, and large volumes of distributed data, which complicate evidence extraction, analysis, storage, and comparison across investigations.

To address these limitations, IoT forensics research should expand through multidisciplinary approaches involving computer science, digital forensics, cybersecurity, and legal and ethical studies. Future work should focus on scalable forensic tools, real-world IoT behavior analysis, evidence integrity, standardized testing methods, industry and law-enforcement collaboration, and privacy-aware forensic practices for lawful IoT data collection and processing.

Several studies have reviewed the current state of IoT forensics. A review on IoT firmware security examined vulnerabilities, detection methods, and protection mechanisms, but lacked a framework for auditing hardware and network communication protocols. Another review analyzed the impact of IoT on digital forensics from 2010 to 2018 and proposed a 3D framework based on temporal, spatial, and technical dimensions to support standardized IoT investigations [3]. Other studies reviewed IoT concepts, digital forensic challenges, and security issues, highlighting the need for continuous research and more effective approaches to IoT forensic investigations. It explores prospects and essential prerequisites for successful IoT forensics, as well as the use of artificial intelligence (AI) in this context. Additionally, this study explores potential avenues for IoT forensics research. Studiawan et al. [4] surveyed forensic investigation methodologies and tools that sup-port operating system log analysis. This survey assesses publicly available datasets used in operating system log forensics research. It also makes recommendations for possible future operating system log forensics research. The key strengths and shortcomings of the previously stated reviews are compiled in Table I.

TABLE I
COMPARISON OF EXISTING IOT FORENSIC STUDIES AND LIMITATIONS

Ref.	Method	Working	Limitations
Nadir et al. [2]	IoT firmware security taxonomy and analysis techniques	Classifies IoT firmware vulnerabilities and reviews methods used to analyses firmware security in IoT devices.	Limited discussion on hardware auditing and network communication protocols related to IoT forensics.
Hou et al. [3]	Digital forensics survey For IoT environments	Provides an overview of IoT digital forensics, identifies challenges, and discusses possible future research directions.	Lacks detailed critical analysis of strengths and weaknesses of reviewed studies.
Studiawan et al. [4]	Operating system log forensic investigation techniques	Analyses forensic methods and tools used for event log analysis and reviews public forensic datasets.	Existing tools are not specifically designed for IoT forensic environments and require adaptation.
Atlam et al. [6]	IoT forensic framework with AI integration	Examines IoT forensic processes, security issues, and the role of artificial intelligence in forensic investigations.	Individual weaknesses of reviewed studies are not critically analyzed in depth.
Chernyshev et al. [7]	IoT forensic process models and open issues	Reviews the need for IoT forensics, discusses process models,and identifies open issues in IoT-related digital investigations.	The study mainly provides conceptual analysis and does not present a fully implemented practical forensic frame-work.
Skowron et al. [8]	Machine-learning-based IoT traffic finger-printing	Applies machine learning to identify IoT devices using network traffic fingerprinting techniques.	The approach supports device identification but does not provide a complete forensic framework for evidence handling and reporting.
Gandhi et al. [11]	Blockchain applications and security threats in IoT	Discusses blockchain concepts, applications, challenges, and security threats in IoT ecosystems.	The study is security-focused and does not deeply evaluate blockchain use for forensic chain of custody in IoT investigations.
Raman and Varadharajan [12]	Honeynet-based preventive IoT forensic model	Proposes a honeynet cloud investigation model to support preventive IoT forensics and threat monitoring.	The model mainly supports detection and prevention, while practical evidence admissibility and large-scale forensic validation remain limited.
Harbawi and Varol [13]	Digital evidence acquisition model for IoT forensics	Proposes a theoretical model for acquiring digital evidence from IoT environments and discusses forensic data collection challenges.	The model requires further validation using real IoT devices and practical investigation scenarios.
Zia et al. [14]	Application-specific IoT forensic investigation model	Combines traditional forensic processes with application-specific investigation requirements for IoT environments.	The approach is limited by IoT device diversity and the absence of unified forensic standards.
Kyei et al. [25]	Digital forensic investigation model review	Reviews existing digital forensic investigation models to identify methodological differences.	The study does not specifically address IoT forensic complexity or device heterogeneity.
Surange and Khatri [26]	Review of IoT forensic trends and challenges	Reviews current trends, and expected challenges in IoT forensics.	The study does not propose a practical framework for IoT investigations.

This study offers a thorough and perceptive overview of IoT forensics, emphasizing its significance and the difficulties that researchers and practitioners face in this field, in response to the shortcomings noted in the body of existing work. It begins by providing a comprehensive overview of IoT forensic methods, grouping them into various areas such as blockchain-based digital forensics, IoT applications, IoT network architecture, artificial intelligence in IoT forensics, and cutting-edge digital forensics. Second, various methods suggested for investigating forensics in an IoT setting are also covered in this study. Thirdly, this study evaluates the effectiveness of the examined methods in terms of artefact extraction, analysis, and reporting by critically analyzing their advantages and disadvantages. Last but not least, the study offers crucial avenues for further investigation that can boost the effectiveness and analytical power of current methods. This paper's remaining sections are organized as follows: An extensive overview of IoT forensics is provided in Section II. The IoT forensic layers are explained in Section III. Previous research on IoT forensics methods using a variety of technologies, such as blockchain, advanced digital forensics, and artificial intelligence, is covered in Section IV. Section V concludes by summarizing the findings and making recommendations for further research.

II. THE INTERNET OF THINGS (IOT) FORENSICS

To address IoT-related crimes, IoT forensics combines methods, instruments, and resources from every facet of digital forensics (DF) science. This entails researching embedded devices, linked sensors, cloud services, and embedded device-connected apps. It is generally known that this domain's varied features pose serious difficulties for cybersecurity research. However, this variation makes the issue more difficult in traditional DF. Multiple iterations of any or all stages of the investigation are common in DF investigations, particularly when new sources of evidence are discovered during examination and analysis. Multiple cycles will inevitably result in a large rise in the amount of data to be evaluated in the context of IoT. Other researchers have argued that concurrent investigative procedures can improve the efficacy, efficiency, and admissibility of digital evidence while reducing the overall time required for evidence analysis [5]. However, some disadvantages are apparent upon closer critical inspection.

Positive results could be achieved by combining these two strategies (concurrent processing and many-iteration techniques). In small-scale investigations involving separate IoT devices found at crime scenes, performance may boost efficiency. However, using this combination technique may prove resource-intensive and burdensome when conducting large-scale IoT investigations involving hundreds or thousands of devices. It is uncertain how many of the billions of IoT devices could be involved in an inquiry. Furthermore, the competitive economic environment and resource limitations of smart devices make it difficult to design and implement complex security features, which makes the Internet of Things infrastructure a desirable target for hackers.

The increase in attack attempts, linked to the growing number of IoT devices serving as network access points, makes this clear. As a result, IoT networks and devices can act both as victims of attacks [8] and as attackers when compromised and weaponized in botnets [9]. Additionally, the IoT interacts with both the virtual and physical worlds simultaneously due to the cyber-physical systems paradigm [10], enabling cybercrime to transition from the virtual to the physical environment.

It should come as no surprise that a large portion of cybersecurity research has focused on using technologies such as blockchain to address security issues and prevent their recurrence [11]. Other studies have explored honeypot-based approaches for detecting, monitoring, and analyzing cyber threats [12]. In addition, machine learning methods have been widely applied to support threat detection, classification, and prediction in cybersecurity environments [15]. Further research has also demonstrated the usefulness of learning-based techniques in improving automated security analysis [16]. DF science, on the other hand, concentrates on finding and disclosing security flaws, supporting the investigation process, retrieving artefacts of evidentiary value, reconstructing events, and identifying attack vectors throughout the incident response phases [17]. IoT forensics offers opportunities to enhance the validity and integrity of forensic investigations [18]. It can also help prevent the expansion of hostile threats by facilitating timely prosecution.

Nonetheless, DF poses unique difficulties in IoT research that are not commonly present in non-IoT research. Non-IoT investigations usually begin by identifying devices associated with a crime using standard DF procedures. However, IoT investigations become increasingly complex, particularly when it is difficult or impossible to physically access the relevant "things." Furthermore, errors in IoT investigations may lead to the inclusion of "things" unrelated to the crime [30]. Lastly, the creation of conceptual frameworks or process models for triage in IoT inquiry is the most commonly used method in research post-incident, since DF science frequently depends on post-incident activities.

III. IoT Forensic Layers

Evidentiary data from heterogeneous network domains are frequently considered in IoT forensic investigations and must be collected collectively throughout the investigation. For this purpose, one study identifies major IoT components, including the internal network, cloud environment, and IoT devices or sensors. Other studies similarly highlight the importance of collecting forensic evidence across device, network, and cloud-based environments [19]. IoT forensics has also been described as a combination of three digital forensic layers: device, network, and cloud. This classification helps divide IoT forensic research into several manageable subproblems. Figure 1 presents the classification of IoT systems according to the three digital forensic layers, adapted from the conceptual IoT forensic model proposed by Ahmed et al. [35].

It is important to note that some IoT configurations operate independently of cloud infrastructure or complex networking environments. In such cases, edge computing supports data processing through a distributed architecture positioned closer to the data source. Although the three-layer forensic model does not cover every possible IoT architecture, it effectively represents three widely adopted computing paradigms: cloud, fog, and edge computing.

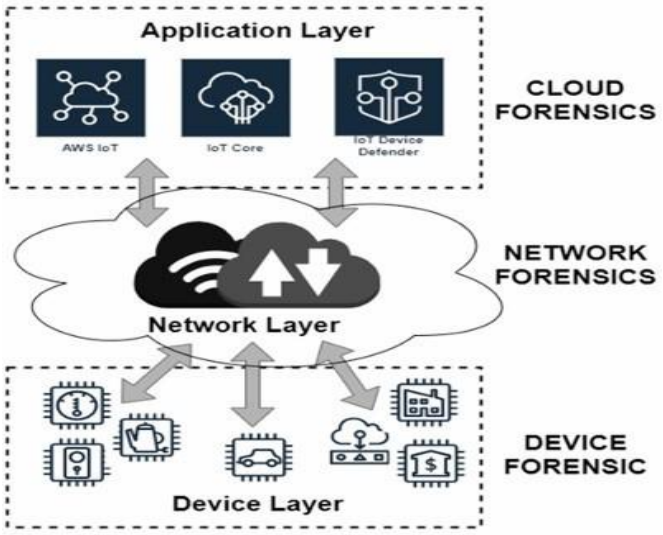

Fig. 1. Classification of IoT forensic research categories [35]

Some IoT devices perform partial or complete data processing locally instead of sending all data to the cloud [20]. Despite its limitations, this classification helps define protocols and procedures for collecting evidence across different IoT infrastructure layers, as illustrated in Fig. 2.

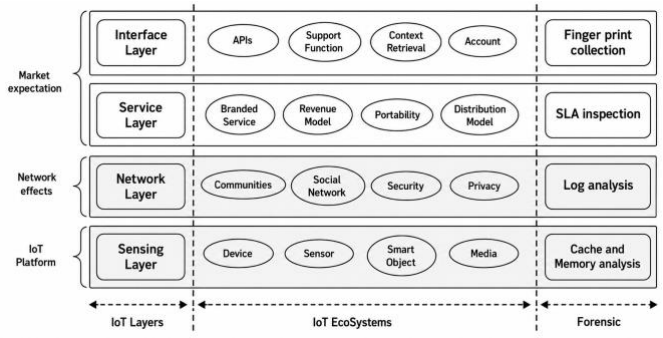

Fig. 2. Layered IoT forensic ecosystem illustrating IoT architecture and corresponding forensic investigation processes.

Device Layer Forensics: There are no uniform forensic techniques due to the versatility of IoT devices. IoT devices' local memory may provide evidence in the form of log files, audio, photos, and videos. Devices like CCTV cameras, medical implants, smart home appliances, networked cars, and UAVs provide this data, which includes user behavior, sensor data, heart rate data, configuration data, telemetry data, and device states.

Network Layer Forensics: PANs, BANs, WANs, HANs, LANs, and other networks that link devices to the internet and each other make up the network layer of the Internet of Things. It is possible to gather legally admissible evidence to track users within the IoT ecosystem by utilizing these networks' logging and auditing capabilities.

Cloud Layer Forensics: Because IoT devices have limited storage and processing power, cloud computing offers benefits such as greater processing capacity and on-demand access. The cloud is essential to IoT forensics since data produced by IoT devices is sent there for processing and storage. To reconstruct cases, client-centric artefacts and other pertinent data, including authentication, access, system, database, and application logs, can be retrieved from the cloud.

IV. IoT Forensic Review

This section reviews current IoT forensic techniques and highlights important future research directions in the field. Existing IoT forensic approaches are grouped into several major categories, as illustrated in Fig. 3. The following subsections provide a detailed discussion of these categories.

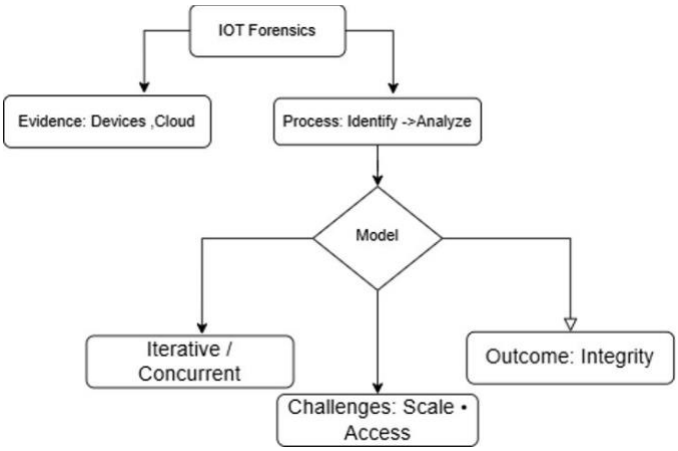

Fig. 3. Categories of IoT forensic techniques and approaches.

A. Artificial Intelligence in IoT Forensics

An in-depth investigation of IoT security preceded an analysis of artificial intelligence (AI) in IoT forensics, highlighting the critical significance of AI in this domain. Current research, recent studies, new opportunities, and necessary conditions for successful IoT forensics were all discussed in the study. IoT forensics' problems and possible fixes were also highlighted. The topic of open avenues for IoT forensic research was then discussed. Digital forensic inquiry was used to explain digital forensics. To give a thorough overview of IoT forensics, the distinctions between traditional, cloud, and IoT forensics, as well as the application of AI in IoT forensics, were also emphasised. Next, the newest and most advanced IoT forensics tools, apps, and investigations were showcased. The discussion of potential future research areas for IoT forensics challenges, potential fixes, and opportunities.

There are still a number of issues in IoT forensics that need further investigation to accelerate the adoption of IoT devices. To comprehend the issues and offer suitable solutions, some of these difficulties were described in detail in the study. This study concluded that more research is required to develop frameworks for IoT forensic investigations that can effectively manage the enormous volumes of data generated by diverse IoT devices. Additionally, throughout the design stage, IoT makers have to take forensic readiness into account. To uncover current evidence from smart home devices that can be successfully utilised in digital investigations, they must create a forensic investigation framework for IoT devices in smart homes in the future. Another study that is pertinent to AI forensics examined some of the IoT forensic problems by analyzing the most prominent technical papers on IoT forensics by 2021 [21]. Based on these issues, it offered a list of requirements that an IoT forensic process model ought to meet.

To identify the remaining gaps, the IoT forensic process models documented in the literature were also evaluated. One key characteristic of these IoT devices is their ability to gather data from a variety of sensors. The owners of the devices may consider a large portion of the data collected to be personal. To facilitate communication among dispersed intelligent objects, such as wearable smart devices that may collect location data without the user's permission, IoT architectures incorporate tracking and identification technologies integrated into actuator and sensor networks [22]. The best practices and guiding principles of digital forensics, including IoT forensics, require that investigative tools and methodologies be examined, calibrated, validated and approved. This ensures that the investigation process can be independently replicated and that the evidence collected remains reliable [23]. When digital evidence is obtained in a forensically sound manner, it is more likely to be accepted in legal proceedings [24].

Process models are therefore essential for standardizing and documenting digital investigations. They also help investigators manage the challenges introduced by emerging technologies and improve the consistency of forensic procedures. Based on these widely accepted principles, various tools and methods have been developed to examine different technologies used in digital forensic investigations.

B. IoT Applications

The study by Kyei et al. [25] focuses on developing efficient digital forensic methods to trace the sources of attacks during IoT investigations. security breaches and guarantee that those responsible are held accountable using trustworthy digital evidence. The variety of devices used in IoT systems and the lack of common standards are major obstacles in this field. The authors examine digital forensics from an Internet of Things viewpoint, highlighting the need for both conventional techniques and application-specific forensics. They examine the top three IoT apps and propose a model that combines traditional and application-specific forensic techniques. In IoT-related investigations, the proposed methodology aims to improve the collection, inspection, analysis, and reporting of solid forensic evidence.

The review study by Surange and Khatri [26] examined current trends, approaches, and foreseen challenges in IoT forensics to highlight gaps, issues, and the breadth of the discipline, while summarising recent developments in the IoT field. Due to socio-technical issues, existing digital forensic techniques are insufficient for Internet of Things systems. The entire spectrum of data, applications, or countries that could be engaged in forensic investigations is not covered by any of the many IoT forensic frameworks. The writers underlined the necessity of an all-encompassing framework that takes these aspects into account. While acknowledging the challenge of integrating different jurisdictional standards, they recommended taking into account similarities among frameworks to streamline and enhance the procedure.

C. IoT Network Architecture

They found that another study proposed a blockchain-based IoT forensic framework to support evidence integrity and identity privacy in IoT investigations. provided an architecture that divides the Internet of Things network into three zones: internal, middleware, and external. The researchers incorporated the notion of triaging into their model by merging the zones. The researchers claim that their approach is appropriate for internal incident responders. IoT apps and devices are not included in the model's definition of IoT forensic investigation. Rather, it functions at the IoT ecosystem's network layer. Additionally, the model does not take user privacy issues into account, which means it does not offer solutions for protecting user identities in the actual data gathered for analysis.

Authors in [27] present a blockchain-based IoT forensic method that safeguards identity anonymity throughout the evidence's lifetime. This method bases the collection phases on whether the victim has enough proof and whether enough evidence has been gathered. This approach has a drawback: it focuses on gathering evidence after other crucial aspects of the IoT probe have been completed. Under the openness, transparency, and notice requirements, a consumer must be informed about the method, guidelines, and procedures of forensic analysis to which his or her data would be submitted. In a similar vein, the client must be able to view their data throughout the investigation. Investigators are encouraged to follow the privacy guidelines set forth for obtaining and evaluating evidence by the accountability requirement. The information security control requirement keeps gathered personal data safe from loss, alteration, and unauthorized access. The creation of an auditing tool to guarantee that the entire inquiry process complies with privacy standards is one of the compliance criteria.

A different study examined the state of IoT-specific digital forensic process models. It outlined the conditions that an IoT forensic process model must meet in order to be used by IoT organizations. To address IoT forensic issues and challenges faced by digital forensic investigators, these needs were compiled from the literature.

This study also examined the gaps in cloud forensics standardization and compared existing cloud forensic process models in the literature to the specified standards. The most recent developments in IoT forensic research were examined through a systematic literature review (SLR) [28]. This review focused on the foundations of IoT, IoT applications, the main effects on IoT forensics, and the suitability of different forensic approaches for IoT environments. The SLR reported that most existing studies remain theoretical rather than applied and identified several research obstacles that still require practical solutions [28].

Realistic and implementable solutions are therefore needed to address the unresolved issues identified in IoT forensic research. Table II summarizes the main findings, limitations, and future research directions reported in previous IoT forensic studies. Table II is adapted from the review by Ahmed et al. [35].

Additional related studies further highlight the need for improved forensic readiness, standardized investigation procedures, and practical IoT forensic frameworks.

TABLE II
RESEARCH FINDINGS AND FUTURE DIRECTIONS IN IOT FORENSICS

Ref.	Research Findings	Future Research Directions
Hou et al. [3]	Provides a review of IoT forensics and highlights key challenges in the literature. It evaluates IoT and digital forensic domains and suggests future directions.	Future research may focus on IoT forensic procedures, multi-jurisdictional challenges, large-scale IoT data analysis, anti-forensic techniques, and forensic readiness.
Atlam et al. [6]	Highlights the role of artificial intelligence in improving IoT forensic investigations and identifies factors for effective forensic analysis.	Future studies can focus on forensic frameworks for smart home evidence collection and the integration of AI into IoT forensic investigations.
Harbawi and Varol [13]	Discusses digital evidence acquisition, file systems, and data analysis techniques for IoT forensic investigations.	Further research is needed to develop intelligent and validated forensic tools for complex IoT environments.
Zia et al. [14]	Explores application-specific forensic methods alongside traditional approaches and proposes a combined forensic investigation model.	Future research may address IoT device diversity and the lack of unified forensic standards.
Surange and Khatri [26]	Reviews recent developments, gaps, and challenges in IoT forensics and highlights limitations of current digital forensic methods.	Future work should investigate privacy concerns, multi-jurisdictional issues, big data forensic analysis, and anti-forensic methods in IoT systems.

D. Cutting-Edge IoT Forensics

Forensic investigators now face greater difficulties due to the development of new technologies, such as inexpensive photo and video recording and information-processing techniques like artificial intelligence and machine learning. Therefore, the main goal of the research was to assess state-of-the-art digital forensic techniques and investigate security flaws in IoT devices from a forensic standpoint. This study provided a concise overview of the fundamental issues, theoretical underpinnings, and emerging fields in IoT forensics research. In order to produce jurisdictional forensic reports and develop best practices for cybersecurity, it stressed the significance of standardizing forensic methodologies.

IoT forensics is still lagging behind other well-established fields of digital forensics and requires more funding and research, a fact that public organisations and legal authorities should be aware of. By analyzing present problems and difficulties in IoT forensics, this research also indicates that standard forensic methods must be expanded and modified in order to retain legally admissible evidence. Furthermore, widely accepted standards and clear IoT security concepts are required.

Modern digital forensic methods for audiovisual biometric data for use in smart city applications were investigated by Ross et al. [29]. Smart technology, which offers clever, useful, and safe solutions to a variety of everyday services, has become an essential part of urban civilisation, whether it takes the shape of smart economies or smart utilities. Smart cities are made up of a network of connected IoT devices that need to communicate with people and with each other. Human-machine interaction can be protected through biometric authentication, in which the device verifies the intended user using biometric information obtained from them. However, while working with biometric data, security and privacy must be guaranteed. This study also examined current forensic techniques based on digital images, audio, and video, which are used alongside biometric data. It covered the challenges facing forensic systems today, with a special emphasis on those posed by deepfake audio and video.

E. Blockchain-Based IoT Forensics

Recently, several blockchain-based models have been developed for IoT forensic investigations. According to the study in [47], these models leverage blockchain's built-in features, ensuring the chain of custody, privacy, integrity, proof, traceability, and verification throughout the investigation process. Permissioned blockchains are the foundation of most of the models. But permissionless blockchains like Bitcoin, Ethereum, Algorand, Avalanche, and Polkadot could use the same structures. Based on their results and performance indicators, the study also assessed the efficacy of several suggested models and proof-of-concept prototypes. Concerns, unresolved problems, and potential subjects for further study were identified as a result of the examination conducted.

Descriptive research on these blockchain-based IoT forensic models is conspicuously lacking due to the absence of prototypes demonstrating their practical use. Future studies should provide empirical analysis of the security features of existing blockchain-based IoT forensic investigation models, as well as potential new models. Another survey reviews IoT security issues, limitations, requirements, and current and future solutions. This survey uses a three-layer IoT architecture as a taxonomy framework to define the security requirements and attributes of each layer.

The main contribution of this survey is its evaluation of possible IoT security flaws and challenges from an architectural perspective. The three-layer architecture is then used to help readers understand how to implement best practices to reduce current IoT security issues.

Table III summaries the main findings and future research recommendations from previous studies on blockchain-based IoT forensics and IoT security adapted from Ahmed et al. [35].

TABLE III
RESEARCH FINDINGS AND FUTURE DIRECTIONS IN BLOCKCHAIN-BASED IOT FORENSICS

Ref.	Research Findings	Future Research Directions
Stoyanova et al. [1]	Reviews theoretical frameworks for preserving digital evidence integrity using decentralized blockchain technologies. It also discusses forensic intelligence, data reduction methods, and the forensics-as-a-service model.	Future research may investigate video-based forensic challenges, privacy protection, AI analytics, runtime verification, and adaptive data collection.
Akinbi et al. [33]	Presents blockchain-integrated IoT forensic investigation frameworks that support evidence integrity, privacy, and chain of custody preservation through a systematic review.	Further studies are needed to develop reliable blockchain-based IoT forensic procedures and evaluate implemented security measures.
HaddadPajouh and Parizi [34]	Provides a classification of IoT security threats and challenges and discusses solutions based on a layered IoT security architecture.	Continuous research is required to address evolving IoT threats and maintain updated security and forensic practices.

F. Advanced IoT Forensic Approaches

1) IoT Forensics using Electromagnetic Side-Channel

To improve digital forensic investigations, the authors of [49] provide a review of electromagnetic (EM) side-channel analysis in IoT devices. EM side-channel analysis uses unintended electromagnetic emissions to monitor computing activities and data processing. EM side-channel attacks are considered useful for digital forensic investigations because they do not require physical modification of the target device. Based on their potential for application in situations requiring the assessment of IoT devices, studies on several EMside-channel analysis assault techniques are analyzed and chosen. The background research data is utilized to determine possible future applications of the technology in the digital forensic examination of Internet of Things devices, which could result in a variety of presently suspended digital investigations.

Conventional digital forensics examines network trails, log files, file storage, and other data that suspects leave on digital equipment. Systems that require complex investigation techniques and expertise can make advantage of live data forensics. As computer systems transition from soft platforms, which are less concerned with privacy and security, to hardened platforms, which are built with security in mind from the beginning, the routine work of digital forensic investigators must change. One of the biggest obstacles to a successful digital forensic investigation is the use of cryptographically protected storage systems. In terms of security, it has been shown that EM side-channel analysis can open the door to cryptographically secure data storage and communication.

It can also be created and applied in digital forensic applications. Sayakkara et al. [30] aimed to modify electromagnetic side-channel analysis methods to support digital forensic investigations on IoT devices.

A thorough analysis of the literature on EM side-channel attacks was conducted to accomplish this goal. Although many mitigation strategies have been developed and implemented to protect against EM side-channel attacks, recent studies show that these initiatives have not been successful in reducing the frequency of this attack vector. In digital forensic applications, EM side-channel analysis is still relatively new. It requires forensically sound, court-admissible processing when used not only for extracting security keys but also for detecting unintentional data loss. However, this technology has the ability to significantly impact the sector and accelerate the advancement of previously halted research on IoT devices and generally safe computer systems.

2) IoT forensic using 3D framework:

The authors of [31] provided one of the early surveys of the Internet of Things, discussing its enabling technologies, applications, and research challenges. They conducted a 3D assessment of the location and looked at the IoT forensic environment. A three-dimensional framework with technological, geographical, and temporal dimensions was developed. The temporal dimension covers the typical digital forensic process, while the geographical component analysis demonstrates how to find evidence sources in an IoT situation. The two elements collaborate to create guidelines and standards for standardizing digital research in the Internet of Things. The technology component directs research methods and instruments to guarantee the use of digital forensics in the dynamic Internet of Things environment.

The authors of [32] provided an overview of the Internet of Things, discussing its main concepts, applications, and technological foundations. They stated that key IoT features significantly impact conventional digital forensics. The quantity, variety, and sources of potential evidence are increased through ubiquitous sensing. Determining the parties involved and establishing the boundaries of the case becomes more challenging when circumstances change. With automatic execution, it becomes difficult to determine who is at fault. The limited resources of an IoT environment make it challenging to locate and gather volatile or non-volatile data. The workload for researchers is significantly increased by diversification. It is challenging to remove or alter such evidence due to the unique security features of the Internet of Things. As public awareness of IoT forensics grows, so does the quantity of studies on the topic. The authors described the IoT forensics environment within a 3D framework encompassing geographical, temporal, and technical aspects to provide a clear understanding of the research goals and the state of this field. To illustrate 3D IoT forensics, a smart home was used as an example. To offer suggestions for forensic researchers and practitioners, current research initiatives were carefully evaluated using the 3D framework.

Forensic models should adhere to the fundamental forensic approach and be modified to account for the IoT environment in real-world applications, thereby directing forensic investigations within the IoT paradigm. Geographically speaking, investigators need access to a wide range of IoT evidence sources, including devices, networks, and cloud environments. Evidence from numerous data sources must be integrated when reconstructing an event scene. Real-time logging, volatile data processing, and support for a variety of hardware and file systems should be included in forensic preparedness systems and in new forensic tools/techniques for IoT settings to handle novel data sources.

3) IoT forensics using operating system logs:

A detailed review of the literature on the forensic examination of operating system logs was conducted. The authors talked about the technologies that support event log analysis and offered a taxonomy of the various methods utilized in this field. The publicly accessible datasets utilized in operating system log forensic studies were also evaluated in this work. They recommended future directions for operating system log forensics as they wrapped up their research. They also provide a thorough analysis of this body of information. With an emphasis on operating system (OS) logs, this article examines several forensic event log analysis techniques. Based on a general inquiry approach that includes event log recovery, event correlation, event reconstruction, and visualization, this study created a taxonomy. They used a general forensic framework to classify recent papers. Each technique's benefits and drawbacks were thoroughly examined. A thorough analysis of OS log forensic study was also provided by the authors. This study is structured using a digital forensic investigative paradigm.

In this publication, the researchers also analyzed the advantages and disadvantages of the strategies used in the literature for each phase, including the instruments required to examine OS logs. Additionally, comprehensive descriptions of publicly accessible datasets were given. Encouraging the research community to use shared datasets to facilitate the assessment and comparison of suggested solutions for efficiency was one of the main issues noted. In addition to other crucial complexities encountered in sophisticated IoT investigations, the report thoroughly addresses all legal, privacy, and cloud security issues. The paper also offers a summary of theoretical frameworks in digital forensics from the past and present, with an emphasis on frameworks that use decentralized blockchain technology to protect evidence integrity. The study also examines a number of cutting-edge methods for forensic intelligence and data minimization, such as the new forensics-as-a-service (FaaS) model. Lastly, the examination of recent research developments and open problems highlights the significance of proactive forensic preparedness programs and generally accepted standards.

The development of innovative methods for OS log analysis also relies heavily on open-source technologies. Over time, attackers have adopted increasingly complex and sophisticated strategies to bypass forensic tools and procedures. Therefore, advanced methods are required to identify, analyse, and evaluate threats affecting computer systems.

Table IV provides a brief summary of the main findings and challenges discussed in previous studies on IoT forensic frameworks and OS log analysis. The table is adapted from the review presented by Ahmed et al. [35]. It also highlights unresolved issues in OS log forensic research and the need for improved forensic methods, tools, and standards.

TABLE IV
RESEARCH FINDINGS AND FUTURE DIRECTIONS IN IOT FORENSIC FRAMEWORKS AND EM SIDE-CHANNEL ANALYSIS

Ref.	Research Findings	Future Research Directions
Hou et al. [3]	Summarizes IoT forensic research from 2010 to 2018 and presents a 3D framework for the IoT forensic ecosystem. It also highlights unresolved challenges and recommendations.	Future research may focus on standard forensic procedures and investigation guidelines for IoT environments.
Studiawan et al. [4]	Reviews event log security, recovery, reconstruction, correlation, anomaly detection, and visualization techniques. It also evaluates datasets and forensic tools for OS log analysis.	Future studies may improve event log security through encryption, centralized logging, and hardware-supported forensic solutions.
Sayakkara et al. [30]	Examines electromagnetic side-channel attacks as a method for supporting digital forensic investigations in IoT devices.	Further research is needed to develop practical EM side-channel forensic tools, methods, and standards for IoT investigations.

V. CONCLUSIONS

To safeguard IoT applications from cybercrime and trace their origins, effective and sufficient digital forensic investigation within IoT networks is necessary. This necessitates the creation of frameworks specifically designed to address the challenges posed by IoT devices. These frameworks ought to create uniform protocols, techniques, and strategies for examining digital evidence in IoT-related cybercrimes. These frameworks may help advance IoT forensic investigations by modifying forensic standards, integrating machine learning methods, and addressing privacy issues. IoT forensics was thoroughly examined in this paper, with an emphasis on present issues and potential directions for further investigation.

It explored the difficulties investigators encounter due to the proliferation of vulnerable devices and the heterogeneity of IoT networks. IoT forensics layers, which describe the collection of specific types of evidence from IoT devices, networks, and cloud storage to reconstruct cases and track individuals across the ecosystem, are described in this study. This paper investigates the difficulties and complications that prevent forensic investigators from carrying out real investigations in IoT networks through a critical analysis. It's draws attention to a number of outstanding issues in IoT forensics, highlighting the necessity for more research to encourage the wider use of IoT devices. Additionally, it outlines future research directions while examining potential solutions and opportunities in IoT forensics.

Future work entails developing a robust forensic investigation framework tailored to IoT devices, leveraging advanced technologies to establish a reliable method for extracting evidence from modern smart home devices.

New forensic tools and methods, data sources, and the integration of IoT forensics with broader cybersecurity and digital forensics will be investigated in future IoT forensics research.

FUNDING STATEMENT

The author(s) received no specific funding for this study.

CONFLICTS OF INTEREST

The authors declare no conflicts of interest to report regarding the present study.

AUTHOR CONTRIBUTIONS

Conceptualization, methodology, validation, writing—original draft preparation, writing—review and editing, K.A., I.A.

INSTITUTIONAL REVIEW BOARD STATEMENT

Not applicable.

INFORMED CONSENT STATEMENT

Not applicable.

DATA AVAILABILITY STATEMENT

Data is available on reasonable request.

REFERENCES

[1] M. Stoyanova, Y. Nikoloudakis, S. Panagiotakis, E. Pal-lis, and E. K. Markakis, "A survey on the internet of things (IoT) forensics: Challenges, approaches, and open issues," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 2, pp. 1191–1221, 2020.

[2] I. Nadir, H. Mahmood, and G. Asadullah, "A taxonomy of IoT firmware security and principal firmware analysis techniques," *International Journal of Critical Infrastruc-ture Protection*, vol. 38, p. 100552, 2022.

[3] J. Hou, Y. Li, J. Yu, and W. Shi, "A survey on digital forensics in Internet of Things," *IEEE Internet of Things Journal*, vol. 7, no. 1, pp. 1–15, 2019.

[4] H. Studiawan, F. Sohel, and C. Payne, "A survey on forensic investigation of operating system logs," *Digital Investigation*, vol. 29, pp. 1–20, 2019.

[5] A. Valjarevic, H. Venter, and R. Petrovic, "ISO/IEC 27043:2015—Role and application," in *Proc. 24th Telecommunications Forum*, Belgrade, Serbia, Nov. 2016, pp. 1–4.

[6] H. F. Atlam, E. E.-D. Hemdan, A. Alenezi, M. O. Alassafi, and G. B. Wills, "Internet of Things forensics: A review," *Internet of Things*, vol. 11, p. 100220, 2020.

[7] M. Chernyshev, S. Zeadally, Z. Baig, and A. Woodward, "Internet of things forensics: The need, process models, and open issues," *IT Professional*, vol. 20, no. 3, pp. 40–49, 2018.

[8] M. Skowron, A. Janicki, and W. Mazurczyk, "Traffic fin-gerprinting attacks on Internet of Things using machine learning," *IEEE Access*, vol. 8, pp. 20386–20400, 2020.

[9] J. Fruhlinger, "The Mirai botnet explained: How IoT devices almost brought down the internet," *CSO Online*, 2018. [Online]. Available: https://www.csoonline.com/article/3258748/the-mirai-botnet-explained-how-teen-scammers-and-cctv-cameras-almost-brought-down-the-internet.html

[10] L. DeNardis, *The Internet in Everything: Freedom and Security in a World with No Off Switch*. New Haven, CT, USA: Yale University Press, 2020.

[11] C. Gandhi, N. Shukla, G. Kaur, and K. Yadav, "Blockchain technology: Concept, applications, chal-lenges, and security threats," in *Blockchain Applications in IoT Ecosystem*. Cham, Switzerland: Springer, 2021, pp. 77–104.

[12] J. A. Raman and V. Varadharajan, "HoneyNetCloud investigation model, a preventive process model for IoT forensics," *Inge´nierie des Syste`mes d'Information*, vol. 26, no. 3, pp. 319–327, 2021.

[13] M. Harbawi and A. Varol, "An improved digital evidence acquisition model for the Internet of Things forensic I: A theoretical framework," in *Proc. 5th International Sym-posium on Digital Forensic and Security*, Tirgu Mures, Romania, Apr. 2017, pp. 1–6.

[14] T. Zia, P. Liu, and W. Han, "Application-specific digital forensics investigative model in internet of things (IoT)," in *Proc. 12th International Conference on Availability, Reliability and Security*, Reggio Calabria, Italy, Aug.–Sep. 2017, pp. 1–7.

[15] P. Yadav, A. Feraudo, B. Arief, S. F. Shahandashti, and V. G. Vassilakis, "Position paper: A systematic framework for categorising IoT device fingerprinting mechanisms," in *Proc. 2nd International Workshop on Challenges in Artificial Intelligence and Machine Learning for Internet of Things*, New York, NY, USA, Nov. 2020, pp. 62–68.

[16] N. Yousefnezhad, A. Malhi, and K. Fra¨mling, "Auto-mated IoT device identification based on full packet information using real-time network traffic," *Sensors*, vol. 21, no. 8, p. 2660, 2021.

[17] R. M. Mohammad, "A neural network based digital forensics classification," in *Proc. IEEE/ACS 15th Inter-national Conference on Computer Systems and Applica-tions*, Aqaba, Jordan, Oct.–Nov. 2018, pp. 1–7.

[18] M. Preda, "Digital forensics of Internet of Things smart heating system investigation," *Journal of Military Tech-nology*, vol. 3, pp. 23–28, 2020.

[19] A. Alenezi, H. Atlam, R. Alsagri, M. Alassafi, and G. Wills, "IoT forensics: A state-of-the-art review, chal-lenges and future directions," in *Proc. 4th International Conference on Complexity, Future Information Systems and Risk*, Crete, Greece, May 2019, pp. 106–115.

[20] V. Sivaraman, H. Gharakheili, C. Fernandes, N. Clark, and T. Karliychuk, "Smart IoT devices in the home: Security and privacy implications," *IEEE Technology and Society Magazine*, vol. 37, no. 2, pp. 71–79, 2018.

[21] N. Almolhis, A. M. Alashjaee, and M. Haney, "Require-ments for IoT forensic models: A review," in *Advances in Security, Networks, and Internet of Things*. Cham, Switzerland: Springer, 2021.

[22] A. N. Moussa, N. B. Ithnin, and O. A. Miaikil, "Con-ceptual forensic readiness framework for infrastructure as a service consumers," in *Proc. IEEE Conference on Systems, Process and Control*, Kuala Lumpur, Malaysia, Dec. 2014.

[23] X. Du, N.-A. Le-Khac, and M. Scanlon, "Evaluation of digital forensic process models with respect to digital forensics as a service," *arXiv preprint arXiv:1708.01730*, 2017.

[24] R. Hegarty, D. J. Lamb, and A. Attwood, "Digital evi-dence challenges in the internet of things," in *Proc. 10th International Network Conference*, Plymouth, UK, Jul. 2014, pp. 163–172.

[25] K. Kyei, P. Zavarsky, D. Lindskog, and R. Ruhl, "A review and comparative study of digital forensic inves-tigation models," in *Digital Forensics and Cyber Crime*. Springer, 2013, pp. 314–327.

[26] G. Surange and P. Khatri, "IoT forensics: A review on current trends, approaches and foreseen challenges," in *Proc. 8th International Conference on Computing for Sustainable Global Development*, New Delhi, India, Mar. 2021, pp. 909–913.

[27] J. James, "DFRWS Forensic Challenge 2017–2018," 2018. [Online]. Available: https://jijames.github.io/DFRWS2018Challenge/

[28] P. Lutta, M. Sedky, M. Hassan, U. Jayawickrama, and B. Bakhtiari Bastaki, "The complexity of internet of things forensics: A state-of-the-art review," *Forensic Science International*, vol. 38, p. 301210, 2021.

[29] A. Ross, S. Banerjee, and A. Chowdhury, "Security in smart cities: A brief review of digital forensic schemes for biometric data," *Pattern Recognition Letters*, vol. 138, pp. 346–354, 2020.

[30] A. Sayakkara, N.-A. Le-Khac, and M. Scanlon, "A survey of electromagnetic side-channel attacks and discussion on their case progressing potential for digital forensics," *Digital Investigation*, vol. 29, pp. 43–54, 2019.

[31] L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," *Computer Networks*, vol. 54, pp. 2787–2805, 2010.

[32] S. Villamil, C. Herna´ndez, and G. Tarazona, "An overview of internet of things," *TELKOMNIKA*, vol. 18, pp. 2320–2327, 2020.

[33] A. Akinbi, Á. MacDermott, and A. M. Ismael, "A systematic literature review of blockchain-based Internet of Things (IoT) forensic investigation process models," *Forensic Science International*, vol. 42, p. 301470, 2022.

[34] H. HaddadPajouh and R. Parizi, "A survey on Internet of Things security: Requirements, challenges, and solu-tions," *Internet of Things*, vol. 14, p. 100129, 2019.

[35] A. A. Ahmed, K. Farhan, W. A. Jabbar, A. Al-Othmani, and A. G. Abdulrahman, "IoT forensics: Current perspec-tives and future directions," *Sensors*, vol. 24, no. 16, Art. no. 5210, 2024, doi: 10.3390/s24165210.