International Journal of Science and Research (IJSR)
ISSN: 2319-7064
Impact Factor 2025: 7.089

Investigating Current Challenges and Issues in IoT Forensics: A Review of Reviews

Ankit Kale[1], Rahul Sonawane[2], Sagar Varade[#3], Priyanka Nikam[4]

[1]Assistant Professor, Ashoka Center for Business & Computer studies, Nashik
Email: *ankitk.acbcs[at]aef.edu.in*

[2]Assistant Professor, Ashoka Center for Business & Computer studies, Nashik
Email: *rahuls.acbcs[at]aef.edu.in*

[3]Assistant Professor, H.P.T. Arts & R.Y.K. Science College, Nasik
Email: *sagarvarade34[at]gmail.com*

[4]Assistant Professor, K. K. Wagh Arts, Science and Commerce College Pimpalgaon B.
Email: *priya12nikam[at]gmail.com*

Abstract: ***These days there is a great escalation in the technology in various fields. This rapid development in the technology proliferated ultra-modern devices with high end services, with the help of devices like smartphones, smart watches, laptops etc. This devices are capable of rendering state-of-the-art services that are based on the cloud like IoT. The IoT systems has arrays of sensors embedded into them that senses various parameters to collect large amount of data for analyzing, monitoring and storage purposes. This modernized technology has significantly changed and eased our lives. But where there is digital data the possibility of theft or digital criminal activities is also more. This makes the IoT technology vulnerable which ultimately impact the society. This paper will focuses on the challenges and issues like data volatility, device diversity, limited storage, security, encryption and lack of standardization faced in this field under the domain of Digital forensics and IoT forensics. The paper aims to create awareness in IoT Forensics by reviewing thoroughly the difficulty in IoT Forensics which will help the fellow researchers to find the research gaps into this field for enhancing the investigation and prosecution of cybercrimes and for the further research into it.***

Keywords: IoT (Internet of Things), Digital Crimes, Digital Forensics, IoT forensics

1. Introduction

IoT is the technology where humans and things are always connected through a network anywhere and anytime. Objects (things) embedded with the sensors, software and connectivity to collect data/information on large amount for analyzing, monitoring and storage purpose [1]. The escalation of this field is due to technological advancements in low-cost sensors and could computing which transformed the sectors like industry, healthcare, agriculture, automation and gave birth to smart systems like smart homes & smart cities. The necessary infrastructure required for seamless and efficient data transfer is provided by the robust protocols like WiFi, Bluetooth low energy (BLE), and cellular technologies like 4G, 5G [2,3]. Globally it is experienced a robust growth in the IoT devices, the market of IoT is driven by widespread adoption in consumer and industrial sectors, with Asia Pacific emerging as a key region for future growth.

Number of connected IoT devices to grow 14% in 2025 and reach 39 billion in 2030; >50 billion by 2035. The number of connected IoT devices reached 18.5 billion in 2024, representing a 12% growth over 2023, according to IoT Analytics' ongoing tracking and analysis of IoT connectivity. Based on H1 2025 IoT connection data, the number of connected IoT devices is expected to grow 14% year-over-year to 21.1 billion by the end of 2025. The 2025 forecast is approximately 300 million connections below the forecast issued by IoT Analytics in September 2024, due to ongoing capex deferrals and softer-than-expected demand in China. (Note: The 2025 forecast is approximately 400 million below the IoT Analytics forecast for 2025 made in 2018). Looking further ahead, the number of connected IoT devices is estimated to reach 39 billion in 2030, reflecting a CAGR of 13.2% from 2025. Artificial intelligence is expected to act as a key growth driver during this period, as the demand for device data rises in line with advances in AI. After 2030, growth is expected to slow as the pool of unconnected devices that can still deliver incremental value from connectivity diminishes. Nonetheless, full market saturation is not expected before well after 2035 [4]. Following figure shows the global IoT market forecast by IoT Analytics.

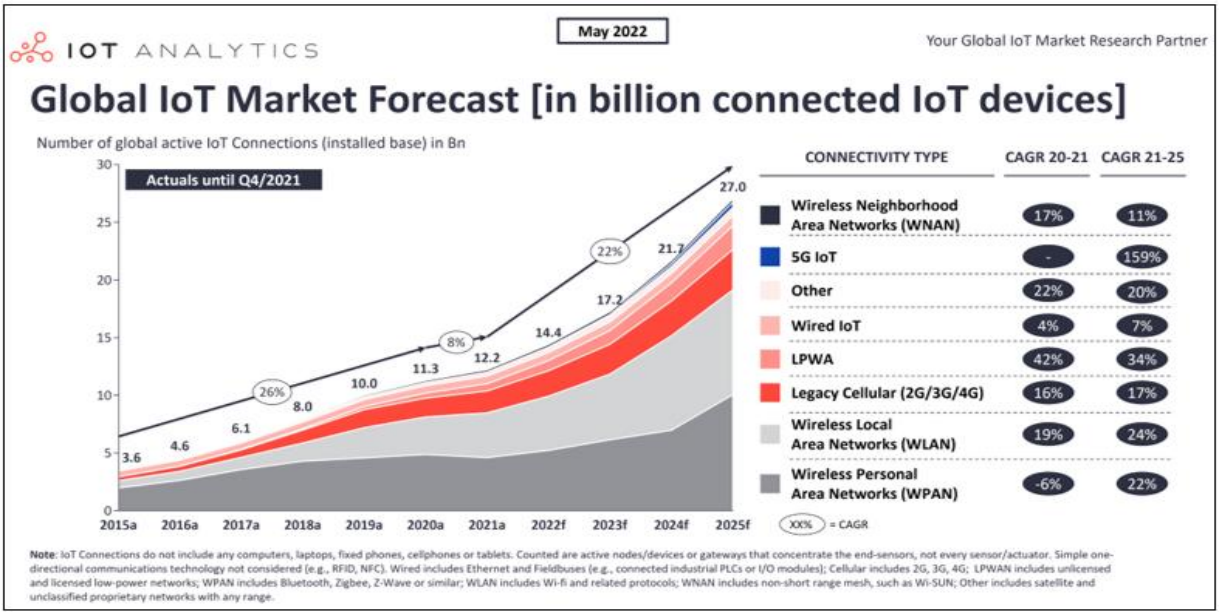

Figure 1: Global IoT Market Forecast

Source: *https://iot-analytics.com/wp-content/uploads/2022/05/Global-IoT-Market-Forecast-in-billion-connected-IoT-devices-min.png*

But as the IoT field is booming, cases of thefts and attacks on its ecosystem has also increased exponentially. There are many factors that makes IoT more vulnerable like user practices of weak passwords & neglecting passwords, malware such as ransomware & spyware, unencrypted communication & weak protocols, outdated software's and physical tampering. Attackers takes the advantages of all these factors breaches the security and harm the privacy of the consumers. Therefore there is a need in urgency of research in IoT forensics to assist in determining who, what, where, when and how for cases [5].

IoT devices generate a massive volume of data, which is both a boon and a burden for forensic investigators. On one hand, the large and diverse data sets provide rich sources of potential evidence, but on the other, they introduce substantial challenges in terms of data acquisition, analysis, and preservation. The data generated by IoT devices is often dispersed across multiple physical and virtual locations, transmitted through various communication protocols, and stored in a wide range of formats. This diversity complicates the process of data collection and analysis, making it difficult to ensure evidence integrity and continuity [6,7,8].

This paper provides a comprehensive review of the current state of IoT forensics, discussing the challenges, methodologies, and tools in use today. It also highlight key gaps in the field and propose corresponding suggestions which ultimately, seeks to contribute to the development of more effective and standardized forensic practices, supporting the successful investigation and prosecution of cybercrimes within the rapidly evolving world of IoT.

2. Background

2.1 Digital forensics and its need

Digital forensics is a part of cybersecurity that focuses on retrieving, analyzing, and examining digital evidence, usually in criminal or legal proceedings. Early forms of digital data first emerged in the late 1970s, but it wasn't until the 1980s that the digital forensics field gained traction. During this time, more people began to purchase personal computers, and computer-related crimes started to occur. By the early 2000s, more people were using the web globally, resulting in widespread cybercrime. In response, the digital forensics field began working toward standardizing its processes. During this time, the International Association of Computer Investigative Specialists (IACIS) and the National Institute of Standards and Technology (NIST) were founded and began guiding best practices. Forensic tools have evolved over the years, aiding in investigations as the scope and ubiquity of technology has changed [9].

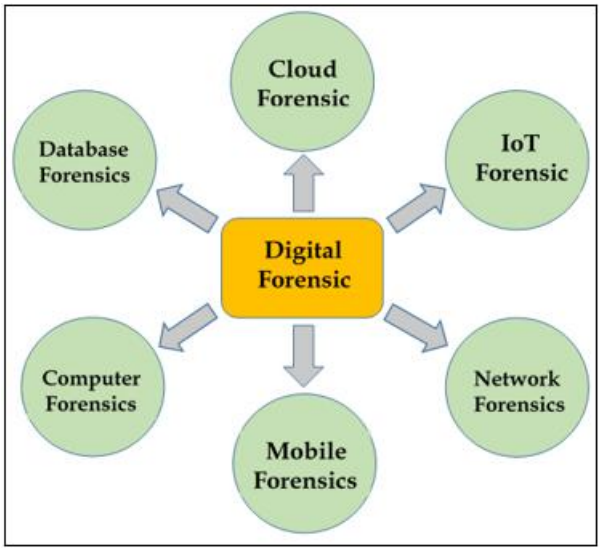

Figure 2: Branches of Digital Forensics

The digital world has profoundly reshaped society, offering immense benefits like instant global communication, vast information access, economic efficiency (e.g., digital payments), and improved healthcare, yet it introduces significant challenges such as threats to personal privacy,

cybersecurity risks (phishing, hacking), demanding proactive governance and user awareness to harness its power responsibly. Thus the need for forensic investigators has increased, and this have led to multiple academic education and certification programs related to digital forensics. Additionally, the complexity of the tasks to be carried out and the required compliance with law and courts' regulations has led to the establishment of strict protocols and procedures to be followed. The continuous appearance of new forms of cybercrime also requires adaptive investigation process models, new technology, and advanced techniques to deal with such incidents [10].

2.2 IoT Forensics

IoT Forensics is branch of Digital Forensics where data from IoT ecosystem are collected, preserved and analyzed as an evidence for the investigation of cybercrimes, security breaches and further for legal prosecutions. The investigation is carried out in three layers viz. device layer, network layer and cloud layer. Each layer consists of different evidences that can be extracted using different tools which is enough to find the attackers.

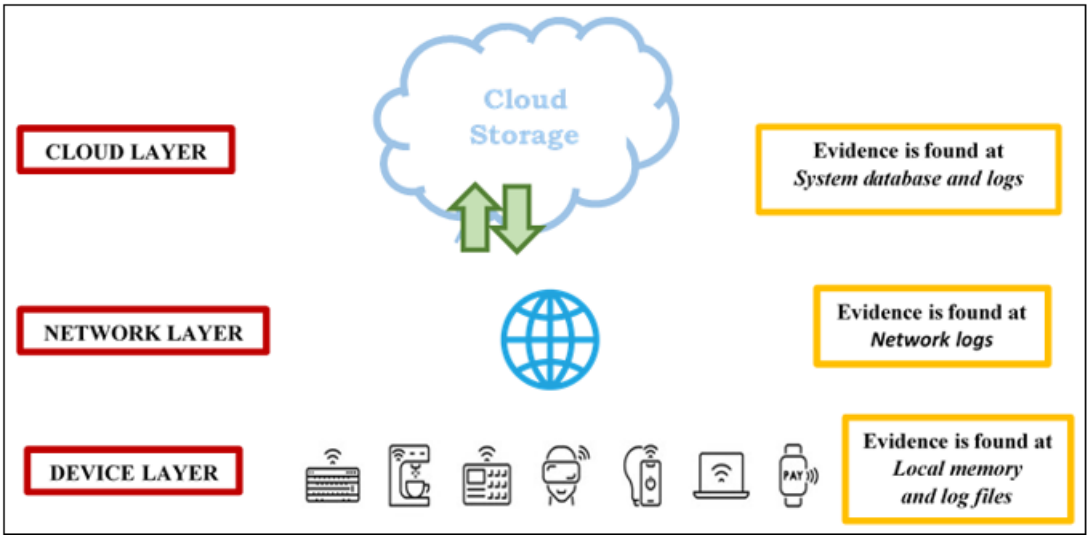

Figure 3: IoT Forensic Layers

IoT forensics can also be classified into three dimensions viz. spatial, temporal and technical dimension which forms a framework to standardize and guide digital investigators. This framework helps forensic practitioners address the unique challenges of the heterogeneous and distributed IoT environment.

a) **Spatial Dimension:** This dimension focuses on the potential geographical sources of evidence in the vast and distributed IoT ecosystem. IoT environments consist of various interconnected components, including devices (sensors, wearables, actuators), local networks, and remote cloud services that can be distributed globally. Investigators must identify all possible physical and virtual locations where relevant data might reside, which often involves dealing with blurred network boundaries and different jurisdictions.
b) **Temporal Dimension:** The temporal dimension addresses the legal acceptance, documentation, and timing of evidence. Key to this dimension is managing data volatility, as much IoT data is transient and can quickly disappear from systems with limited storage and processing power. This requires investigators to follow a modified standard digital forensic process, focusing on timely and proper preservation of the chain of custody to ensure evidence is admissible in court.
c) **Technical Dimension:** This dimension guides the exploration and use of necessary tools, technologies, and techniques for effective data collection, analysis, and preservation. The diverse nature of IoT devices, with their varied operating systems, communication protocols (like Wi-Fi, Bluetooth, ZigBee), and data formats, means conventional digital forensic tools are often insufficient. The technical dimension pushes for the development and adaptation of specialized tools and methodologies for extracting and interpreting data from this wide range of sources [3].

3. Literature Review on IoT Forensics

3.1 Literature Selection Process

To picturized the challenges and issues in IoT forensics, below section provides a thorough literature review on methodologies and tools, assessing their effectiveness and limitations in addressing these challenges faced in it. The strategy to select the paper consists of three main stages:

Stage 1: To search relevant papers from electronic databases like IEEE Explorer, Science Direct etc. proper keywords were defined like IoT (Internet of Things), Digital Crimes, Digital Forensics, IoT forensics.

Stage 2: Selection of papers was done based on title, publications and year. For study, only high-quality publications were included, we focused on journal publications and conferences papers published by Elsevier, IEEE, Springer, MDPI, Wiley and so on, also authentic web articles like IoT Analytics.

Stage 3: Selected papers were reviewed by considering abstracts and full-texts to verify the relevance. The cited

information, abstracts, and keywords of the papers were recorded for further analysis.

At the end, 17 papers published from 2018 to 2025 were studied.

3.2 Literature Survey

The survey studies papers from 2018-2025 to identify the challenges faced in IoT forensics which will help the fellow researchers to find the research gaps into this field for enhancing the investigation and prosecution of cybercrimes and for the further research into it.

Ahmed, A. A., et al., provides a comprehensive review of Internet of Things (IoT) forensics, examines the state-of-the-art solutions, identifies current challenges, and outlines key future research directions in the domain. It focuses on how forensic practices need to adapt for IoT systems, which differ significantly from traditional computing environments. The authors' highlights technological challenges like heterogeneous IoT devices vary widely in capabilities, OSs, storage formats, and connectivity, making standardised evidence extraction complicated, resource constraints of devices having limited processing power or outdated firmware, hindering traditional forensic techniques. It also explores complications faced of data acquisition from cloud and network as the data spans over multiple layers.

Stoyanova et al. specifically analyze IoT forensics across three layers: device, network, and cloud. At the device layer, they highlight challenges such as limited memory, proprietary firmware, and volatile data that make evidence acquisition difficult. At the network layer, the paper discusses encrypted communications, dynamic IP addressing, and heterogeneous protocols that hinder traffic analysis and attribution. At the cloud layer, issues such as data distribution, multi-tenancy, jurisdiction, and dependency on service providers complicate evidence access and chain of custody.

The survey reviews concrete forensic solutions, including forensic-ready IoT architectures, cloud-assisted evidence collection, blockchain-based logging for integrity and non-repudiation, and Forensics-as-a-Service (FaaS) models. It concludes by identifying open issues such as the absence of standardized IoT forensic procedures, limited automation and scalability, and the unresolved trade-off between user privacy and lawful forensic investigation.

AlShaer et al. reviews the IoT forensic investigation process by mapping it explicitly to standard forensic phases—identification, collection, preservation, examination, analysis, and presentation- and examining how each phase is affected by IoT characteristics. In the identification phase, the paper notes difficulties in locating evidence due to device heterogeneity, dynamic network topologies, and the coexistence of edge, fog, and cloud components. During evidence collection, it highlights technical constraints such as limited device storage, volatile memory, proprietary firmware, and lack of physical access, which often force investigators to rely on network traffic logs or cloud service provider data.

For the preservation and examination phases, the authors emphasize challenges in maintaining evidence integrity and chain of custody, particularly in cloud and multi-tenant environments where investigators have limited control. The analysis phase is complicated by fragmented evidence sources, encrypted communications, and inconsistent data formats across devices and platforms. Finally, in the presentation phase, the paper discusses legal and procedural issues, including admissibility of IoT-derived evidence and the need for clear documentation and standardized reporting.

The review also categorizes existing IoT forensic frameworks and models, identifying gaps such as insufficient automation, lack of standardized tools, and weak forensic readiness. The authors conclude that future research should focus on process-oriented IoT forensic frameworks, proactive forensic-by-design approaches, and scalable tools that support the entire investigation lifecycle rather than isolated phases.

Neha S et al. provides a comprehensive survey of security issues in Internet of Things (IoT) systems, with a strong focus on machine learning (ML) and blockchain technologies as solutions to the vulnerabilities inherent in IoT environments. It begins by outlining the broad security challenges IoT faces, such as device heterogeneity, limited computational resources, wireless vulnerabilities, insecure interfaces, authentication weaknesses, and privacy risks across different IoT architectural layers (perception, network, and application).

The authors then organize security threats and requirements by layer, enabling a clear understanding of where specific vulnerabilities occur and what protections are needed. They review ML-based techniques for anomaly detection, threat classification, and adaptive security enforcement that help identify and mitigate attacks in real time. They also examine blockchain-based solutions that enhance decentralization, data integrity, trust, and secure access control- highlighting how blockchain can mitigate centralized points of failure and improve secure data sharing.

Additionally, the survey discusses integration challenges of ML and blockchain in IoT contexts, such as blockchain's resource and scalability limitations in constrained devices and the complexity of designing efficient consensus protocols. It identifies open research directions for improving the scalability, performance, and practical deployment of these technologies in IoT security frameworks. In summary, the paper categorizes IoT security threats, evaluates ML and blockchain-centred defenses, and outlines future research needs for building robust, intelligent, and decentralized IoT security architectures.

Hassan et al. provide a comprehensive comparative review of key IoT forensic frameworks, focusing on how these models adapt traditional digital forensic processes to the complex and heterogeneous Internet of Things environment. The paper begins by explaining how IoT systems generate diverse types of digital evidence across devices, networks, and clouds, and how this diversity challenges conventional forensic procedures such as identification, collection, preservation, and analysis of evidence. The core contribution of the study

is a detailed examination of three major IoT forensic frameworks:

- Digital Forensic Investigation Framework (DFIF) – A generalized model outlining forensic phases tailored to IoT, emphasizing systematic evidence gathering from device and network sources.
- IoTDOTS (Digital Forensic Framework for Smart Environments) – Designed to support forensic investigations in smart IoT environments by embedding forensic logging and context tracking to improve traceability of device interactions.
- FSAIoT (Forensic State Acquisition from IoT) – Focuses on capturing and reconstructing the forensic state of IoT devices to preserve volatile and distributed evidence.

The authors compare these frameworks against traditional digital forensic stages, highlight where they succeed or fall short, and discuss common challenges such as handling volatile data, integrating evidence from different layers (device, network, cloud), and maintaining evidence integrity in distributed systems. They also suggest strategies and improvements for addressing these challenges, such as enhancing automation and standardization in IoT forensic processes. Overall, the paper is valuable for researchers seeking an organized comparison of existing IoT forensic models, an understanding of how these frameworks extend classical digital forensic methods, and insight into areas where further development is needed. Igonor et al. provides a systematic literature review on the application of blockchain technology in digital forensics, examining how blockchain's core properties- immutability, decentralization, transparency, and traceability- are leveraged to address longstanding challenges in forensic investigations such as evidence integrity, secure chain of custody, and tamper resistance. The review synthesizes findings from a broad set of studies across multiple forensic domains, including IoT forensics, cloud forensics, and storage forensics, showing that blockchain is commonly applied to enhance evidence collection, preservation, and reporting processes by creating tamper-proof records and automated audit trails. It further discusses the use of private, consortium, and permissioned blockchains to balance access control with transparency, and highlights ongoing challenges such as scalability, integration barriers, legal and jurisdictional issues, and limited research on blockchain's role in identification and examination phases of digital forensics. The authors conclude by identifying open research directions for more comprehensive blockchain-based forensic frameworks and improved adoption in real-world investigations.

Janarthanan, et.al. provides a detailed overview of the key challenges and issues facing IoT forensics, emphasizing how the unique characteristics of IoT environments complicate traditional digital forensic processes. The chapter explains that the heterogeneity of IoT devices, the sheer volume and diversity of data, and the distributed nature of IoT ecosystems make tasks such as evidence identification, acquisition, and analysis far more complex than in conventional computing environments. Specific technical challenges discussed include ambiguous data location, volatility of IoT data, diversity of device types and data formats, limited forensic tools for accessing proprietary hardware and interfaces, and the difficulty of preserving chain of custody across networked and cloud-based sources. It also highlights non-technical challenges such as defining what constitutes an IoT device in an investigation, legal and jurisdictional issues when accessing cloud-hosted data, and the lack of standardized forensic methodologies and policies. The chapter reviews existing IoT forensic frameworks and their limitations, and concludes by identifying open research directions, particularly the need for enhanced forensic readiness, comprehensive tool support, and standards to support effective forensic investigations in complex IoT scenarios.

Below is summary of the some reviewed paper.

Table 1

Reference	Primary Focus	Key Contributions	Identified Challenges	Future Work
Ahmed et al. (2024)	General IoT Forensics Survey	Reviews state-of-the-art IoT forensic techniques and adaptation of traditional forensics to IoT	Device heterogeneity, resource-constrained devices, distributed evidence across layers	Standardized extraction methods, lightweight forensic tools, cross-layer evidence correlation
Stoyanova et al. (2020)	Layer-based IoT Forensics	Analyzes forensics at device, network, and cloud layers; reviews FaaS and blockchain logging	Limited memory, encrypted traffic, cloud multi-tenancy, jurisdiction issues	Automation, scalability, standardized procedures, privacy vs lawful access
AlShaer et al. (2023)	IoT Forensic Investigation Process	Maps IoT challenges to forensic phases (identification to presentation)	Evidence identification, volatile data, chain of custody in cloud environments	Process-oriented frameworks, forensic-by-design, lifecycle-wide tool support
Neha S et al. (2025)	IoT Security using ML & Blockchain	Surveys ML-based threat detection and blockchain-based trust mechanisms	Resource constraints, blockchain scalability, consensus complexity	Efficient ML models, scalable blockchain integration, real-world deployment
Hassan et al. (2022)	IoT Forensic Frameworks	Comparative analysis of DFIF, IoTDOTS, and FSAIoT frameworks	Volatile data, cross-layer evidence integration, limited automation	Improved automation, standardized IoT forensic frameworks
Igonor et al. (2025)	Blockchain in Digital Forensics	Reviews blockchain use for evidence integrity and chain of custody	Scalability, legal acceptance, limited early-phase forensic use	Blockchain support for evidence identification and examination
Janarthanan et al. (2021)	IoT Forensic Challenges Overview	Identifies technical and non-technical IoT forensic challenges	Data volatility, ambiguous data location, proprietary interfaces, legal issues	Forensic readiness, standard tools, global forensic standards

A critical analysis of recent literature on IoT security and IoT forensics reveals several persistent research gaps that limit the effectiveness, scalability, and legal reliability of forensic investigations in IoT ecosystems.

1) Absence of Unified End-to-End IoT Forensic Frameworks

Although multiple forensic models and frameworks have been proposed, existing solutions largely address isolated stages or layers of IoT systems. Studies by Ahmed et al. and Hassan et al. demonstrate that current frameworks such as DFIF, IoTDOTS, and FSAIoT provide partial forensic coverage, lacking seamless integration across device, network, edge, and cloud layers. Consequently, there is a clear gap in developing a comprehensive, end-to-end IoT forensic framework capable of supporting real-time, cross-layer investigations.

2) Limited Forensic-by-Design Integration

Most IoT architectures prioritize functionality, scalability, and performance, while forensic readiness is treated as an afterthought. Janarthanan et al. and Ahmed et al. highlight the lack of built-in mechanisms for proactive evidence generation, logging, and preservation. The absence of forensic-by-design principles results in missing or incomplete evidence during post-incident analysis, indicating a strong need for IoT systems that natively support forensic investigations.

3) Evidence Volatility and Real-Time Acquisition Challenges

IoT environments generate highly transient and distributed data, which is often overwritten or lost due to limited storage and real-time processing constraints. Stoyanova et al. emphasize that existing forensic tools are inadequate for real-time evidence acquisition in dynamic IoT systems. Reliable techniques for capturing volatile data without disrupting system operation remain insufficiently explored.

4) Scalability and Heterogeneity Constraints

With the exponential growth of IoT devices, scalability remains a significant challenge. Proposed solutions are typically validated in small-scale or simulated environments, as noted by Stoyanova et al. and Hassan et al. Moreover, IoT heterogeneity- stemming from diverse hardware, protocols, and operating systems- continues to hinder standardized forensic processes. Scalable forensic solutions that can operate effectively in large, heterogeneous IoT deployments are still lacking.

5) Inadequate Automation and Intelligence in Forensic Processes

While machine learning and artificial intelligence have been widely explored for IoT security, their application in automated forensic investigation and evidence correlation is limited. Neha Sharma et al. highlight the potential of ML and blockchain but note the absence of practical models that integrate these technologies into forensic workflows. Automated evidence analysis, attack reconstruction, and timeline generation remain open research challenges.

6) Blockchain Overhead and Practical Deployment Issues

Blockchain-based approaches, as discussed by Igonor et al., offer strong guarantees for evidence integrity and chain of custody. However, high computational, storage, and energy overheads restrict their adoption in resource-constrained IoT devices. There is a notable research gap in designing lightweight or hybrid blockchain solutions suitable for real-world IoT forensic applications.

7) Legal, Privacy, and Multi-Stakeholder Challenges

Legal admissibility, privacy preservation, and jurisdictional issues remain insufficiently addressed in existing studies. Ahmed et al. and Janarthanan et al. point out that IoT forensic investigations often involve multiple stakeholders, including device manufacturers, cloud service providers, and network operators, yet current models lack clear mechanisms for stakeholder coordination and responsibility allocation. Aligning technical forensic solutions with legal and regulatory requirements remains an open challenge.

4. Proposed Solution to the Identified Research Gaps

To address the identified limitations in existing IoT forensic research, this study proposes an integrated, scalable, and forensic-by-design IoT forensic framework that enables reliable evidence acquisition, preservation, and analysis across heterogeneous IoT environments.

1) End-to-End Cross-Layer Forensic Framework

The proposed solution introduces a unified end-to-end forensic framework that spans the device, network, edge, cloud, and application layers of IoT systems. Unlike existing partial models, this framework ensures seamless evidence collection and correlation across layers, enabling comprehensive event reconstruction and attack attribution.

2) Forensic-by-Design IoT Architecture

To overcome the absence of forensic readiness, forensic capabilities are embedded at the design phase of IoT systems. Lightweight logging, timestamping, and contextual metadata generation mechanisms are integrated into IoT devices and gateways, ensuring that critical evidence is generated proactively without impacting system performance.

3) Real-Time and Volatile Evidence Acquisition

The framework incorporates real-time evidence acquisition mechanisms using edge-based monitoring and buffering techniques. Volatile data is captured at the edge layer before being overwritten, thereby mitigating evidence loss caused by limited storage and high data velocity in IoT environments.

4) Scalability through Edge–Cloud Collaboration

To address scalability and heterogeneity challenges, the solution adopts an edge–cloud collaborative architecture. Resource-intensive forensic analysis is offloaded to cloud platforms, while time-sensitive data capture is performed at the edge. This approach enables efficient operation in large-scale and heterogeneous IoT deployments.

5) Intelligent and Automated Forensic Analysis

The proposed framework integrates machine learning-based automation for anomaly detection, evidence correlation, and timeline reconstruction. AI-driven analysis reduces manual intervention, accelerates investigations, and improves accuracy while preserving forensic soundness.

6) Lightweight Blockchain-Based Evidence Integrity

To ensure evidence integrity and chain of custody without imposing excessive overhead, the solution employs a lightweight or hybrid blockchain model. Only cryptographic hashes and metadata are stored on the blockchain, while raw evidence remains in secure off-chain repositories, making the approach suitable for resource-constrained IoT devices.

7) Legal Compliance and Multi-Stakeholder Coordination

The framework incorporates privacy-aware data handling, access control, and audit mechanisms aligned with legal and regulatory requirements. Clear roles and interfaces are defined for stakeholders such as device manufacturers, cloud providers, and investigators, ensuring accountability and improving evidence admissibility.

5. Conclusion

The reviewed literature collectively demonstrates that IoT forensics is a rapidly evolving but still immature domain, facing significant technical, procedural, and legal challenges. Unlike traditional digital forensics, IoT environments are characterized by heterogeneous devices, limited resources, volatile and distributed data, and strong dependence on cloud and network infrastructures, all of which complicate evidence identification, acquisition, preservation, and analysis. Existing forensic practices and tools are largely inadequate for handling these complexities without substantial adaptation.

Across the studies, there is strong agreement on the need for layer-aware and process-oriented forensic frameworks that integrate device, network, and cloud evidence while ensuring integrity and chain of custody. Emerging solutions such as forensic-ready system design, cloud-assisted forensics, machine learning, and blockchain-based mechanisms show promise in improving automation, scalability, and trustworthiness of investigations. However, challenges related to standardization, interoperability, scalability, privacy, and legal admissibility remain largely unresolved.

Overall, future research must focus on developing standardized, scalable, and proactive IoT forensic frameworks that support the full investigation lifecycle, incorporate intelligent and decentralized technologies, and balance forensic effectiveness with privacy and legal constraints. Addressing these gaps is essential for enabling reliable and legally sound forensic investigations in increasingly complex IoT ecosystems.

References

[1] Touqeer, H., Zaman, S., Amin, R., Hussain, M., Al-Turjman, F., & Bilal, M. (2021). Smart home security: Challenges, issues and solutions at different IoT layers. *The Journal of Supercomputing*. https://doi.org/10.1007/s11227-021-03825-1

[2] Karale, A. (2021). The challenges of IoT addressing security, ethics, privacy, and laws. *Internet of Things, 15*, Article 100420. https://doi.org/10.1016/j.iot.2021.100420

[3] Hou, J., Li, Y., Yu, J., & Shi, W. (2020). A survey on digital forensics in Internet of Things. *IEEE Internet of Things Journal, 7*(1), 1–15. https://doi.org/10.1109/JIOT.2019.2940713

[4] IoT Analytics. (2022). *Number of connected IoT devices worldwide*. https://iot-analytics.com/number-connected-iot-devices-2022/ **(Accessed December 8, 2025)**

[5] Mukhtar, B., Elsayed, M., Jurcut, A., & Azer, M. (2023). IoT vulnerabilities and attacks: SILEX malware case study. *Symmetry, 15*(11), Article 1978. https://doi.org/10.3390/sym15111978

[6] Soni, N. (2024). IoT forensics: Challenges, methodologies, and future directions in securing the Internet of Things ecosystem. *Computer and Telecommunication Engineering, 2*(4), Article 3070. https://doi.org/10.54517/cte3070

[7] Daryabar, F., Dehghantanha, A., & Choo, K. R. (2015). Forensics of two cloud storage services: Dropbox and Ubuntu One. *Australian Journal of Forensic Sciences, 47*(1), 94–107. https://doi.org/10.1080/00450618.2014.922286

[8] Zhou, B., Yang, F., & Rao, L. (2019). Smartphone forensics: Enhanced state consistency with contextual information. In *Proceedings of the IEEE International Conference on Communications (ICC)* (pp. 1–6). IEEE.

[9] Pollitt, M. (2010). A history of digital forensics. In K. P. Chow & S. Shenoi (Eds.), *Advances in digital forensics VI* (pp. 3–15). Springer. https://doi.org/10.1007/978-3-642-15506-2_1

[10] Casino, F., Del Alamo, J. G., Fernandez-Gago, C., & Hernandez-Ramos, J. L. (2022). Research trends, challenges, and emerging topics in digital forensics: A review of reviews. *IEEE Access, 10*, 25464–25493. https://doi.org/10.1109/ACCESS.2022.3154059

[11] Ahmed, A. A., Farhan, K., Jabbar, W. A., Al-Othmani, A., & Abdulrahman, A. G. (2024). IoT forensics: Current perspectives and future directions. *Sensors, 24*(16), Article 5210. https://doi.org/10.3390/s24165210

[12] 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. https://doi.org/10.1109/COMST.2019.2962586

[13] AlShaer, M., AlShehhi, K., & Abdulla, S. (2023). The Internet of Things (IoT) forensic investigation process. *Journal of Information Security and Cybercrimes Research, 6*, 150–161. https://doi.org/10.26735/DBEU2801

[14] Sharma, N., & Dhiman, P. (2025). A survey on IoT security: Challenges and their solutions using machine learning and blockchain technology. *Cluster Computing, 28*, 3–40. https://doi.org/10.1007/s10586-025-05208-0

[15] Hassan, M. A., Samara, G., & Abu Fadda, M. (2022). IoT forensic frameworks (DFIF, IoTDOTS, FSAIoT): A comprehensive study. *International Journal of*

Advanced Soft Computing and Its Applications, 14(1), 1–15.

[16] Igonor, O., Amin, M., & Garg, S. (2025). The application of blockchain technology in the field of digital forensics: A literature review. *Blockchains, 3*(1), Article 5. https://doi.org/10.3390/blockchains3010005

[17] Janarthanan, T., Bagheri, M., & Zargari, S. (2021). IoT forensics: An overview of the current issues and challenges. In S. Zargari & T. Janarthanan (Eds.), *Cybersecurity in IoT-enabled smart environments* (pp. 101–120). Springer