International Journal of Computer Applications Technology and Research
Volume 14–Issue 11, 35 – 39, 2025, ISSN:-2319–8656
DOI:10.7753/IJCATR1411.1004

An Investigation of Existing Digital Forensic Models for Internet of Things (IoT) Environments

Elvine Saikwa Satia
Student
Kabarak University
Nakuru, Kenya

Prof. Simon Karume
Lecturer
Kabarak University
Nakuru, Kenya

Dr. Nelson Masese
Lecturer
Kabarak University
Nakuru, Kenya

Abstract: The rapid proliferation of Internet of Things (IoT) devices in smart homes has created new challenges for digital forensic investigations. Traditional forensic models, designed for personal computers and mobile devices, are inadequate for heterogeneous IoT ecosystems characterized by distributed architectures, proprietary protocols, and volatile data. This paper investigates existing digital forensic models for IoT devices, focusing on their applicability to smart home environments. A systematic review of frameworks such as Oriwoh's 1-2-3 Zone model, Perumal's Top-Down approach, Zawoad and Hasan's Forensic-Aware IoT, and Kebande and Ray's DFIF-IoT, Zia et al.'s application-specific model, Goudbeek et al.'s smart home framework, Sathwara et al.'s three-step model, Al-Sadi et al.'s open-source geared approach, and Babun et al.'s IoTDots reveals that most remain conceptual, lack real-world validation, and struggle with scalability, interoperability, and evidentiary admissibility. Comparative analysis highlights deficiencies in event reconstruction, chain of custody, and automated correlation. The study identifies research gaps and proposes opportunities for integrating AI, blockchain, and standardized protocols to strengthen IoT forensic investigations. Findings contribute to the foundation for event reconstruction in smart home forensic models.
Keywords: Digital Forensics, IoT, Smart Home, Forensic Models, Event Reconstruction, Cybersecurity

1.0 INTRODUCTION

Digital forensics (DF) underpins the acquisition, preservation, analysis, and presentation of digital evidence so that it is admissible in judicial processes. The scope and rigor of DF differ from conventional investigations by emphasizing standardized procedures that reduce error and preserve probative value [1], [2]. The IoT paradigm broadened DF's landscape: smart homes interconnect sensors, actuators, and appliances that communicate via heterogeneous protocols and produce short-lived, distributed, and often proprietary data flows [3]. These characteristics complicate traditional forensic workflows designed for stand-alone computers or mobile devices.

IoT devices frequently ship with insufficient security configuration and patching discipline [4], increasing exploitability and complicating post-incident investigations. High-profile security incidents, such as botnet-driven DDoS attacks exploiting consumer IoT devices, emphasize the urgency of robust IoT forensic capabilities [14]. Concurrently, cybercrime losses are expected to reach trillions of dollars annually [12], while IoT adoption expands across consumer and enterprise contexts [13]. The thesis frames a central problem: IoT ecosystems, especially smart homes, often lack native evidence retention and reconstruction mechanisms, hindering investigators' ability to determine who initiated commands, when, how, and why. Consequently, investigating existing IoT forensic models is essential to benchmark capabilities and inform model design decisions that enable event reconstruction, timely analysis, and evidentiary reliability.

The remainder is organized as follows: Section II outlines IoT forensics background and challenges. It also summarizes existing models and processes. Section III provides the research methodology. Section IV provides results of the research. Section V concludes the study and section VI gives future recommendations.

2.0 LITERATURE REVIEW

2.1 Background of Digital Forensics in IoT

IoT forensics extends DF principles—identification, preservation, acquisition, examination, analysis, and reporting—across distributed, multi-stakeholder environments. IoT ecosystems combine device, network, gateway, and cloud tiers, each emitting potential evidence with differing retention, accessibility, and jurisdictional constraints [4]. Evidence volatility, data heterogeneity, resource constraints (power, compute, storage), and proprietary stacks degrade real-time capture and post-hoc reconstruction fidelity.

Event reconstruction is central to DF: it reduces reasoning errors, formalizes sequence inference, and improves analytical rigor [8],[9]. Foundational research emphasized reconstructing timelines and causal chains via formal methods and empirical validation [8];[9],[10]. In IoT contexts, however, live data windows may be narrow, ephemeral logs, and cross-tier correlation non-trivial. Recent studies highlight ongoing deficits in real-time correlation of distributed IoT events and limited scalability of existing frameworks when device counts and evidence sources grow [16], [17]. These observations align with the thesis's position that IoT DF requires an ecosystem view spanning device, network, and cloud layers, backed by readiness measures and integrity-preserving processes grounded in ISO/IEC 27043:2015 [4].

2.2 Existing Digital Forensic Models

This research reviewed IoT forensic models and frameworks that collectively illustrate the state of practice and theory.

1-2-3 Zone and Next Best Thing Triage [5]. This pair of approaches segments the investigative scope into internal, middle, and external zones to guide where and how evidence is

International Journal of Computer Applications Technology and Research
Volume 14–Issue 11, 35 – 39, 2025, ISSN:-2319–8656
DOI:10.7753/IJCATR1411.1004

collected. The triage component proposes alternate avenues for evidence acquisition when primary sources are unavailable or obfuscated [5]. Strengths include structured scoping and investigator guidance; limitations involve lack of real-world validation and insufficient attention to integrity and legal aspects under heterogeneous conditions.

Top-Down Forensic Approach: A seven-part methodology covering planning, authorization, platform identification, triage, and archival [6]. It resembles conventional DF processes extended to IoT, offering clarity but remaining high-level. The thesis notes complexity and limited adaptability to fast-evolving device ecosystems.

Forensic-Aware IoT (FAIoT): Emphasizes secure evidence preservation (encryption, central repositories), provenance (chain-of-custody), and API access for law enforcement and courts [7]. It targets device, network, and cloud evidence sources. While conceptually strong on integrity and provenance, implementation and heterogeneity handling remain under-addressed.

DFIF-IoT: A generic IoT DF framework aligned to ISO/IEC 27043:2015, spanning proactive (readiness), concurrent, IoT forensics, and reactive phases [4]. It integrates authorization, documentation, evidence protection, and physical investigation, but is still preliminary and lacks prototype validation; synchronization and scalability across diverse IoT landscapes are open issues.

Application-Specific Model [38]: Argues investigations should adapt to the application domain while preserving core DF principles. It divides efforts across application-specific forensics and the device-network-cloud triad, acknowledging cloud complexity and jurisdictional constraints. It is flexible but can be narrow and hard to generalize.

Smart Home Framework [33]: Proposes a seven-phase process tailored to smart homes, including preparation, identification of automation systems, preservation, workflow understanding, security assessment, evidence acquisition, and analysis. Practical focus on sensor and log evidence is valuable; however, real-time capture and event reconstruction are not fully integrated.

Three-Step IoT DF Model [34]: Centers on identification, preservation, and analysis, with emphasis on end-device evidence and open-source tooling. It articulates known constraints (log sparsity, preservation difficulty, attacker attribution) and admits lack of testing.

Open-Source Gears for IoT DF [35]: Maps open-source forensic tools to IoT layers (device, network, top) and suggests a layered investigation architecture [Al-Sadi thesis ref]. Tooling improves practicality but faces compatibility and robustness concerns; high-level nature persists without thorough validation.

IoTDots [36]: Introduces a two-tier framework for smart environments that modifies application source code to emit forensic logs and uses machine learning to infer user activities and device states; it reports high accuracy under constrained settings. Platform specificity and accuracy degradation under scale and compromise conditions limit broader applicability.

After reviewing the models, it was evident that many IoT DF models are conceptual, constrained by heterogeneity, and insufficiently validated at scale or in live environments [18], [19]. Jurisdictional, privacy, and provenance challenges remain observable across cloud and network layers, underscoring the need for integrity-preserving, interoperable evidence-handling models.

3.0 RESEARCH METHODOLOGY

A systematic literature review served as the foundational methodology to comprehensively map and analyze existing digital forensics investigation models specifically designed for Internet of Things (IoT) devices. This structured approach involved defining precise search strategies across multiple academic databases such as IEEE Xplore among others using carefully constructed search strings that combined terms related to digital forensics, investigation models, IoT devices, and smart home systems.

Through this systematic approach, the research extracted and synthesized critical information about each identified forensics investigation model, including their architectural frameworks, investigation phases, evidence collection techniques, chain of custody procedures, and specific adaptations for IoT device constraints. The review enabled comparative analysis to identify strengths, limitations, gaps, and common patterns across existing models, revealing whether current frameworks adequately addressed unique challenges posed by smart home devices such as data volatility, device heterogeneity, cloud integration, and interconnectivity issues.

4.0 RESULTS

4.1 Weaknesses of Existing Models

In order to justify the need for a new model, existing models should have inefficiencies. Accordingly, the models were evaluated according to the following assessment criteria: forensic readiness(A), chain of custody(B), accuracy(C), reliability(D), scalability(E), auditability(F), completeness(G), ease of integration(H), data security(I), timeliness(J). Table 1 below shows how the models were evaluated according to the assessment criteria.

Table 1. Weaknesses According to Assessment Criteria

Model	A	B	C	D	E	F	G	H	I	J
[5]	X	X	P	P	X	X	X	X	X	P
[6]	X	P	P	X	P	X	X	X	X	X
[7]	P	P	P	X	P	X	X	X	X	X
[4]	P	P	P	P	P	P	P	X	X	X
[38]	X	X	P	X	X	X	X	X	X	X
[33]	X	P	P	X	P	X	X	X	X	X
[34]	X	X	P	P	X	X	X	X	X	X
[35].	X	X	P	X	X	X	X	X	X	X
[36]	P	X	P	P	P	X	P	X	X	P

X-denotes absence, P-denotes presence

X-denotes absence, P-denotes presence

Analysis on table 1 highlighted the following recurring deficiencies:

i. Event reconstruction capability: Most models do not implement automated timeline generation or cross-device correlation suitable for dynamic, multi-device smart homes. Empirical validation is scarce, with limited tooling for synchronizing multi-source timestamps and context [5],[6],[7].

ii. Data integrity and chain of custody: While FAIoT and DFIF-IoT foreground integrity and provenance, many frameworks lack robust, tamper-evident logging across device, gateway, and cloud layers. Standardized chain-of-custody procedures are inconsistently specified [4], [7].

iii. Scalability and heterogeneity: Model scalability falters as device counts, log volumes, and protocol diversity increase. Proprietary stacks impede evidence acquisition, and resource-constrained devices undermine persistent logging [18], [19].

iv. Accuracy and auditability: Without consistent, standardized logging and validation controls, auditability and reconstruction fidelity suffer. Platform-specific approaches (e.g., IoTDots) show promising accuracy but degrade with increased user/device complexity [36].

v. Forensic readiness: Insufficient proactive logging, secure timestamping, and evidence retention policies tailored for IoT devices and gateways. The ISO/IEC 27043:2015 readiness intent is rarely realized with concrete IoT tooling [4].

vi. Integrity and provenance: Weak chain-of-custody documentation and lack of tamper-evident audit trails across tiers reduce legal admissibility. Integrity-preserving architectures (e.g., HMAC hashing, secure provenance chaining, or blockchain-assisted records) require deployment patterns suited to constrained IoT [7], [21].

Recent comparative studies reinforce these observations, concluding that practical IoT DF remains hindered by heterogeneity, scalability, and limited readiness tooling [20]. Proposed integrity enhancements, such as blockchain-backed provenance, can aid chain-of-custody assurance but require careful integration to avoid latency and complexity penalties [21].

Table 2 below shows design recommendations to counter the identified weaknesses as per the assessment criteria.

Table 2: Design recommendations based generalized weaknesses

Assessment Criterion	**Design Recommendations**
Forensic Readiness	Design IoT systems embedding forensic readiness: proactive policies, secure logging, timely evidence captures, and training tools to prepare for investigations early. This includes integrating evidence logging and secure timestamps in IoT devices.
Chain of Custody	All evidence handling should be documented using a physical, paper-based chain of custody log. Every transfer, inspection, or change of possession must be documented in a bound ledger with numbered pages to avoid removal or manipulation. Each record must include the date, time, handler name, role, signature, and an explanation of what the person was doing with the evidence.
Accuracy	Integrate AI and machine learning to automate anomaly detection, reduce human error, and correlate evidence across heterogeneous devices, thereby improving accuracy and completeness of forensic data. Use cryptographic measures to validate data authenticity.
Scalability	Adopt hybrid fog-cloud forensic architectures distributing processing closer to data sources but relying on cloud for extensive storage and analytics, facilitating horizontal scalability and low latency evidence acquisition. Implement big data management frameworks.
Auditability	Implement standardized logging formats and protocols to ensure comprehensive, tamper-proof audit trails that provide a clear record of events. This allows independent parties to fully review and verify forensic procedures and results.
Completeness	Cover all forensic phases end-to-end: readiness, identification, acquisition (including real-time), examination, analysis, and presentation. Implement adaptive workflows sensitive to IoT's

	dynamic and distributed environment.
Reliability	To enhance the robustness of evidence collection and analysis in IoT environments, incorporate redundant systems, such as parallel data stores, to prevent data loss. Implement comprehensive error handling protocols by detecting and logging exceptions, and apply fault-tolerance mechanisms, such as system rollback or failover. Conduct continuous monitoring with real-time alerts and perform regular validation of system performance by scheduled audits and performance tests.
Ease of Integration	To implement open interfaces and protocol abstraction layers, identify target interoperability standards, select compatible APIs, and design modular architecture components. This enables seamless integration with forensic and security tools, IoT management platforms, and cross-jurisdictional systems.
Data Security	The model should implement multilayered security controls: encryption, access controls, secure transmission, and privacy-preserving techniques (data minimization, anonymization) throughout the forensic process to protect evidence confidentiality and integrity.
Timeliness	The model should be able to enable near real-time or live evidence acquisition and automated analysis using fog computing and AI, facilitating swift investigation responses vital in ephemeral and fast-changing IoT states.

5.0 CONCLUSION

Findings urge a pivot from high-level frameworks to operational models with embedded forensic readiness, automated reconstruction, and integrity-by-design across device, gateway, and cloud tiers. For practice, smart-home deployments should incorporate secure logging, trusted timestamping, and provenance from inception, enabling swift and reliable investigations. Investigators benefit from protocol-agnostic acquisition layers, standardized logging formats, and validated toolchains that support multi-source correlation.

For governance and policy, legal frameworks must recognize IoT evidence complexities: volatile data, distributed custody, and third-party cloud involvement and provide admissibility guidance that aligns with standardized processes (e.g., ISO/IEC 27043:2015) [4]. Earlier IoT governance work identified operational benefits and risks [11]; recent perspectives emphasize the need for comprehensive policies addressing privacy, jurisdiction, and forensic access [24]. Research implications center on building interoperable, scalable architectures and conducting empirical validations via controlled and real-world smart-home testbeds.

6.0 CONCLUSION

Future work should prioritize (i) forensic readiness (secure logging, timestamps, retention) at device and gateway levels; (ii) automated reconstruction via AI-driven correlation and formal methods adapted to constrained IoT; (iii) provenance and integrity through lightweight cryptography and, where suitable, blockchain-assisted records; and (iv) interoperability via protocol abstraction and standardized logging. Rigorous testbeds and empirical validations at scale are essential to transition IoT DF from conceptual frameworks to robust, court-ready practice, thereby enabling event reconstruction with improved certainty and speed in smart homes.

7. REFERENCES

[1] G. Palmer, “A Road Map for Digital Forensic Research,” *Technical Report, First Digital Forensic Research Workshop (DFRWS)*, 2001.

[2] M. Donovan, Integrated Digital Forensic Process Model, *University of Pretoria*, 2012.

[3] IEEE, “Internet of Things: Definition and Scope,” *IEEE Standards Association*, 2015.

[4] V. R. Kebande and I. Ray, “A Generic Digital Forensic Investigation Framework for Internet of Things (IoT),” *Proc. 2016 IEEE 4th Int. Conf. Future Internet of Things and Cloud (FiCloud)*, pp. 356–362, 2016.

[5] E. Oriwoh, D. Jazani, G. Epiphaniou, and P. Sant, “Internet of Things Forensics: Challenges and approaches*,” Proc. 9th IEEE Int. Conf. Collaborative Computing*, 2013.

[6] S. Perumal, M. Norwawi, and R. Raman, “Internet of Things (IoT) digital forensic investigation model: Top-down forensic approach methodology,” *Proc. 5th Int. Conf. Digital Information Processing and Communications (ICDIPC)*, pp. 19–23, 2015.

[7] S. Zawoad and R. Hasan, “FAIoT: Towards Building a Forensics Aware Eco System for the Internet of Things,” *Proc. 2015 IEEE Int. Conf. Services Computing (SCC)*, pp. 279–284, 2015.

[8] P. Gladyshev, “Formalising event reconstruction in digital investigations,” *Ph.D. thesis*, 2004.

[9] R. S. C. Ieong, "FORZA—Digital forensics investigation framework that incorporate legal issues," *Digital Investigation*, vol. 3, pp. 29–36, 2006.

[10] S. Soltani and S. A. H. Seno, "A formal model for event reconstruction in digital forensic investigation," *Digital Investigation*, vol. 30, pp. 148–160, 2019.

[11] P. Brous and M. Janssen, "The dual effects of IoT on public sector performance," *Government Information Quarterly*, vol. 32, no. 3, pp. 338–345, 2015.

[12] Cybersecurity Ventures, "Official Cybercrime Report, 2022," 2022.

[13] International Data Corporation (IDC), "Worldwide Internet of Things Spending Guide," 2020.

[14] C. Dunlap, "The Mirai botnet facilitated a DDoS attack on a service provider," 2017.

[15] S. A. Baho and J. Abawajy, "Analysis of Consumer IoT Device Vulnerability Quantification Frameworks," *Electronics*, vol. 12, no. 5, 2023.

[16] S. F. Ahmed et al., "Real-Time Event Correlation for IoT Forensics," *IEEE Internet of Things Journal*, vol. 10, no. 2, pp. 1520–1535, 2023.

[17] H. Mahmood, M. Arshad, I. Ahmed, S. Fatima, and H. ur Rehman, "Comparative study of IoT forensic frameworks," *Forensic Science International: Digital Investigation*, vol. 49, 301748, 2024.

[18] D. R. Garcia Avila, J. F. Miller, and S. S. Iyengar, "Current Challenges in IoT Security and Forensics: Strategies for a Secure Connected Future," *IntechOpen*, 2024.

[19] A. A. Ahmed, K. Farhan, W. A. Jabbar, A. Al-Othmani, and A. G. Abdulrahman, "IoT Forensics: Current Perspectives and Future Directions," *Sensors*, vol. 24, no. 16, 5210, 2024.

[20] M. Ivy, T. Brown, and S. Ahmed, "Comparative Study of IoT Forensic Frameworks," *Journal of Digital Forensics*, vol. 15, no. 2, pp. 120–138, 2022.

[21] J. Chen, Y. Wang, and H. Zhang, "Blockchain-Enhanced IoT Forensics for Integrity Assurance," *IEEE Access*, vol. 12, pp. 33045–33060, 2024.

[22] K. Soltani and M. Seno, "Formal Methods for Event Reconstruction in IoT," *Computers & Security*, vol. 122, pp. 101–115, 2025.

[23] A. Kumar, R. Gupta, and S. Singh, "AI-Driven Event Reconstruction in Smart Homes," *IEEE Transactions on Information Forensics and Security*, vol. 19, no. 4, pp. 2100–2115, 2024.

[24] H. Brous and M. Janssen, "IoT Forensics and Governance Challenges," *Government Information Quarterly*, vol. 41, no. 1, pp. 55–70, 2024.

[25] A. Årnes, Digital Forensics, *Wiley*, 2018.

[26] R. Kothari and G. Gaurav, Research Methodology: Methods and Techniques, 4th ed., New Age International, 2019.

[27] I. Sommerville, Software Engineering, 10th ed., Pearson, 2016.

[28] R. Pressman and B. Maxim, Software Engineering: A Practitioner's Approach, 9th ed., McGraw-Hill, 2020.

[29] A. Valjarevic, H. S. Venter, and R. Petrovic, "ISO/IEC 27043:2015—Role and application," *TELFOR*, 2016.

[30] A. Valjarevic and H. S. Venter, "A Comprehensive and Harmonized Digital Forensic Investigation Process Model," *Journal of Forensic Sciences*, vol. 60, no. 6, pp. 1467–1483, 2015.

[31] J. Tan, "Forensic Readiness," 2001.

[32] V. R. Kebande et al., "How an IoT-enabled 'smart refrigerator' can play a clandestine role in perpetuating cyber-crime," *IST-Africa*, 2017.

[33] A. Goudbeek, K. K. R. Choo, and N. A. Le-Khac, "A Forensic Investigation Framework for Smart Home Environment," *Proc. 17th IEEE TrustCom/BigDataSE*, pp. 1446–1451, 2018.

[34] S. Sathwara, N. Dutta, and E. Pricop, "IoT Forensic: A digital investigation framework for IoT systems," *Proc. 10th Int. Conf. Electronics, Computers and Artificial Intelligence (ECAI)*, 2019.

[35] M. B. Al-Sadi, L. Chen, and R. J. Haddad, "Internet of Things Digital Forensic Investigation Using Open-Source Gears," *Proc. IEEE SoutheastCon*, 2018.

[36] L. Babun, A. K. Sikder, A. Acar, and A. S. Uluagac, "IoTDots: A Digital Forensics Framework for Smart Environments," 2018.

[37] ISO/IEC 27043:2015, Information Technology-Security Techniques-Incident investigation principles and processes,2015.

[38] S. Zia, M. Shafiq, and M. Farooq, "Application-specific digital forensic model for Internet of Things (IoT)," *Proc. 2017 Int. Conf. on Computer and Information Sciences (ICCOINS)*, Kuala Lumpur, Malaysia, pp. 1–6, 2017.