INNOVATIONS IN INFORMATION TECHNOLOGY
https://www.worldlinkpub.com/journals/innovations-in-information-technology/
ISSN: 3141-6004

# MOBILE AND IoT FORENSICS: OVERCOMING ENCRYPTION AND DEVICE DIVERSITY

*[1]Adamu Ado Aminu, [2]Alamin Dahiru, [3]Mubarak Sani
[1]Department of Computer Science, Joseph Sarwuan Tarka University, Makurdi, Benue State.
[2]Deparment of Forensic Science, Vivekananda Global University, Jaipur, Rajasthan, India.
[3]Department of Mechanical Engineering, Vivekananda Global University, Jaipur, Rajasthan, India.
adamuadoaminudfir@gmail.com*; aminu.adamu@uam.edu.ng

**Received: 12 May 2026**
**Accepted for publication: 15 June 2026**
**Published: 01 July 2026**

## ABSTRACT

The spread of mobile and Internet of Things (IoT) devices is posing a critical threat to digital forensics, with warrant-proof encryption and unprecedented heterogeneity of devices and operating systems. Such topography undermines the capacity of the law enforcers to have scaled investigations. The current techniques like live memory analysis, cloud forensics, and data standardization (DFXML) have been found to be inadequate. Technical circumfusion is unscalable, expensive and often based on proprietary software. More importantly, the unavailability of legally shareable, high-quality forensic data is an issue that poses a serious challenge when it comes to creating intelligent Artificial Intelligence (AI) and Large Language Models (LLMs). The paper contends that a paradigm shift is necessary based on long-term success: it involves going beyond temporary technical solutions to Forensic Readiness that is imposed by harmonizing policies and reforming architecture. The paper suggests the Zero Trust Architecture (ZTA) as the most viable design mechanism that can be used to enforce standardized and continuous logging to make evidence available not only but also legally admissible internationally.

**Keywords:** Mobile and IoT Forensics, Encryption, Device Diversity, Scalability, Large Language Models (LLMs), Zero Trust Architecture (ZTA).

## 1.0 INTRODUCTION

### 1.1 The Problem: From Lawful Access to Erosion

The speeding up growth of mobile gadgets and the Internet of Things (IoT) including smart home platforms, wearables, and industrial control systems (Yin, 2025) has completely changed the digital environment. It is an interconnected ecosystem with ever-expanding, frequently dispersed digital footprint where essential evidence used by modern criminal investigations can be found (Z. B. J. R., 2023). Nonetheless, there are structural challenges confronting investigators on a scale never experienced before that damage the scalability and reliability of their efforts. Two architectural pillars, that are strong, warrant-proof encryption and deep device diversity are used to define this issue. The use of strong, hardware-based encryption that makes the data inaccessible even with a court order, a growing trend of modern mobile operating systems and IoT platforms makes the going dark issue even worse.

This is compounded by the diversity of the operational density of devices, which is typified by fragmented operating systems, proprietary hardware, custom firmware, and a multiplicity of communication protocols. These issues are also compounded by volatile nature of data, use of distributed cloud storage, ultra-modern anti-forensic measures


**Figure 1: Encryption and Diversity: The Architectural Bottlenecks Crippling Scalable Digital Forensics**

### 1.2 Existing Strategies and Paper Purpose

Current forensic methodologies are trying to bypass these obstacles using technical workarounds (live memory analysis or hardware exploits), legal process (cloud/network forensics), and standardization (DFXML) (NIST, 2014; Al-Shamsi and Ghaith, 2020). The possibility of using the

Artificial Intelligence (AI) and Large Language Models (LLMs) to automate contextual analysis of massive data streams of the IoT is also noted in academic literature (W. L. J., 2016). Since recent technical adventures will never be non-scalable and hard to maintain legally (Kerr and School, 2019), the paper provides evaluation of existing approaches and the roadmap of the future of mobile and IoT forensics. The study suggests the combination of technological answers and main lawful and governmental modifications. To achieve scalability, forensic sound, and admissible evidence collection, the development should be aimed at the concerted efforts of manufacturers to integrate Forensic Preparedness requirements, that is, by utilizing the newly developed security models, including the Zero Trust Architecture (ZTA) (G. K. P. J., 2022).

### 1.3 The Simultaneous Dual Challenge and Mitigation Measures

The available literature has been mostly in agreement that the issue with mobile and IoT forensics are two-fold namely, the omnipresence of robust encryption and the impossibility of controlling environmental heterogeneity (Yin, 2025; NIST, 2014). The mitigation strategies can be categorized in three fronts:

**Technical Workarounds:** They are based on the access to unencrypted information, usually through live memory analysis or low-level hardware exploitation (Kerr and School, 2019).

**Standardization and Interoperability:** The focus on frameworks, offered by such organizations as NIST (NIST, 2020; UNODC, 2025) and the application of structured data models, such as Digital Forensics XML (DFXML) (Garfinkel, 2019).

**Smart Automation:** The combination of Artificial Intelligence (AI) and Machine Learning (ML) to handle theenormous amount of self-generated IoT data that is not possible to process manually (S. W., 2019).

### 1.4 Failure of Reactive Technical Solutions

One of these criticisms is that the introduction of hardened cryptographic functionality, including Apple Secure Enclave Processor (SEP) and Android File-Based Encryption (FBE) (Al-Quraishi *et al*., 2018), has made most traditional, low-level acquisition methods ineffective on powerless devices. This forces the investigators to adopt encryption workarounds, which are always known to be probabilistic, costly, and temporary (Kerr and School, 2019). Hack attacks, such as hardware ones, are also expensive and soon to be patched out by vendor.

The table below explains the overlap of the technological and legal limitations, which supports the argument that non-scalable determinants dominate unless the policy is drastically changed.

**Table 1: Taxonomy of Encryption Workarounds and Legal Hurdles**

| Category | Examples of Techniques / Approaches | Technological Hurdles | Legal/Policy Hurdles | Relevance to Non-Scalability Claim |
|---|---|---|---|---|
| **Compel the Key** | Court orders to disclose device keys or passcodes | SEP/FBE protections; hardware-backed keys | Privacy concerns; cross-border data access | Demonstrates reliance on legal processes rather than scalable technical solutions |
| **Access Plaintext** | Live memory analysis, memory dumps | Transient data; encryption at rest; volatility risk | Legal standards for memory data; chain of custody complexities | Indicates non-scalability due to volatility and legal constraints |
| **Exploit Flaws** | TEEs, hardware vulnerabilities | Patch rates; high resource cost; risk to vendor trust | Coordinated disclosure timelines | Highlights transience and vendor-responded risk, reinforcing non-scalability |
| **Cloud Extraction** | Data extraction from service providers with warrants | Data availability, API access limitations | Cross-jurisdictional data sharing; privacy regimes | Shifts reliance from device-level techniques to legal data access strategies |
| **Forensic Readiness** | Standardized data models (DFXML) | Interoperability between tools; adoption curve | International data access harmonization | Supports architectural approach over ad hoc technical hacks |
| **Policy-Driven Access** | Zero Trust architectures, data governance | Integration into existing workflows; data minimization | GDPR/privacy, local laws | Points to systemic reforms as scalable path forward |

This operational fragmentation is also reflected in commercial tools where tools such as Cellebrite UFED and Magnet AXIOM have different strengths depending on the operating system and type of data and this confirms the absence of a universal and scalable approach


**Figure 2: The Paradigm Shift: Contrasting Non-Scalable Reactive Technical Exploits with Proactive Architectural and Policy Solutions**

### 1.5 Gap and Motivation Policy, Privacy, Foresight

Although AI, ML, and LLMs are regarded as needed to handle the large volumes of data, there is a lack of data. The absence of realistic, publicly accessible forensic data is an acute bottleneck of the development and scientific validation of intelligent tools, which can be explained by the severe privacy laws (V. M. V., 2020). Moreover, a disconnection exists in the solution of reactive technical fixes to a proactive architectural policy. Although it is proposed that collaboration with the manufacturers is the way to go, the literature covering the idea of using the Zero Trust Architecture (ZTA) to produce high-fidelity and ongoing audit trails to use in the forensic context is presented sparsely (G. K. P. J., 2022). The gap in technical potential and the systemic reality is, therefore, the reason why this paper is inspired to fill the gap between these two concepts and present an architectural vision of a scalable and legally acceptable evidence collection paradigm centered on ZTA integration and data sharing by the policy.

## 2.0 MATERIALS AND METHODS

### 2.1 Strategic and Architectural Analysis: Approach and Design

The research design that is applied in this study is conceptual and analytical as it proceeds beyond a systematic literature review to the architectural evaluation and policy modelling.

**Systematic Literature Synthesis:** Searching published articles to develop the technical and legal core problems and find the solutions that already exist, such as AI/ML, industry standardization, and cloud forensics.

**Architectural Assessment and Policy Model:** The fundamental approach is the overall analysis of the principles of Zero Trust Architecture (ZTA) and its alignment with the necessities of digital forensics preparedness. Conceptual modeling illustrates how the audit trails of evidence created by the demands of ZTA to keep constant monitoring and to log evidence in context is naturally high fidelity, and thus systemic response to forensic problems in distributed environments.

### 2.2 Methods and Data Sources

This analysis will be based on high level standards, technical requirements and comparative market intelligence:

**Industry Standards and Guidelines:** Standards by the National Institute of Standards and Technology (NIST) (e.g., SP 800-101r1 and SP 800-207) are standards defining minimum procedures and architecture.

**Technical Specifications:** Documentation of the current encryption schemes (Android FBE, Apple SEP) to investigate the level of complication of the low-level approach.

**Commercial Tool Intelligence:** Comparative reports on mainstream solutions (Cellebrite UFED, Magnet AXIOM) to test the sustainability and fragmentation management. There were three major methods of analysis:

**Comparative Analysis:** Applied to compare the high price, scaling, and legality of transient technical workarounds and trained systemic network-centric access techniques.

**Taxonomy Development:** Develop a systematic classification of encryption bypass methods and fragmentation causes (Table 1) to explicitly project the space of forensic problems and potential solutions to them.

**Policy and Architectural Mapping:** Map the ZTA principles (strong authentication, authorization, detailed logging) directly onto the main requirements of digital forensic preparedness (data preservation, chain of custody) to come up with the final prescriptive roadmap.

### 2.3 Validation

The proposed roadmap is tested on three aspects; Conformance to Established Standards, Scalability and Generalization and Policy and Privacy Compliance so that the ZTA framework is sound, broadly applicable and ethically responsible.

## 3.0 RESULTS

### 3.1 Non-Scalability Constraint Analysis

As the analysis proves, the mobile and IoT forensic domain is characterized by underlying scalability crisis that is determined by two mutually reinforcing problems:

**Technical Non-Scalability:** Hardware-protected encryption and device diversity to an extreme level provide a combined impediment that effectively counters the device-centric forensics. Technical workarounds (exploits, attacks) are probabilistic, expensive and temporary, which establishes a resource imbalance in which low-level accessibility is not scalable and proprietary.

**The lack of scientific data:** The scientific creation and testing of sophisticated equipment, including intelligent automation (AI and LLMs), are fundamentally underprivileged. The lack of publicly available realistic forensic datasets, the natural consequence of tough privacy laws and legal constraints on the spread of sensitive evidence, is an acute constraint to full automation. The overall conclusion is that it is not technical circumvention but architectural policy that is the long-term solution. Zero Trust Architecture (ZTA) provides a framework that, with its need to continue authentication, enhanced authorization, and descriptive context-affirmative following is automatically generated the high-fidelity audit trail essential to forensic preparedness.

## 4.0 DISCUSSION

### 4.1 Interpretation and Paradigm Shift

These conclusions prove that the forensic integrity is radically changing. It has to shift off the notion of an error-free bit-to-bit image of one device to the integrity and admissibility of synthetic information utilizing a range of, fragmented, and decentralized sources: the cloud, the network edge, and device logs. The requirements of data representation such as DFXML are necessary in order to document the provenance of digital forensic evidence and establish the legal admissibility of aggregated information. The legacy of reactive technical exploits cannot withstand the advancement of cryptographical protection. This compels the investigators to focus on legally permitted methods such as forcing key disclosure or retrieving cloud data whereby the negotiation of cross-jurisdictional laws often takes precedence over technical skills. The bottleneck on data scarcity means that the most potent future forensic tools (AI/LLM) will not be created until the policy and legislation address the ethics and legal concerns of controlled data sharing.

### 4.2 Correlation with existing Literature

Such findings are consistent with the literature that requires standardization and developing intelligent tools that are

scientifically proven. They argue in favor of the notion that socio-technical issues, including multi-jurisdictional evidence and policy, represent a larger long-term barrier as compared to short-term technical problems. It directly involves the research of forensic readiness by directly stating ZTA as the path towards proactive readiness and is no longer a mere suggestion of the need to have better standards but a literal architectural necessity. The need of ZTA to monitor and log continuously offers the functional policy mechanism to seal the gaps identified by researchers on the lack of forensically-conscious standards across devices.

## 5.0 CONCLUSION

*Synthesis and Architecture Roadmap*

The research concludes that the current mobile and IoT forensics is brought to its knees by a structural failure of scalability in dealing with strong encryption and extreme device heterogeneity that is hardware-defended. Reactive measures-expensive technical adventures or complex litigation against cloud data information are time-dependent and are not scalable. Success in the long term requires a paradigm shift between reactive technical circumventions to the proactive policy and architectural based forensic preparedness. The very idea of forensic integrity should be reinvented: it is no longer about the integrity of a single physical image but about the admissibility and provability of summed-up evidence of different sources, standardized on the basis of such models as DFXML. The easiest design that can achieve this is the Zero Trust Architecture (ZTA) whose requirement of continuously logged, context-sensitive transaction and access decisions are effective in resolving the problem of who-done-what-when in a distributed environment.

*Implications in practice and Future directions*

Practical implications of the work are far-reaching to the law enforcement, cybersecurity practitioners and manufacturers:

*To Investigators:* The required shift towards non-physical acquisition (ZTA analysis of logs, cloud access) and readiness to make use of smart resources (AI/LLMs) as soon as proven datasets are accessible.

*To Manufacturers:* Mounting pressure is necessary to adapt to ZTA model particularly in Industrial IoT and enterprise devices, making sure that standardized logging is a predetermined attribute.

*Policy and Legal Harmonization:* Future studies need to be concerned with the development of international data access policies and ethical, controlled systems of data sharing in order to facilitate AI training and validation.

*Edge and 5G Frameworks:* Novel investigation frameworks are necessary to handle the increased amount and the speed of information in 5G and distributed edge/fog computing environments.

## REFERENCES


Ahmed (2024). Deep Learning Based Side-Channel Attack Detection for Mobile Devices Security in 5G Networks," *Tsinghua Science and Technology*, 30(3) DOI: 10.26599/TST.2024.9010123.

Alahmadi, N. (2022). Cyber-Security Threats and Side-Channel Attacks for Digital Agriculture," *Sensors*, 22(9)

Alahmadi, S. (2023). *IoT Forensics: An Overview of the Current Issues and Challenges*, *Int. J. Inf. Comput. Sec.* Available: https://aber.apacsci.com/index.php/CTE/article/viewFile/3070/3616 .

Al-Quraishi, H. (2018). Extending the privacy capabilities of the digital witness approach with PRoFIT," *PMC/NCBI*, Available: https://pmc.ncbi.nlm.nih.gov/articles/PMC5856102/.

Al-Shamsi, A., and S. S. A. Ghaith (2020). IoT Forensics: An Overview of the Current Issues and Challenges. *Int. J. Comput. Appl.*, 183(31)

Android Developers (2025). *Encryption: File-based encryption*. Available: https://source.android.com/docs/security/features/encryption.

Apple (2025). *Secure Enclave Processor*, *Apple Platform Security Guide*. Available: https://support.apple.com/guide/security/secure-enclave-sec59b0b31ff/web.

Federal Bureau of Investigation (FBI) (2025). *Lawful Access*, 2024. Available: https://www.fbi.gov/how-we-investigate/lawful-access.

Garfinkel, S. (2019). "Digital forensics XML and the DFXML toolset,"*ResearchGate*Available: https://www.researchgate.net/publication/257687889_Digital_forensics_XML_and_the_DFXML_toolset.

Jug, R. (2023). Integration of Zero-Trust Architecture with Digital Forensic Readiness in Enterprises," *ResearchGate*, 2023. Available:https://www.researchgate.net/publication/395835840_Integration_of_ZeroTrust_Architecture_with_Digital_Forensic_Readiness_in_Enterprises_Ruby_Jug.

Kerr, O., and T. H. B. K. S. School (2019). Encryption Workarounds," *UC Berkeley Law School*, 2019. Available: https://www.law.berkeley.edu/wp-content/uploads/10/Kerr-Encryption-Workarounds.pdf.

National Institute of Standards and Technology (NIST) (2014), *Guidelines on Mobile Device Forensics*, NIST Special Publication

National Institute of Standards and Technology (NIST), *Zero Trust Architecture (ZTA)*, NIST Special Publication 800-207, Aug. 2020.

ThingsBoard Team, *ThingsBoard Open-source IoT platform* (2025). Available: https://thingsboard.io/.

Tsyvarev (2025). *Demystifying Android Physical Acquisition*, ElcomSoft blog, Available: https://blog.elcomsoft.com/2018/05/demystifying-android-physical-acquisition/.

UNODC (2025). *Standards and Best Practices for Digital Forensics*, UNODC Education for Justice. Available: https://www.unodc.org/e4j/en/cybercrime/module-4/key-issues/standards-and-best-practices-for-digital-forensics.html.

Yin, Z. (2025). Digital Forensics in the Age of Large Language Models," *arXiv preprint, arXiv:2504.02963*. DOI: 10.48550/arXiv.2504.02963.