Cyber Forensics on Advanced Technology Platforms

Cheryl Ann Alexander[1,*] and Lidong Wang[2]

[1]*Institute for IT Innovation and Smart Health, Mississippi, USA*

[2]*Institute for Systems Engineering Research, Mississippi State University, Mississippi, USA*

Abstract: The motivation of the research in this paper is to extend cyber forensics to advanced technology platforms that are beyond traditional workstations and servers. Specifically, these technology platforms include cloud and virtual machines (VMs), the Internet of Things (IoT), and mobile devices that are significant for cyber forensics. Digital forensics process and challenges in cloud forensics are presented. VMs are helpful for cyber forensics. IoT forensics has been categorized into three dimensions: technical, spatial, and temporal. Mobile device forensics helps detect cyber risks or threats, investigate crimes, and recover deleted or lost data. Mobile forensic tools are compared and summarized based on their functions. Cyber forensics on advanced technology platforms in healthcare is presented. Applications of mobile device forensics in healthcare lie in regulatory compliance, data security, and privacy.

Keywords: Cyber forensics, Cloud, Virtual machines, Internet of Things (IoT), Mobile device forensics, Healthcare.

1. INTRODUCTION

Post-forensic refers to a process of analyzing evidence after a cyber-attack or a death. Continuous forensic can refer to forensic auditing, forensic readiness, or forensic science training. Cloud computing and its relevant ecosystem make forensic readiness very complicated due to the heterogeneous log formats, data locations, the increasing amount of data, and the multi-tenant environment [1].

Solutions that are dependent on cloud service provider forensics can be categorized into log-based solutions and agent-based solutions. Logs are essential for digital investigations and security control, and help detect incidents, malicious activities, and security violations. Agent-based solutions (e.g., using bots and botnets as forensic agents) have been proposed. Botnet-as-a-Service (BaaS) permits access to information on a centralized site, but it may be questioned in a court of law because the bot malware compromises the machine [1].

Cloud computing and the Internet of Things (IoT) have introduced challenges to cyber forensics. There are challenges in IoT forensic tools and processes because these processes and tools must adapt to the changing environment and devices. In addition, weak authentication mechanisms of access to IoT devices make it difficult to authenticate users in forensic evidence [2].

An IoT forensics model, named the HoneyNetCloud Investigation Model (HIM), was presented. The modules in the model include detection, evidence collection, preservation, and examination. The modules are integrated into the IoT HoneyNetCloud. HIM utilizes honeypots to attract hackers and record hackers' intentions and behaviors. The types of attacks are categorized by the algorithm based on Dempster-Shafer Theory (DST) [3].

The primary purpose of the research in this survey paper is to extend cyber forensics to advanced technology platforms (beyond traditional workstation and server approaches), specifically, including cloud and virtual machines, IoT, and mobile devices. The remainder of this paper will be organized as follows: the second section introduces cyber forensics of cloud and virtual machines; the third section presents cyber forensics of the Internet of Things; the fourth section introduces mobile device forensics; the fifth section presents cyber forensics on advanced technology platforms in healthcare, including cloud forensics in healthcare, cyber forensics of virtual machines in healthcare, IoT forensics in healthcare, and mobile device forensics in healthcare; and the sixth section is the conclusion.

2. CYBER FORENSICS OF THE CLOUD AND VIRTUAL MACHINES

Cloud forensics involves dealing with challenges regarding data ownership, jurisdiction, and the ever-changing nature of cloud storage. Multi-tenancy and data segregation make forensic investigations complicated. The management and assurance of log integrity within a distributed environment is an inherent challenge [4]. Three main legal challenges were identified from the cloud-based technological landscape. They are: 1) the loss of

*Address correspondence to this author at Institute for IT Innovation and Smart Health, Mississippi, USA; E-mail: cannalexander68@gmail.com

Table 1: Digital Forensics Process and Challenges in Cloud Forensics [6]

Stages of digital forensics	Challenges in Cloud Forensics
Identification	Unknown physical locations, data duplication, decentralized data, jurisdiction, encryption, dependency chains, and dependence on Cloud Service Provider (CSP).
Preservation	Chain of custody, distributed storage, evidence segregation, data integrity, and data volatility.
Collection	Inaccessibility, trust, jurisdiction, multi-tenancy, deleted data, dependence on CSP, and lack of specialist commercial tools.
Examination & analysis	Lack of a log framework, encrypted data, an evidence timeline, and evidence data integration.

location (data territoriality, dealing with the multilocation of cloud-stored data), 2) the cloud content ownership (possession, dealing with how it changes when moving to a virtual environment), and 3) user authentication and data preservation (confiscation procedure, dealing with the distinguishability of cloud-stored evidence in a shared pool) [5].

Cloud forensics has presented multifaceted challenges regarding evidence collection and forensics investigation due to its virtualized, heterogeneous, and scattered architecture [1]. Table **1** lists the challenges in various stages of digital forensics.

A virtual machine (VM) is a software-based computer that mimics a physical computer. VMs can store data, run programs, and connect to networks. They are portable and can be utilized in cloud computing to virtualize the resources of the cloud service provider's servers. They can mimic real systems and record users' activities; therefore, they are helpful for cyber forensics in the following aspects: 1) track and record users' activities, 2) test software, 3) analyze evidence, and 4) recreate crime scenes (utilizing real evidence) [7, 8]. In a cloud environment, the transient nature of resources, such as virtual machines and containers, can result in volatile data [4].

3. CYBER FORENSICS OF INTERNET OF THINGS

IoT digital forensics is an important research field. IoT repositories are environments that are rich with forensic data; however, IoT devices are complicated areas for conducting forensic analysis. The landscape of IoT has been categorized into three dimensions: technical, spatial, and temporal [2]. Forensics in the IoT environment was studied with a unified 3D framework, as illustrated in Figure **1**.

Evidence sources in an IoT environment vary with specific applications; therefore, investigators should have various focuses. Main evidence sources in various IoT applications are listed in Table **2** [2].

Table **3** [9] lists the difference in process complexity between IoT and conventional digital investigations. Table **4** [9] summarizes the difference between IoT and conventional digital investigations in evidence sources, data usage, network boundaries, and storage.

Biometrics in IoT, also called the Internet of Biometric Things (IoBT), has been utilized to protect IoT devices from unauthorized access [10]. An example of IoT forensics based on biometric authentication was presented with three various forensic schemes (i.e., cloud forensics, network

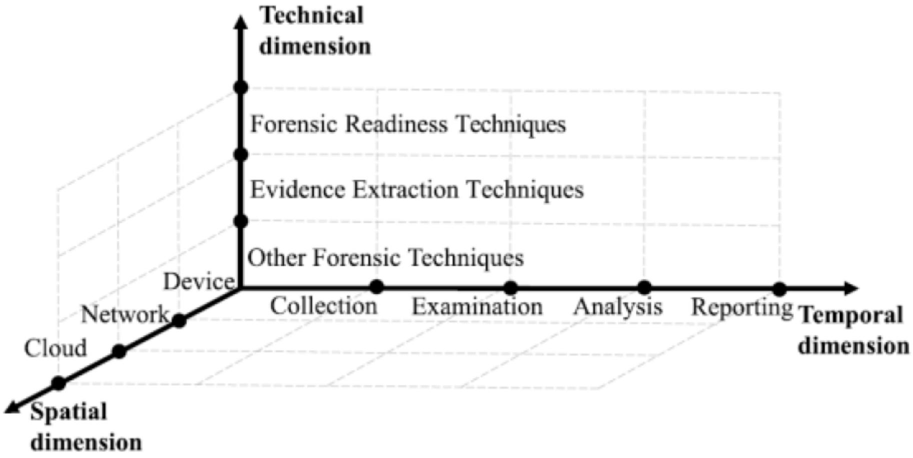

Figure 1: Three Dimensions of IoT Forensics [2].

Table 2: Main Evidence Sources in Various IoT Applications

Applications	Evidence sources
Wearables	Wearable devices Cloud services Device communication data Apps on PCs & smartphones
Smart vehicles	Automotive sensors GPS systems Advanced automotive applications Automotive networks & bus systems
Smart homes	Smart hubs Local networks Cloud servers Smart appliances Apps on the web & smartphones
Control systems	System logs Field devices Control system networks
Cloud-enabled IoT devices	Customers & web applications Computer memory & hard drives

Table 3: A Comparison of the Process Complexity between IoT and Conventional Digital Investigations

Investigation Process	IoT	Conventional
Identification	High	Medium-high
Collection	Medium-high	Low-medium
Organization	High	Medium-high
Presentation	Low-medium	Low-medium

Table 4: A Comparison between IoT and Conventional Digital Investigations in Evidence Sources, Data Usage, Network Boundaries, and Storage

Aspects of the Investigation Process	IoT	Conventional
Evidence Sources	Embedded sensors & tags, IoT smart devices, radio frequency identification (RFID) devices	Laptop & desktop computer customers
Data usage	Exabyte	Terabyte
Network boundaries	Obscured & blurred boundaries in IoT forensics because of many devices	Defined boundary (depending on the case or ownership)
Storage	Micro cards, memory, & RAM-based to collect the state of a disk	Disks

forensics, and device-level forensics), as illustrated in Figure **2**.

4. MOBILE DEVICE FORENSICS

Mobile device forensics is a process of extracting and analyzing digital evidence from mobile devices, such as tablets and smartphones. Specialized tools are employed to extract data from the storage media or memory of a mobile device. Mobile device forensics helps detect cyber risks or threats (such as data breaches and malware), investigate crimes (such as fraud and theft), and recover deleted or lost data (e.g., videos, texts, photos, call logs, and GPS data) [11, 12].

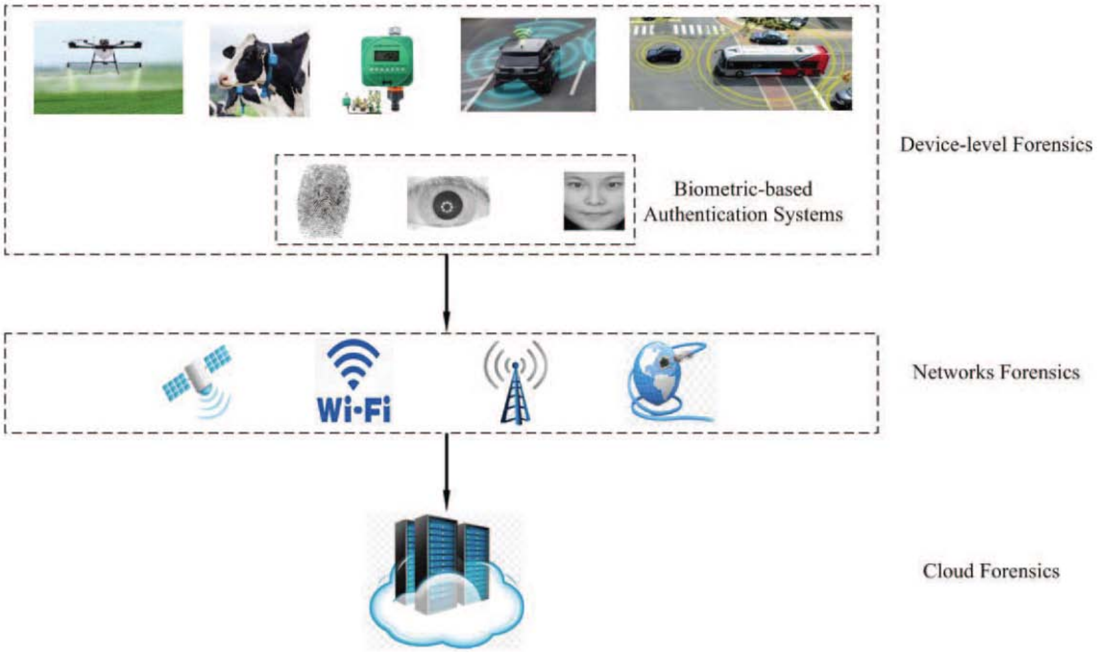

Figure 2: An Example of IoT Forensics [10].

Table 5: Examples of Mobile Forensic Evidence

No.	Types of mobile evidence
1	Contact lists & phonebooks.
2	Incoming, outgoing, missed call history—Call detail records.
3	Videos, pictures, audio, voicemail messages, etc.
4	Spreadsheets, presentation files, documents, & other user-created data.
5	Search history, Internet browsing history, content, cookies, & analytics information.
6	Wi-Fi connection information, historical geolocation data, & location data related to cell phone towers.
7	User dictionary contents.
8	Data from different installed apps.
9	Passcodes, swipe codes, passwords, & credentials of user accounts.
10	To-do lists, calendar entries, notes or memos, etc.
11	Multimedia messaging content, SMS (short message service) texts, etc.
12	Removed files or data from all the above.
13	System files, usage logs, error messages, etc.

Some examples of mobile forensic evidence are listed in Table **5** [13, 14].

Mobile forensic tools for Android (a mobile operating system) and iOS (formerly iPhone OS) platforms were studied. Autopsy, Oxygen, and MOBILedit are Android forensic tools, while Cellebrite Universal Forensic Extraction Device (UFED) and iPhone Backup Analyzer are iOS forensic tools. The autopsy tool is utilized to extract and analyze data from Android image files. Oxygen permits reading information from phones. MOBILedit is a logical data acquisition tool that is utilized for gathering evidence. UFED enables extraction, decoding, analysis, and reporting for mobile data. iPhone Backup Analyzer deals with the difficulty of using iOS to back up and analyze files and data [13].

A comparison of these mobile forensic tools is summarized in Table **6** [13, 15] based on their functions. Device identification is the function of identifying a device. Data decryption is the function of decoding data from the device. Data extraction enables

Table 6: Functions of Some Mobile Forensic Tools

Forensic tools	Autopsy	Oxygen	MOBILedit	UFED	iPhone backup analyzer
Device identification		Yes	Yes	Yes	
Data decryption		Yes			Yes
Data extraction	Yes	Yes	Yes	Yes	Yes
Messenger application analysis	Yes	Yes	Yes	Yes	Yes
Data report		Yes	Yes	Yes	
Recovery of deleted data	Yes	Yes	Yes	Yes	Yes

the retrieval of data from the device. Messenger application analysis is the ability to view Messenger application content. The data report is the function of recording information in a text file. Recovery of deleted data is the function of recovering data [13].

Investigators often follow the following procedures: 1) seize the device (seizing the device from a user and documenting the chain of custody), 2) acquire the device (creating a duplicate of the device's data), 3) analyze data (such as videos, photos, and text messages), and 4) preserve evidence (protecting evidence from being destroyed or altered). The challenges of mobile device forensics lie in 1) mobile devices are not isolated, stationary, and static; and 2) digital evidence from mobile devices is often volatile and fragile; therefore, it is easy to be destroyed due to inappropriate treatment [11, 12].

5. CYBER FORENSICS ON ADVANCED TECHNOLOGY PLATFORMS IN HEALTHCARE

5.1. Cloud Forensics in Healthcare

Cloud forensics in healthcare utilizes digital forensics to investigate and respond to security incidents in a cloud-based healthcare system. It is important in healthcare due to the security of sensitive healthcare data and compliance (guaranteeing adherence to HIPAA and other healthcare regulations). It can be utilized to analyze logs and other digital evidence to detect possible compliance problems. Forensic analysis tools (e.g., FTK) help create forensic images of cloud data, analyze file systems, and examine metadata. Cloud forensics has been utilized in healthcare: 1) internal investigation (identifying potential misuse or unauthorized access), 2) investigating data (e.g., patient information in the cloud) breach, 3) compliance audit, and 4) incident response. Cloud forensic investigation in healthcare involves the analysis of cloud logs, access controls, user activity, and other digital evidence for identifying suspicious behaviors or potential breaches. The challenges of cloud forensics in healthcare are as follows: 1) data volatility—cloud data in healthcare could be overwritten or deleted quickly, requiring rapid actions to preserve evidence; 2) data dispersion—cloud healthcare data could be scattered across various servers, making it complicated to collect evidence; and 3) third-party provider reliance—healthcare providers frequently rely on cloud service providers, making an investigation process complex [16, 17].

5.2. Cyber Forensics of Virtual Machines in Healthcare

VMs permit an investigator to analyze potential digital evidence from patients' medical records or a healthcare system in a safe and isolated space, which helps detect possible security breaches or malicious activities in healthcare. Specific applications are as follows: 1) preserving evidence integrity—an investigator enables data analysis without altering the original records of patients by creating a virtual copy of a suspect system, 2) isolated analysis environment—a VM provides users with a separate environment to analyze data and run forensic tools, 3) reproducible investigations—replicating the virtual environment easily to examine evidence again or share analysis with colleagues, 4) testing security measures—evaluating the effectiveness of security protocols in a healthcare system by simulating various attacks without affecting real patient data, and 4) forensic analysis of medical devices—analyzing the data and logs of the medical devices that are suspected to be compromised. There are challenges for virtual machines in healthcare forensics: 1) complicated virtual environments, 2) possible data manipulation and modification of VM images by malicious actors to cover their tracks, and 3) a possible requirement of much processing power if big medical datasets are analyzed in a virtual environment [7, 8, 18].

5.3. IoT Forensics in Healthcare

Electrocardiogram (ECG) biometrics has been utilized for user authentication in IoT, and it was observed that ECG biometrics was reliable and easy to use. A biometric authentication framework was proposed to provide authentication for patient monitoring (guaranteeing the right patients and the right data) in the healthcare environment with IoT. There are three authentication stages in the framework: 1) patients to smartphones, 2) smartphones to the network, and 3) patients to the remote server [10].

IoT forensics involves the collection and analysis of evidence to prevent future attacks on IoT. IoT devices create logs, including access records, timestamps, and users' behavior data. Challenges in IoT forensics include the variety of systems, devices, manufacturers, and communication standards utilized in IoT devices [19].

IoHT (Internet of Healthcare Things) forensics is the process of collecting and analyzing evidence from IoHT devices to investigate crimes. The major procedures of IoHT are: 1) acquire and preserve—collect data from IoHT devices securely while preserving evidence integrity, and 2) analyze—analyze malware, examine data formats, and review log files. Challenges of IoHT forensics lie in patient privacy, device diversity (many various types of IoHT devices), and 3) resource constraints (limitations on resources available for forensic analysis). Internet of Medical Things (IoMT) devices include sensors, smart meters, health implants, etc. IoMT forensics is the process of collecting, analyzing, and reporting evidence from IoMT devices. Advantages of IoMT forensics include 1) protecting data (preventing unauthorized access and data breaches), enhancing security (rapid responses to cyber incidents), and preventing future incidents [19, 20].

A remote attestation protocol, BDMFA (Blockchain-supported and Deep Learning Medical Forensic-enabling Attestation), was presented. It was demonstrated that BDMFA is resilient to many attacks, and it is a forensic-enabling attestation technique for IoMT. Figure **3** illustrates an IoMT-network model treated by BDMFA. The model includes a blockchain, a Trust Authority (TA), a cloud server, hospital networks, wireless body area networks (WBANs), etc. Healthcare data (e.g., heart rate and blood pressure) is captured by WBANs via their sensors. The data is sent to the cloud server. The TA is the trusted party of the system, and it is responsible for initializing and attesting the system. Blockchain helps enhance the system's security and resilience to many attacks [21].

5.4. Mobile Device Forensics in Healthcare

Mobile device forensics can be utilized in healthcare as follows: 1) regulatory compliance (compliance with regulations regarding healthcare data), and 2) data

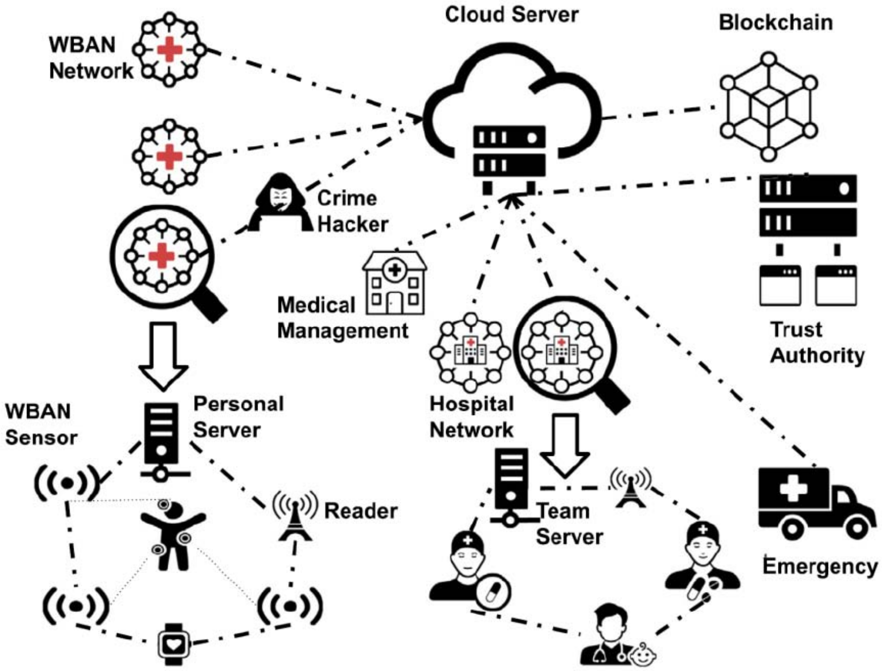

Figure 3: An IoMT-network Model Treated by BDMFA [21].

security and privacy (detecting and dealing with vulnerabilities in healthcare data systems). The following procedures are often followed: 1) secure the device (physically securing the device), 2) acquire data (a copy of the device's storage), and 3) analyze data (finding relevant information and evidence). The challenges of mobile device forensics in healthcare lie in 1) data volatility—data can be deleted or overwritten easily, 2) encryption—it is often difficult to access and analyze data due to the encryption of many devices, and 3) communication shielding—customers often employ encrypted messaging apps or burner phones, making it difficult to recover data [11, 12].

6. CONCLUSION

Cloud forensics involves dealing with challenges regarding data ownership, jurisdiction, and the ever-changing nature of cloud storage. In a cloud environment, the transient nature of resources, such as virtual machines and containers, can lead to volatile data. IoT forensics can be categorized into technical, spatial, and temporal dimensions. Mobile device forensics helps detect cyber risks or threats, investigate crimes, and recover deleted or lost data. Cloud forensic investigation in healthcare involves the analysis of cloud logs, access controls, user activity, and other digital evidence. VMs permit an investigator to analyze potential digital evidence from patients' medical records or a healthcare system. IoT forensics involves the collection and analysis of evidence to prevent future attacks on IoT. Applications of mobile device forensics in healthcare lie in regulatory compliance, data security, and privacy.

ACKNOWLEDGEMENTS

The authors would like to express thanks to Technology and Healthcare Solutions, USA, for its help and support.

DECLARATION OF THE USE OF AI TOOLS

The authors declare that they did not use AI tools in writing this paper.

CONFLICT OF INTEREST

The authors would like to announce that there is no conflict of interest.

ETHICS

In this article, ethical principles related to scientific research articles are observed. The corresponding author confirms that both authors have read, revised, and approved the paper.

REFERENCES

[1] Manral B, Somani G, Choo KK, Conti M, Gaur MS. A systematic survey on cloud forensics challenges, solutions, and future directions. ACM Computing Surveys (CSUR) 2019; 52(6): 1-38. https://doi.org/10.1145/3361216

[2] Hou J, Li Y, Yu J, Shi W. A survey on digital forensics in Internet of Things. IEEE Internet of Things Journal 2019; 7(1): 1-15. https://doi.org/10.1109/JIOT.2019.2940713

[3] Jayakrishnan AR, Vasanthi V. Internet of things forensics honeynetcloud investigation model. In2020 International Conference on Electronics and Sustainable Communication Systems (ICESC) 2020; pp. 660-666. IEEE. https://doi.org/10.1109/ICESC48915.2020.9155775

[4] Morić Z, Dakić V, Kapulica A, Regvart D. Forensic Investigation Capabilities of Microsoft Azure: A Comprehensive Analysis and Its Significance in Advancing Cloud Cyber Forensics. Electronics 2024; 13(22): 4546. https://doi.org/10.3390/electronics13224546

[5] Karagiannis C, Vergidis K. Digital evidence and cloud forensics: contemporary legal challenges and the power of disposal. Information 2021; 12(5): 181. https://doi.org/10.3390/info12050181

[6] Ali SA, Memon S, Sahito F. Analysis of cloud forensics techniques for emerging technologies. In2020 International Conference on Computing, Networking, Telecommunications & Engineering Sciences Applications (CoNTESA) 2020; pp. 106-111. IEEE. https://doi.org/10.1109/CoNTESA50436.2020.9302862

[7] Purnaye P, Kulkarni V. BiSHM: Evidence detection and preservation model for cloud forensics. Open Computer Science 2022; 12(1): 154-70. https://doi.org/10.1515/comp-2022-0241

[8] Zhang J, Gao C, Gong L, Gu Z, Man D, Yang W, Li W. Malware detection based on multi-level and dynamic multi-feature using ensemble learning at hypervisor. Mobile Networks and Applications 2021; 26(4): 1668-1685. https://doi.org/10.1007/s11036-019-01503-4

[9] Amiroon S, Fachkha C. Digital forensics and investigations of the internet of things: A short survey. In2020 3rd International Conference on Signal Processing and Information Security (ICSPIS) 2020; pp. 1-4. IEEE. https://doi.org/10.1109/ICSPIS51252.2020.9340150

[10] Yang W, Johnstone MN, Sikos LF, Wang S. Security and forensics in the internet of things: Research advances and challenges. In2020 Workshop on Emerging Technologies for Security in IoT (ETSecIoT) 2020; pp. 12-17. IEEE. https://doi.org/10.1109/ETSecIoT50046.2020.00007

[11] Bernardo BM, São Mamede H, dos Santos VM, Barroso JM. Mobile device forensics framework: a toolbox to support and enhance this process. Emerging Science Journal 2024; 8(3): 972-998. https://doi.org/10.28991/ESJ-2024-08-03-011

[12] Fukami A, Stoykova R, Geradts Z. A new model for forensic data extraction from encrypted mobile devices. Forensic Science International: Digital Investigation 2021; 38: 301169. https://doi.org/10.1016/j.fsidi.2021.301169

[13] Aljahdali A, ALSAIDI N, Alsafri M, Alsulami A, Almutairi T. Mobile device forensics. Romanian Journal of Information Technology & Automatic Control/Revista Română de Informatică și Automatică 2021; 31(3). https://doi.org/10.33436/v31i3y202107

[14] Horsman G. “I couldn't find it, your honour, it mustn't be there!”–Tool errors, tool limitations and user error in digital forensics. Science & justice 2018; 58(6): 433-440. https://doi.org/10.1016/j.scijus.2018.04.001

[15] Beard I. Digital Photos, Embedded Metadata and Personal Privacy. In The Complete Guide to Personal Digital Archiving 2018; pp. 201-212. ALA Editions. https://doi.org/10.7282/T3TH8QR9

[16] Jayaraman I, Stanislaus Panneerselvam A. A novel privacy preserving digital forensic readiness provable data possession technique for health care data in cloud. Journal of Ambient Intelligence and Humanized Computing 2021; 12(5): 4911-4924. https://doi.org/10.1007/s12652-020-01931-1

[17] Mishra AK, Govil MC, Pilli ES, Bijalwan A. Digital Forensic Investigation of Healthcare Data in Cloud Computing Environment. Journal of Healthcare Engineering 2022; 1: 9709101. https://doi.org/10.1155/2022/9709101

[18] Fernández-Fuentes X, Pena TF, Cabaleiro JC. Digital forensic analysis of the private mode of browsers on Android. Computers & Security 2023; 134: 103425. https://doi.org/10.1016/j.cose.2023.103425

[19] Alqahtany SS, Syed TA. ForensicTransMonitor: a comprehensive blockchain approach to reinvent digital forensics and evidence management. Information 2024; 15(2): 109. https://doi.org/10.3390/info15020109

[20] Grispos G, Tursi F, Mahoney W. A digital forensic analysis of an electrocardiogram medical device: A first look. Wiley Interdisciplinary Reviews: Forensic Science 2024; 6(6): e1535. https://doi.org/10.1002/wfs2.1535

[21] El-Zawawy MA, Vasudev H, Conti M. BDMFA: Forensic-enabling attestation technique for Internet of Medical Things. Internet of Things 2025; 29: 101464. https://doi.org/10.1016/j.iot.2024.101464

Received on 08-09-2025 Accepted on 27-10-2025 Published on 04-11-2025

https://doi.org/10.65879/3070-5789.2025.01.01