

IoT and smart devices : A forensic framework for digital evidence footprint collection

Bamidele Busari Abdullahi [†]

Jayant Shekhar ^{*}

Pushpendra Kumar Rajput [§]

Department of Computer Science and Engineering

Sharda School of Computing Science & Engineering

Sharda University

Greater Noida 201310

Uttar Pradesh

India

Abstract

In almost all most 99% investigations, the main issue is to determine whether or not a particular person was present at the crime scene. The internet of things (IoT) and smart devices have been very helpful in this area of investigations, as it is digital device which make it easy for digital forensic tools in playing a roll. Detective depend on these smart devices in other to bring light digital proofs and identify the actual criminal or persons who was there. Fingerprint are no longer the only source of evidence; now even footprints can be use as scientists have proved through countless publications and research that every footprint is different like every fingerprint. Digital crime on the other hand is not getting slow again. Most probably due to the fact that a large number of people are using network computer and communication devices, which contain vast amounts of data, the number of cases is constantly on the rise. Our dependence on digital technologies is inversely proportional to the number of traces that we leave behind, traces that are easily detected by investigators. This transition is not just about comfort, it has affected court systems in quick decision. Digital evidence shows up in courtrooms all the time now.

Digital forensics is a core part of most investigations, Sometimes the computer and the smart device is the tool used to commit the crime, other times it holds key info about

^{*} ORCID-ID: 0009-0003-1757-1854

[§] ORCID-ID: 0000-0002-1784-3157

[†] E-mail: 2024873546.bamidele@pg.sharda.ac.in

^{*} E-mail: Jayant.shekhar@sharda.ac.in (Corresponding Author)

[§] E-mail: Pushpendrakumar.rajput@sharda.ac.in

what happened either way, if a smart device was around you then you get investigators in checking for the clues.

Subject Classification: 68U35, 68M14, 68M18.

Keywords: IoT forensics, Digital evidence, Digital footprints, Footprint identification, Cybercrime investigation, Digital trace analysis, Criminal identification, Mobile forensics.

I. Introduction

Digital footprints can refer to the trace of information left behind by the user when they are using internet or smart devices, Media and social media posts, detail of word or data share by you become the digital footprints on the net. It also contains passwords, demographic information, online purchases and IP addresses tied to someone's digital profile. The last decade has seen an impressive development in digital forensics. This can only be attributed to or attached to the body of scientific literature which is becoming more available and the developing literature from various others [1], [2]. With the increasing diffusion of Internet of Things (IoT) in our daily routines, the importance and the need for comprehensive forensic frameworks has become evident. Almost our daily use items, from our mobile phones to our smart home devices are internet of thing (IoT) enabled and can contain large quantities of sensitive information which can be use or exploited for criminal activities if bindery is not set and forensic investigators make heist why sun set. The penetration of the same has been described in Figure 1. The inadequacies offered forensic strategies are to a great extent due to the lack of adequate security measures and government policy in dealing with the possible breaches of the user privacy [8]. The primary goal of this research is to illustrate the significance of the need for tailored. Holistic approach in the design of a forensic framework to meet the obstacles involved in the acquisition of digital evidence from this system. This research seeks to apply emerging technologies such as blockchain and machine learning to provide innovative approaches to the management of digital evidence and the retrieval of evidence in a manner or away that protects the integrity of the information [9]. The challenges of IoT devices as components of digital forensics are illustrated in a diagram that depicts some of the elements involved in the collection data in digital evidence.

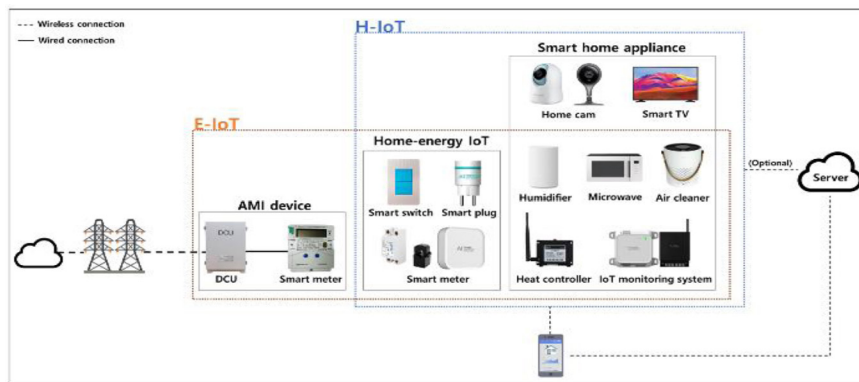


Figure 1

Integration of IoT Technologies in smart homes

Overview of IoT and Smart Devices in Modern Society

There is no denying that smart devices and the Internet of Things (IoT) have revolutionized the way we interact with technology. The communication, sharing and interaction of data worldwide is the best ever; notwithstanding, the innovation in devices is producing and oftentimes exposes sensitive personal information like usage habits, medical details and the feature which is needed in retrieving devices monitoring through large forensic investigator techniques, Type B in Figure 2, and evaluating sensitive data [4]. The good thing about it is that vast IoT devices world is very complicated and thus difficult handle coming along with it. It is mixture and combination of different operating systems together with their various data information storage methods that is the factor increasing difficulties surrounding data retrieval and preservation [1]. Most of the devices either have no security or very basic security only (standardized security protocols). As a result of it, the chances of cyber-attacks and data leaks are very high. It will take a very creative and critical thinking solution to tackle this problem, in fact, the systems that are utilizing AI and ML might as well be the ones to improve our forensic capability [5], [6]. Besides, interconnectivity really brings out how tough such networks are and thus it clearly depicts how important it is to have excellent forensic practices in our gradually digital world.

II. The Importance of Digital Evidence in Forensics

In digital forensics landscape, though dynamic can still be appreciated for the significant role that digital evidence and especially that from Internet of Thing (IoT) devices. With the IoT ecosystem getting bigger and better, these connected devices are becoming very important for the investigation of the IoT as the 'digital evidence' ecosystem. Each smart device helps its smart partners, can capture, storing and send valuable forensic evidence in the form of user interaction(s) and environmental changes. Considering the large amount of evidence and the variety of data (plus vigilant threats) it is very important to come up with a comprehensive strategy that would give Figure 2 Type D function the collection. Retention, preservation and secure storage of this evidence. IoT devices are probably the biggest enabler of digital CSI capabilities, as shown by CSI Sniffer tools, this enables the user to grasp the behavioral patterns of users and the corresponding threats that will be present through the data it captures and analyzes [4]. The previously mentioned factors, along with other obvious and imminent dangers such as fingerprint spoofing, are the reasons why the continued evolution of forensic methods is a necessity in tackling digital crimes [6]. Even the researchers have explored about different materials that can help in spoofing fingerprint sensors that are biodegradable [7, 8]. Besides having a good, structured method for collecting digital evidence, like some framework lay out is, just reinforce the necessity of organized efforts for securing the right data for thorough analysis. With all this interconnectivity, it simply indicates the complexity of these networks. It truly makes one realize the importance of having strong forensic practices in this digital age.

Types of Digital Evidence Collected from IoT Devices

Device of Internet of Things comes in variety of different types; for instance, the smart and prompt thermostat, wear devices and the refrigerator in your kitchen, at the point of forensic investigation each of them generates it unique stream of digital evidence. In summary we get everything. User activities, device measurement parameters, logs with timestamps of actions taken by different personalities and so on. The interconnectivity between this device shows results in Figure 2 Type A, sometimes even in unpredicted ways. The point still remains that at every stage the situation gets more complicated. Every IoT appliance for instance, acts differently. It could be difference in operating systems, different type of data storages and a lot of the times no storage at all just some simple

memory storage [1]. The identifiable factors result as the capturing of evidence into a large problem. Even critical, smart devices are capable of generating huge amounts of data in a very short period. Forensic scholar needs quality and dedicated tools just in keeping tracks [2]. There for they are glimmer of hope, Artificial Intelligence (AI) is gradually and systematically growing and getting rid of the old forensic frameworks. Meanwhile Artificial Intelligence (AI) speeds up the process of evidence collection and analysis the the factor surrounding it, making it not only quicker but also more precise and dependable making Internet of Thing (IoT) security a greater lift [7]. When you take a step backward, it becomes clear that the different types of evidence created by IoT devices in smart area are mostly interconnected in every intricate manners. The situation is nice and also full of opportunities.

Recent research has highlighted the growing importance of cybersecurity and digital technologies across sustainable development and healthcare applications [11], [12]. Advances in digital forensics have further expanded into areas such as e-bike systems, aviation, IoT devices, mobile devices, and forensic science technologies [13]-[18]. Emerging digital-care networks also emphasize the need for secure and reliable next-generation communication systems [19]. Foundational research on dermatoglyphics and digital forensic practices continues to support biometric and forensic investigations [20], [21].

III. Objective

To provide and create easy digital evidence data gathering for forensic practitioners and researchers with strategic framework in developing effective systematic methodologies in tackling many data privacy concerns digital evidence footprint collection related to digital forensics. To discusses evidence gathering in footprint techniques used in digital forensic environ concerning privacy preservation and explore some of their behaviors considering trusted third parties, many investigator and multi-keyword researchers in the area of evidence footprint collection.

IV. Methodology

Anomaly detection: This can be define as the systematical involve in identifying or recognizing similarities between data found on different drives or processor in other to establish fact and detect suspicious activities.

Correlation and comparison: This can be defined as systematical involve in analyzing data information from multiple drives in other to establish relevant fact and information with building a comprehensive picture of an event.

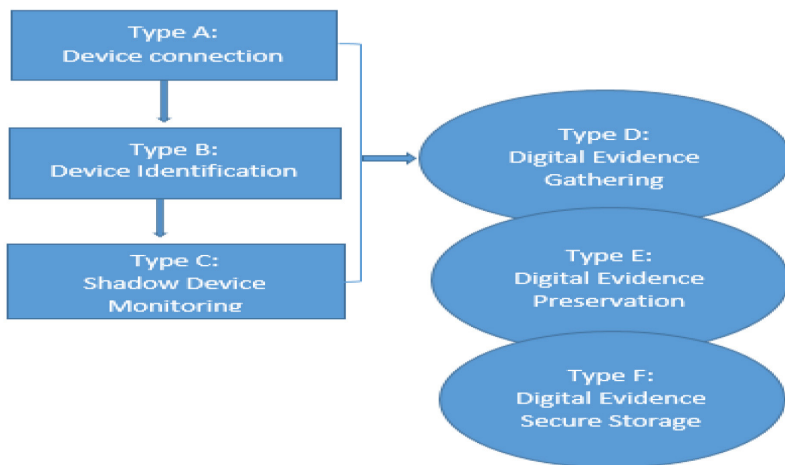


Figure 2
Device Setup Evidence Collection

Device Connection: The process of device connection is having full access to the device which the connection bring it online for investigation.

Data Collection: This process involve data collected or gather for identified and investigation.

Examination: This process involves collection of data and examine it carefully.

Analysis: Is an act that involve different tools and techniques in collecting evidence to be analyze to a final conclusion.

Reporting: This process gives final step of all the documentation and reports are compiled so it can be tender in court as evidence.

Barriers and Techniques in Forensic Investigations

When talking about digital forensic investigation, the issues get complicated when IoT and smart devices are included. That roadmap, both technical and legal, make it a tough and difficult task to collect and protect the digital evidence. The whole ecosystem of devices generate more complex to the issue. The whole process of data extraction is just the

starting, data protection is another quarreling, that also is a big one. Never the less, weak privacy laws and fast and grow moving technology makes it even harder [9-10]. Digital evidence law! It is popularly in the process of meeting up. Consequently forensic scholars face a lot of perplexing questions like what evidence is admissible in the court and how to handle it appropriately, Finance is another hindrance, it is expensive in other to build up strong forensic capabilities, thus, always the smaller police department, cannot afford the necessary tools or training. This keeps digital investigation in the old part. A real flowchart of the step for collection of digital evidence portrays the intricacies include when IoT devices are in action, All this requires very precise and vigilant approach both in terms of the technology inclusion and the legal aspects. As for the crime detection techniques, which work in most cases but are still open to deceive if mischief makers are present. All the digital data collection and storage phenomenon has to be controlled through a more sophisticated system. This would mean every Internet of Thing (IoT) or device have to be registered and licensed before it used. Picture a central database, owned by the state, containing information on every devices. Forensic investigators can immediately gather data information and monitor crime activities more closely, This would allow for better management of data trails and at the same period, make it more difficult for the criminals to destroy their track.

How it can work:

- i. High-level process
 - Register of IoT and communication device before use.
 - Store device data information in a base, government controlled database.
 - Use the data collected in the data base to proof and secure digital data footprints.
 - Authorize people will only be allow to have access to the database.

Algorithm Step-by-Step (pseudo-code style):

1. Registration request will be submitted by the user or manufacturer to the central system base.

2. Legalize system verification and impose compliance
3. License and logs device detail will be issues like ID, Owner, and Location etc.
4. Activation of device to begin operations
5. Every communication devices with data footprints are logged in the central system base in real time
6. An investigator access data needed through secure legal channels

Visual Workflow (sequence-style narrative):

The scope is this, if tries to set up a new IoT device but before it can be use registration is mandated to have the user details in government-run database. The system checks all the information details give out license after recorded everything in the database. Now as the device do its things, coding messages decoding data, whatever all digital footprints collected down into central system. If an investigation that have to do with digital devise so the investigator will have a trace where to go and fetch needed data from the central base. Which the center base is trusted base on government own set up, which every one plat by same rules due to the policy guiding it.

V. Data Analysis

This where the sample of my data is described in Table 1 that is used for analyzing and investigating some of the data or information a user used or behavior with through the analysis of digital footprints (DF). Essentially, a digital footprint (DF) is a record comprehensively gathered and generated during the use of digital technology and services. It included all the record about the user such as user name, email address, application use and messages sent. The information provided in the data set, which table shows below, shows that it is either meant for digital profiling experimentation or part of an actual centralize design system for digital footprint behaviors in real time investigation. Once you lay hands on or having access to data set you will notice that it incorporates personal information which can be seeing in the central database design such as Names, e-mail address, phone numbers, and date of birth with behavioral data. Both are fundamental in determining a person digital footprint (DF). Individual can be easily identify and located with columns like "Personal ID", "First Name", "Last Name", "Email", "Phone", and "Date of Birth" "Sex". This are the types of data that the smart or IoT devise commonly

gather and accumulated when creating and account or working on a devices either by using applications or doing any transaction on the a devise. There for the must eye catching or target is the presence of “Application” column. The data indicates google.in.com.andriod. googlefastsearchbox as an example that implies the tracing of a footprint data includes the recording details of the system users along with the period they use the devise for things best known to them. Below is the statistical summary of one individual person from the dataset tag to be track from the digital footprint database.

Table 1
Data Description using the statistics about the different candidates

Column	Count	Unique	Top	Freq	Min	Max	Mean	Std
Index	60	60	1	—	1	60	30.5	17.46
Person Id	60	20	BF0BbA03C29Bb3b	8	—	—	—	—
First Name	60	20	Sheila	8	—	—	—	—
Last Name	60	20	Ross	8	—	—	—	—
Sex	60	2	Male	42	—	—	—	—
app	60	21	google. in.comandroid. googlefast searchbox	8	—	—	—	—
Email	60	20	huangcathy@example.com	8	—	—	—	—
Phone	60	20	895.881.4746	8	—	—	—	—
Date of birth	60	20	2008-03-20	—	—	—	—	—
Job Title	60	20	Advertising account executive	8	—	—	—	—

Combination of data identification and digital footprint (DF) collection statistics, and measures in that can track their behavioral patterns adhered to procedure embrace in digital forensic (DF). Targeted device, or user analytics. This demonstrates how subject to systematic examination, digital footprints may grow useful information about the system users. In brief the classification is a report and example of a methodical attempt to collect, categorize and examine user information.

The simple graph describing the frequency of the App usage has been described in Figure 3.

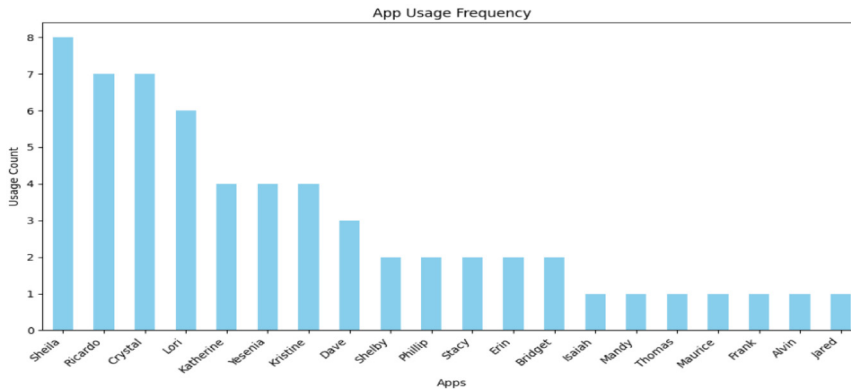


Figure 3
App Usage Frequency

VI. Challenges in Collecting Digital Evidence from Smart Device

The timely paced development of IoT and smart devices is indicating a myriad of difficulties in the collection and gathering of digital evidence. The main problem is the disparities between this technology equipment and the extent of the attacker's behaviors in evading detection. Each internet of things (IoT) equipment comes with unique behavior identity in different architecture, varies operating systems, and methods of storing information data. With this make digital forensic interesting but more complex to difficult in setup, it difficult in any processing power at all in common devices, which it not even possible to run regular forensic tools to it. Which likely not to be made for them for investigation. Going by some experts it is right moment they develop new forensic framework for investigation that will be for compatible to IoT smart device environment. But there is more to the understanding than that. Yes the universe have become more intelligent, and the use of Anti-Digital Forensics (ADFs) techniques has become prevalent [3], making it easier for them to turn investigations upside down. Furthermore, the overwhelming amount of data generated by each connected device goes on to make the situation even more difficult. Sifting through that noise to get to the useful evidence is no easy feat. This is the reason why new technologies, such as AI are slowly becoming more integral in determining the feasibility of forensic

work [2]. Having an understanding of all these difficulties is not only beneficial but rather essential when it comes to establishing actual plans for investigating smart devices. Theoretical aspect is no longer visible in the growth-paced and technologies world of digital forensics; one must rely on practice and essential [22].

At the concluding part, It is imperative to recognize that the IoT and smart devices system rapidly changing world demanding a large forensic framework. Reason behind this? These technologies are alongside with authentically security problem which we cannot ignore. In a simple terms the number of devices is many than they are they are permanently collecting user data ID. If data is not protected it will be distortion and trouble that cannot be manage, The healthcare industry really exemplifies this and it indicates that insecurity and forensic unpreparedness are still dangerous and difficulties to overcome, especially in developing countries where infrastructural weaknesses are pronounced. it is time we had our forensic protocols well established not merely as an afterthought but incorporated right from the beginning. Take a look at the airports and all the cutting-edge technologies they have deployed. It is evident that we cannot just install smart systems and then leave everything to chance. Instead, we have to devise a scheme that would entail juggling seamless operations along with robust forensic measures. All this speaks to the fact that researchers and practitioners need to align forensic methods with the newest trends in the Internet of Things (IoT) very closely. Also, there exists a rather nice visual summary that highlights all the phases involved in digital forensic system investigations. This visual aid does a great job of simplifying these intricate issues. Future Directions for Forensic Frameworks (FDFF) in IoT and Smart Device Evidence Collection framework when one assesses the future of forensic frameworks for IoT and smart device evidence, one will realizes that the ability to flex is not merely desirable but a prerequisite. Definitely, technology is no longer slow. In one second, a brand new gadget or a software update that comes with all new peculiarities is already on the market. Specifically, IoT devices create such huge dense areas of electronic data.

VII. Conclusion

The rapid growth of the Internet of Things (IoT) and smart devices has created significant opportunities for digital forensic investigations by generating valuable digital footprints related to user activities, device interactions, application usage, timestamps, and environmental events.

However, the heterogeneous nature of IoT systems, diverse operating environments, limited device resources, distributed data storage, large volumes of evidence, and anti-forensic techniques create significant challenges for investigators.

This paper presented a systematic forensic framework for collecting, preserving, examining, analyzing, and reporting digital evidence from IoT and smart devices. The proposed approach emphasizes structured evidence collection, data correlation, anomaly detection, and secure evidence management. Artificial intelligence and machine learning can further improve the identification of suspicious activities and the analysis of large and complex IoT datasets.

The proposed centralized IoT registration and evidence-management concept can improve device traceability and facilitate authorized access to relevant forensic evidence. However, its implementation must address privacy, cybersecurity, legal authorization, access control, and data-protection requirements. Blockchain-based mechanisms may also strengthen evidence integrity and chain of custody.

Future research should focus on standardized IoT forensic tools, automated evidence acquisition, privacy-preserving techniques, AI-driven analysis, and secure evidence-management mechanisms. A flexible and forensic-ready IoT framework will be essential for reliable digital investigations while protecting user privacy and maintaining the integrity of digital evidence.

References

- [1] A. Alazab, A. Khraisat, and S. Singh, "A review on the Internet of Things (IoT) forensics: Challenges, techniques, and evaluation of digital forensic tools," in *The Role of Cybersecurity in the Industry 5.0 Era*, C. Kalloniatis, Ed. London, U.K.: IntechOpen, pp. 1–23 (2023), doi: 10.5772/intechopen.109840.
- [2] R. Rizal, S. R. Selamat, M. Z. Mas'ud, and N. Widiyasono, "Enhanced readiness forensic framework for the complexity of Internet of Things (IoT) investigation based on artificial intelligence," *Journal of Advanced Research in Applied Sciences and Engineering Technology*, vol. 50, no. 1, pp. 121–135 (2024), doi: 10.37934/araset.50.1.121135.
- [3] M. Raciti, "Conceptualising anti-digital forensics kill chain for smart homes," in *Proc. 10th Int. Conf. Information Systems Security and Privacy (ICISSP)*, vol. 1, Rome, Italy, pp. 831–837 (2024), doi: 10.5220/0012449700003648.

- [4] F. Iqbal, A. Jaffri, Z. Khalid, A. MacDermott, Q. E. Ali, and P. C. K. Hung, "Forensic investigation of small-scale digital devices: A futuristic view," *Frontiers in Communications and Networks*, vol. 4, Art. no. 1212743 (2023), doi: 10.3389/frcmn.2023.1212743.
- [5] F. Palmese and A. E. C. Redondi, "Collecting channel state information in Wi-Fi access points for IoT forensics," in *Proc. 21st Mediterranean Communication and Computer Networking Conference (MedComNet)*, pp. 1–6 (2023), doi: 10.1109/MedComNet58619.2023.10168865.
- [6] D. Dunsin, M. C. Ghanem, K. Ouazzane, and V. Vassilev, "A comprehensive analysis of the role of artificial intelligence and machine learning in modern digital forensics and incident response," *Forensic Science International: Digital Investigation*, vol. 48, Art. no. 301675 (2024), doi: 10.1016/j.fsidi.2023.301675.
- [7] G. Dorai, M. Jozani, and P. Rad, "From seaweed to security: The emergence of alginate in compromising IoT fingerprint sensors," *arXiv preprint arXiv:2404.02150* (2024), doi: 10.48550/arXiv.2404.02150.
- [8] J. Fairbanks, M. M. Arifin, S. Afreen, and A. Curtis, "Survey and analysis of IoT operating systems: A comparative study on the effectiveness and acquisition time of open source digital forensics tools," *arXiv preprint arXiv:2407.01474* (2024), doi: 10.48550/arXiv.2407.01474.
- [9] S. F. Ahmed, S. Shuravi, A. Bhuyian, S. Afrin, A. Mehjabin, S. A. Kuldeep, M. S. B. Alam, and A. H. Gandomi, "Navigating the IoT landscape: Unraveling forensics, security issues, applications, research challenges, and future," *arXiv preprint arXiv:2309.02707* (2023), doi: 10.48550/arXiv.2309.02707.
- [10] M. H. A. Ratul, S. Mollajafari, and M. G. Wynn, "Managing digital evidence in cybercrime: Efforts towards a sustainable blockchain-based solution," *Sustainability*, vol. 16, no. 24, Art. no. 10885 (2024), doi: 10.3390/su162410885.
- [11] N. N. Mohamed and B. H. H. Abuobied, "Cybersecurity challenges across sustainable development goals: A comprehensive review," *Sustainable Engineering and Innovation*, vol. 6, no. 1, Art. no. 207 (2024), doi: 10.37868/sei.v6i1.id207.
- [12] A. Arega and D. P. Sharma, "Towards smart and green features of cloud computing in healthcare services: A systematic literature review," *Journal of Information Systems Engineering and Business Intelligence*, vol. 9, no. 2, pp. 161–180 (2023), doi: 10.20473/jisebi.9.2.161-180.

- [13] M. Stachak, J. Geus, G. Pugliese, and F. C. Freiling, "Nyon unchained: Forensic analysis of Bosch's eBike board computers," *arXiv preprint arXiv:2404.12864* (2024), doi: 10.48550/arXiv.2404.12864.
- [14] C. A. S. Dias, "Smart airports: Analysing digital transformation and technological advancements in aviation. The cases of Ponta Delgada and Beijing Capital International Airports," *M.S. thesis*, Univ. Beira Interior, Covilhã, Portugal (2024).
- [15] A. Feliberty, "Basic digital forensic course," *Ph.D. dissertation*, Helms School of Government, Liberty Univ., Lynchburg, VA, USA (2024).
- [16] A. Almogbil, "Into the digital abyss: Exploring the depths of data collected by IoT devices," *Ph.D. dissertation*, Johns Hopkins Univ., Baltimore, MD, USA (2024).
- [17] X. Chango Llerena, O. Flor-Unda, P. Gil-Jiménez, and H. Gómez-Moreno, "Technology in forensic sciences: Innovation and precision," *Technologies*, vol. 12, no. 8, Art. no. 120 (2024), doi: 10.3390/technologies12080120.
- [18] A. Fukami, "Effective mobile forensics through exploiting the memory security," *Ph.D. dissertation*, Univ. Amsterdam, Amsterdam, The Netherlands (2024).
- [19] R. Ahmad, M. Hämäläinen, R. Wazirali, and T. Abu-Ain, "Digital-care in next generation networks: Requirements and future directions," *Computer Networks*, vol. 224, Art. no. 109599 (2023), doi: 10.1016/j.comnet.2023.109599.
- [20] H. Cummins and C. Midlo, *Finger Prints, Palms and Soles: An Introduction to Dermatoglyphics*. New York, USA: Dover Publications (1961).
- [21] J. R. Lyle, D. R. White, and R. P. Ayers, "Digital forensics at the National Institute of Standards and Technology," *National Institute of Standards and Technology*, Gaithersburg, MD, USA, NISTIR 7490 (2008), doi: 10.6028/NIST.IR.7490.
- [22] B. Suri, S. Taneja, S. Sharma, V. Verma, D. Parashar, P. Sikka, M. Aro-ra, and S. S. Ahmad, "A blockchain-based private framework for facilitating digital forensics using IoT," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 26, no. 5, pp. 1249–1263 (2023), doi: 10.47974/JDMSC-1733.

Received December, 2025