JCBI
Journal of Computing & Biomedical Informatics
ISSN: 2710 - 1606
ICASET
2024

*Research Article*
Collection: Intelligent Computing of Applied Sciences and Emerging Trends

# Application-Specific Investigative Paradigm, Issues, and Prospective Solutions Addressed in IoT Forensics

**Muhammad Jasim Shah[1*], Muhammad Saleem[1], Muhammad Akhter[2], Muhammad Wajid[1], Javaid Ahmad Malik[2], and Muhammad Shehzad[3]**

[1]Emerson University Multan, Multan, Pakistan.
[2]National College of Business Administration and Economics, Lahore, Pakistan.
[3]Department of Agricultural Engineering, Muhammad Nawaz Shareef University of Agriculture, Multan 60000, Pakistan.
[*]Corresponding Author: Muhammad Jasim Shah. Email: jasim@eum.edu.pk

**Academic Editor:** Salman Qadri **Published:** April 01, 2024

**Abstract:** The Internet of Things (IoT) is now covering a huge area in order to transfer data between particular things and devices. It has a wide range of benefits for business, medical, and consumer segments, therefore. However, IoT is in constant development but it is also accompanied with certain technical complications and hurdles that must be solved during implementation. The technical obstacles represent several fields like the hardware, software, application frameworks, and communication standards and protocols. However, apart from that, there are some other concerns including security, privacy, and safety issues. Computer networks are plagued by cybercrime and the situation aggravates with IoT-based systems. Investigation of this nature becomes problematic because of the added complexities of the IoT infrastructure, which comprises several IoT devices and ecosystems. With the number of internet-connected gadgets being so vast, cyber criminals are able to launch attacks over the network at the speed of light. This process of the crimes in the IoT-based application is difficult. Traditional digital forensic investigation methods are not sufficient for investigating IoT-based systems due to the unique nature of IoT systems. This paper introduces an application-specific investigation model for tracking attackers in IoT-based systems. It also identifies the obstacles associated with this investigation and outlines the future path of IoT forensic.

**Keywords:** Internet of Things; Cybercrime; IoT Forensic; Digital forensic investigation.

## 1. Introduction

The Internet of Things (IoT) is experiencing a tremendous increase in popularity. The Internet of Things (IoT) provides numerous advantages to homes, cities, organizations, industries, and other entities. Deploying IoT in business, medical, and city sectors has numerous benefits. It improves our quality of life, enhances productivity in organizations, reduces time and cost in the supply chain, and creates better customer experiences, healthcare, and city life. IoT technology has revolutionized various industries, unlocking numerous benefits such as the Industrial Internet of Things (IIoT), Internet of Medical Things (IoMT), V2X communications (Vehicle to Everything Communications), Internet of Vehicles (IoV), and the internet of battlefield Things (IoBT) [33], are being obtained in favor of the general-to-specific approach. The Internet of Things (IoT) does not refer to any specific entity, gadget, or technological innovation. The term "Internet of Things" refers to the integration of sensors, gadgets, communication technologies, data analytics, software, and cloud computing technology.

Simultaneously, the paradigm IoT has generated a security apprehension for users. The Internet of Things (IoT) is currently linked to billions of devices, yet the security of IoT devices is insufficient, which puts users' privacy at risk. Cybercriminals can swiftly breach computer systems and pilfer important data. The Internet of Things (IoT) has revolutionized multiple industries including manufacturing, healthcare, transport, and agriculture. In the near future, IoT will extend its presence to everyday items such as food

packages, furniture, paper-based documents, and other supplementary objects as predicted by the US National Intelligence Council (NIC) [1].

According to Microsoft's digital defense report for 2022, the security of IT hardware and software products has improved in recent years. However, the security of IoT has not been adequately addressed. In 2017, the US Food and Drug Administration issued a warning that an individual skilled in IoT hacking can exploit system vulnerabilities using hacking tools, posing a significant risk to the lives of patients with pacemakers. Furthermore, numerous intelligent gadgets are susceptible to exploitation by users as a result of manufacturers. The appliance offers numerous capabilities and information, but it does not explicitly disclose the location of the captured information, whether it is stored in the cloud or locally [9, 7, 8]. This type of incident leads to an attack due to a vulnerability, which is why it necessitates the use of digital forensics for investigation. However, standard digital forensics is insufficient for analyzing IoT systems and uncovering evidence. IoT forensics is becoming increasingly imperative at its own rate of progression. Utilizing IoT forensics presents numerous challenges for inquiry, although it also offers novel opportunities to examine incidents. The Internet of Things (IoT) utilizes wearable gadgets and other interconnected objects that can provide as evidence for investigators.

This paper aims to discuss IoT forensics from three perspectives. Firstly, we examine a case study that focuses on an IoT application targeted for attack. Secondly, we explore the methods of gathering authentication from the IoT framework. Lastly, discovered the challenges involved in conducting IoT forensic investigations and propose future directions for IoT forensics.

**2. Literature Review**

The definitions of digital forensics are going to be discussed in this part. The writers, specialists, and organizations that have contributed to these definitions come from a far wider variety of backgrounds. A discussion of these definitions is going to take place in this portion of the article. The subsequent stage will involve identifying the several varieties of digital forensics as well as the process model that corresponds to each of these specific types of digital forensics. This will be done in order to move forward with the process. Following that, we will proceed to provide a case study on the idea of the smart house, which will be a continuation of the explanation that came before it for the purpose of providing further insight.

"Digital forensics" (DF) is an abbreviation for the term "digital forensics," which refers to the methodical process that is involved in the identification, gathering, extraction, inspection, and documenting of digital evidence. The word "digital forensics" (DF) is an abbreviation for the phrase "digital forensics." In the course of this procedure, the primary purpose is to identify any digital footprints that might be connected to illegal activities. It is via the utilization of this strategy that this objective will be achieved. Considering the circumstances surrounding this particular case, the subject of digital evidence is one that is of the utmost importance. Digital evidence can be traced back to digital sources, which include, but are not limited to, mobile phones, computers, digital audio and video, and a wide variety of other digital devices. Digital evidence can be used to establish certain facts. It is possible to trace the provenance of digital evidence all the way back to digital sources that led to digital documentation. The number that should be used is [3-4]. We have prepared a list of definitions that have been offered by a wide variety of authors, organizations, and government bodies for your convenience. These definitions have been provided by a variety of sources. These definitions are contained in this collection, which includes the following:

To facilitate and advance the reconstruction of criminal events or the detection of unauthorized actions that can disrupt planned operations, the utilization of methodologies that have been scientifically validated and secure digital evidence by preserving, collection, validating, identifying, analyzing, interpreting, documenting, and presenting it with expertise and care. This is done to accomplish the goals. This action is taken to achieve the objectives that were indicated earlier. In no way is it [5].

The process of recognizing an occurrence using scientific procedures in a practical situation is referred to as a scientific investigation. Additionally, the process of gathering, examining, and interpreting data with the intention of providing evidence is also contained within a scientific investigation [6]. Or, to put it another way, by definition, scientific research is an investigation that is comprehensive.

[7] Digital forensics focuses on the recognition, accessing, manipulation, preception, and documentation of information that has been electronically saved. The primary goals of digital forensics are to accomplish these things. In the realm of forensic science, digital forensics encompasses a subfield. There is a subfield that falls under the umbrella of forensic science that is known as digital forensics.

Among the subfields that fall under the umbrella of forensics, digital forensics is one that focuses on the safeguarding, investigation, and interpretation of digital evidence. The implementation of methods such as preservation, inspection, and analysis are utilized in order to attain this goal. Specifically, the phrase "digital forensics" refers to this subfield of forensics that is being discussed here.

Digital forensics is a subfield of forensic science that focuses largely on the retrieval and evaluation of digital resources that are present in electronic devices and are relevant to the investigation of cybercrime [8]. This subfield of forensic science is a subfield of forensic science. Another name for digital forensics is digital forensic research. Both terms are used interchangeably. There is a subfield that falls under the umbrella of forensic science that is known as digital forensics.

The process of obtaining, preserving, assessing, and storing electronic data that may be exploited in an investigation is referred to as "deep learning" in the field of digital forensics. This technique is also known as "deep learning." Another name for this technique is "digital reconstruction," which is similar to the one described above. There is a possibility that this evidence does not pertain to the investigation, despite the fact that it is being taking into consideration. Information obtained from a wide variety of digital devices is included in this category. These digital devices include, but are not limited to, computer hard drives, smartphones, smart home appliances, automotive GPS systems, digital locks, and significantly more [9]. The information that is included in this category is that which is collected via a wide variety of digital media devices.

## 3. Materials and Methods

The practice of combining digital evidence with materialistic evidence is what is known as Internet of Things (IoT) forensics. This is because the Internet of Things (IoT) is a cyber-physical system. This is the reason why this holds true. On the other hand, in contrast to the forensic investigation system for the Internet of Things (IoT), which holds a device accountable for its actions, the digital forensic investigation model does not place any emphasis on the physical evidence of the digital systems. The IoT system uses an encoded device that dictates proper functioning of the devices. Internet of things is actually a network of many such supplementary networks, sensors and devices that communicate with each other. However, the Internet is just a small part of the whole Internet of Things. Investigation into the Internet of things device application forensics starts with data collection of both digital and physical data. In order to achieve this purpose, digital as well as physical evidence should undergo an analysis. There are 3 IoT investigative models employed in the process of conducting forensic investigations [10]. These are the Digital forensic investigation model (DFIM), the Hybrid model, and the 1-2-3 zones of digital forensics. The huge and intricate IoT areas require you to choose a model that is the most suitable to the research situation. Choose the model that suits the research the most. Moreover, for the objective to be achieved, the admissibility of the evidence and its credibility should be established too because it enables us to spend less money and time on the pursuit and the process is accepted completely. Keeping this in mind at all times is something that should be done consistently. In general, it is carried out with a concentrate on the technical and legal components of the problem that is being dealt with. For a decision to be made, it is essential for it to satisfy both the facts that are relevant to the situation and its own competence. Only then can a decision be made. As a piece of information that is dependable and correct, this is something that is required in order for the court or any other authority to be able to use it by themselves. The design of systems that are connected to the Internet of Things has led us to identify four distinct types of digital forensics layers. These layers are based on the connections between the systems.

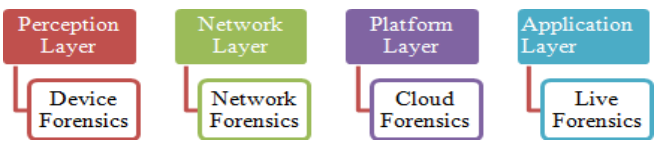


**Figure 1.** IoT forensics phase

Figure 1 depicts the layered approach to Internet of Things (IoT) forensics, which can be seen here. This approach may be viewed here. Device forensics is utilized in the perception layer, network forensics is utilized in the network layer, cloud forensics is utilized in the platform layer, and live forensics is utilized in the application layer of the Internet of Things application. All of these forensics techniques are utilized in the Internet of Things application. Figure 2 illustrates the forensic prototype of a smart home that has

been affected by the architecture of Internet of Things (IoT) applications. This prototype was developed by our team.

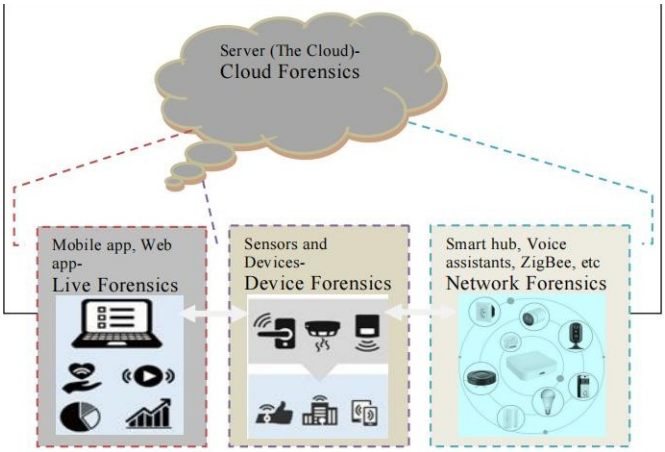


**Figure 2.** IoT Forensics prototype of smart home

3.1 Challenges For IoT Forensics

The forensic examination of the gives rise to certain issues, the character of IoT devices and networks being very peculiar [5, 10-16]:

1) In addition to offering a wide range of capabilities, Internet of Things devices can take the form of anything from wearable devices to small objects. These devices can also use a variety of operating systems, protocols, and data formats. Considering this, the creation of generalized forensic techniques that are capable of being deployed on all Internet of Things devices is called into question.
2) The volume of data: It may be challenging to analyze the data produced by these Internet of Things devices because of their huge potential to generate data. Furthermore, the data that is being produced by Internet of Things equipment is frequently unstructured, which may necessitate the utilization of specific analytical techniques and approaches to comprehend it.
3) Distributed nature: The devices in the Internet of Things are typically connected to several networks, like mobile, cloud, and local networks. Since data is distributed around the system in fragments, this suggests that the data flow becomes non-linear.
4) Privacy and security concerns: "The Internet of Things (IoT) devices communicate with one another and retain sensitive information, such as health statistics or financial data. Privacy is of the utmost importance during forensic investigations, and it will be protected at all costs in order to prevent unauthorized access or publication of information as much as possible.
5) Lack of standardization: It is difficult to build uniform forensic methods that can be applied to all Internet of Things devices because there is a lack of operational consistency in the Internet of Things devices.
6) Limited resources: Due to the fact that dozens of Internet of Things devices have a limited computer power, it may be impossible for them to accomplish forensic accounting. Moreover, the devices may have storage limitation which would make it impossible for law enforcement personnel to be able to save material for examination".
7) As a result of the fact that Internet of Things devices generate data in real time, it might be difficult to swiftly discover, evaluate, and respond to security breaches.
8) As the IoT law and regulation is still in emerging stage, investigators have to necessarily study the recent law and regulations related to IoT devices forensics.

   Consequently, IoT gadget investigation implementation involves using skills and tools that have specialized techniques to circumvent these obstacles and obtain more important information from the IoT datasets. With the rapid development of IoT technology it would be no surprise that new challenges and opportunities would arise to an even greater extent for the field of IoT forensics. This is likely to require more frequent innovation and adaptation to these new developments.

3.2 Future Aspects For IoT Forensics

Future considerations of IoT forensic investigations [17-22]:

1) When it comes to conducting forensic investigations involving the Internet of Things (IoT), the development of standardized tools and methods has the potential to improve both efficiency and results. On the other hand, the development of similar technologies and techniques can be of assistance in resolving issues pertaining to standardization, data collection, analysis, and other related issues.
2) In order to enable automation in the data analysis process while simultaneously improving the accuracy and speed of the analysis, it is possible to apply a mix of artificial intelligence and machine learning. These technologies have the potential to assist in the identification of trends and outliers in data, even those that are beyond the human capacity to notice.
3) Improved time synchronization techniques are a major enabler for the data collected from numerous devices to be synchronized to the same time reference. This is why these approaches are so important. Because of this, the specialists are able to provide a more accurate timeline of the events that included their research.
4) The construction of application-specific profiling designs will serve to tackle the problems that are caused by the unstable environment and resource limits that are typical of devices that are connected to the Internet of Things. The use of these models allows for the identification of data that has been highlighted, as well as the reduction of the amount of needless data that is gathered during the investigation process.
5) It is of the utmost significance to ensure that the data acquired by the Internet of Things (IoT) for both individuals and businesses are protected. Looking into ways to secure the privacy and security of data in order to prevent data from being tampered with is the next step that Internet of Things forensic investigations will take in the future.
6) There is the possibility of implementing forensic readiness, which entails the design of Internet of Things devices to aid future forensic investigations. This includes the capability to collect data and store it in a secure location for subsequent analysis.
7) There is a pressing need for the development of sophisticated forensic tools that are able to manage the vast amounts of complicated data that are produced by Internet of Things devices. These tools ought to make it possible to conduct forensic analysis and respond in real time.
8) When it comes to Internet of Things (IoT) forensic investigations, the future directions should primarily concentrate on addressing the issues that are brought by IoT devices while simultaneously improving the efficiency and accuracy of investigations.

**4. Conclusion**

The research underlines the evolution of the pivotal role of cyber forensic analysis in the context of increasing spread of IoT devices and their capabilities to influence the confidentiality and the enterprise data. The piece underlines the very challenges associated with this type of work: getting and processing data, protecting individual privacy and guaranteeing security, agreeing to a common set of regulations, synchronizing clocks, and adapting to new conditions in space and the other three.

The outlined application-specific model for investigations here provides a structured approach to address the problems and hence improves the precision and effectiveness of the IoT forensic investigations. The article details what points should be improved in order further improve the efficacy of these methods. In essence, the article stresses the importance of using efficient tools when doing IoT Forensics. Moreover, it presents some of the possible solutions for the mentioned issues and gives the directions for the future of investigations of the IoT incidents.

**References**


1. S. Zawoad and R. Hasan, "FAIoT: Towards Building a Forensics Aware Eco System for the Internet of Things," Proc. 2015 IEEE International Conference on Services Computing, SCC 2015, pp. 279-284, Jul. 2015. https://doi.org/10.1109/SCC.2015.46
2. S. Alabdulsalam, K. Schaefer, T. Kechadi, and N.-A. Le-Khac, "Internet of things forensics–challenges and a case study," presented at the Advances in Digital Forensics XIV: 14th IFIP WG 11.9 International Conference, New Delhi, India, January 3-5, 2018, Revised Selected Papers 14, Springer, 2018, pp. 35–48.
3. S. Ballou, Electronic crime scene investigation: A guide for first responders. Diane Publishing, 2010.https://www.ojp.gov/pdffiles1/nij/219941.pdf
4. Baryamureeba and F. Tushabe, "The enhanced digital investigation process model," Digital Investigation, 2004.https://dfrws.org/wpcontent/uploads/2019/06/2004_USA_paperthe
5. _enhanced_digital_investigation_process_model.pdf
6. Hany F. Atlam , Ezz El-Din Hemdan , Ahmed Alenezi , Madini O. Alassafi , Gary B. Wills , Internet of Things Forensics: A Review,
7. Internet of Things (2020),doi: https://doi.org/10.1016/j.iot.2020.100220
8. Digital evidence. [Online]. Available: https://www.nist.gov/digital- evidence
9. Digital forensics. [Online]. Available: https://www.interpol.int/en/How- we work/Innovation/Digital-forensics
10. What is digital forensic. [Online]. Available: https://www.eccouncil.org/what-is-digital-forensics/
11. Margaret Rouse. (2022, Aug. 24). Digital forensics. [Online].Available: https://www.techopedia.com/definition/27805/digital-forensics
12. S. Perumal, N. M. Norwawi, and V. Raman, "Internet of Things (IoT) digital forensic investigation model: Top-down forensic approach methodology," presented at the 2015 Fifth International Conference on Digital Information Processing and Communications (ICDIPC), IEEE, 2015, pp. 19–23.
13. . Zhang, X. Liu, Z. Huang, X. Tao and W. Dou, "IoT Forensics: Recent Advances, Challenges, and Future Research Directions," in Journal of Network and Computer Applications, vol. 146, pp. 102-114, Jan. 2020, doi: 10.1016/j.jnca.2019.09.016.
14. N. H. N. Zulkipli, A. Alenezi, and G. B. Wills, "IoT Forensic: Bridging the Challenges in Digital Forensic and the Internet of Things.," presented at the IoTBDS, 2017, pp. 315–324.
15. A. Alazab, A. Khraisat, and S. Singh, "A Review on the Internet of Things (IoT) Forensics: Challenges, Techniques, and Evaluation of Digital Forensic Tools," 2023.
16. M. A. Hassan, G. Samara, and M. A. Fadda, "IoT Forensic Frameworks (DFIF, IoTDOTS, FSAIoT): A Comprehensive Study," arXiv preprint arXiv: 2203.15705, 2022.
17. W. Yang, M. N. Johnstone, L. F. Sikos, and S. Wang, "Security and forensics in the internet of things: Research advances and challenges," presented at the 2020 Workshop on Emerging Technologies for Security in IoT (ETSecIoT), IEEE, 2020, pp. 12–17.
18. T. Janarthanan, M. Bagheri, and S. Zargari, "IoT forensics: an overview of the current issues and challenges," Digital Forensic Investigation of Internet of Things (IoT) Devices, pp. 223–254, 2021.
19. S. Sathwara, N. Dutta, and E. Pricop, "IoT Forensic A digital investigation framework for IoT systems," presented at the 2018 10th international conference on electronics, computers and artificial intelligence (ECAI), IEEE, 2018, pp. 1–4.
20. O. Yakubu, O. Adjei, and B. C. Narendra, "A review of prospects and challenges of Internet of Things," International Journal of Computer Applications, vol. 139, no. 10, pp. 33–39, 2016.
21. J. Hou, Y. Li, J. Yu, and W. Shi, "A survey on digital forensics in Internet of Things," IEEE Internet of Things Journal, vol. 7, no. 1, pp. 1–15, 2019.
22. U. Karabiyik and K. Akkaya, "Digital forensics for IoT and WSNS," Mission-Oriented Sensor Networks and Systems: Art and Science: Volume 2: Advances, pp. 171–207, 2019.
23. M. Stoyanova, Y. Nikoloudakis, S. Panagiotakis, E. Pallis, and E. K. Markakis, "A survey on the internet of things (IoT) forensics: challenges, approaches, and open issues," IEEE Communications Surveys & Tutorials, vol. 22, no. 2, pp. 1191–1221, 2020.
24. R. Patel and Z. Malek, "Brief overview of existing challenges in IoT," International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), vol. 9, no. 3, 2020.