ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)
Vol. 9, Issue 7, July 2023

A Review Article on The Internet of Things and Digital Forensics: An Overview of Challenges and Opportunities

Nimisha Doshi[1], Aarti Sardhara[2], Dr. Neeta Doshi[3]

Student, Department of Computer Engineering, Vishwakarma University, Pune, India [1]
Assistant Professor, Department of Computer Engineering, Vishwakarma University, Pune, India [2]
Associate Professor, EnTc Department, SVPM COE, Pune, India [3]

***Abstract*—The Digital Forensics involves collecting, analyzing and presenting computer-based evidence in court. The Internet of Things (IoT) is a network of electronic devices that are linked to the internet. As IoT devices multiply and integrate into our lives, the need for them to be covered by digital forensics is increasing. However, collecting and analyzing data from IoT devices present unique challenges such as limited storage, processing capabilities, the use of multiple communication channels and proprietary data formats. Digital forensic investigators need specialized knowledge and skills to manage IoT devices and the data they produce. This article reviews recent literature on IoT forensics, outlines the digital investigation process, lists IoT-related computer crimes and discusses open problems faced in IoT Forensics.**

***Index Terms*—Digital Investigation Process, Digital Forensics, Internet of Things (IoT), IoT Forensics**

I. INTRODUCTION

Digital Forensics comprises collecting, preserving, analyzing, and presenting computer-based proof in a court of law. Digital devices and systems are required to be investigated using scientific methods and techniques to ascertain the source, nature, and scope of any alleged illegal or unauthorized activity as well as to retrieve crucial data.

The term "Internet of Things" (IoT) describes a network of electronic devices, sensors, and appliances that are linked to the internet and can exchange data. IoT is significant because it makes it easier to automate processes, increase productivity, and better user experiences. As more and more devices connect to the internet, IoT is becoming more and more significant, opening up new possibilities for both individuals and businesses to improve their everyday lives and business operations. IoT can be used fraudulently by hackers, just like any other technology, for nefarious ends. Data breaches, identity theft, and other types of cybercrime may result from cyberattacks on a huge number of connected devices and the enormous quantity of data they produce. Additionally, if IoT devices are compromised, they could seriously disrupt essential infrastructure like power grids and transportation systems.

As IoT devices multiply and become more integrated into facets of our lives, there is a rising need for IoT to be covered by digital forensics. These devices produce enormous amounts of data, which may be useful in investigations, court cases, and intelligence collecting. In digital forensics, having a thorough grasp of the tools and technologies used in a case is essential. IoT devices present particular difficulties for data collection, preservation, and research as they proliferate. For instance, IoT devices frequently have constrained storage and processing capability, which can make it challenging to collect and analyze the data they produce. Additionally, IoT devices frequently use multiple communication channels and protocols, which can make gathering and analyzing data more challenging. Additionally, they might use proprietary or unusual data formats that call for specialized tools and methods to analyze them. To manage IoT devices and the data they produce, digital forensic investigators must possess specialized knowledge and abilities. This entails comprehending the hardware and software elements of IoT devices, the communication methods they employ, and the techniques used for data storage and processing.

The following are the values supplied by the paper:

1) Selecting and investigating the recent literature on IoT forensics and clarifying the development of IoT forensics research;
2) Highlighting the distinctions within standard and IoT digital forensic procedures;
3) Enumerating IoT-related criminal activity involving computers;
4) Mentioning open IoT forensics issues.

The remainder of this publication is divided as follows: A literature survey is provided in Section II. A brief description of the IoT and digital investigation method is provided in Section III. The different attack types against IoT technologies are discussed in Section IV. Some open problems are covered in Section V. Paper is concluded in Section VI.

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)
Vol. 9, Issue 7, July 2023

II. LITERATURE REVIEW

This section provides a thorough literature review of IoT forensics research in order to obtain a thorough understanding of digital forensics in an IoT environment. In order to accomplish it first journals were selected [1-65] namely, Elsevier, IEE, Springer, AMC and Weiley. In these high impact journals, different combinations of the following keywords “Forensic", "Investigation", "Evidence", "Things", "Internet of Things", and "IoT were searched. From the list of papers available, journal publications and conference papers published in English were included keeping a check on their title, publication year, and language. Complete texts and abstracts of the chosen papers were examined to confirm their applicability. For further analysis, the cited data, abstracts, and keywords of the articles were noted. As shown in the Figure 1, the following process led to the extraction of 58 papers written between 2010 and 2018.

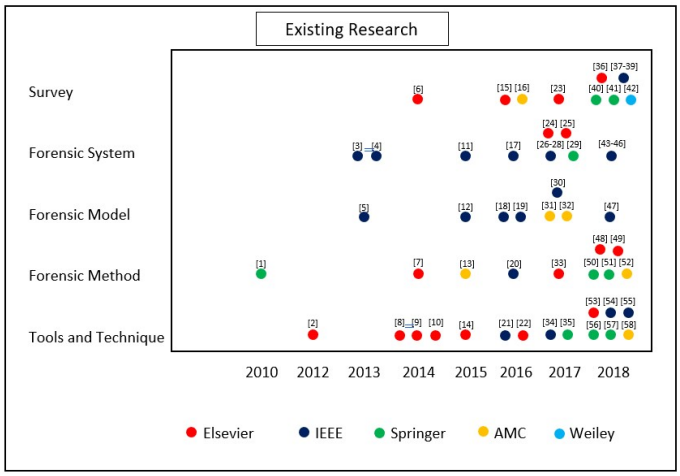

Fig 1. Distribution of research papers [1-65]

According to the classification of research papers by their publishing year from 2010 to 2018, the overall number of papers increased substantially in 2018, whereas it increased gradually in the other years. This suggests that, as a result of the widespread use of IoT devices in industry and everyday life since 2016, the study on IoT forensics is moving into a new era of rapid growth. Five categories—survey papers, models/frameworks, forensic methods, forensic systems, and forensic techniques/tools—are used to group the 58 papers that were retrieved.

Forensic methods to analyse IoT were the subject of continuing study between 2010 to 2018 with the goal of providing recommendations for inquiries into various sources of evidence. The key objective of this research was to investigate workable forensic methodologies and approaches that could handle the novel issues presented by digital forensics in the IoT context. The major objectives of this research endeavour were to create forensic systems and investigate IoT forensic frameworks/models to provide guidelines for regular forensic operations.

Early IoT forensics research was primarily conceptual, concentrating on topics like frameworks and models. By way of example, Oriwoh et al. (2013) investigated theoretical digital forensic models for the Internet of Things forensics to direct forensic investigations comprising the IoT, that served as the foundation for additional forensic theories and structures study. In order to prepare IoT environments for forensic analysis before prospective cases emerged, they also looked into automating forensic solutions. A few survey studies, including those by [37] Chernyshev et al., 2018, who primarily concentrated on theoretical digital forensic frameworks that could be implemented in IoT contexts, addressed the difficulties of IoT forensics. In order to deliver accurate information, Bréda et al. examined the least functional forensic needs of IoT devices. IoT forensics gathering and analysing information raise a number of legal issues, which Losavio et al. in-depth analysed. [4] presented an innovative visual aid framework for completely blind people, which takes the form of a pair of glasses. The following are some of the most essential characteristics of the proposed device. The complicated algorithm processing is carried out on the Raspberry Pi 3 Model B+, which has low-end computing power. Using a combination of camera and ultrasound sensors and GPSbased location tracking for use in a navigation system, this Internet of things-based device offers advanced dual detection and distance measurement capabilities. This device makes it possible to have better access, solace, and navigational ease to blind people [6] discussed that Smart wearables are redefining the way people move and behave in real-time. Workers will be alerted to the presence of toxic gases as well as be tracked in the event of an accident if this system is implemented. Additionally, the instrument has sensors for methane and carbon monoxide gases included in its design. The prototype can detect gas in the air, the rate of the miner's breathing, the change in temperature and humidity, and the miner's location at all times. Wi-Fi will be used to transmit all of these parameters to a dynamic internet protocol. Every one of them will be able to make it through the shield. This way, all mineworkers can be monitored, and if something goes wrong, the miner can be rescued as quickly as possible. Using a pulse sensor on the miner's body, the base camp can track the miner's GPS location. It may be necessary to dig a coal mine as soon as possible to save the most people in a disaster. With the help of IoT, we can build a database and, if necessary, communicate with a nearby hospital. Our final consideration will look at market trends and challenges for WHDs to keep in mind

There have also been surveys looking into IoT forensics in various applications for the Internet of Things, including smart TVs, fitness trackers, cars, and smart cities as well. In this regard, some academics examined the forensic issues raised by smart TVs, whereas some concentrated on equipment for health and fitness. In addition, some academics looked at forensic difficulties in cars, while others looked into forensic difficulties in smart cities. The goal of

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)
Vol. 9, Issue 7, July 2023

IoT forensics research from 2010 to 2018 was to build forensic systems that could handle the additional problems of digital forensics in the IoT context as well as to investigate workable forensic procedures and techniques.

III. IOT AND DIGITAL FORENSICS

Identification, acquisition, data recovery, forensic analysis, and reporting are the phases of digital forensics. The step of identification involves finding the digital devices that could have important evidence on them. This involves determining the kind of device, where it is, and any possible sources of proof. The second stage of acquisition involves how a forensic image of the gadgets or data storage media is obtained. In this procedure, the device or media are precisely duplicated without any alteration or loss of the original data. Data Recovery involves retrieving deleted, hidden, or encrypted data with the help of specialized tools and methods. This phase entails locating and gathering any pertinent information that might be used as proof. The forensic analyst examines the data during the analysis phase to determine its authenticity and significance. Examining the data is necessary to find any trends, associations, or irregularities that might point to criminal behavior or other important information. The forensic analyst then produces an in-depth report that outlines the analysis' results during the reporting stage. All pertinent information that might be relevant in legal procedures should be included in the report, which should be precise, unambiguous, and straightforward. To ensure that the evidence is eligible to be in a court of law, it is essential that one bears in mind that all of these steps must be performed without compromising the purity of the evidence.

A. Difference in standard Digital Forensics and IoT Digital Forensics

There may need to be some adjustments made to the standard digital forensics procedure for digital inquiries involving IoT devices. This is due to the fact that IoT devices frequently have distinctive properties and may be linked in intricate ways that call for specialized skills and equipment. The sheer quantity of devices employed is one of the key distinctions between digital forensics and IoT digital investigations. IoT equipment can be found in a range of locations, including homes, workplaces, public areas, and industrial settings. In order to locate, gather, and evaluate data from an extensive number of devices, analysts might require to use specialized equipment and techniques. The type of data that is gathered is another significant distinction. A broad range of data types, including sensor data, network traffic, and user activity logs, may be collected by IoT devices. It's possible that this data is unstructured or semi-structured, which can make it more challenging to interpret and evaluate.

B. Stages in IoT Forensics

The stages of identification, acquisition, data recovery, and forensic analysis used in digital forensics are comparable to those in conventional digital investigations as in Figure 2. There are, however, some extra factors that are unique to IoT devices:

Identification: A broad range of devices, such as sensors, gateways, and controllers, may need to be identified during IoT investigations. To recognize these devices and ascertain their role within the network, investigators may require the use of specialized tools.

Acquisition: Because IoT devices may be constantly transmitting data over networks, it may be necessary for investigators to use specialized tools to capture network traffic in real-time. Additionally, they might need to buy firmware and other software parts tailored to the gadget.

Data Recovery: In IoT inquiries, data recovery may entail gathering information from numerous hardware and software components, such as sensors, gateways, and cloud-based services. In order to extract and analyze information from these sources, investigators might need to use specialized tools.

In IoT inquiries, forensic analysis may entail comparing information from various sources to reconstruct events and pinpoint the origin of an incident. To spot patterns and anomalies in data from sensors, network traffic, and other sources, investigators may need to use specialized tools.

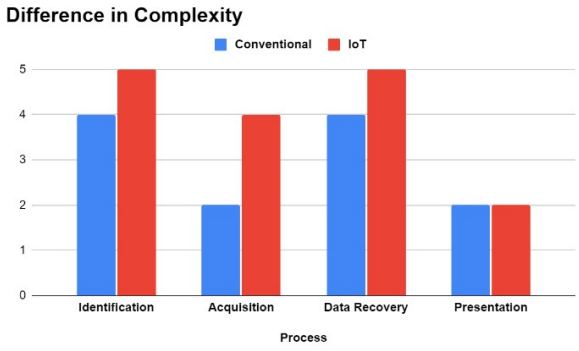

Figure 2. Comparison between conventional and IoT investigation complexities

IV. ATTACKS ON IOT AND DIGITAL FORENSICS

IoT devices are being used in a variety of areas with their applications growing in popularity. However, they are also susceptible to various types of crimes, such as side-channel attacks, malware, DoS attacks, and MitM attacks. By examining digital evidence to ascertain the source and extent of the attack, digital forensics methods can help in both

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

identifying and mitigating such attacks. By using this data, security steps can be strengthened, future incidents can be avoided, and attackers can be made accountable. However, because of the enormous volume of data generated, the complexity of the system, and the requirement for real-time monitoring and response, digital forensics in IoT environments poses particular difficulties.

The perception layer, network layer, and application layer are the three main layers in IoT device's function. To make it possible for IoT devices to work properly, each layer must carry out specific tasks. These levels are nevertheless susceptible to various cyberattacks that may jeopardize the availability, integrity, and confidentiality of IoT systems and data.

Attacks on the layer of perception may entail modifying or replacing sensors to produce incorrect measurements or data. By examining the sensor data to find discrepancies or inconsistencies, digital forensics can help identify these kinds of crimes. Network layer attacks may involve intercepting or changing data transfers, leading to unauthorized access or data loss. Such attacks can be detected and mitigated using digital forensics methods like packet analysis and network traffic tracking.

Attacks on the application layer could involve using advantage of flaws in the firmware or software used for data processing and analysis. By examining application logs and system data to ascertain the origin and extent of the attack, digital forensics can help detect and mitigate such attacks.

A. Physical Attacks

Any type of attack on IoT technology that includes direct physical contact with an IoT device or network infrastructure, such as stealing or tampering with IoT devices, is referred to as a physical attack. Any form of attack, such as node tampering, that takes advantage of weaknesses in IoT systems to breach the security and privacy of IoT networks and their users is considered an IoT crime.

Table 1. Physical Attacks

Sr. No	Attack Name	Description	Mitigation	Ref
1.	Node Tampering	An attacker who gains physical access to an IoT node may use that access to perform unauthorized actions, key retrieval, and key destruction.	This type of attack can be stopped by authentication and cryptography. It can also be reduced by using tamper-resistant designs, inspecting IoT devices frequently, and using security features that can spot tampering efforts.	[59]
2.	Sleep deprivation attack	The intruder's objective is to deplete the power supply, which will ultimately lead to the IoT node to close down. The attack entails keeping the node in an active state longer than necessary, which eventually leads to its shutdown. IoT sensors have a limited power supply because they depend on batteries.	Such attacks can be recognized and predicted with the help of intrusion monitoring systems and methods like deep learning.	[60]
3.	Malicious code injection	When a hacker introduces harmful code into an Internet of Things network, there is a chance that the node will shut down or, in the worst situation, that the attacker will gain full control of the node.	The attacker can access all of the node's security data, including its replication and injection if they work together with the injected attack.	[61]

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)
Vol. 9, Issue 7, July 2023

4.	Physical theft	The intruder sneaks into the actual hardware or important items. Many different sectors and locations will have internet of things (IoT) equipment put in place, allowing access to them easy. This is particularly true given that sensors will be dispersed throughout accessible and public spaces, such as agricultural fields, roads, and transportation systems.	Implementing physical security measures, such as locks, cameras, or GPS monitoring, can lessen the impact of this kind of attack.	

B. Software Attacks

Any form of attack that takes advantage of software weaknesses in IoT systems is referred to as a software attack that targets IoT technology. Such attacks have the potential to threaten the security and privacy of IoT networks and their users, which could lead to data theft or identity theft.

Table 2. Software Attacks

Sr. No	Attack Name	Description	Mitigation	Ref
1.	Phishing attacks	The attacker can obtain information like login and password through email spoofing. The information obtained can be used by the attacker to gain unauthorized access to a the target's account, which may have gained access to an IoT device control system, in the context of IoT, where passwords serve as a gateway to sensitive data.	One of the best strategies for preventing phishing attacks is awareness.	
2.	Malicious script	The attacker introduces a harmful program into the server, which allows the attacker entry into the system.	The Randomized Watermarking Filtering Scheme (RWFS) has a sensor that detects and removes deceitful data. This approach generates a watermark that records all data and is useful for forensics.	[62]
3.	Malware	The intruder can harm the system through the usage of malicious code, such as viruses, worms, and Trojan horses. These snippets of code spread themselves via email and download from the internet. The worms can reproduce without assistance from individuals.	Performing a signature-based detection and keeping a record of all malware are forensic methods to stop this malware attack. Furthermore, malware attack detection may be aided by machine learning and the development of zero-day skills.	[60]

C. Network Attacks

Attacks that can arise from the networks that link different IoT components together are called network attacks. IoT system protocols may have security flaws that have an

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)
Vol. 9, Issue 7, July 2023

impact on the complete system. IoT devices are also vulnerable to well-known network attacks like spoofing and denial of service (DoS).

Table 3. Network Attacks

Sr. No	Attack Name	Description	Mitigation	Ref
1.	Denial of Service	The attacker floods the network with large amounts of data, consuming the system and rendering it inaccessible to legitimate users.	JPCAP, a forensic technique, can be employed to capture traffic and differentiate between cyberattacks and genuine live traffic. CEPID (Complex Event Processing Intrusion Detection), another forensic tool, also proposed a layered framework for conducting traffic monitoring, network analysis, and event handling to limit unusual behaviour.	[60]
2.	Man-in-the-middle attack	A hacker obscenely eavesdrops on or manipulates two parties' private conversations. The attacker might even deceive the target in order to learn more.	The attempt can be stopped by employing an electronic signature-driven authentication technique and continuously keeping an eye on the IoT nodes.	[60]
3.	Sybil attacks	An infected node that can assume the names of numerous IoT nodes is known as a Sybil attack. Duplication and misleading data are the consequences of this.	By incorporating an RSS-based identification technique, the attack can be forensically examined, and its efficacy can be evaluated using network distinct configurations.	[63] [64]

V. OPEN ISSUES

IoT technology generally faces a number of difficulties, including key management, an essential job for IoT security. The absence of perfect forensic tools, however, continues to be the biggest problem facing the subject and community of digital forensics. Although technology has greatly advanced, the community of digital forensic professionals has not effectively used the tools to their benefit. It is unavoidable to choose cloud storage given the novel paradigm of rising space utilization. Storage issues may be less of a problem if the forensic case has a dedicated cloud space. The previously mentioned problem has a close connection to a second issue: the forensic tools must be user-friendly and adaptable to the degree of expertise of the forensic staff. An important discovery [65] is a tool that can handle a huge amount of IoT intelligence, determine keywords, and analyze the resulting proof. Data analysis is a vital and time-consuming process.

VI. CONCLUSION

The paper provides a brief overview of digital forensics and investigations in IoT systems and technologies. Device security and attack-related investigations are crucial given the growing interconnection of devices. We've compiled a list of recent works in the area of IoT forensics. Regarding the typical procedure and key differences, we have outlined the primary distinctions between conventional and Internet of Things (IoT) investigations. Except for the presentation stage, our findings indicate that the complexity of IoT investigations will increase in different ways. Additionally, we provided a summary of the majority of typical computer attacks against the Internet of Things and some investigative techniques to help with some of their challenges. We have taken into account the fact that IoT digital forensics is an emerging in technology for investigators.

REFERENCES

[1] S. Al-Kuwari and S. D. Wolthusen, "On the feasibility of carrying out live real-time forensics for modern intelligent vehicles," in Forensics in Telecommunications, Information, and Multimedia - Third

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)
Vol. 9, Issue 7, July 2023

International ICST Conference, e-Forensics 2010, Shanghai, China, November 11-12, 2010, Revised Selected Papers, 2010, pp. 207–223.

[2] B. Inglot, L. Liu, and N. Antonopoulos, "A framework for enhanced timeline analysis in digital forensics," in 2012 IEEE International Conference on Green Computing and Communications, Conference on Internet of Things, and Conference on Cyber, Physical and Social Computing, GreenCom/iThings/CPSCom 2012, Besancon, France, November 20-23, 2012, 2012, pp. 253–256.

[3] I. Homem, S. Dosis, and O. Popov, "LEIA: the live evidence information aggregator: Towards efficient cyber-law enforcement," in 2013 World Congress on Internet Security, WorldCIS 2013, London, United Kingdom, December 9-12, 2013, 2013, pp. 156–161.

[4] Christo Ananth, M. Kameswari, R. Srinivasan, S. Surya, and T. Ananth Kumar, "A Novel Low-cost Visual Aid System for the Completely Blind People", Machine Learning in Information and Communication Technology, Lecture Notes in Networks and Systems 498, ISBN: 978-981-19-5090-2, pp. 177-183..

[5] E. Oriwoh, D. Jazani, G. Epiphaniou, and P. Sant, "Internet of things forensics: Challenges and approaches," in 9th IEEE International Conference on Collaborative Computing: Networking, Applications and Worksharing, Austin, TX, USA, October 20-23, 2013, 2013, pp. 608–615.

[6] Christo Ananth, B.Sri Revathi, I. Poonguzhali, A. Anitha, and T. Ananth Kumar, "Wearable Smart Jacket for Coal Miners Using IoT", 2022 2nd International Conference on Technological Advancements in Computational Sciences (ICTACS), 2022, pp. 669-672, doi: 10.1109/ICTACS56270.2022.9987834.

[7] R. M. van der Knijff, "Control systems/scada forensics, what's the difference?" Digital Investigation, vol. 11, no. 3, pp. 160–174, 2014.

[8] L. Tobin, A. F. Shosha, and P. Gladyshev, "Reverse engineering a CCTV system, a case study," Digital Investigation, vol. 11, no. 3, pp. 179–186, 2014.

[9] J. Park and S. Lee, "Data fragment forensics for embedded DVR systems," Digital Investigation, vol. 11, no. 3, pp. 187–200, 2014.

[10] V. Kumar, G. C. Oikonomou, T. Tryfonas, D. Page, and I. W. Phillips, "Digital investigations for ipv6-based wireless sensor networks," Digital Investigation, vol. 11, no. S-2, pp. S66–S75, 2014.

[11] S. Zawoad and R. Hasan, "Faiot: Towards building a forensics aware eco system for the internet of things," in 2015 IEEE International Conference on Services Computing, SCC 2015, New York City, NY, USA, June 27 - July 2, 2015, 2015, pp. 279–284.

[12] S. Perumal, N. M. Norwawi, and V. Raman, "Internet of things(iot) digital forensic investigation model: Top-down forensic approach methodology," in 2015 Fifth International Conference on Digital Information Processing and Communications (ICDIPC), 2015, pp. 19–23.

[13] E. Sohl, C. Fielding, T. Hanlon, J. L. Rrushi, H. Farhangi, C. Howey, K. Carmichael, and J. Dabell, "A field study of digital forensics of intrusions in the electrical power grid," in Proceedings of the First ACM Workshop on Cyber-Physical Systems-Security and/or PrivaCy, CPS-SPC 2015, Denver, Colorado, USA, October 16, 2015, 2015, pp. 113–122.

[14] A. Boztas, A. R. J. Riethoven, and M. Roeloffs, "Smart TV forensics: Digital traces on televisions," Digital Investigation, vol. 12, no. Supplement-1, pp. S72–S80, 2015.

[15] S. Watson and A. Dehghantanha, "Digital forensics: the missing piece of the internet of things promise," Computer Fraud & Security, vol. 2016, no. 6, pp. 5–8, 2016.

[16] D. Vandervort, "Medical device data goes to court," in Proceedings of the 6th International Conference on Digital Health Conference, DH 2016, Montréal, QC, Canada, April 11-13, 2016, 2016, pp. 23–27.

[17] V. Kumar, G. C. Oikonomou, and T. Tryfonas, "Traffic forensics for ipv6-based wireless sensor networks and the internet of things," in 3rd IEEE World Forum on Internet of Things, WF-IoT 2016, Reston, VA, USA, December 12-14, 2016, 2016, pp. 633–638.

[18] N. H. A. Rahman, W. B. Glisson, Y. Yang, and K. R. Choo, "Forensicby-design framework for cyber-physical cloud systems," IEEE Cloud Computing, vol. 3, no. 1, pp. 50–59, 2016.

[19] V. R. Kebande and I. Ray, "A generic digital forensic investigation framework for internet of things (iot)," in 4th IEEE International Conference on Future Internet of Things and Cloud, FiCloud 2016, Vienna, Austria, August 22-24, 2016, 2016, pp. 356–362.

[20] E. Bajramovic, K. Waedt, A. Ciriello, and D. Gupta, "Forensic readiness of smart buildings: Preconditions for subsequent cybersecurity tests," in IEEE International Smart Cities Conference, ISC2 2016, Trento, Italy, September 12-15, 2016, 2016, pp. 1–6.

[21] A. Nieto, R. Roman, and J. López, "Digital witness: Safeguarding digital evidence by using secure architectures in personal devices," IEEE Network, vol. 30, no. 6, pp. 34–41, 2016.

[22] G. Horsman, "Unmanned aerial vehicles: A preliminary analysis of forensic challenges," Digital Investigation, vol. 16, pp. 1–11, 2016.

[23] Z. A. Baig, P. Szewczyk, C. Valli, P. Rabadia, P. Hannay, M. Chernyshev, M. Johnstone, P. Kerai, A. Ibrahim, K. Sansurooah, S. N. Firdous, and M. Peacock, "Future challenges for smart cities: Cyber-security and digital forensics," Digital Investigation, vol. 22, pp. 3–13, 2017.

[24] H. Chung, J. Park, and S. Lee, "Digital forensic approaches for amazon alexa ecosystem," Digital Investigation, vol. 22, pp. S15–S25, 2017.

[25] N. Ellouze, S. Rekhis, N. Boudriga, and M. Allouche, "Cardiac implantable medical devices forensics: Postmortem analysis of lethal attacks scenarios," Digital Investigation, vol. 21, pp. 11–30, 2017.

[26] X. Feng, E. S. Dawam, and S. Amin, "A new digital forensics model of smart city automated vehicles," in 2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Exeter, United Kingdom, June 21-23, 2017, 2017, pp. 274–279.

[27] V. R. Kebande, N. M. Karie, and H. Venter, "Cloud-centric framework for isolating big data as forensic evidence from iot infrastructures," in 2017 1st International Conference on Next Generation Computing Applications (NextComp). IEEE, 2017, pp. 54–60.

[28] M. Hossain, R. Hasan, and S. Zawoad, "Trust-iov: A trustworthy forensic investigation framework for the internet of vehicles (iov)," in 2017 IEEE International Congress on Internet of Things (ICIOT). IEEE, 2017, pp. 25–32.

[29] N. Koroniotis, N. Moustafa, E. Sitnikova, and J. Slay, "Towards developing network forensic mechanism for botnet activities in the iot based on machine learning techniques," in Mobile Networks and Management - 9th International Conference, MONAMI 2017, Melbourne, Australia, December 13-15, 2017, Proceedings, 2017, pp. 30–44.

[30] M. Harbawi and A. Varol, "An improved digital evidence acquisition model for the internet of things forensic i: A theoretical framework," in 2017 5th International Symposium on Digital Forensic and Security (ISDFS), 2017, pp. 1–6.

[31] T. A. Zia, P. Liu, and W. Han, "Application-specific digital forensics investigative model in internet of things (iot)," in Proceedings of the 12th International Conference on Availability, Reliability and SecurityReggio Calabria, Italy, August 29 - September 01, 2017, 2017, pp. 55:1–55:7.

[32] C. Meffert, D. Clark, I. M. Baggili, and F. Breitinger, "Forensic state acquisition from internet of things (fsaiot): A general framework and practical approach for iot forensics through iot device state acquisition," in Proceedings of the 12th International Conference on Availability, Reliability and Security, Reggio Calabria, Italy, August 29 – September 01, 2017, 2017, pp. 56:1–56:11.

[33] Y. Teing, A. Dehghantanha, K. R. Choo, and L. T. Yang, "Forensic investigation of P2P cloud storage services and backbone for iot networks: Bittorrent sync as a case study," Computers & Electrical Engineering, vol. 58, pp. 350–363, 2017.

[34] C. Shin, P. Chandok, R. Liu, S. J. Nielson, and T. R. Leschke, "Potential forensic analysis of iot data: An overview of the state-of-the-art and future possibilities," in 2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Exeter, United Kingdom, June 21-23, 2017, 2017, pp. 705–710.

[35] [35] N. K. Bharadwaj and U. Singh, "Acquisition and analysis of forensic artifacts from raspberry pi an internet of things prototype platform," Recent Findings in Intelligent Computing Techniques: Proceedings of the 5th ICACNI 2017, vol. 1, p. 311, 2017.

[36] [36] N.-A. Le-Khac, D. Jacobs, J. Nijhoff, K. Bertens, and K.K.R. Choo, "Smart vehicle forensics: Challenges and case study," Future Generation Computer Systems, 2018. [Online]. Available: https://doi.org/10.1016/j.future.2018.05.081.

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)
Vol. 9, Issue 7, July 2023

[37] [37] M. Chernyshev, S. Zeadally, Z. A. Baig, and A. Woodward, "Internet of things forensics: The need, process models, and open issues," IT Professional, vol. 20, no. 3, pp. 40–49, 2018.

[38] [38] Á. MacDermott, T. Baker, and Q. Shi, "Iot forensics: Challenges for the ioa era," in 9th IFIP International Conference on New Technologies, Mobility and Security, NTMS 2018, Paris, France, February 26-28, 2018, 2018, pp. 1–5.

[39] [39] G. Bréda, P. J. Varga, and Z. Illési, "Forensic functional profile of lot devices-based on common criteria," in 2018 IEEE 16th International Symposium on Intelligent Systems and Informatics (SISY), 2018, pp. 000 261–000 264.

[40] S. Alabdulsalam, K. Schaefer, M. T. Kechadi, and N. Le-Khac, "Internet of things forensics - challenges and a case study," in Advances in Digital Forensics XIV - 14th IFIP WG 11.9 International Conference, NewDelhi, India, January 3-5, 2018, Revised Selected Papers, 2018, pp. 35–48.

[41] M. G. Devi and M. J. Nene, "Security breach and forensics in intelligent systems," vol. 2. Springer, 2018, p. 349.

[42] M. M. Losavio, K. Chow, A. Koltay, and J. James, "The internet of things and the smart city: Legal challenges with digital forensics, privacy, and security," Security and Privacy, vol. 1, no. 3, p. e23, 2018.

[43] E. Al-Masri, Y. Bai, and J. Li, "A fog-based digital forensics investigation framework for iot systems," in 2018 IEEE International Conference on Smart Cloud (SmartCloud). IEEE, 2018, pp. 196–201.

[44] M. M. Hossain, R. Hasan, and S. Zawoad, "Probe-iot: A public digital ledger based forensic investigation framework for iot," in IEEE INFOCOM 2018 - IEEE Conference on Computer Communications Workshops, INFOCOM Workshops 2018, Honolulu, HI, USA, April 1519, 2018, 2018, pp. 1–2.

[45] M. M. Hossain, Y. Karim, and R. Hasan, "Fif-iot: A forensic investigation framework for iot using a public digital ledger," in 2018 IEEE International Congress on Internet of Things, ICIOT 2018, San Francisco, CA, USA, July 2-7, 2018, 2018, pp. 33–40.

[46] R. Hussain, D. Kim, J. Son, J. Lee, C. A. Kerrache, A. Benslimane, and H. Oh, "Secure and privacy-aware incentives-based witness service in social internet of vehicles clouds," IEEE Internet of Things Journal, vol. 5, no. 4, pp. 2441–2448, 2018.

[47] V. R. Kebande, S. Malapane, N. M. Karie, H. S. Venter, and R. D. Wario, "Towards an integrated digital forensic investigation framework for an iot-based ecosystem," in 2018 IEEE International Conference on Smart Internet of Things (SmartIoT), 2018, pp. 93–98.

[48] Q. Do, B. Martini, and K. R. Choo, "Cyber-physical systems information gathering: A smart home case study," Computer Networks, vol. 138, pp. 1–12, 2018.

[49] A. Awasthi, H. Read, K. Xynos, and I. Sutherland, "Welcome pwn: Almond smart home hub forensics," Digital Investigation, vol. 26, pp.S38–S46, 2018.

[50] J. H. Ryu, S. Y. Moon, and J. H. Park, "The study on data of smart home system as digital evidence," pp. 967–972, 2017.

[51] D. H. Kasukurti and S. Patil, "Wearable device forensic: Probable case studies and proposed methodology," in International Symposium Security in Computing and Communication. Springer, 2018, pp. 290–300.

[52] G.Dorai, S. Houshmand, and I. Baggili, "I know what you did last summer: Your smart home internet of things and your iphone forensically ratting you out," in Proceedings of the 13th International Conference on Availability, Reliability and Security. ACM, 2018, p. 49.

[53] D. Quick and K. K. R. Choo, "Digital forensic intelligence: Data subsets and open source intelligence (DFINT+OSINT): A timely and cohesive mix," Future Generation Comp. Syst., vol. 78, pp. 558–567, 2018.

[54] M. B. Al-Sadi, L. Chen, and R. J. Haddad, "Internet of things digital forensic investigation using open source gears," in SoutheastCon 2018IEEE, 2018, pp. 1–5.

[55] D. Quick and K. R. Choo, "Iot device forensics and data reduction," IEEE Access, vol. 6, pp. 47 566–47 574, 2018.

[56] S. Kang, S. Kim, and J. Kim, "Forensic analysis for iot fitness trackers and its application," Peer-to-Peer Networking and Applications, 2018.[57] G. S. Chhabra, V. P. Singh, and M. Singh, "Cyber forensics framework for big data analytics in iot environment using machine learning," Multimedia Tools and Applications, 2018.

[57] G. S. Chhabra, V. P. Singh, and M. Singh, "Cyber forensics framework for big data analytics in iot environment using machine learning," Multimedia Tools and Applications, 2018.

[58] F. Bouchaud, G. Grimaud, and T. Vantroys, "Iot forensic: identification and classification of evidence in criminal investigations," in Proceedings of the 13th International Conference on Availability, Reliability and Security, ARES 2018, Hamburg, Germany, August 27-30, 2018, 2018, pp. 60:1–60:9.

[59] Messai, Mohamed-Lamine. (2014). Classification of Attacks in Wireless Sensor Networks.

[60] Imdad, Maria & Jacob, Deden & Mahdin, Hairulnizam & Baharum, Zirawani & Shaharudin, Shazlyn & Azmi, Mohd. (2020). Internet of things: security requirements, attacks and counter measures. Indonesian Journal of Electrical Engineering and Computer Science.

[61] Kandah, Farah & Singh, Yashaswi & Wang, Chonggang. (2011). Colluding injected attack in mobile ad-hoc networks. 20 IEEE Conference on Computer Communications Workshops, INFOCOM WKSHPS 2011. 235 – 240.

[62] Alromih, A., Al-Rodhaan, M., & Tian, Y. (2018). A Randomized Watermarking Technique for Detecting Malicious Data Injection Attacks in Heterogeneous Wireless Sensor Networks for Internet of Things Applications. Sensors (Basel, Switzerland), 18(12), 4346.

[63] Abbas, Sohail & Haqdad, Muhammad & Begum, S. & KhanMuhammad Zahid. (2018). Detecting sybil attacks using heterogeneous topologies in static wireless sensor network. Journal of Theoretical and Applied Information Technology. 96. 49284940.

[64] Abbas, Sohail & Haqdad, Muhammad & Begum, S. & Khan, Muhammad Zahid. (2018). Detecting sybil attacks using heterogeneous topologies in static wireless sensor network. Journal of Theoretical and Applied Information Technology. 96. 49284940.

[65] Nicole Lang Beebe and Jan Guynes Clark. "A Hierarchical, Objectives-Based Framework for the Digital Investigations Process" (2005)