

INTERNET OF THINGS INVESTIGATIONS AND DIGITAL FORENSICS CHALLENGES

K. Venkatagurunatham Naidu

Dept. of Computer Science and Engineering Dr.M.G.R.E.R.I, Chennai, India.

Email: venkatspmvv@gmail.com

Dr. V. N. Rajavarman

Dept. of Computer Science and Engineering, Dr.M.G.R.E.R.I Chennai, India.

Email: nrajavarman2003@gmail.com

Abstract

The Internet of Things (IoT) has evolved into a daily technology component that unifies all of the disparate systems and data into one process that is integrated and cohesive. Digital world currently lacking the favourable capacity for Internet of Things digital forensics despite the introduction of cutting-edge technologies offering precise solutions. As a result, the extraordinary growth in the number of electronic devices and the vast gathering and consumption of data have made Internet of things forensics necessary in the scenario of cybercrimes. We summarise the distinctions among IoT and traditional digital forensic techniques in this study and also provided a list of three types of IoT-related computer crimes.

Keywords: IoT Investigation, IoT devices, Data Integrity, digital forensics, IoT Forensics

I. INTRODUCTION

Productivity and connectivity have increased with the online interconnection of numerous electronic devices, such as IoT. These things have created a system that is being used to orchestrate and control devices in crucial infrastructures including nuclear as well as power plants, the building industry, and the healthcare industry, among other places. There are an increasing number of these dispersed devices in the networked environment, commonly known as cyberspace. Hence, digital evidence, such as information from social networks, mobile SIM cards, CCTV camera footage, and more, has been used in some way in the majority of criminal activities across the public, private sectors. A compelling case study for demonstrating the value of multilayered digital forensics in identifying culprits is the Boston Marathon Bombing incident [1]. Despite changes in data and technology, forensics processes have not changed. The tools used to commit the crime or the objects on which it is committed have been identified as eyewitnesses. The interconnectedness of today's technologies has made it simpler for hackers to exploit private information, which reduces the dependability of misused equipment. IoT forensics must be triggered as a result of this. Gartner predicts that by the end of 2020, there will be 5.8 million IoT devices supporting various industries, resulting in a significant amount of unsafe data [2]. IoT forensics is a branch of digital forensics and involves gathering evidence from all connected devices through a variety of methods. IoT includes data in terms of quantity, variety, and speed. IoT technologies use sensors and tracking tags to continuously gather activity logs, which is an excellent source of witness. IoT forensics is therefore of utmost significance. Here is a list of what we contributed to this work:

- The distinctions between conventional and Internet - of - things digital forensic methods are highlighted.
- Internet-of-things related computer crimes are listed.
- R& D contributions to the field of IoT forensics are categorised.

II. IOT AND DIGITAL INVESTIGATION PROCEDURE

It takes several years for a traditional court to accept and integrate digital evidence. With the advancement of technology, growing reliance on, and comprehension of, the Policies have been updated for the digital age to hasten the legal system’s acceptance. Digital forensics is indeed an scientific discipline that helps to identify an occurrence, gather evidence, examine, analyse, and report findings, according to NIST [3]. According to the definition given above, there are four major stages or steps that make up digital forensics:

- Identification, which entails the identification of the incident and the identification of the evidence;
- Digital investigator collects all forensic data from various media, such as a hard disc, during the collection process; and
- Inspection and analysis are as part of organisation. As part of the evaluation, all data and attributes are extracted and looked at. The facts and information obtained during the analysis phase are analysed and reviewed by the investigator.
- The presenter then continues on to the presentation phase, when they create a well-organized report that is submitted to the proper court or process.

The Internet of Things (IoT) differs from traditional (normal) devices in a number of ways. IoT devices are first motivated by business, which indicates that, at least for enterprises, the purpose of its deployment is to lower costs and boost productivity. Second, because IoT devices are much more dispersed and diverse in nature, they produce a tonne of data of all different kinds. Finally, IoT makes it possible to link to operational technology (OT) as well as other IT equipment. Finally, the IoT requires complete automation and near real-time incident monitoring due to the geographically distributed nature of its components. Our projection assumes that the detection of evidence within Internet of things will be more difficult in this situation. The identification step of any digital forensic inquiry would be more challenging due to the many kinds of electronic gadgets and sensors, as well as the various data types produced by these IoT pieces. For instance, network forensics will be mostly used while examining a cyber-attack that affected numerous firewalls and routers. However in an IoT situation, sensors [4] that might be installed in a power plant’s SCADA system will also be involved. As a result, trying to gain access to such gadgets that are housed in essential infrastructure may be challenging. Critical infrastructure is moreover typically segregated from, disconnected from, or connected online via secure connections via VPN tunnelling. As a result, detecting or fingerprinting such external devices is more difficult than doing so for publicly accessible IT assets. In this instance, special authorization is needed to gain access to such equipment for additional research. IoT device collection will also be more difficult than with traditional devices. As IoT devices are included in the digital inquiry, we anticipate seeing more challenges from the perspective of the company. This is due to the previously noted fact that IoT devices will be more widely dispersed and produce more data in a wider range of formats. As a result, however addition to the novel underlying technologies in IoT, researchers will require additional time to develop their skills and comprehend the necessary resources (such as tools that interpret the data from multiple sensors), which will ultimately make the organisation phase more complex. Finally, because it is autonomous of hardware and data, we forecast that the presentation phase won’t be impacted by the IoT trend. Table 1 summarises the key difficulty differences between traditional and IoT digital forensics. In the same way,

TABLE I COMPARING TRADITIONAL AND INTERNET OF THINGS (IOT) INVESTIGATIONS, AND THE RESULTING COMPLEXITY.

Process of Digital Investigation	Traditional	IoT
Identification	Medium to High	High

Collection	Low to Medium	Medium to High
Organization	Medium to High	High
Presentation	Low to Medium	Low to Medium

the key distinctions between evidence types, data utilisation, network limits, and data storage are highlighted in Table 2.

III. ATTACKS ON DIGITAL FORENSICS AND IOT

The perception layer, network layer, and application layer are the three layers on which the IoT devices operate. Bar codes,RFID or essentially sensors that gather data from the outside environment and transmit it to the network layer make up the physical layer. The network layer’s goal is to transmit the perception layer’s findings to an information processing system over the Internet or another trustworthy

TABLE II KEY DIFFERENCES BETWEEN TRADITIONAL AND IOT INVESTIGATIONS

Digital Forensics	Traditional	IoT
Provenance of the evidence	Electronic devices including portable and stationary computers	Sensors and tags embedded in electronics; RFID; Internet of Things gadgets
Use of Data Network	Terabyte determined boundary based on the circumstances or ownership	Exabyte Due to the large number of devices, IoT forensics does have a blurry and confused boundary
Storage	Disk Analysis	To record the disk’s present state, micro cards, memory, and RAM-based systems are used [7].

network. Lastly, users use IoT intelligence and analytics at the application layer to accomplish their objectives (such as increase productivity, connectivity, scalability, etc.). Security of these levels has become a difficult problem in modern times due to the growing usage and inclusion of interconnected devices. Each feature change across all three levels has the potential to jeopardise any essential security aspect, such as Integrity,confidentiality& availability [6]. Three types of assaults or cybercrimes against IoT technology are listed in this section.

A. PHYSICAL ATTACKS

Node tampering:It includes physical access by an attacker to a node in order to recover keys, node destruction, and operating on an IoT node. This attack can be stopped with authentication and cryptography [21].

-Sleep deprivation attack: The attacker attempts to drain power, which ultimately causes the IoT node to shut down. The assault includes keeping the node conscious for a very long time, which ultimately causes the node to shut down. IoT sensors are battery-powered and have a finite amount of power.

Such attacks can be identified and predicted by using an intrusion detection system and techniques like deep learning [14]. Malicious code injection: When an attacker injects malicious code into a node, the node may be shut down or, in the worst situation, the attacker may have complete access to the node. The sensitive data of the attacker's node replicating and injection will be saved if there is collusion with the injected attack [15].

Physical theft: The assailant sneaks into the physical hardware or valuable items. IoT devices will be put in several industries and locations, making access to them simple. This is especially true when sensors are dispersed over open and public spaces (such as agricultural fields, roadways, and transportation systems).

B. SOFTWARE ATTACKS

- Phishing attacks: By email spoofing, the attacker gains access to user name and password information. With IoT, where credentials are the entrance to private data, the information collected can be utilised by the attacker to gain unauthorised access to a victim's account, which may have access to an IoT device management system. One of the best strategies for thwarting phishing attacks is awareness.

-Malicious Script:Script that is malicious Via the injection of malicious script, the attacker accesses the system. The Randomised Watermarking Filtering Scheme (RWFS) has a sensor that detects and removes fraudulent data. This methodology generates an all-encompassing watermark that can be used in forensics [12].

-Malware: The attacker can harm the computer by using harmful code, such as viruses, worms, and Trojan horses. These codes spread themselves via email and download from the internet. Maintaining a repository of all viruses and attempting a signature-based detection are forensic methods to address this malware assault [14]. Additionally, malware attack detection may be aided by machine learning and the development of zero-day capabilities.

C. NETWORK ATTACKS

Denial of Service: In this attack, the attacker floods the network with large amounts of traffic (for example, bandwidth), exhausting the system and rendering it unavailable to legitimate users. This has an impact on all IoT layers, but particularly the perception layer. In order to distinguish between attack and real-time traffic, packets might be captured using the forensic technique known as JPCAP (network packet capture library). CEPID (Complex Event Processing Intrusion Detection), a different forensic tool, also suggested a multilayered architecture to conduct traffic monitoring, packet analysis, and event handling to restrict suspicious activity [14].// - Man-in-the-middle attack: An intruder horribly eavesdrops on or manages two parties' private communication. The attacker also might deceive the victim in order to learn more. By using a digital signature-based authentication method and continuously monitoring the IoT nodes, this attack can be prevented [14]. A rogue node that may assume the identities of numerous IoT nodes is known as a Sybil attack. Redundancy and incorrect information are the effects of this [13]. An RSS-based detection mechanism can be embedded to conduct a forensic study into the Sybil attack, and network heterogeneity topologies can be used to gauge performance [11].

IV. IMPORTANT IMPLEMENTATIONS IN IOT FORENSICS

The term "LoRa" stands for "long-range," and it refers to a low power technology that allows for communication between remote sensing devices and LPWANs. This technology is absolutely essential since it offers security, precise positioning, and two-way communication. End-to-end encryption, a unique and specialized 128 bit AES key, and a pervasive global identity are all implemented by LoRa. Lora WAN is extremely important for providing security, however if the safety keys are not handled effectively, there is a chance that the security of network devices could be compromised [10]. Since

the Internet of Things relies on data from sensors. The tracing of constellation trace figure, which shows information about the radio frequency properties of LoRa devices and their distinctive features, is a security method for the physical layer. This functionality aids forensic investigations in understanding the sensor assault [16].

V. DISCUSSION

IoT technology generally faces a number of difficulties, including key management, an essential responsibility for IoT security. The absence of suitable forensic tools, however, continues to be the biggest problem facing the field and community of digital forensics. Although technology has greatly evolved, the community of digital forensic experts has not effectively used the capabilities to its advantage. It is a necessity to choose cloud storage given the unique paradigm of rising space utilisation. Storage issues may be less of a concern if the forensic case has a dedicated cloud space. Another difficulty is strongly related to the aforementioned; the forensic tools must be adaptable to the level of knowledge of the forensic team and user-friendly. A programme that can handle a vast number of IoT intelligence, extracts keywords, and analyses the gathered evidence is an important discovery [4] since data analysis is a crucial and time-consuming phase.

VI. CONCLUSION

The paper provides a brief overview of digital forensics and investigations in IoT systems and technologies. Device security and attack-related forensics are crucial due to the growing interconnectedness of devices. About the normal procedure and key variances, we've identified the primary distinctions between conventional and Internet of Things investigations. excluding the presentation stage, our data indicate that the complexity of IoT studies will expand in numerous ways. Also, we listed the most common cybercrime (or attacks) against by the Internet of Things and suggested some investigative strategies to address some of their difficulties. We have taken into account the fact that Internet - of - things digital forensics and investigations are still a relatively recent development in technology for both public and commercial sector investigators.

REFERENCES

- [1] Johnny Nhan, Laura Huey, Ryan Broll, *Digilantism: An Analysis of Crowdsourcing and the Boston Marathon Bombings*, *The British Journal of Criminology*, Volume 57, Issue 2, 1 March 2017, Pages 341361.
- [2] Egham, U.K., *Gartner Forecasts Global Device January (2020)*
- [3] Patel, Keyur K., and Sunil M. Patel. *Internet of things-IOT: definition, characteristics, architecture, enabling technologies, application & future challenges*. *International journal of engineering science and computing* 6, no. 5 (2016).
- [4] Nicole Lang Beebe and Jan Guynes Clark. *A Hierarchical, Objectives- Based Framework for the Digital Investigations Process* (2005).
- [5] 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*, in *IEEE Communications Surveys & Tutorials*, vol. 22, no. 2, pp. 11911221.
- [6] *Internet of Things-IOT: Definition, Characteristics, Architecture, Enabling Technologies, Application & Future Challenges* Keyur K Patel, Sunil M Patel
- [7] M. A. M.Sadeeq, S. R. M. Zeebaree, R. Qashi, S. H. Ahmed and K. Jacksi, *Internet of Things Security: A Survey*, 2018 *International Conference on Advanced Science and Engineering (ICOASE)*, Duhok, 2018, pp. 162-166
- [8] Simson L Garfinkel. 2010. *Digital forensics research: The next 10 years*. *Digital investigation* 7 (2010), S64S73.

- [9] H. Rajab and T. Cinkelr, IoT based Smart Cities, 2018 International Symposium on Networks, Computers and Communications (ISNCC), Rome, 2018, pp. 1-4.
- [10] B. Hammi, R. Khatoun, S. Zeadally, A. Fayad and L. Khoukhi, IoT technologies for smart cities, in IET Networks, vol. 7, no. 1, pp. 1-13, 1 2018.
- [11] Abbas, Sohail & Haqdad, Muhammad & Begum, S. & Khan, Muham- mad Zahid. (2018). Detecting sybil attacks using heterogeneous topolo- gies in static wireless sensor network. Journal of Theoretical and Applied Information Technology. 96. 49284940.
- [12] 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.
- [13] Abbas, Sohail & Haqdad, Muhammad & Begum, S. & Khan, Muham- mad Zahid. (2018). Detecting sybil attacks using heterogeneous topolo- gies in static wireless sensor network. Journal of Theoretical and Applied Information Technology. 96. 49284940.
- [14] 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.
- [15] Kandah, Farah & Singh, Yashaswi& Wang, Chonggang. (2011). Collud- ing injected attack in mobile ad-hoc networks. 2011 IEEE Conference on Computer Communications Workshops, INFOCOM WKSHPs 2011. 235 240.
- [16] Jiang, Y., Peng, L., Hu, A. et al. Physical layer identification of LoRa devices using constellation trace figure. J Wireless Com Network 2019, 223 (2019).
- [17] Liu, X., Abdelhakim, M., Krishnamurthy, P., & Tipper, D. (2018). Identifying Malicious Nodes in Multihop IoT Networks using Dual Link Technologies and Unsupervised Learning. Open J. Internet Things, 4, 109-125.
- [18]] H. Achi, A. Hellany and M. Nagrial, Network security approach for digital forensics analysis, 2008 International Conference on Computer Engineering & Systems, Cairo, 2008, pp. 263-267.
- [19] Boztas, A. & Riethoven, A.R.J. & Roeloffs, Mark. (2015). Smart TV forensics: Digital traces on televisions. Digital Investigation.
- [20] S. Becirovic and S. Mrdovic, Manual IoT Forensics of a Samsung Gear S3 Frontier Smartwatch, 2019 International Conference on Software, Telecommunications and Computer Networks (SoftCOM), Split, Croa- tia, 2019, pp. 1-5.
- [21] Messai, Mohamed-Lamine. (2014). Classification of Attacks in Wireless Sensor Networks.
- [22] Sutherland, Iain & Read, Huw & Xynos, Konstantinos. (2014). Forensic analysis of smart TV: A current issue and call to arms. Digital Investi- gation.