BOOK CHAPTER | IoT Forensics

Privacy Preserving Internet of Things (IoT) Forensics

Frederick Asumang Odame
Digital Forensics and Cyber Security Graduate Programme
Department of Information Systems & Innovations
Ghana Institute of Management & Public Administration
Greenhill, Accra, Ghana
E-mail: odamefrederick@yahoo.com
Phone: +233243479123

ABSTRACT

The Internet of Things (IoT) envisions a network of pervasive, connected, and intelligent nodes that interact autonomously and provide a variety of services. IoT objects were a perfect target for cyber assaults because of their wide dispersion, openness, and relatively high processing power. Furthermore, because many IoT nodes collect and process personal or private data, they are becoming a goldmine of information for cybercriminals. As a result, security, particularly the ability to detect compromised nodes, as well as the collection and preservation of evidence of an attack or malicious activity, emerge as a top priority in the effective deployment of IoT networks.

Key words: Information Security, IoT, Privacy Preserving, Cyber Security, Cyber Criminals

BOOK Chapter | Research Nexus in IT, Law, Cyber Security & Forensics. Open Access. Distributed Free

Citation: Frederick Asumang Odame (2022): Privacy Preserving Internet of Things (IoT) Forensics
Book Chapter Series on Research Nexus in IT, Law, Cyber Security & Forensics. Pp 109-112
www.isteams.net/ITlawbookchapter2022. dx.doi.org/10.22624/AIMS/CRP-BK3-P18

1. INTRODUCTION

interconnected computing devices with various components to facilitate smooth connectivity and data transfer. Machine-to-machine communication (M2M), context-aware computing, and radiofrequency identification are technologies that are often implemented in the IoT area (RFID). Typical proactive sensing and adapting objects includes wide range of devices. Firstly, wearable devices such as smartwatches, glasses, and health monitoring systems. Secondly, smart home appliances such as smart locks, sensors for temperature, gas, and ambient light; and thirdly, smart vehicles, drones, and applications for industrial automation and logistics. IoT devices communicate with millions of other devices worldwide. This form of open, large-scale communication is particularly attractive to people with unlawful or criminal intentions. In many instances, intruders do not directly target IoT devices, but rather use them as a weapon to attack other systems or platforms (Alabdulsalam, etal, 2018). Consequently, cybercrime has become the second most commonly reported crime worldwide (PwC, 2018).

IoT systems appear to be simple targets for attackers due to the fact that while developing IoT devices, manufacturers frequently prioritize cost, size, and usability, while neglecting security and forensics. As explained by Lally and Sgandurra (2018) that some manufacturers undertake security procedures because an eventual exploitation of one of their IoT products will harm the company's reputation.

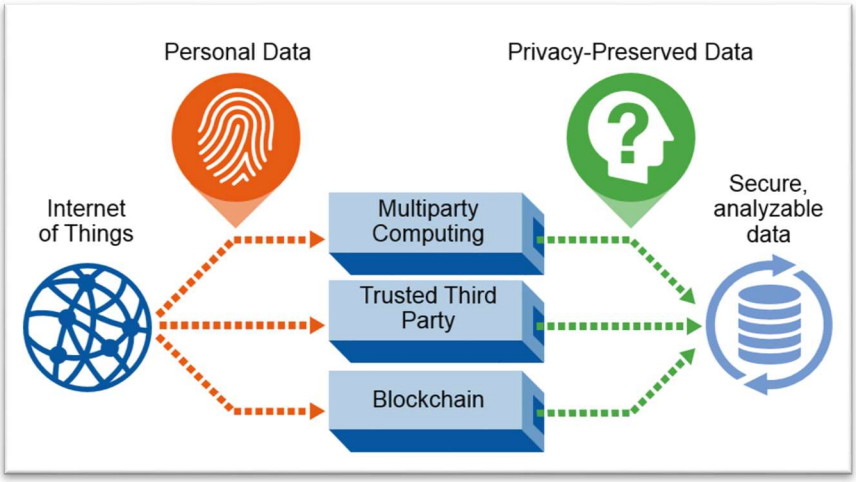

Fig 1: Privacy Preserving IoT Framework
Source: https://twitter.com/antgrasso/status/1118393710587404288

1.1 Background to the Study

Even though recent technological developments, such as low-cost image and video capture and information processing techniques like artificial intelligence and machine learning, have improved the level of forensic analysis, there are still some significant challenges that need to be overcome in the future. As a result, the primary objective of this article is to take a more in-depth look at the vulnerability issues that are present inside IoT systems from a forensic point of view and investigate the state-of-the-art techniques to digital forensics. To be more specific, work examines the fundamental difficulties, theoretical frameworks, and trends in the field of Internet of Things (IoT) forensics. In addition, it highlights the importance of standardizing the forensics process by arguing that doing so is an essential step towards producing high-quality forensics reports that are applicable across several jurisdictions and cyber-security best practices.

The discussion of the extremely difficult problems that arise when attempting to access personal data in a way that maintains individuals' privacy is yet another objective of this study that is of equal importance. This document, when viewed in its whole, attempts to provide answers to the following questions: If the data generated by Internet of Things devices may be used for forensic purposes, how valuable can it be in the process of conducting a forensic investigation if this is the case? Is there a method or model that can efficiently collect, preserve, and evaluate data for a forensic investigation? Do specialists in the field of digital forensics have access to any standards, rules, or recommendations for best practice that could be of benefit to them?

2. RELATED LITERATURE

Since cloud and fog computing's inception, researchers (Kumar and Goyal, 2019) have studied cloud-based security. They posit that security and forensics are different disciplines while having similar problems. Unlike security specialists, forensics professionals assess damage and attack origin post-mortem. They employ diverse instruments and procedures (Table I). This poll acknowledges the overlap between forensics and security by noting that digital forensics rules might be considered security best practices.Both cloud and traditional computers benefit from forensic readiness. Some cloud and network security efforts according to Cook eta al (2018), could be applicable to IoT-centered forensics investigations. IoT networks have the same vulnerabilities as computer networks. IoT systems interact more with the physical environment, attracting greater physical and digital risks. So much research is devoted to safeguarding the IoT area (Khan and Salah, 2018).

Nearly every aspect of the IoT has been studied extensively (Lu and Xu, 2019), from essential enabling technologies and architectural features to deployment fields and open difficulties. Many studies deal with IoT wireless networks however, Al-Turjman et al (2019) examine how 5G will change wireless communication. IoT Forensics literature is scant despite several studies on cellular networks, cloud, and IoT security, Conti et al (2018). IoT systems and their applications need to be able to deal with harmful information exposure and provide strategies that protect sensitive data. Examples of sensitive data include patient data in the healthcare industry, data on energy use from smart energy meters, and location data. The Internet of Things presents concerns with regards to privacy, which highlights the need for innovative approaches to data protection and privacy (Ning, 2012).

3. RESEARCH GAPS/FINDINGS

The abundance of obstacles in IoT Forensics demonstrates the lack of internet security. Therefore, academics and forensics specialists exert considerable effort to find methods and solutions that facilitate the proper gathering and preservation of evidence. Additionally, legal authorities, cloud service providers, and device manufacturers could help eliminate IoT security issues. Manufacturers of devices, for instance, should evaluate the need for a precise and lawful method to collect data from their goods, as they may become subjects of an investigation in the future. On the other hand, public institutions and legal authorities should recognize that IoT Forensics is now lagging behind the established field of Digital Forensics, and consequently, additional research and financing is required.

4. CONCLUSION

The scientific community has already acknowledged that forensic science has reached a turning point. This study recognises the necessity of adapting and extending traditional forensics techniques to the Internet of Things (IoT) domain, while keeping forensics principles for retrieving and preserving legally admissible evidence by highlighting current problems and unresolved questions in the field. In addition, defined IoT security policies and universally accepted standards are required. Research, business, and legal organizations should collaborate, as the spread of IoT development will continue to create new obstacles.

5. RECOMMENDATION FOR POLICY AND PRACTICES

1. **Identification of IoT devices and Data location**: Possible evidence may live in IoT devices, network infrastructures, and cloud servers, so it's necessary to identify these devices and places.
2. **Data type and lifespan:** The data format and type in IoT systems are variable for different devices, so it's vital to return the data to its native format before forensic examination. It's difficult to collect, process, analyse, and display live data (RAM, cache, etc.) in a court-acceptable manner.
3. **Cloud-level forensics:** Most IoT apps are supplied as cloud services, therefore evidence can be disseminated among cloud servers outside the investigator's control. Cloud-based forensics require more advanced forensic analysis tools.
4. **Lack of security:** Device kind, attack scenarios, etc. must be addressed to build IoT investigation methods/tools. IoT forensics will become more crucial as more devices become networked (e.g. a private home or office network). There are many challenges and how can forensic capabilities and anti-forensic measures keep up with emerging IoT devices?

6. DIRECTION FOR FUTURE WORKS

Future work is aimed at the formal definition of privacy policies for digital evidence collected from personal devices, considering different user profiles, resources and functionalities in the devices. Furthermore, the paper is not intended to give all the technical details on how to implement the methodology into a specific hardware. Indeed, there is no single way of implementing the methodology and this is a matter of current and future work.

REFERENCES

1. S. Alabdulsalam, K. Schaefer, T. Kechadi, and N. A. Le-Khac, "Internet of Things forensics—Challenges and a case study," in *Proc. IFIP Adv. Inf. Commun. Technol.*, vol. 532, 2018, pp. 35–48
2. PwC. (2018). *Global Economic Crime and Fraud Survey 2018*. Accessed: Feb. 25, 2019. [Online]. Available: https://www.pwc.com/gx/en/forensics/global-economic-crime-and-fraud-survey-2018.pdf
3. G. Lally and D. Sgandurra, *Towards a Framework for Testing the Security of IoT Devices Consistently*. Cham, Switzerland: Springer, 2018, pp. 88–102.
4. R. Kumar and R. Goyal, "On cloud security requirements, threats, vulnerabilities and countermeasures: A survey," *Comput. Sci. Rev.*, vol. 33, pp. 1–48, Aug. 2019
5. Cook *et al.*, *Internet of Cloud: Security and Privacy Issues*. Cham, Switzerland: Springer, 2018, pp. 271–301
6. M. A. Khan and K. Salah, "IoT security: Review, blockchain solutions, and open issues," *Future Gener. Comput. Syst.*, vol. 82, pp. 395–411, May 2018.
7. Y. Lu and L. D. Xu, "Internet of Things (IoT) cybersecurity research: A review of current research topics," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 2103–2115, Apr. 2019.
8. F. Al-Turjman, E. Ever, and H. Zahmatkesh, "Small cells in the forthcoming 5G/IoT: Traffic modelling and deployment overview," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 1, pp. 28–65, Aug. 2019
9. M. Conti, A. Dehghantanha, K. Franke, and S. Watson, "Internet of Things security and forensics: Challenges and opportunities," *Future Gener. Comput. Syst.*, vol. 78, pp. 544–546, Jan. 2018.
10. H.L. Huansheng Ning, Cyber-physical-social based security architecture for future Internet of things, Adv. Internet Things 2 (1) (2012) 1–7