Privacy-Preservation and Containment in IoT Forensics Investigations: A Comparative Study

*Note: Sub-titles are not captured in Xplore and should not be used

Norman Nelufule
Council for Scientific and Industrial Reseach (CSIR)
Defence and Security Cluster
Pretoria, South Africa
nnelufule@csir.co.za

Tanita Zothile Singano
Council for Scinetific and Industrial Research (CSIR)
Defence and Security Cluster
Pretoria, South Africa
zsingano@csir.co.za

Daniel Shadung
Council for Scientific and Industril Research (CSIR)
Defence and Security Cluster
Pretoria, South Africa
dshadung@csir.co.za

Kele Masemola
Council for Scientific and Industrial Research (CSIR)
Defence and Security Cluster
Pretoria, South Africa
kmasemola1@csir.co.za

***Abstract*—The Internet of Things has enabled unprecedented levels of devices connectivity and communication through data collection and sharing from multiple devices. These massive communications also introduced new challenges to digital forensics, particularly with respect to data security and privacy preservation. Internet of Things devices generate and collect massive amounts of sensitive data, including but not limited to personally identifiable information. These data may be valuable for digital forensics investigations, but it also raises significant data security and privacy. Digital forensic investigators must balance the need to collect and analyze evidence with the obligation to protect individual privacy. This article presents a concise but comprehensive comparative analysis of privacy-preserving Internet of Things forensic investigation techniques. The article also identifies some of the key challenges and opportunities in this emerging field and compares the different techniques available to digital forensic investigators. The article highlights the strengths, weaknesses, and applicability of each technique in various scenarios, providing valuable information for digital forensic investigators and researchers on how to select and implement the most appropriate techniques for their specific needs.**

Keywords— IoT, Digital Forensics, Privacy Preservation, Comparative Study, Lightweight Cryptography, Differential Privacy, Homomorphic Encryption, Zero-Knowledge Proofs, Trusted Execution Environments.

I. INTRODUCTION

The birth of the Fourth Industrial Revolution (4IR) has advanced the development of technologies and enabled the ease of connecting and communicating data with multiple devices [1]. As a result, the Internet of Things (IoT) also emerged and has now transformed the digital world by allowing the connectivity and communication of billions of devices in an environment such as smart cities, smart homes, health facilities, manufacturing, agriculture, and other sectors [2]–[4]. These devices are also used to generate massive wealth of useful data. However, this widespread connectivity and communications of multiple devices over the Internet has also raised critical concerns about the security and privacy of information they exchange, particularly in digital forensic investigations activities [5]–[10]. The IoT devices are often deployed in sensitive environments, such as healthcare, smart homes, agriculture, and smart manufacturing, for the purpose of collecting and transmitting massive amounts of personal and sensitive data [11], [12]. When investigating IoT-related crimes, digital forensic investigators must collect and analyze evidence from these devices without compromising the privacy of individuals [2], [3], [13], [14]. This can be challenging, as IoT devices are often resource-constrained and may not support conventional digital forensics techniques [2], [3].

The main objective of this paper is to provide a concise but comprehensive overview of the privacy-preserving tools and technologies used in IoT forensic investigations. To achieve the mentioned objective, the main aims are to:

- Identify the key challenges and opportunities in privacy-preserving IoT forensic investigations.
- Compare and contrast the different privacy-preserving tools and technologies available in IoT forensic investigation.

The work presented here is a novel comparative analysis because it provides the first comprehensive comparative study of privacy-preserving IoT forensic investigation techniques. It compares the different available techniques, highlighting their strengths, weaknesses, and applicability in various scenarios. This work is also significant because it provides a timely and relevant overview of the privacy-preserving IoT digital forensic investigation techniques. It helps investigators to understand the different available techniques, their strengths, weaknesses, and their applicability in various scenarios.

The remainder of this work is presented as follows: section II presents the literature survey, section III presents the methodology, section IV presents the discussion of the challenges and analysis, and section VI concludes the work and presents future directions.

II. LITERATURE SURVERY

The comparative study of data security and privacy-preserving technology in IoT is an emerging field and less explored in the literature. However, there has been some progress in establishing this emerging active area of research. In [15], a privacy-oriented and log-preserving architecture was presented which was explored in the fog-enabled cloud using the Holochain and containerization technologies. Security analysis was performed, and the automatic log harvesting gave a 95% confidence interval. Nieto *et al.* [16] used the digital witness approach to promote the privacy and preservation of data through the cooperation of digital devices. The challenges with this approach are that it is subjective and strongly depends on the willingness of individuals. Li *et al.* [17], implemented a blockchain approach based on decentralized solutions that accounts for protocols and privacy-preserving abilities. This approach improves data access control and data security through cryptographic mechanisms. Yang *et al.* [18] presented a review of several security challenges faced by the IoT and introduced a component of biometric verification to data access. Regardless of the efforts of researchers in implementing tools and legal entities that establish data security and privacy laws, other solutions need to be intensively explored and implemented.

III. RESEARCH METHODOLOGY

The methodology followed in this work adheres to the qualitative comparative assessment. In this methodology, few technologies have been identified and evaluated in terms of their strength, weaknesses, and applicability. The description of these technologies is presented in TABLE *1*.

TABLE 1: TABLE OF DESCRIPTION OF TECHNOLOGIES USED IN PRIVACY-PRESERVING FORENSIC INVESTIGATIONS TECHNIQUES [16], [19]– [21]

Technology	**Description**
Lightweight cryptography	Lightweight cryptographic algorithms are designed for resource-constrained devices, providing a balance between security and performance.
Differential privacy	Differential privacy is a privacy enhancement technique that allows data collection and analysis of data while protecting individual privacy.
Homomorphic encryption	Homomorphic encryption allows for the computation and analysis of encrypted data without the need to decrypt it.
Zero-knowledge proofs	Zero-knowledge proofs allow one party to prove to another party that they know a piece of information without revealing the information itself.
Trusted execution environments	Trusted execution environments (TEEs) provide a secure and isolated environment for executing sensitive code and data.

This methodology aims to compare, contrast and assess the tools and technologies by adhering to the following steps.

- Identifying key security and data privacy concerns in IoT forensic investigations.
- Identify the different security and data privacy preserving IoT forensic investigation techniques available that preserve privacy and security.
- Compare the different techniques according to their strengths, weaknesses, and applicability in various scenarios. The study will compare the different techniques based on their strengths, weaknesses, and applicability in various scenarios, such as the type of evidence being collected, the available resources, and the level of privacy protection required.
- Develop recommendations for investigators on how to select and implement the most appropriate privacy-preserving techniques for their specific needs.

IV. DISCUSSION OF ANALYSIS AND CHALLENGES

This section presents the discussion and analysis of tools and technologies that are used to enhance data security and privacy preserving mechanism for IoT forensic investigations. This analysis of different privacy-preserving IoT forensic investigation techniques is assessed in terms of their strengths, weaknesses, and applicability in different modes of applications.

There is another challenge of inherent trade-off between data security and privacy in IoT forensic investigations. This is because the more privacy-preserving a technology becomes, there will be some difficulties in data collection and analysis for digital evidence. Conversely, when the technology is more advanced and effective in data collection and analysis, it becomes prone to data security and privacy preserving because there may be multiple loopholes in the data collection pipelines.

There are also several ethical considerations involved in conducting privacy preserving IoT forensic investigations that need to be adhered to. Forensic investigators must balance the need to collect and analyze digital evidence with the obligation to protect individual privacy. This principle should be accompanied by the adherence to data privacy policies such as consent from the data subject, transparency when it comes to informing the data subjects about the privacy-preserving technologies that will be used, and accountability in terms of how the data will be collected and processed.

A summary of some of the technologies and tools is shown in TABLE *2*, in terms of strengths, weaknesses, and applicability in various scenarios of IoT forensic investigations.

TABLE 2. A SUMMARY OF TECHNIQUES IN TERMS OF THEIR STRENGTHS, WEAKNESSES, AND APPLICABILITY [16], [19]–[21]

Techniques	Strengths	Weaknesses	Applicability
Light weight cryptography	This approach is effective, efficient, and more secure, even on more resource constrained connected devices.	The challenges with this approach are that there will be a need for significant computational power and computational resources.	This approach is very suitable for collecting and analyzing a wide range of IoT forensic digital evidence from the IoT, across multiple devices.
The Differential privacy	This approach is implemented to protect individual privacy by adding an element of noise to available data.	The challenge with this method is that there may be an element of lack of data accuracy, and this may inform wrong data analysis.	This approach is suitable for analyzing large datasets of IoT forensic evidence from the Internet of Things.
Homomorphic encryption	This technology is used to allow computations to be performed on encrypted data files without decrypting the data	The challenges of this approach are the use of significant computational power and resources	This approach is mainly used to analyze sensitive IoT forensic data
The Zero knowledge proofs	This technology is used to allow one party to prove to another party that they know a secret PIN or code without revealing the secret code itself	This challenge with this technology is that it is too complex to implement	This technology is used for the verification of the authenticity of IoT forensic evidence.
The Trust execution environments (TEE)	This technology is mainly implemented and exploited to protect mainly sensitive data and process computations from unauthorized access.	The challenge with the use of this technology is that it may be limited in availability on IoT devices.	This technology is most suitable for the protection of sensitive IoT forensic digital evidence for forensic IoT during the collection, analysis, and storing of evidence.

V. THE IMPACT OF EMERGING TECHNOLOGIES ON PRIVACY-PRESERVING IOT FORENSIC INVESTIGATIONS

There are several emerging technologies such as blockchain and federated learning that have a huge potential impact in terms of revolutionizing security and data privacy by preserving forensic investigations. The blockchain technology specifically could be used to create a secure and tamper-proof record of forensic digital evidence. Federated learning, on the other hand, could be used to enable the distributed analysis of IoT digital forensic evidence without compromising any individual data privacy.

The implementation of other tools and intelligent technologies such as lightweight cryptography could also provide a balance between data security and resource constraints, while hardware security mechanisms can offer a robust defence against physical cyberattacks. The data privacy-preserving technologies also enable data processing and analysis while safeguarding sensitive information within the cybersecurity infrastructure.

There is still more room for research to explore the full potential of these emerging technologies for privacy-preserving IoT forensic investigations. This is significant because these technologies can significantly improve the ability and capacity of digital forensic investigators to collect and analyze digital evidence while protecting individual data privacy. Future research in this field of data security and data privacy preservation in the context of IoT digital forensic investigations should also focus on areas such as the following:

- The development of more effective, efficient, and secure privacy-preserving IoT forensic investigation techniques.
- The integration of data privacy preservation techniques into existing digital forensics tools and frameworks.
- The development of standards, guidelines, policies, and best practices for the use of privacy-preserving IoT forensic investigation techniques.
- The intensive and broad investigation on the use of emerging technologies such as blockchain and federated learning for privacy-preserving IoT forensic investigations.

The comparative study in this paper is also designed to assist IoT forensic investigators in understanding the notion and preserving the impact of security and data privacy throughout investigations. This will also allow them to select and adopt the most effective privacy preservation approaches for their specific

needs, thereby safeguarding individual privacy while still allowing the collection and use of data. In summary, digital forensic investigation who conduct their investigations on IoT and other related systems should take note of the following:

- Use blockchain technology for a secure and temper-proof record of their digital evidence.
- Use federated learning for distributed analysis of digital evidence without compromising the individual data privacy.
- Use lightweight cryptography to balance between data security and resource constraints.
- Employ robust hardware security tools that will guard against cyberattacks.

VI. Conclusion:

The principle of data security and preservation of data privacy has a critical challenge in forensic IoT forensic investigations. Digital forensic investigators in IoT systems must balance the need to collect and analyze evidence with the obligation to protect individual privacy. A wide range of privacy-preserving IoT forensic investigation techniques are available, each with its own strengths, weaknesses, and applicability in various scenarios as presented in Section IV TABLE 2.

Forensic investigators must carefully select and implement the most appropriate privacy-preserving techniques for their specific needs, considering the trade-offs between privacy and security, the ethical considerations involved, and the potential impact of emerging technologies.

References

[1] J. C. Jansen Van Vuuren and A. Jansen Van Vuuren, "Preparing for the Fourth Industrial Revolution: Recommendations to Adapt Cyber Security Governance and Skills in South Africa," *Journal of Information Warfare*, vol. 21, no. 1, pp. 1–19, 2022.

[2] A. Alenezi, H. F. Atlam, R. Alsagri, M. O. Alassafi, and G. B. Wills, "IoT forensics: A state-of-the-art review, challenges and future directions," in *COMPLEXIS 2019 - Proceedings of the 4th International Conference on Complexity, Future Information Systems and Risk*, SciTePress, 2019, pp. 106–115. doi: 10.5220/0007905401060115.

[3] T. Janarthanan, M. Bagheri, and S. Zargari, "IoT Forensics: An Overview of the Current Issues and Challenges," in *Advanced Sciences and Technologies for Security Applications*, 2021. doi: 10.1007/978-3-030-60425-7_10.

[4] J. P. A. Yaacoub, H. N. Noura, O. Salman, and A. Chehab, "Advanced digital forensics and anti-digital forensics for IoT systems: Techniques, limitations and recommendations," *Internet of Things (Netherlands)*, vol. 19. Elsevier B.V., Aug. 01, 2022. doi: 10.1016/j.iot.2022.100544.

[5] C. Esposito, A. Castiglione, B. Martini, and K.-K. Choo, "Cloud Manufacturing: Security, Privacy, and Forensic Concerns," *Cloud and the Law Column*, pp. 1–7, 2016.

[6] M. Plachkinova, A. Vo, and A. Alluhaidan, "Emerging Trends in Smart Home Security, Privacy, and Digital Forensics," in *Twenty-second Americans Conference on Information Systems, San Diego*, San Diego: AMCIS, Aug. 2016, pp. 1–9.

[7] E. Shaikh, I. Mohiuddin, and A. Manzoor, "Internet of Things (IoT): Security and Privacy Threats," in *2nd International Conference on Computer Applications & Information Security (ICCAIS' 2019)* , Daudi Arabia: IEEE, 2019, pp. 1–6.

[8] F. Assaderaghi *et al.*, "Privacy and Security: Key Requirements for Sustainable IoT Growth.," in *2017 Symposium on VLSI Technology : Digest of technical papers : June 5-8, 2017, Kyoto*, Kyoto: IEEE, Jun. 2017, pp. 1–6.

[9] S. Wilson, N. Moustafa, and E. Sitnikov, "A Digital Identity Stack to Improve Privacy in the IoT," in *2016 IEEE 3rd World Forum on Internet of Things ((WF-IoT)* , IEEE, Dec. 2016, pp. 1–5.

[10] K.-C. Li, B. B. Gupta, and D. P. Agrawal, *Recent Advances in Security, Privacy, and Trust for Internet of Things (IoT) and Cyber-Physical Systems (CPS)*, First Edition. Parkway, NW: CRC Press, 2021.

[11] H. Choura, F. Chaabane, M. Baklouti, and T. Frikha, "Blockchain for IoT-Based Healthcare using secure and privacy-preserving watermark," in *Proceedings of the 2022 15th IEEE International Conference on Security of Information and Networks, SIN 2022*, Institute of Electrical and Electronics Engineers Inc., 2022. doi: 10.1109/SIN56466.2022.9970492.

[12] S. Rudrakar and P. Rughani, "IoT based agriculture (Ag-IoT): A detailed study on architecture, security and forensics," *Information Processing in Agriculture*, vol. 10, no. 3, Sep. 2023, doi: 10.1016/j.inpa.2023.09.002.

[13] T. Wu, F. Breitinger, and I. Baggili, "IoT ignorance is digital forensics research bliss: A survey to understand IoT forensics definitions, challenges and future research directions," in *ACM International Conference Proceeding Series*, Association for Computing Machinery, Aug. 2019. doi: 10.1145/3339252.3340504.

[14] K. Priyadharshini and R. A. Canessane, "Blockchain-based security algorithm on IoT framework for shielded communication in smart cities," in *Proceedings of the 3rd International Conference on Intelligent Communication Technologies and Virtual Mobile Networks, ICICV 2021*, Institute of Electrical and Electronics Engineers Inc., Feb. 2021, pp. 320–327. doi: 10.1109/ICICV50876.2021.9388497.

[15] K. Janjua, M. A. Shah, A. Almogren, H. A. Khattak, C. Maple, and I. U. Din, "Proactive forensics in IoT: Privacy-aware log-preservation architecture in fog-enabled-cloud using holochain and containerization technologies," *Electronics (Switzerland)*, vol. 9, no. 7, pp. 1–39, Jul. 2020, doi: 10.3390/electronics9071172.

[16] A. Nieto, R. Rios, and J. Lopez, "Iot-forensics meets privacy: Towards cooperative digital investigations," *Sensors (Switzerland)*, vol. 18, no. 2, Feb. 2018, doi: 10.3390/s18020492.

[17] M. Li, J. Weng, J. N. Liu, X. Lin, and C. Obimbo, "Toward Vehicular Digital Forensics from Decentralized Trust: An Accountable, Privacy-Preserving, and Secure Realization," *IEEE Internet Things J*, vol. 9, no. 9, pp. 7009–7024, May 2022, doi: 10.1109/JIOT.2021.3116957.

[18] W. Yang, M. N. Johnstone, L. F. Sikos, and S. Wang, "Security and Forensics in the Internet of Things: Research Advances and Challenges," in *Proceedings - 2020 Workshop on Emerging Technologies for Security in IoT, ETSecIoT 2020*, Institute of Electrical and Electronics Engineers Inc., Apr. 2020, pp. 12–17. doi: 10.1109/ETSecIoT50046.2020.00007.

[19] M. A. Wani, "Privacy Preserving Anti-forensic Techniques," 2021. doi: 10.1007/978-981-15-8711-5_5.

[20] A. K. Verma and K. Ramanathan, "Data privacy preservation in digital forensics investigation," in *AIP Conference Proceedings*, 2022. doi: 10.1063/5.0109813.

[21] S. Brotsis *et al.*, "Blockchain meets Internet of Things (IoT) forensics: A unified framework for IoT ecosystems," *Internet of Things (Netherlands)*, vol. 24, Dec. 2023, doi: 10.1016/j.iot.2023.100968.