A Comprehensive Exploration of Digital Forensics Investigations in Embedded Systems, Ubiquitous Computing, Fog Computing, and Edge Computing

Norman Nelufule
Information and Cybersecurity Centre
Council for Scientific and Industrial Research (CSIR)
Pretoria, South Africa
Nnelufule@csir.co.za

Tanita Singano
Information and Cybersecurity Centre
Council for Scientific and Industrial Research (CSIR)
Pretoria, South Africa
Zsingano@csir.co.za

Mfundo Masango
Information and Cybersecurity Centre
Council for Scientific and Industrial Research (CSIR)
Pretoria, South Africa
Mmasango1@csir.co.za

***Abstract*—The rapid evolution of digital ecosystems, characterized by the intricate interplay of diverse technologies, has necessitated a shift in the digital forensics' paradigm. Traditional investigative methods are inadequate to perform digital forensic exercises in the new paradigm of dynamic digital ecosystem landscapes. The emergence of complex digital ecosystems encompassing an array of interconnected devices and data repositories poses formidable challenges for conventional digital forensics. There is a dire need to adapt and advance digital forensic methodologies to effectively combat cybercrime because the evolving landscape of digital ecosystems presents a critical juncture for the field of digital forensics. This study proposes a systematic literature review to understand the extent of these challenges and proposes a collaborative and innovative approach to digital forensic investigation within the context of digital ecosystems. The proposed approach emphasizes collaboration across diverse sectors and integration of innovative technologies by combining a spectrum of digital forensic experts, technologists, and legal professionals to produce a massive wealth of collective intelligence.**

Keywords-Digital Forensics, Cloud Computing, Embedded Systems, Industry 4.0, Ubiquitous Computing, Fog Computing, Edge Computing

I. INTRODUCTION

The Fourth Industrial Revolution (4IR) introduced technological advances in the field of data communication and sharing [1], [2], [3], [4]. 4IR is attributed to emerging technologies such as the Internet of Things (IoT), Industrial Internet of Things (IIoT), cloud computing technologies, Artificial Intelligence (AI), blockchain technologies, machine learning (ML) and many others, which have led to massive data generation and data-sharing platforms [2], [3], [5], [6], [7], [8], [9]. The ubiquity of connected devices, especially IoT devices, has been increasing since 2010, as shown by report depicted in Fig. 1 [10]. In many instances, as new technological advances are being deployed, new challenges emerge that exploit such technologies to steal and defraud legitimate users. The proliferation and ubiquity of cloud, fog, and edge computing technologies have presented many opportunities but have also introduced several challenges.

These challenges are posed to technologies traditionally designed for digital forensic investigations [7], [11], [12]. In addition to the opportunities and challenges, the interconnectedness of devices and the human population has also introduced new complexities in digital forensic investigations [13], [14], [15], [16], [17]. Some of the many challenges that affect forensic investigations in emerging technologies, such as embedded IoT systems, fog computing, and edge computing, face several formidable challenges that include, but are not limited to, device heterogeneity and data scalability, distributed and interconnected systems, real-time data processing and analysis, data privacy and data security, and limited resources required for forensic investigations [18], [19], [20], [21], [22].

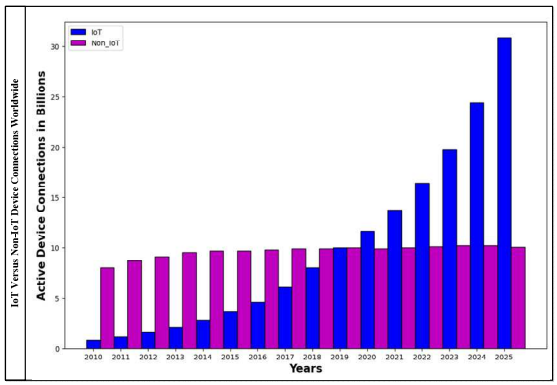

Fig. 1. Figure showing IoT and non-IoT connected devices between years 2010-2025 [10].

Traditional forensic techniques also struggle to adapt to the unique characteristics of these environments, such as the heterogeneity of hardware and software, the distribution of data between multiple devices, and the real-time processing demands of edge computing [21], [22]. This is because these traditional forensic investigation methods and technologies are ill-equipped and unsuitable for handling the complexities of digital forensic investigations in such computing environments. The decentralized nature of data storage and processing, coupled with a wide range of devices and communication protocols, also requires a novel approach to ensure effective digital forensic investigations and analyses [18], [23].

The significance of these challenges is attributed to the growing adoption of decentralized computing paradigms in critical applications, such as IoT, smart cities, and industrial automation. Inability to effectively conduct digital forensic investigations in these environments can have severe and dire consequences that hamper and hinder the forensic investigation of cybercrimes, data breaches, and other digital incidents, leading to financial losses, reputational damage, legal challenges, and potential threats to national and international security. This study aims to contribute by providing the following:

- Comprehensive overview of challenges and opportunities.
- Analysis of the systematic literature based on existing and available data.

The remainder of this paper is organized as follows. Section II presents a literature survey, Section III presents the adopted methodology, Section IV presents the discussion and analysis, and Section V concludes the paper.

II. Literature Survey

A. Cloud Computing

Cloud technologies are widely adopted due to their reliability, ease of data storage, and accessibility. According to Hraiz [24], the introduction of cloud services has brought many benefits to several organizations, but has also brought many challenges to digital forensic investigations. In a digitally connected world, multiple devices access data from a single data storage unit, which may introduce security vulnerabilities [11], [25], [26], [27], [28]. One of the biggest challenges is that traditional forensic investigation tools and procedures are not designed for cloud and IoT technologies, and that such tools cannot be used in new technologies. According to Geetha *et al.*[29], cloud computing and the services they offer are prone to many security and vulnerability challenges. Some of these challenges include phishing attacks, which may harvest user credentials; targeted shared memory attacks; malware injections that can encrypt the entire database; or some portion of the database, making it difficult for a corporate organization to function optimally. Tracing the origins of these threats requires sophisticated forensic tools and human expertise. Rao and Deebak emphasized the importance of cloud computing technology in smart city and industry setups. However, they also argued that cloud computing technologies have severe security and privacy concerns, especially in smart cities and smart industry environments [30].

Several research articles have published the process of acquiring evidence from cloud platforms. The main challenge is that this evidence relies on the collaboration of cloud service providers, who may, in some circumstances, not comply with the request from the investigators. Ali *et al.,* [31], presented a framework which addresses the issue of non-compliant cloud service providers. The framework introduced the detection of cybercrimes or data breaches from the cloud and kept the logs for such incidents on a separate forensic server [31]. Liu *et al.,* also proposed a framework to deploy forensic tools which can be automated to gather evidence from both the clients and the cloud services [32].

B. Embedded Systems

Marwedel defined embedded systems as a type of information processing system that is embedded into an enclosed product[18], as depicted in Fig. 2. Such systems are mainly found in self-driving cars, aircraft, and telecommunications equipment [18]. Data privacy and security are major concerns for embedded systems, consequently making digital evidence collection more complicated. Forensic processes in embedded systems require the collection and analysis of logs from the physical memory of the systems [33]. Flood and Schukat addressed the issues of data security and privacy in embedded systems [34]. To address this issue, a combination of zero-knowledge proofs and key-sharing protocols between machines is proposed to ensure that the systems are secure. Although this approach seems effective, it can only be applied to small embedded systems and is not suitable for large systems, making the forensic investigation more complicated. Furthermore, this process requires the services of knowledgeable network engineers [34]. Yun, *et al.,* [19] emphasized that a behavior rule base can be useful in ensuring the safety of embedded devices, especially in a smart home environment. This is done to prevent intrusion and detect intrusion early, trace the origin of such threats, and address the identified threat promptly [19].

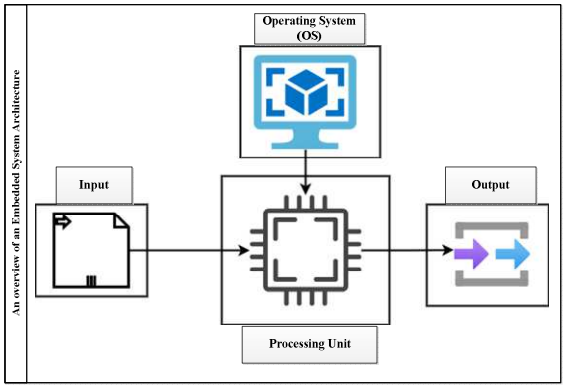

Fig. 2. An example of an embedded system architecture

C. IoT and Ubiquitous Computing

Ubiquitous computing requires the communication of multiple devices through the interconnectedness of a communication network, as depicted in Fig. 3. With the rise of cloud and IoT technologies, most homes are now equipped with smart home devices. Kim *et al.* [35], conducted a study on smart home forensic analysis to analyze the data generated from IoT devices. The main objective was to understand the types of data that can be recovered from Google Nest Hub, Samsung SmartThings, and Kasa, which can be useful for digital forensic purposes. Kasa smart light was also used as a case study to perform a forensic analysis of automated smart home devices [36]. Another interesting aspect of forensic IoT research is related to rule-based behavior IoT devices and the safety of embedded smart home IoT devices [19]. It was established that due to resource constraints of the IoT setup, security

support is limited, and behavior-based behavior was proposed as a countermeasure philosophy.

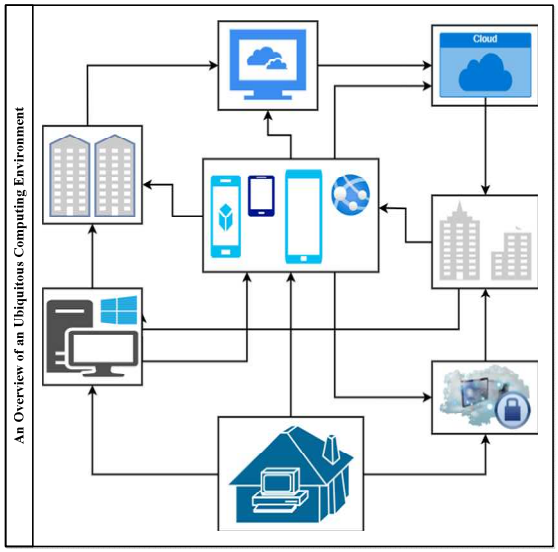

Fig. 3. An example of a ubiquitous environment

D. FOG and Edge Computing

Fig and Edge computing bring data and data processing closer to edge devices, as depicted in Fig. 4. This concept makes digital forensic investigations more complex due to privacy and data integrity concerns [37]. This is because of the distributed nature of embedded systems running in cloud datacenters that then share and exchange information with fog nodes, which ultimately communicate with a multitude of edge devices at the edge level [20]. Ometov *et al.* [11] conducted a security survey of emerging technologies, such as cloud computing, fog computing and edge computing, to establish the relationship among these technologies[11]. This survey further investigated how threats can be detected and prevented by considering the heterogeneous nature of these technologies [11]. The outcome of this survey explains that the security of such technologies is difficult to implement across the board, which poses a threat to their security [11]. Once security measures become difficult to implement, it becomes difficult to conduct successful digital forensic investigations.

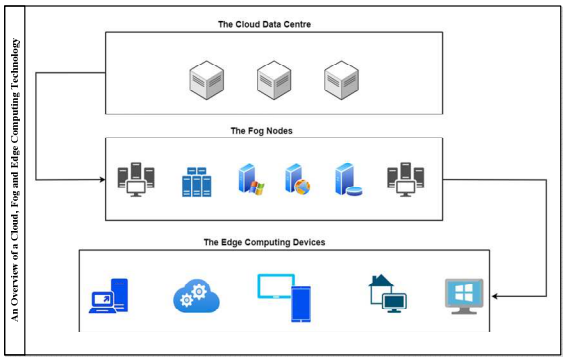

Fig. 4. An example of a connectivity of Fog and Edge Computing devices

The accessibility of Fog and Edge computing technology is not limited to local jurisdictions, and this creates more room for cyber threats. In [37], an investigation of digital evidence in fog computing was conducted and it was established that due to the high number of connected devices, traditional forensic investigation tools, principles, laws, and ethical issues are not equipped for the new landscape of technology, making it difficult to use the existing framework to tackle current cases. Several surveys on fog and edge computing have been conducted that converge on the same analysis [11], [13], [15], [17], [38], [39], [40]. This analogy is also evident in surveys conducted on edge computing technology in forensic investigations [12], [14], [41], [42], [43], [44]. The remaining pressing concern is that current forensic investigation frameworks are not yet applicable and appropriate for these emerging technologies, and a new framework is urgently needed.

III. PROPOSED METHODOLOGY

The adopted framework used a systematic literature review process that incorporated the principle of preferred reporting items for systematic reviews and meta-analyses (PRIMSA) [45]. A systematic review methodology was chosen because it has the potential to synthesize state-of-the-art research within the digital forensic domain [45]. The main reason why this methodology is useful is that it can identify trends for new knowledge and direct future research directions and provide some of the answers to research questions that have not been properly addressed through other studies [45], [46]. A schematic of the proposed PRISMA framework is shown in Fig. 5.

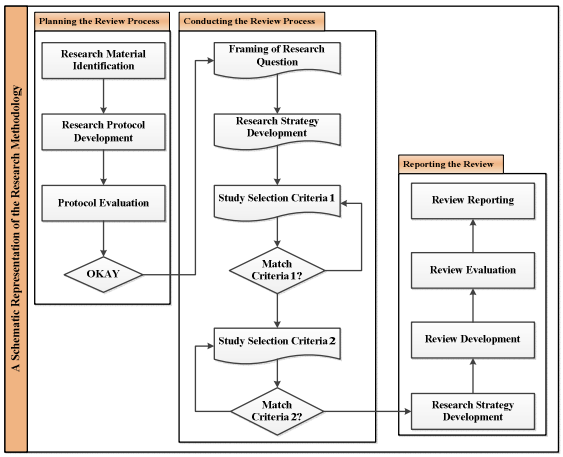

Fig. 5. Overview of the proposed methodology.

Once the review framework is identified, the next step is to build the survey by adhering to the required phases and procedures. Kitchenham *et al.,* [47] presented a structure to follow to reach an informed conclusion during systematic literature surveys in engineering fields. Such a structure involves the following main stages, also depicted in Fig. 6:

- Planning, which involves the identification of study objectives, formulating research questions, and developing the search protocol.
- Selection, which involves the selection of articles.
- Qualitative extraction, which involves the inclusion and exclusion criteria of the identified articles.

The main research questions this study aims to answer are:

- What is the impact of emerging technologies on forensic investigations?
- What are the main challenges of conducting digital forensics in emerging technologies?
- What are the prospects of successfully conducting forensic investigations in emerging technologies?

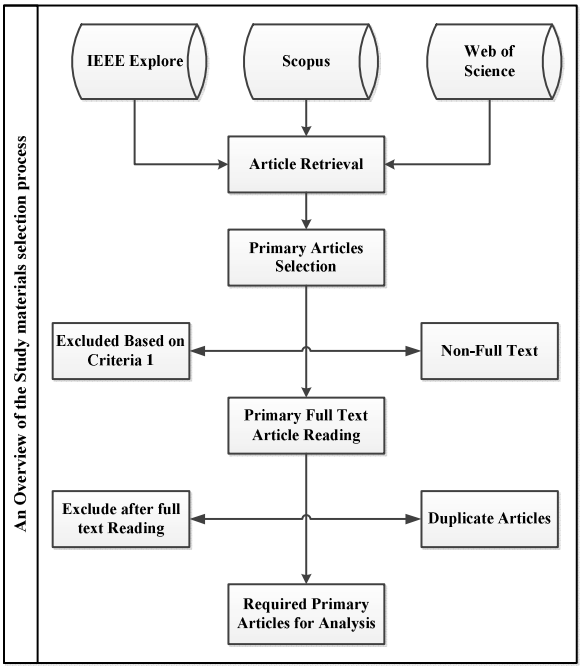

Fig. 6. A figure depicting a Schematic representation of the study material and classification.

A. *Identification of Research Materials*

As shown in Fig. 6, only three indexing databases were selected, namely the IEEE Explore, Scopus (Elsevier), and Web of Science. The reason for this choice was based on the databases that publish peer review conferences and journal articles. The Google Scholar indexing database was not included because it is a standard practice that peer reviewed articles indexed in either of the three will also be indexed in Google Scholar, but another reason was that other articles that are not peer reviewed can also be found.

B. *Selection of study materials*

The main study materials required were peer-reviewed conference papers and journal articles. The selection of these materials was based on the search strategy developed using keywords, phrases, and combinations of keywords such as 'embedded systems', 'digital forensic', 'ubiquitous computing', 'fog computing', 'edge computing', 'Big data', 'digital evidence', security and privacy.'

C. *Inclusion and exclusion of study materials*

The inclusion criteria were based on articles published in English. These included articles which talk about surveys, experimental works, framework development, etc. The exclusion criteria were based on duplication articles, articles that were not from engineering or computer science fields of study, and articles publication in other languages other than English. Future selection for quality assessment was based on title analysis and abstract scanning. The spreadsheet was used as a tool to remove duplicates, analyze the title, and abstract. The remaining articles were studied with full texts and form part of the assessment.

IV. Experimental Results and Discussion

This section evaluates the effectiveness of the proposed framework through a detailed discussion of the components of the framework that were identified against the results obtained from the reviews. This analysis considers the advantages offered against the disadvantages faced by traditional systems. The analyses of some of the relevant literatures are summarized in TABLE 1. Some of the quality measures of interest include scalability, adaptability, and accuracy in digital forensic investigations within diverse computing environments.

TABLE 1. TABLE OF ASSESSMENT OF LITERATURE SURVEYS

No.	Some Major Research Contribution in the literature		
	References	**Contribution**	**Gaps**
1	Sadler *et al.*, [20]	Development of Fog- and Edge Oriented Embedded systems	No frameworks tested on digital forensics
2	Omotevo *et al.*, [11]	Survey on security of Cloud, Edge, and Fog computing	Not tested for forensics investigations
3	Anawar *et al.*, [38]	An overview of Big IoT Data Analysis on Fog Computing	Does not address the issue of data security and data privacy.
4	Alwakeel [39]	Security and privacy issues on fog and edge computing	No emphasis on the required frameworks for digital forensic
5	Mouradian *et al.*, [17]	Survey on Fog Computing	Comparison of several frameworks
6	Hazra *et al.*, [40]	Analysis of state of the art and research challenges	Does not address big data security and privacy concerns in a ubiquitous environment
7	De Donno *et al.*, [7]	Analysis of the evolution of modern computing paradigm	Analysis of several challenges facing forensic
8	Abdali *et al.*, [15]	Analysis of Fog computing environment	Does address or propose a framework for digital forensic
9	Alotaibi [44]	Survey of IIOT	Analysis of AI and Edge Computing Opportunities
10	Prakash *et al.*, [14]	Analysis of challenges in cloud and edge computing forensics	Various assessment of forensic frameworks
11	Marwedel [18]	Embedded system designs of cyberphysical systems and Internet of Things	Does not address the security and forensic related frameworks
12	Lee and Shon [33]	Physical memory collection in smart grid embedded system	Does not address the evidence acquisition from other media.
13	Yun *et al.*, [19]	Behavior rule-based IDS for embedded devices	Extraction of data related to forensic was not conducted
14	Zawoad and Hasan [22]	Survey of digital forensic challenges in the age of big data	No proposition of new frameworks to address the identified challenges
15	Nelufule *et al.*, [48]	Comparative study of privacy preserving technologies of IoT	Does not address the comparison on other technologies besides IoT
16	Nelufule *et al.*, [49]	Adaptive framework for evolving digital landscape	Selective in scope of identified technologies
17	Kebande *et al.*,	Cloud centric framework for isolating evidence	Does not cover other emerging technologies except IoT
18	This paper	Survey of Digital Forensic Investigations in Emerging technologies	Does not cover extraction of digital evidence for analysis

A. Summery of challenges and proposed solution

Table 2 summarizes some of the challenges identified and proposed solutions.

TABLE 2: SUMMARY OF CHALLENGES AND PROPOSED SOLUTION

No.	Challenge	Proposed Solution
1	Data security and privacy	Implementing encryption technology, and access control
2	Evidence preservation and chain of custody	Implementing blockchain technology to preserve the integrity of evidence and maintain the chain of custody
3	Volume of digital evidence	Employing AI technologies to ingest and process data much faster and with high accuracy
4	Legal and ethical issues	Develop legal framework to aid forensic investigations
5	Cross Border Collaboration	Develop legal frameworks to aid forensic investigation beyond the national borders
6	Device heterogeneity	Employ various technologies and merge the extracted data
7	Cloud and Device data encryption	Develop multi stakeholder Collaborative framework to ease data access
8	Security patches and software updates	Develop new forensic tools to match the current state of updated technologies
9	Global Standards	Develop global standards with internal counterparts to aid in cross-border investigations

V. CONCLUSION AND FUTURE WORK

This article presents a survey of the challenges faced by traditional digital forensic technologies in emerging technologies. This article also explained the benefits offered by these emerging technologies to advance some of the digital forensic investigations. As presented in TABLE 1, literature has some of the technologies and frameworks proposed to aid forensic investigations in these industry 4.0 emerging technologies; however, the presented technologies are not one size fit all and require other frameworks to be developed.

In the future, this study will focus on the continuous evolution of digital forensics in response to emerging technologies and cyber threats. The main areas of focus will include the integration of artificial intelligence for automated forensic analysis, the development of forensic tools for specific embedded systems, and the ongoing refinement of frameworks to address evolving challenges in decentralized computing.

ACKNOWLEDGMENT

The authors extend their gratitude to the Department of Science and Innovation (DSI) of South Africa for funding support.

REFERENCES

[1] M. T. Okano, "IOT and Industry 4.0: The Industrial New Revolution," *ICMIS-17 - International Conference on Management and Information Systems*, no. September, 2017.

[2] M. A. Rahim, M. A. Rahman, M. M. Rahman, A. T. Asyhari, M. Z. A. Bhuiyan, and D. Ramasamy, "Evolution of IoT-enabled connectivity and applications in automotive industry: A review," *Vehicular Communications*, vol. 27. Elsevier Inc., Jan. 01, 2021. doi: 10.1016/j.vehcom.2020.100285.

[3] V. R. Kebande, "Industrial internet of things (IIoT) forensics: The forgotten concept in the race towards industry 4.0," *Forensic Science International: Reports*, vol. 5, Jul. 2022, doi: 10.1016/j.fsir.2022.100257.

[4] S. H. Ali, H. A. Al-Sultan, and M. T. Al Rubaie, "Fifth Industrial Revolution," *International Journal of Business, Management and Economics*, vol. 3, no. 3, pp. 196–212, Jul. 2022, doi: 10.47747/ijbme.v3i3.694.

[5] 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.

[6] M. Wazid, A. K. Das, R. Hussain, G. Succi, and J. J. P. C. Rodrigues, "Authentication in cloud-driven IoT-based big data environment: Survey and outlook," *Journal of Systems Architecture*, vol. 97, pp. 185–196, Aug. 2019, doi: 10.1016/j.sysarc.2018.12.005.

[7] M. De Donno, K. Tange, and N. Dragoni, "Foundations and Evolution of Modern Computing Paradigms: Cloud, IoT, Edge, and Fog," *IEEE Access*, vol. 7, pp. 150936–150948, 2019, doi: 10.1109/ACCESS.2019.2947652.

[8] K. Gai, M. Qiu, and S. A. Elnagdy, "A Novel Secure Big Data Cyber Incident Analytics Framework for Cloud-Based Cybersecurity Insurance," in *2016 IEEE 2nd International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS)*, IEEE, Apr. 2016, pp. 171–176. doi: 10.1109/BigDataSecurity-HPSC-IDS.2016.65.

[9] A. Ghafarian, "Foreniscs Analysis of Cloud Computing Services," in *Science and Information Conference 2015*, 2015, pp. 1–5. [Online]. Available: www.conference.thesai.org

[10] L. S. Vailshery, "IoT and non-IoT connections worldwide 2010-2025," Sep. 2022. Accessed: May 17, 2024. [Online]. Available: https://www.statista.com/statistics/1101442/iot-number-of-connected-devices-worldwide/

[11] A. Ometov, O. L. Molua, M. Komarov, and J. Nurmi, "A Survey of Security in Cloud, Edge, and Fog Computing," *Sensors*, vol. 22, no. 3. MDPI, Feb. 01, 2022. doi: 10.3390/s22030927.

[12] N. Abbas, Y. Zhang, A. Taherkordi, and T. Skeie, "Mobile Edge Computing: A Survey," *IEEE Internet of Things Journal*, vol. 5, no. 1. Institute of Electrical and Electronics Engineers Inc., pp. 450–465, Feb. 01, 2018. doi: 10.1109/JIOT.2017.2750180.

[13] D. Spiekermann and J. Keller, "Challenges of Network Forensic Investigation in Fog and Edge Computing," *Future Internet*, vol. 15, no. 10, p. 342, Oct. 2023, doi: 10.3390/fi15100342.

[14] V. Prakash, A. Williams, L. Garg, C. Savaglio, and S. Bawa, "Cloud and edge computing-based computer forensics: Challenges and open problems," *Electronics (Switzerland)*, vol. 10, no. 11. MDPI AG, Jun. 01, 2021. doi: 10.3390/electronics10111229.

[15] T. A. N. Abdali, R. Hassan, A. H. M. Aman, and Q. N. Nguyen, "Fog Computing Advancement: Concept, Architecture, Applications, Advantages, and Open Issues," *IEEE Access*, vol. 9, pp. 75961–75980, 2021, doi: 10.1109/ACCESS.2021.3081770.

[16] C. Huang, R. Lu, and K. K. R. Choo, "Vehicular Fog Computing: Architecture, Use Case, and Security and Forensic Challenges," *IEEE Communications Magazine*, vol. 55, no. 11, pp. 105–111, Nov. 2017, doi: 10.1109/MCOM.2017.1700322.

[17] C. Mouradian, D. Naboulsi, S. Yangui, R. H. Glitho, M. J. Morrow, and P. A. Polakos, "A Comprehensive Survey on Fog Computing: State-of-the-Art and Research Challenges," *IEEE Communications Surveys and Tutorials*, vol. 20, no. 1. Institute of Electrical and Electronics Engineers Inc., pp. 416–464, Jan. 01, 2018. doi: 10.1109/COMST.2017.2771153.

[18] P. Marwedel, *Embedded System Design: Embedded Systems Foundations of Cyber-Physical Systems, and the Internet of Things*, Fourth Edition., vol. 4. Germany: Springer, 2021. [Online]. Available: http://www.springer.com/series/8563

[19] K. Yun, P. V. Astillo, S. Lee, J. Kim, B. Kim, and I. You, "Behavior-Rule Specification-based IDS for Safety-Related Embedded Devices in Smart Home," in *2021 World Automation Congress (WAC) : August 1-5, 2021, online.*, Taiwan: IEEE, Aug. 2021, pp. 1–6.

[20] H. Sadler, A. Barros, and W. Kelly, "Fog and Edge Oriented Embedded Enterprise Systems Patterns: Towards Distributed Enterprise Systems That Run on Edge and Fog Nodes," in *Proceedings of the 55th Hawaii International Conference on System Sciences*, 2022, pp. 1–10. [Online]. Available: https://hdl.handle.net/10125/80132

[21] D. S. Tundalwar, R. A. Pandhare, and M. A. Digalwar, "A Taxonomy of IoT Security Attacks and Emerging Solutions," in *2023 2nd International Conference on Paradigm Shifts in Communications Embedded Systems, Machine Learning and Signal Processing, PCEMS 2023*, Institute of Electrical and Electronics Engineers Inc., 2023. doi: 10.1109/PCEMS58491.2023.10136032.

[22] S. Zawoad and R. Hasan, "Digital Forensics in the Age of Big Data: Challenges, Approaches, and Opportunities," in *2015 IEEE 17th International Conference on High Performance Computing and Communications, 2015 IEEE 7th International Symposium on Cyberspace Safety and Security, and 2015 IEEE 12th International Conference on Embedded Software and Systems*, IEEE, Aug. 2015, pp. 1320–1325. doi: 10.1109/HPCC-CSS-ICESS.2015.305.

[23] Y. Shah and S. Sengupta, "A survey on Classification of Cyber-attacks on IoT and IIoT devices," in *2020 11th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON) : 28th- 31st October 2020, New York, USA, virtual conference*, New York: IEEE, Oct. 2020, pp. 1–8.

[24] S. Hraiz, "Challenges of Digital Forensic Investigation in Cloud Computing," in *ICIT 2017 : the 8th International Conference on Information Technology : Internet of Things IoT : conference proceedings : May 17th - 18th, 2017, Amman, Jordan.*, 2017, pp. 1–4.

[25] Victor. R. Kebande, Nickson. M. Karie, and H. S. 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) : 19th-21st July 2017, Mauritius*, Mauritius: IEEE, Jul. 2017, pp. 1–7.

[26] K.-K. R. Choo, C. Esposito, and A. Castiglione, "Evidence and Forensics in the Cloud: Challenges and Future Research Directions," *IEEE Cloud Computing*, vol. 4, no. 3, pp. 1–6, Jun. 2017.

[27] K. Marshall and A. Rea, "Legal challenges in cloud forensics," in *27th Annual Americas Conference on Information Systems, AMCIS 2021*, 2021.

[28] J. J. Shah and L. G. Malik, "Cloud forensics: Issues and challenges," in *International Conference on Emerging Trends in Engineering and Technology, ICETET*, IEEE Computer Society, 2013, pp. 138–139. doi: 10.1109/ICETET.2013.44.

[29] R. Geetha, A. K. Suntheya, and G. U. Srikanth, "Cloud Integrated IoT Enabled Sensor Network Security: Research Issues and Solutions," *Wirel Pers Commun*, vol. 113, no. 2, pp. 747–771, Jul. 2020, doi: 10.1007/s11277-020-07251-z.

[30] P. M. Rao and B. D. Deebak, "Security and privacy issues in smart cities/industries: technologies, applications, and challenges," *J Ambient Intell Humaniz Comput*, vol. 14, no. 8, pp. 10517–10553, Aug. 2023, doi: 10.1007/s12652-022-03707-1.

[31] S. A. Ali, S. Memon, L. Das Dhomeja, D. Djokic, and F. Sahito, "CLOUD FORENSICS FRAMEWORK FOR LAW ENFORCEMENT AGENCIES," *Journal of Southwest Jiaotong University*, vol. 57, no. 2, 2022, doi: 10.35741/issn.0258-2724.57.2.8.

[32] C. Liu, A. Singhal, and D. Wijesekera, "Identifying Evidence for Implementing a Cloud Forensic Analysis Framework," in *Thirteenth IFIP WG 11.3 International Conference on Digital Forensics*, Orlando, US: Advances in Digital Forensics XIII, Sep. 2017, pp. 1–22.

[33] S. Lee and T. Shon, "Physical memory collection and analysis in smart grid embedded system," *Mobile Networks and Applications*, vol. 19, no. 3, 2014, doi: 10.1007/s11036-014-0504-0.

[34] P. Flood and M. Schukat, "Peer to Peer Authentication for Small Embedded Systems.," in *The 10th International Conference on Digital Technologies 2014 : 9-11 July 2014 : Žilina, Slovakia*, Slovakia: IEEE, Jul. 2014, p. 375.

[35] S. Kim, M. Park, S. Lee, and J. Kim, "Smart home forensics—data analysis of iot devices," *Electronics (Switzerland)*, vol. 9, no. 8, 2020, doi: 10.3390/electronics9081215.

[36] F. E. Salamh, "A Forensic Analysis of Home Automation Devices (FAHAD) Model: Kasa Smart Light Bulb and Eufy Floodlight Camera as Case Studies," *International Journal of Cyber Forensics and Advanced Threat Investigations*, vol. 1, no. 1–3, 2021, doi: 10.46386/ijcfati.v1i1-3.16.

[37] R. Hegarty and M. Taylor, "Digital evidence in fog computing systems," *Computer Law and Security Review*, vol. 41, Jul. 2021, doi: 10.1016/j.clsr.2021.105576.

[38] M. R. Anawar, S. Wang, M. Azam Zia, A. K. Jadoon, U. Akram, and S. Raza, "Fog Computing: An Overview of Big IoT Data Analytics," *Wireless Communications and Mobile Computing*, vol. 2018. Hindawi Limited, 2018. doi: 10.1155/2018/7157192.

[39] A. M. Alwakeel, "An overview of fog computing and edge computing security and privacy issues," *Sensors*, vol. 21, no. 24, Dec. 2021, doi: 10.3390/s21248226.

[40] A. Hazra, P. Rana, M. Adhikari, and T. Amgoth, "Fog computing for next-generation Internet of Things: Fundamental, state-of-the-art and research challenges," *Computer Science Review*, vol. 48. Elsevier Ireland Ltd, May 01, 2023. doi: 10.1016/j.cosrev.2023.100549.

[41] D. Li *et al.*, "Ubiquitous intelligent federated learning privacy-preserving scheme under edge computing," *Future Generation Computer Systems*, vol. 144, pp. 205–218, Jul. 2023, doi: 10.1016/j.future.2023.03.010.

[42] W. Rafique, L. Qi, I. Yaqoob, M. Imran, R. U. Rasool, and W. Dou, "Complementing IoT Services through Software Defined Networking and Edge Computing: A Comprehensive Survey," *IEEE Communications Surveys and Tutorials*, vol. 22, no. 3, pp. 1761–1804, Jul. 2020, doi: 10.1109/COMST.2020.2997475.

[43] M. Yahuza *et al.*, "Systematic review on security and privacy requirements in edge computing: State of the art and future research opportunities," *IEEE Access*, vol. 8, pp. 76541–76567, 2020, doi: 10.1109/ACCESS.2020.2989456.

[44] B. Alotaibi, "A Survey on Industrial Internet of Things Security: Requirements, Attacks, AI-Based Solutions, and Edge Computing Opportunities," *Sensors*, vol. 23, no. 17. Multidisciplinary Digital Publishing Institute (MDPI), Sep. 01, 2023. doi: 10.3390/s23177470.

[45] M. J. Page *et al.*, "The PRISMA 2020 statement: An updated guideline for reporting systematic reviews," *The BMJ*, vol. 372. 2021. doi: 10.1136/bmj.n71.

[46] J. Paul, P. Khatri, and H. Kaur Duggal, "Frameworks for developing impactful systematic literature reviews and theory building: What, Why and How?," *J Decis Syst*, 2023, doi: 10.1080/12460125.2023.2197700.

[47] B. Kitchenham, O. Pearl Brereton, D. Budgen, M. Turner, J. Bailey, and S. Linkman, "Systematic literature reviews in software engineering - A systematic literature review," *Information and Software Technology*, vol. 51, no. 1. pp. 7–15, Jan. 2009. doi: 10.1016/j.infsof.2008.09.009.

[48] N. Nelufule, T. Z. Singano, D. Shadung, and K. Masemola, "Privacy-Preservation and Containment in IoT Forensics Investigations: A Comparative Study," in *2023 11th International Japan-Africa Conference on Electronics, Communications, and Computations (JAC-ECC)*, IEEE, Dec. 2023, pp. 121–125. doi: 10.1109/JAC-ECC61002.2023.10479652.

[49] N. Nelufule, T. Singano, K. Masemola, D. Shadung, B. Nkwe, and J. Mokoena, "An Adaptive Digital Forensic Framework for the Evolving Digital Landscape in Industry 4.0 and 5.0," in *2nd International Conference on Intelligent Data Communication Technologies and Internet of Things, IDCIoT 2024*, Institute of Electrical and Electronics Engineers Inc., 2024, pp. 1686–1693. doi: 10.1109/IDCIoT59759.2024.10467482.