Digital Forensics in Industry 4.0 and Industry 5.0: Major Challenges and Opportunities

Norman Nelufule, Mfundo Masango, Tanita Singano
Council for Scientific and Industrial Research (CSIR), Pretoria, South Africa
nnelufule@csir.co.za

***Abstract*— The rapid advancements in Industry 4.0 and 5.0, along with the increasing adoption of edge computing, have brought about a significant transformation in industrial landscapes. These advancements have ushered in a new era of interconnected devices, real-time data processing, and decentralized decision making, creating an unprecedented volume of digital data. This surge in data generation has also heightened the need for robust digital forensics capabilities to investigate and respond to cyberattacks, data breaches, and other security incidents. This paper provides an overview of digital forensics in the context of Industry 4.0, Industry 5.0, and edge computing. It discusses the challenges and opportunities associated with forensic investigations in these environments, highlighting the unique characteristics of these technologies and their impact on the collection, preservation, and analysis of digital evidence. The paper also explores the potential applications of digital forensics in these industries, including incident response, fraud detection, and regulatory compliance.**

Keywords*— *Digital forensics, Industry 4.0, Industry 5.0, Edge Computing, Cybercrime, Cybersecurity.

I. INTRODUCTION

The Fourth Industrial Revolution that is intimately known as 4IR, or Industry 4.0 has marked a paradigm shift in manufacturing, which is characterized by the integration of cyberphysical systems, the Internet of Things (IoT), Artificial Intelligence (AI), Machine Learning (ML), and Big Data analytics [1]-[3]. This transformation has led to hyperconnected factories, real-time data analysis, and autonomous decision making. The Fifth Industrial Revolution (5IR) also called Industry 5.0 builds on Industry 4.0 by focusing on human-centricity and sustainability components, emphasizing the collaborative interaction between the humans and their machines [4]-[10].

Edge computing has also emerged as a critical enabler of Industry 4.0 and 5.0, bringing data processing and analysis closer to edge devices [11], [12]. This decentralized approach is advantageous for forensic investigations because it reduces latency and improves responsiveness, thereby enabling the real-time decision making and optimization. However, these amazing benefits are also accompanied by a variety of intricate and unprecedented challenges, such as the volume of data generated by IoT devices which includes sensitive information such as Personal Identifiable Information (PII), which poses data security risks.

The advent of these widely desired and embraced digital technologies has brought many technological benefits, but they have also introduced new challenges for digital forensics, specifically within the ambit of cybersecurity, data acquisition and protection, law, and ethics [13]-[15]. An example of some of the technologies in Industry 4.0 and 5.0 is depicted in Fig. 1.

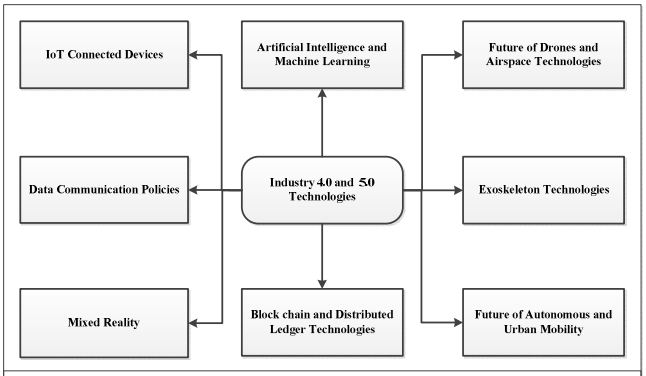

Fig. 1. A figure showing some of the industry 4.0 and 5.0 Technologies.

Advancements in Industry 4.0, 5.0, and edge computing have created a complex and interconnected digital ecosystem, generated vast amounts of data, and presented unique challenges for digital forensics investigations [12].

Traditional digital forensics techniques may not be adequately equipped to handle the volume, diversity, and distribution of data in these environments [15]-[19]. The decentralized nature of edge computing and the increasing reliance on cloud-based services further complicate the evidence collection and analysis. This essence calls for a new framework that will accommodate the emerging challenges of conducting digital forensics in the era of Industry 4.0, 5.0 and edge computing environments.

This research aims to provide a comprehensive understanding of digital forensics in the context of Industry 4.0, 5.0, and edge computing. This is achieved by addressing the challenges and opportunities in this emerging research area. This research also provides a comprehensive analysis of the digital forensics landscape in Industry 4.0, 5.0, and edge computing environments. It will identify the key challenges and

opportunities associated with forensic investigations in these settings and propose potential solutions to address them.

This research represents a novel contribution to the field of digital forensics by exploring the application of principles and techniques in the context of Industry 4.0, 5.0, and edge computing. It provides a fresh perspective on the complex challenges and future opportunities for digital forensics' investigations in this landscape of emerging technologies.

The remainder of this paper is organized as follows: Section II presents the literature review related to Industry 4.0, 5.0 and edge computing technologies, section III presents the methodology, section IV presents the discussions and analysis of the systematic review, and section V concludes the paper.

II. LITERATURE SURVEY

The arrival of Industry 4.0 brought many advantages by transforming the way humans connect to each other and to other devices which are enabled by IoT technologies. This has also led to the adoption of so many foreign technologies that generate and process massive data at an incredible speed without the conscious mind of the user of the technology. This has also escalated the rate of cybercrime in the world and opened more tools to create intelligence malwares that can spread much faster due to the high connectivity of devices and data subjects.

There are several studies that have been conducted on digital forensics in Industry 4.0, 5.0 and edge computing environment. These studies focused on the intricate challenges and possible future opportunities regarding digital forensic investigations in this era of emerging technologies.

Industry 4.0 introduces the use of cloud storage for the purpose of fast retrieval and processing, which has introduced massive challenges for digital forensics. Pichan *et al.* [18] conducted a comparative study and presented the technical challenges and the proposed solution to perform forensics in a cloud environment. The cloud environment has many benefits, but there are also rising concerns due to the fragile platform that is fertile for cybercriminals to conduct their criminal activities. In addition to the challenges, the cloud environment also preserves digital clues to keep traces of the committed crimes as presented in [17]-[20]. In many instances, some of the digital evidence is deleted from the local device but traces can be recovered from the cloud environment, and this can also be useful towards successful prosecution in a court of law.

Stoyanova *et al*, [21] presented a survey on forensics of IoT to analyze the challenges, approaches, and open issues. This survey revealed that although IoT has more benefits for digital evidence retrieval, they also present intricate challenges such as end-to-end encryptions on some applications which may cause invasion to privacy, data preservation, and cloud security challenges. The solution to these types of challenges is to develop new frameworks that will accommodate new technologies and legal requirements. There is more research along the lines of cloud forensics such as [14], [22]-[30].

Another pressing challenge is the legal and ethical aspect of conducting digital forensic investigation in Industry 4.0, 5.0 and edge computing environments. This is because cybercrimes know no borders and with these advanced technologies, cybercriminals can exploit technology services from other countries to send malicious files and to defraud people and organizations in another country. This also demands the multi-stakeholder collaboration with other countries which may play part in cross-border jurisdictions investigations. Nguyen *et al.* [31] presented a list of legal challenges encountered in forensic investigation through a Vietnamese case study. Various researchers have also converged on the similar point that IoT forensic has created more legal and ethical concerns than a solution to investigations [15], [32]-[36].

The emergence of Industry 5.0 technologies which incorporate human-centric capability with machines has also brought many production benefits in many industrial setups. Some comparative analysis indicates that Industry 5.0 will be more superior than its predecessor Industry 4.0 and will transform production that what its predecessor did [4], [6]-[8], [37], [38]. The ethical and legal aspects remain a course for concern in digital forensic investigations on such technologies, and this challenge can only be overcome through the development of new frameworks which will include the multi-stakeholder collaboration, the technology component, expertise, cross-border jurisdiction, and the use of edge computing technologies [39]. There are secondary authors who have also raised concerns about possible investigations of the cross-border jurisdiction investigations such as [40]-[43].

In [44], an evaluation of legal issues that surrounds computer forensics was discussed based on the information collected through questionnaires and interviews from professionals within the space of government law enforcement, government regulators, private consulting companies, and academics. They discovered that not all countries have the same legal principles regarding the acquisition of digital evidence. In South Africa, for instance, the cybercrime law came into effect in 2021, and before that it was difficult to pursue cybercrimes and persecute without the relevant legal aspects.

In [45], it was argued that humans are not safe when using these technologies, and they raised the ethical concerns that need to be addressed to ensure that users are aware of the data that they create, consume, share, and process. This is an issue because it can also hamper the success of forensic investigations.

In [3], it was also discussed that digital forensic investigation becomes difficult to carry out in a construction industry setup due to the lack of adoption of these technologies in the construction sector. The lack of this adoption; it was said to be due to the lack of support from politicians and other state organs. Another issue that raises concerns is the heterogeneity of connected systems since they may be running different software that may not be compatible with each other and it may be difficult to extract data in the same way [9].

In [11], edge computing technology was described as a key technology enabler to sustain the digital transition from Industry 4.0 and Industry 5.0 to a circuit economy due to the new benefits of the technology as depicted in Fig. 2.

This work was funded by the Department of Science and Innovation (DSI), South Africa.

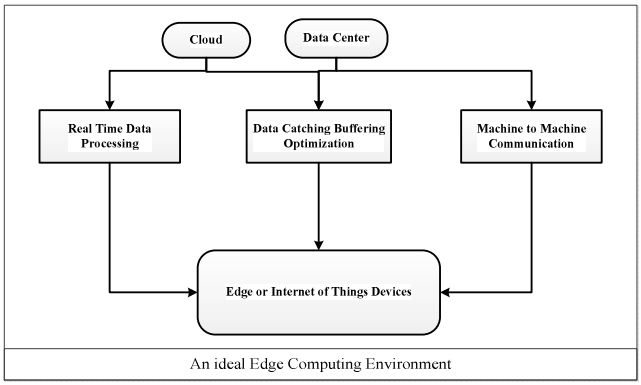

Fig. 2. A figure showing an overview of an ideal edge computing environment.

III. Proposed Methodology

This research has adopted a mixed research methodology which employs a combination of a comprehensive literature review which is relevant to Industry 4.0, 5.0 and edge computing, comparative assessment of technologies and their challenges in conducting digital forensic investigation and the presentation of few case studies.

The combination of comparative analysis and literature survey research helps produce a deeper understanding of similarities and differences in digital forensic practices across Industry 4.0, Industry 5.0, and edge computing. This can inform the development of new frameworks, models, and tools for digital forensics in these emerging technologies based on the captured experiences, perceptions, and some of the challenges presented by digital forensic practitioners and other experts in the digital forensics space.

The resource materials used in this methodology include journal articles and conference papers from IEEE explore, Scopus, and Web of Science. The three indexing libraries were chosen because of their reliability in indexing high-quality peer reviewed journal articles and conference papers.

The process of acquiring these resource materials includes searching in all three databases using the index phrases such as ("Emerging Technologies", "Digital Forensics", "Industry 4.0", "Industry 5.0", "Edge Computing", "Internet of Things", "Artificial Intelligence", "Machine Learning", "Digital Evidence"). There were some papers that included the search phrases, but the content did not discuss the aspect of digital forensics, such papers were not included in the references in this paper. The remaining materials were based on the relevance and applicability of this qualitative systematic review.

The adopted methodology is also informed by the research questions that this study aims to answer which include the following.

- What are the key challenges and opportunities for digital forensic investigations in Industry 4.0, 5.0, and edge computing environments?
- How can traditional digital forensics techniques be adapted and extended to effectively handle the unique characteristics of these technologies?

IV. Discussion and Analysis

The process of digital forensics investigation on industry 4.0 and industry 5.0 technologies in is complex and challenging. However, this is also an essential component of responsive cybersecurity, to safeguard and detect digital clues within an organization. There are several emerging technology trends that make digital forensics investigation in Industry 4.0 and 5.0 more effective, such as the development of new tools and techniques, the increasing use of cloud computing and big data analytics, and the development of international standards and best practices [33], [46]-[54].

This research proposed to answer two significant questions as mentioned in Section III. The first question that entails the key challenges and opportunities for digital forensics investigations in industry 4.0, 5.0, and edge computing environments has been summarized as per the bullet items below.

A. Volume, velocity, and variety of data

Industry 4.0 technologies such as IoT devices and AI systems generate a massive amount of data, which can be difficult to collect and analyze using traditional digital forensic investigation technologies. For example, an IoT-enabled factory may generate millions of data points per day from sensors and other devices. Such data can be in a variety of formats, such as text, images, audio, video, and other data formats. These massive data can be difficult to integrate during digital forensic investigations. A solution to this problem is to employ recent technologies such as AI based and blockchain technologies in digital evidence acquisition and processing. Machine learning technologies can consume huge datasets and process the data in a short space of time. Blockchain technologies can help in maintaining the chain of custody and preserving the integrity of extracted and processed digital evidence.

B. Complexity of Interconnected Systems and devices

Industry 4.0 and 5.0 systems are often complex and interconnected. This means that digital forensics investigators must be able to understand the relationships between different systems and devices to collect all relevant digital evidence. For example, a digital forensics investigator who is investigating a cybercrime incident in an Industry 4.0 factory may need to collect evidence from a variety of sources, such as production systems, IT systems, and security systems. Some of the systems may not be heterogeneous and this may create limitations in terms of the tools that are used to collect digital evidence. The use of a technology expert in this area will be useful in collecting the required information.

C. Need to protect privacy

Digital forensic investigators must be careful to protect the privacy of individuals and organizations when collecting and analyzing digital evidence from Industry 4.0 and 5.0 systems. This is especially important because Industry 4.0 and 5.0 systems often collect and store sensitive data, such as personal

information and trade secrets. Failure to protect such sensitive data can create more problems than solutions in a court of law, as investigators can be sued. One way to preserve the privacy and security of data is to employ blockchain technology which preserves the integrity of data and maintains the chain of custody.

D. Lack of standards and best practices

There is a lack of standards and best practices for digital forensics in Industry 4.0 and 5.0 technologies. This can make it difficult for digital forensics investigators to ensure that their investigations are conducted in a consistent and effective manner. If the investigation is not carried out according to the set standards, policies, and procedures, the digital evidence may not be admissible in a court of law, and the case may not stand. This can be resolved by worldwide collaboration in ensuring that there are common best practices and standards relating to digital forensic investigation especially relating to these emerging technologies.

The second research question talks to how can traditional digital forensics techniques be adapted and extended to effectively handle the unique characteristics of these technologies? This can be done by enhancing existing technologies by incorporating emerging technologies to match existing challenges. Some of the opportunities that can be exploited to equip the existing digital forensic technologies to match the emerging technologies include but are not limited to the following list of emerging fields in Industry 4.0 and 5.0:

- Development of new forensic tools and techniques that can automatically collect, process, and analyze digital evidence for emerging technologies such as the IoT. The new technologies are essential for incorporating emerging technologies such as Blockchain, AI and ML systems, and quantum computing into the existing digital forensic technologies. This may also include the development of a new method to identify and collect all relevant digital evidence from complex and interconnected industry 4.0 and 5.0 systems.
- Studying the impact of new technologies on the digital forensic process. The impact of new technologies on the digital forensic process needs to be studied in more detail. This includes understanding how the new technologies affect the collection, analysis, and presentation of digital evidence. This will include conducting a survey of international digital forensics practitioners to identify key challenges and opportunities in digital forensics for Industry 4.0 and 5.0.
- Development of guidelines and best practices for digital forensics in industry 4.0 and 5.0 environments. Guidelines and best practices for digital forensics in Industry 4.0 and 5.0 environments must be developed and disseminated to the digital forensics community. This should also include the design and implementation of privacy-preserving digital forensics framework for industries 4.0 and 5.0 environments.
- Promoting awareness training of digital forensics among stakeholders in Industry 4.0 and 5.0. Awareness and training in digital forensics need to be promoted among stakeholders in Industry 4.0 and 5.0, such as organizations, system operators and users. This will help ensure that organizations are prepared to respond to digital forensic incidents.

Based on the possible answers to these questions, the article also suggests that a framework for conducting forensic investigations technologies in Industry 4.0, 5.0 and Edge computing environments, as depicted in Fig. *3*, can be very useful. This framework entails the incorporation of other stakeholders into the existing digital forensic frameworks, which will offer several advantages.

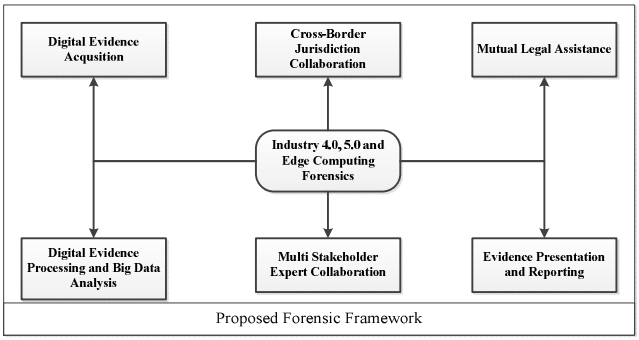

Fig. 3. Figure depicting the proposed forensic investigation framework.

The presented framework offers several advantages over traditional digital forensic frameworks which include but are not limited to:

- Advanced evidence acquisition using edge computing due to its capability to have devices next to the data.
- Advantage data processing using machine learning and AI-powered tools.
- Evidence preservation using blockchain technology ensures that a transaction cannot be easily reversed.
- Multi-stakeholder collaboration which enhances and addresses the issue of cross-border jurisdictions and sharing of digital evidence with other experts beyond the local jurisdiction.

V. Conclusion and Future Work

Digital forensics on technologies in Industry 4.0, 5.0 and edge computing is a complex and challenging field. The challenges of digital forensics in these emerging technologies are complex but are also significant. However, there are several emerging trends and technologies that are making digital forensics in these technologies more productive and effective.

In this article, several challenges have been discussed, and suggestion have been made to adopt emerging technologies and build on existing frameworks to produce well equipped, robust, and effective framework and technologies for digital forensics in the new industrial revolution era.

The authors have also identified several areas for future work in digital forensics on technologies in Industry 4.0 and 5.0 and edge computing. These areas include the development of new tools and techniques for emerging technologies, the study of the impact of new technologies on the digital forensic process, the development of guidelines and best practices for digital forensics in industries 4.0 and 5.0 environments, and the promotion of awareness of digital forensics among industry 4.0.

ACKNOWLEDGMENT

The authors wish to acknowledgment the Department of Science and Innovation (DSI) for their 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] L. Thames and D. Schaefer, "Software-defined Cloud Manufacturing for Industry 4.0," in *Procedia CIRP*, Elsevier B.V., 2016, pp. 12–17. doi: 10.1016/j.procir.2016.07.041.

[3] T. D. Oesterreich and F. Teuteberg, "Understanding the implications of digitisation and automation in the context of Industry 4.0: A triangulation approach and elements of a research agenda for the construction industry," *Computers in Industry*, vol. 83. Elsevier B.V., pp. 121–139, Dec. 01, 2016. doi: 10.1016/j.compind.2016.09.006.

[4] A. Raja Santhi and P. Muthuswamy, "Industry 5.0 or industry 4.0S? Introduction to industry 4.0 and a peek into the prospective industry 5.0 technologies," *International Journal on Interactive Design and Manufacturing*, vol. 17, no. 2, pp. 947–979, Apr. 2023, doi: 10.1007/s12008-023-01217-8.

[5] X. Xu, Y. Lu, B. Vogel-Heuser, and L. Wang, "Industry 4.0 and Industry 5.0—Inception, conception and perception," *J Manuf Syst*, vol. 61, pp. 530–535, Oct. 2021, doi: 10.1016/j.jmsy.2021.10.006.

[6] E. L. Alvarez-Aros and C. A. Bernal-Torres, "Technological competitiveness and emerging technologies in industry 4.0 and industry 5.0," *An Acad Bras Cienc*, vol. 93, no. 1, 2021, doi: 10.1590/0001-3765202120191290.

[7] M. Golovianko, V. Terziyan, V. Branytskyi, and D. Malyk, "Industry 4.0 vs. Industry 5.0: Co-existence, Transition, or a Hybrid," in *Procedia Computer Science*, Elsevier B.V., 2022, pp. 102–113. doi: 10.1016/j.procs.2022.12.206.

[8] A. Cimino, M. Elbasheer, F. Longo, L. Nicoletti, and A. Padovano, "Empowering Field Operators in Manufacturing: a Prospective Towards Industry 5.0," in *Procedia Computer Science*, Elsevier B.V., 2022, pp. 1948–1953. doi: 10.1016/j.procs.2022.12.395.

[9] P. Thakur and V. Kumar Sehgal, "Emerging architecture for heterogeneous smart cyber-physical systems for industry 5.0," *Comput Ind Eng*, vol. 162, Dec. 2021, doi: 10.1016/j.cie.2021.107750.

[10] A. Adel, "Future of industry 5.0 in society: human-centric solutions, challenges and prospective research areas," *Journal of Cloud Computing*, vol. 11, no. 1. Springer Science and Business Media Deutschland GmbH, Dec. 01, 2022. doi: 10.1186/s13677-022-00314-5.

[11] P. Fraga-Lamas, S. I. Lopes, and T. M. Fernández-Caramés, "Green iot and edge AI as key technological enablers for a sustainable digital transition towards a smart circular economy: An industry 5.0 use case," *Sensors*, vol. 21, no. 17, Sep. 2021, doi: 10.3390/s21175745.

[12] 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. 2021. doi: 10.3390/electronics10111229.

[13] A. O. Akinbi, " Digital forensics challenges and readiness for 6G Internet of Things (IoT) networks ," *WIREs Forensic Science*, 2023, doi: 10.1002/wfs2.1496.

[14] 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.

[15] M. M. Losavio, K. P. 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, May 2018, doi: 10.1002/spy2.23.

[16] M. Cook, A. Marnerides, C. Johnson, and D. Pezaros, "A Survey on Industrial Control System Digital Forensics: Challenges, Advances and Future Directions," *IEEE Communications Surveys and Tutorials*, 2023, doi: 10.1109/COMST.2023.3264680.

[17] F. Casino *et al.*, "Research Trends, Challenges, and Emerging Topics in Digital Forensics: A Review of Reviews," *IEEE Access*, vol. 10. Institute of Electrical and Electronics Engineers Inc., pp. 25464–25493, 2022. doi: 10.1109/ACCESS.2022.3154059.

[18] A. Pichan, M. Lazarescu, and S. T. Soh, "Cloud forensics: Technical challenges, solutions and comparative analysis," *Digit Investig*, vol. 13, pp. 38–57, Jun. 2015, doi: 10.1016/j.diin.2015.03.002.

[19] 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.

[20] P. Jain and A. Mahalkari, "Review of Cloud Forensics: Challenges, Solutions and Comparative Analysis," *Int J Comput Appl*, vol. 178, no. 34, 2019, doi: 10.5120/ijca2019919220.

[21] 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," *IEEE Communications Surveys and Tutorials*, vol. 22, no. 2. Institute of Electrical and Electronics Engineers Inc., pp. 1191–1221, Apr. 01, 2020. doi: 10.1109/COMST.2019.2962586.

[22] 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.

[23] M. Herman *et al.*, "NIST cloud computing forensic science challenges," Gaithersburg, MD, Aug. 2020. doi: 10.6028/NIST.IR.8006.

[24] S. Ahmed Ali, S. Memon, and F. Sahito, "Challenges and solutions in cloud forensics," in *ACM International Conference Proceeding Series*, Association for Computing Machinery, Aug. 2018, pp. 6–10. doi: 10.1145/3264560.3264565.

[25] G. Horsman and J. R. Lyle, "Dataset construction challenges for digital forensics," *Forensic Science International: Digital Investigation*, vol. 38, Sep. 2021, doi: 10.1016/j.fsidi.2021.301264.

[26] Institute of Electrical and Electronics Engineers, "Forensics Investigation Challenges in Cloud Computing Environments," in *Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), 2012 International Conference on.*, 2012, pp. 1–5.

[27] O. Akter, A. Akther, M. A. Uddin, and M. Manowarul Islam, "Cloud Forensics: Challenges and Blockchain Based Solutions," *International Journal of Wireless and Microwave Technologies*, vol. 10, no. 5, pp. 1–12, Oct. 2020, doi: 10.5815/ijwmt.2020.05.01.

[28] S. Sonia Akter and M. Shahriar Rahman, "Cloud Forensic: Issues, Challenges and Solution Models," *ArXiv*, pp. 2–23, 2023.

[29] B. Martini and K.-K. Choo, "Cloud Forensic Technical Challenges and Solutions: A Snapshot," *Cloud and The Law Column*, pp. 1–6, 2014.

[30] E. M. Lopez, S. Y. Moon, and J. H. Park, "Scenario-based digital forensics challenges in cloud computing," *Symmetry (Basel)*, vol. 8, no. 10, 2016, doi: 10.3390/sym8100107.

[31] T. Van Nguyen, T. V. Truong, and C. K. Lai, "Legal challenges to combating cybercrime: An approach from Vietnam," *Crime Law Soc Change*, vol. 77, no. 3, pp. 231–252, Apr. 2022, doi: 10.1007/s10611-021-09986-7.

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

[33] A. AboBakr and M. Azer, "IoT Ethics Challenges and Legal Issues," in *2017 12th International Conference on Computer Engineering and Systems (ICCES)*, Cairo: IEEE, Dec. 2017, pp. 1–5.

[34] Z. Sattar, S. Riaz, Shafia, and A. U. Mian, "Challenges of cybercrimes to implementation of legal framework," in *2018 14th International Conference on Emerging Technologies, ICET 2018*, 2019. doi: 10.1109/ICET.2018.8603645.

[35] N. Rawindaran, "Legal Considerations and Ethical Challenges of Artificial Intelligence on Internet of Things and Smart Cities," in *Data Protection in a Post-Pandemic Society*, 2023. doi: 10.1007/978-3-031-34006-2_8.

[36] 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.

[37] K. P. Iyengar *et al.*, "Industry 5.0 technology capabilities in Trauma and Orthopaedics," *J Orthop*, vol. 32, pp. 125–132, Jul. 2022, doi: 10.1016/j.jor.2022.06.001.

[38] P. K. R. Maddikunta *et al.*, "Industry 5.0: A survey on enabling technologies and potential applications," *Journal of Industrial Information Integration*, vol. 26. Elsevier B.V., Mar. 01, 2022. doi: 10.1016/j.jii.2021.100257.

[39] 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.

[40] F. Casino, C. Pina, P. López-Aguilar, E. Batista, A. Solanas, and C. Patsakis, "SoK: cross-border criminal investigations and digital evidence," *Journal of Cybersecurity*, vol. 8, no. 1. Oxford University Press, 2022. doi: 10.1093/cybsec/tyac014.

[41] E. Allegra, R. Di Pietro, M. La Noce, V. Ruocco, and N. V. Verde, "Cross-border co-operation and education in digital investigations: A European perspective," *Digit Investig*, vol. 8, no. 2, pp. 106–113, 2011, doi: 10.1016/j.diin.2011.09.001.

[42] L. C. Díaz-Pérez, A. L. Quintanar-Reséndiz, G. Vázquez-Álvarez, and R. Vázquez-Medina, "A review of cross-border cooperation regulation for digital forensics in LATAM from the soft systems methodology," *Applied Computing and Informatics*, 2022, doi: 10.1108/ACI-01-2022-0010.

[43] P. Olber, "The survey on cross-border collection of digital evidence by representatives from Polish prosecutors' offices and judicial authorities," *Journal of Digital Forensics, Security and Law*, vol. 16, no. 2, Sep. 2021, doi: 10.58940/1558-7223.1700.

[44] A. Brungs and R. Jamieson, "Identification of legal issues for computer forensics," *Information Systems Management*, vol. 22, no. 2, pp. 57–66, 2005, doi: 10.1201/1078/45099.22.2.20050301/87278.7.

[45] M. El-Khoury and C. L. Arikan, "From the internet of things toward the internet of bodies: Ethical and legal considerations," *Strategic Change*, vol. 30, no. 3, pp. 307–314, May 2021, doi: 10.1002/jsc.2411.

[46] 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.

[47] D. Quick and K. K. R. Choo, "IoT Device Forensics and Data Reduction," *IEEE Access*, vol. 6, pp. 47566–47574, Aug. 2018, doi: 10.1109/ACCESS.2018.2867466.

[48] 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.

[49] 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.

[50] 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.

[51] 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.

[52] A. Karale, "The Challenges of IoT Addressing Security, Ethics, Privacy, and Laws," *Internet of Things (Netherlands)*, vol. 15. Elsevier B.V., Sep. 01, 2021. doi: 10.1016/j.iot.2021.100420.

[53] S. M. Muzamma and R. K. Murugesan, "A study on Leveraging Blockchain Technology for IoT Security Enhancement.," in *2018 Fourth International Conference on Advances in Computing, Communication & Automation (ICACCA) : proceedings* , Malaysia: IEEE, Oct. 2018, pp. 1–6.

[54] 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.