Universal Privacy Model for Electronic Health Record Systems

Subjects: Health Policy & Services

Contributor: Raza Nowrozy, Khandakar Ahmed, Hua Wang, Timothy Mcintosh

High-profile data breaches in systems such as Australia's My Health Record (MHR) and the UK's National Health Service (NHS) have exposed millions of records, resulting in substantial financial losses for the healthcare industry.

Keywords: privacy ; privacy policy ; ontology ; health information privacy ; machine learning

1. Introduction

The growing adoption of Electronic Health Records (EHRs) has led to a significant increase in privacy and security concerns [1][2][3][4][5]. Despite the implementation of numerous privacy and security measures, patients' privacy continues to be compromised, often due to unreliable information-sharing methods and inadequate privacy policies [1][6][7][8][9][10]. High-profile data breaches in systems such as Australia's My Health Record (MHR) and the UK's National Health Service (NHS) have exposed millions of records, resulting in substantial financial losses for the healthcare industry [11]. Additionally, the expanding use of Machine Learning in healthcare for diagnostics, drug discovery, and precision medicine intensifies these concerns [12][13]. To achieve high accuracy, ML models often need to rely on analyzing vast amounts of patient data, including sensitive genetic and clinical information [14][15]. The prevalent application of ML in healthcare underscores the need to address the ethical, legal, and privacy challenges associated with implementing artificially intelligent systems (AIS) such as ML, deep learning, and Natural Language Processing (NLP) algorithms.

Context-sensitive privacy policies play a vital role in ensuring that privacy settings and access controls are meticulously adapted to the specific circumstances surrounding data [16][17][18]. For example, sensitive health information may necessitate more stringent privacy controls compared to less critical data [19]. Numerous privacy policies, such as the Health Insurance Portability and Accountability Act (HIPAA), General Data Protection Regulation (GDPR), and other privacy acts, regulations, and principles [20][21], have been established to address both local and global contexts. However, despite these local and international privacy policies, existing EHR systems have experienced privacy breaches, diminishing trust in health-related IT systems [18]. Many users have opted out of systems such as Australia's MHR system. These privacy standards tend to be generic, highlighting the need for a novel privacy model that better protects patients' privacy in EHR settings.

Current strategies to safeguard EHRs involve systems that emphasize confidentiality, authentication, integrity, trust, verification, and authorization [22][23]. Intrusion Detection Systems (IDS) have been suggested to detect and categorize suspicious activities and security breaches [22][23]. However, these systems might still be vulnerable due to outdated repositories and potential alterations in patient data caused by malware or unauthorized access [24]. Privacy-preserving ML frameworks have been proposed as potential solutions, using techniques such as homomorphic encryption, secure multiparty computation, and differential privacy to protect sensitive patient information while preserving analytical accuracy [25][26]. Despite these advancements, there remains a need for more robust and comprehensive solutions to safeguard health information. As a result, additional research is necessary to address this gap, focusing on a secure and privacy-preserving health data-sharing framework within the EHR sector that considers all relevant stakeholders and ensures patients' privacy.

2. Personally-Controlled EHR Systems

Personal Electronic Health Record (PCEHR) systems enable individuals to manage their health information and control access. However, this also requires individuals to safeguard their data. Privacy is a crucial factor in sensitive sectors such as healthcare, and non-compliance can lead to substantial penalties. Regrettably, many large health information systems still display privacy issues and identification risks for users due to inadequate implementation of legal requirements [27][28]. Various proposals (e.g., [29][30]) have been presented to address privacy concerns in personal health records, but they

frequently lack empirical evidence and real-world testing, and failed to address potential ethical and legal concerns of implementing such systems [31]. Likewise, a proposed privacy-preserving personal health record (P3HR) system lacked a comprehensive evaluation of security and performance [32], while a proposed Hippocratic database approach did not furnish empirical evidence or case studies to support its efficacy [33]. One essential aspect to consider when developing personally controlled EHR systems is striking a balance between privacy and accessibility [34]. It is critical to safeguard patients' health information privacy while ensuring that authorized healthcare providers can access the information they need to deliver effective care. Another important factor when developing personally controlled EHR systems is ensuring they are user-friendly and accessible to all patients [35][36], regardless of age, education, or technological literacy. This is challenging due to the complex nature of health information and the variety of devices and platforms used to access EHR systems. Mamum et al. [37] proposed a homomorphic encryption approach to encrypt patients' information. The decryption key will be used by the patient, ensuring no other person can access their information without prior authorization. To enhance reliability and privacy, a cryptographic verification technique is introduced to ensure that only the authorized person has access to corresponding records [38].

Privacy is a vital factor in sectors such as healthcare, banking, and defense, where confidential and sensitive data must be protected from unauthorized parties [39]. Numerous legislative rules and regulations have been introduced in European countries to ensure citizens' privacy [39][40]. Global data protection standards have been established, which outline specific data protection requirements and non-compliance penalties. According to Baker [27], patient care involves providing relevant care for individual patients based on their preferences, needs, and values, and ensuring good clinical decisions are made. This patient care includes involving, informing, and listening to patients. Due to recent digital transformations in healthcare sectors and associated data and privacy breaches, rebuilding trust in health-related IT systems has become an urgent challenge.

While personally controlled EHR systems have the potential to enhance privacy and patient empowerment in healthcare, several challenges must be addressed to ensure their effectiveness and acceptability. These challenges include balancing privacy and accessibility, making EHR systems more user-friendly and accessible, and acknowledging the cultural and social context of EHR system development and implementation. Overcoming these challenges will require further research, collaboration, and innovation among healthcare providers, researchers, and technology developers.

3. Ensuring Privacy through Smart Contract—Healthcare Blockchain Systems

Blockchain-based EHR systems are increasingly gaining recognition for their potential to enhance security and privacy in managing health data. By leveraging distributed ledger technology, these systems can effectively prevent unauthorized access and data breaches. However, challenges still need to be addressed when implementing blockchain systems in healthcare, particularly when sharing patient information with multiple stakeholders.

Recent studies have explored the use of blockchain technology to improve security and privacy in healthcare IT systems. In [41], the authors proposed a consortium blockchain for secure and privacy-preserving data sharing in e-health systems. Although their study provided an in-depth description of the proposed architecture and its benefits, it lacked empirical evidence and real-world evaluations, and did not discuss potential limitations or challenges associated with implementing such a system. In [42], the study examined the applications of blockchain distributed ledger technologies in biomedical and healthcare settings [42]. While the authors thoroughly reviewed existing literature and proposed various use cases, the study was published in 2017, and blockchain technology has evolved significantly since then. Moreover, the authors did not address potential drawbacks or limitations of using blockchain in healthcare settings. In [43], the authors focused on the potential of blockchain technology for improving security and privacy of healthcare data stored in the cloud. The authors provided a comprehensive overview of the challenges and explained how blockchain could address them. However, the article did not critically evaluate the technology's limitations and challenges, such as scalability and interoperability issues. In [44], the authors proposed a blockchain-based incentive mechanism for privacy-preserving crowd-sensing applications. Despite presenting an interesting idea, the paper lacked sufficient detail on technical implementation and evaluation and did not compare the proposed mechanism to existing solutions or discuss limitations or future work. In [45], the authors introduced a blockchain-based solution called Medblock for efficient and secure sharing of medical data. The authors claimed that their system could overcome traditional centralized data storage limitations but they did not provide a comprehensive evaluation of the proposed system's scalability and efficiency or detailed information about its implementation. Finally, in [46], the authors proposed a healthcare blockchain system using smart contracts for secure automated remote patient monitoring. While the authors presented a detailed description of the proposed system and a theoretical analysis of its security and privacy features, they lacked empirical evidence to support the system's

feasibility and effectiveness and did not address potential challenges in implementing the system in a real-world healthcare setting.

While blockchain-based EHR systems can offer significant benefits in terms of security and privacy, there are still challenges and limitations to be addressed, especially when sharing patient data with multiple stakeholders. Further research, validation, and critical analysis are needed to ensure the practicality, scalability, and effectiveness of these systems in real-world healthcare scenarios.

4. Context-Sensitive Privacy Policies

In recent years, there has been a growing interest in context-sensitive approaches within the EHR domain. In [47], the paper presented a context-aware access control model for cloud-based data resources, incorporating imprecise context information. The authors utilized fuzzy logic to model the uncertainty in context information and developed a context-aware access control framework. However, the paper did not comprehensively evaluate of the proposed model, including comparative analysis with other state-of-the-art approaches, scalability, and performance testing. Additionally, there was no mention of any practical implementation of the proposed framework in real-world settings. While the proposed approach seemed promising, the lack of evaluation and practical implementation made it difficult to assess its effectiveness and feasibility. In [48], the article introduced a policy model and framework for context-aware access control to information resources. Their model integrated contextual factors such as user identity, location, and time to determine access privileges. However, it lacked empirical validation of the proposed framework, leaving its effectiveness in real-world scenarios uncertain. Moreover, the article did not address potential ethical implications of context-aware access control, such as privacy and discrimination concerns. Further research and analysis are required to address these issues. In [49], the article proposed a fog-based context-aware access control (CAC) system to achieve security scalability and flexibility. The authors argued that their system could enhance security in fog computing environments by providing dynamic and context-aware access control. The article offered a comprehensive overview of the proposed CAC system and discussed its implementation details. However, the article lacked empirical evaluation of the proposed system's performance and scalability. Additionally, it did not address the potential challenges and limitations of implementing such a system in real-world scenarios. Overall, the proposed system appeared promising, but further research is necessary to validate its effectiveness and practicality. In [50], the paper suggested an ontology-based approach for dynamic contextual role-based access control in pervasive computing environments. The authors described the architecture of the proposed system and evaluated its effectiveness through simulations. Nevertheless, the evaluation of the system was limited to simulations, and a real-world implementation and evaluation of the approach would be advantageous. Additionally, the paper could benefit from a more in-depth discussion of related work in the field of contextual role-based access control.

To summarize, while these context-sensitive approaches have made strides in proposing enhanced protection for EHRs, they have proven insufficient for accurately modeling relevant stakeholders and health information.

5. Homomorphic Encryption in EHR Systems

The role of homomorphic encryption in preserving the privacy of EHRs has been explored in various studies, which have claimed that the approach offers computation on encrypted data without necessitating decryption, effectively facilitating secure data sharing and collaboration. Paul et al. [51] constructed a privacy-preserving framework, leveraging homomorphic encryption for protecting EHRs during collaborative machine learning processes. Although the proposed framework held potential, the study did not sufficiently address the framework's limitations, including potential vulnerabilities of the encryption scheme, scalability, and maintaining confidentiality during collective learning. Ikuomola et al. [52] addressed privacy concerns in e-health clouds using homomorphic encryption and access control. However, the research was marked by the absence of a detailed analysis of the solution's effectiveness. Furthermore, potential vulnerabilities or attacks that could undermine the security of the proposed system, and scalability issues related to large-scale e-health cloud environments were not adequately addressed. Vengadapurvaja et al. [53] developed an efficient homomorphic medical image encryption algorithm for secure medical image storage in the cloud. Despite its focus on medical images, the approach did not extend to the encryption of other types of EHR data. This narrow scope limited its comprehensive application to broader EHR privacy concerns. Alzubi et al. [54] integrated homomorphic encryption with deep neural networks to secure the transmission and diagnosis of medical data. However, unspecified inadequacies were identified in preserving the privacy of EHR. A thorough examination of the study would provide a better understanding of these limitations. Subramaniyaswamy et al. [55] implemented a somewhat homomorphic encryption scheme for IoT sensor signal-based edge devices. However, without detailed insights from the paper, it is difficult to identify specific inadequacies in preserving EHR privacy. Potential challenges could include scalability, performance, or vulnerability of the implemented scheme when applied to real-world EHR systems. Finally, Vamsi et al. [56] investigated various homomorphic encryption

schemes for securing EHR in the cloud environment. Despite potential benefits, several inadequacies were noted in the application of homomorphic encryption for preserving EHR privacy. Challenges, such as the performance overhead of homomorphic encryption, integration difficulties with existing healthcare systems, and the need for efficient key management strategies, were some identified concerns.

While various studies have explored the role of homomorphic encryption in preserving the privacy of EHR, each presents certain inadequacies. Key among these are the vulnerability of the encryption schemes employed, limitations in scalability, difficulties in maintaining the confidentiality of sensitive data, and the substantial computational overhead that their encryption techniques have introduced. Furthermore, a narrow focus on specific data types, such as medical images, excludes comprehensive coverage of EHR privacy concerns. Challenges in integrating homomorphic encryption schemes into existing healthcare systems, including issues of interoperability, data access control, and key management strategies, further compound the problem.

References

1. Wang, H.; Song, Y. Secure cloud-based ehr system using attribute- based cryptosystem and blockchain. J. Med. Syst. 2018, 42, 152.
2. Dagher, G.G.; Mohler, J.; Milojkovic, M.; Marella, P.B. Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology. Sustain. Cities Soc. 2018, 39, 283–297.
3. Bani Issa, W.; Al Akour, I.; Ibrahim, A.; Almarzouqi, A.; Abbas, S.; Hisham, F.; Griffiths, J. Privacy, confidentiality, security and patient safety concerns about electronic health records. Int. Nurs. Rev. 2020, 67, 218–230.
4. Keshta, I.; Odeh, A. Security and privacy of electronic health records: Concerns and challenges. Egypt. Inform. J. 2021, 22, 177–183.
5. Ozair, F.F.; Jamshed, N.; Sharma, A.; Aggarwal, P. Ethical issues in electronic health records: A general overview. Perspect. Clin. Res. 2015, 6, 73.
6. Zaghloul, E.; Li, T.; Ren, J. Security and privacy of electronic health records: Decentralized and hierarchical data sharing using smart contracts. In Proceedings of the 2019 International Conference on Computing, Networking and Communications (ICNC), Honolulu, HI, USA, 18–21 February 2019; pp. 375–379.
7. Akarca, D.; Xiu, P.; Ebbitt, D.; Mustafa, B.; Al-Ramadhani, H.; Albey-Atti, A. Blockchain secured electronic health records: Patient rights, privacy and cybersecurity. In Proceedings of the 2019 10th International Conference on Dependable Systems, Services and Technologies (DESSERT), Leeds, UK, 5–7 June 2019; pp. 108–111.
8. Omar, A.H.A. The Effect of Electronic Health Records on Undergraduate and Postgraduate Medical Education: A Scoping Review; University of Toronto: Toronto, ON, Canada, 2019.
9. Rezaeibagha, F.; Mu, Y. Distributed clinical data sharing via dynamic access-control policy transformation. Int. J. Med. Inform. 2016, 89, 25–31.
10. Farhadi, M.; Haddad, H.; Shahriar, H. Static analysis of hippa security requirements in electronic health record applications. In Proceedings of the 2018 IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC), Tokyo, Japan, 23–27 June 2018; Volume 2, pp. 474–479.
11. Vimalachandran, P.; Zhang, Y.; Cao, J.; Sun, L.; Yong, J. Preserving data privacy and security in australian my health record system: A quality health care implication. In Proceedings of the International Conference on Web Information Systems Engineering, Dubai, United Arab Emirates, 12–15 November 2018; pp. 111–120.
12. Budd, J.; Miller, B.S.; Manning, E.M.; Lampos, V.; Zhuang, M.; Edelstein, M.; Rees, G.; Emery, V.C.; Stevens, M.M.; Keegan, N.; et al. Digital technologies in the public-health response to COVID-19. Nat. Med. 2020, 26, 1183–1192.
13. Mooney, S.J.; Pejaver, V. Big data in public health: Terminology, machine learning, and privacy. Annu. Rev. Public Health 2018, 39, 95–112.
14. Ahmed, Z. Practicing precision medicine with intelligently integrative clinical and multi-omics Data Analysis. Hum. Genom. 2020, 14, 35.
15. Kumaar, M.; Samiayya, D.; Vincent, P.M.; Srinivasan, K.; Chang, C.Y.; Ganesh, H. A hybrid framework for intrusion detection in healthcare systems using Deep Learning. Front. Public Health 2021, 9, 824898.
16. Alagar, V.; Alsaig, A.; Ormandjiva, O.; Wan, K. Context-based security and privacy for healthcare IoT. In Proceedings of the 2018 IEEE International Conference on Smart Internet of Things (SmartIoT), Xi'an, China, 17–19 August 2018; pp. 122–128.

17. Demuro, P.R.; Petersen, C. Managing privacy and data sharing through the use of health care information fiduciaries. In Context Sensitive Health Informatics: Sustainability in Dynamic Ecosystems; IOS Press: Amsterdam, The Netherlands, 2019; pp. 157–162.
18. Kisekka, V.; Giboney, J.S. The effectiveness of health care information technologies: Evaluation of trust, security beliefs, and privacy as determinants of health care outcomes. J. Med. Internet Res. 2018, 20, e9014.
19. Rieke, N.; Hancox, J.; Li, W.; Milletari, F.; Roth, H.R.; Albarqouni, S.; Bakas, S.; Galtier, M.N.; Landman, B.A.; Maier-Hein, K.; et al. The future of digital health with federated learning. NPJ Digit. Med. 2020, 3, 119.
20. Kruse, C.S.; Smith, B.; Vanderlinden, H.; Nealand, A. Security techniques for the electronic health records. J. Med. Syst. 2017, 41, 127.
21. Otlowski, M.F.A. Disclosing genetic information to at-risk relatives: New Australian privacy principles, but uniformity still elusive. Med. J. Aust. 2015, 202, 335–337.
22. Ahmed, Z.; Mohamed, K.; Zeeshan, S.; Dong, X.Q. Artificial Intelligence with multi-functional machine learning platform development for better healthcare and Precision Medicine. Database 2020, 2020, baaa010.
23. Chen, M.; Decary, M. Artificial Intelligence in healthcare: An essential guide for health leaders. Healthc. Manag. Forum 2019, 33, 10–18.
24. Koczkodaj, W.W.; Mazurek, M.; Strzałka, D.; Wolny-Dominiak, A.; Woodbury-Smith, M. Electronic health record breaches as social indicators. Soc. Indic. Res. 2019, 141, 861–871.
25. Abramson, W.; Hall, A.J.; Papadopoulos, P.; Pitropakis, N.; Buchanan, W.J. A distributed trust framework for privacy-preserving machine learning. In Trust, Privacy and Security in Digital Business; Springer: Cham, Switzerland, 2020; pp. 205–220.
26. Islam, T.U.; Ghasemi, R.; Mohammed, N. Privacy-preserving federated learning model for healthcare data. In Proceedings of the 2022 IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 26–29 January 2022.
27. Baker, A. Crossing the quality chasm: A new health system for the 21st century. BMJ Clin. Res. 2001, 323, 1192.
28. Olive, M.; Rahmouni, H.B.; Solomonides, T.; Breton, V.; Legré, Y.; Blanquer, I.; Hernández, V.; Andoulsi, I.; Herveg, J.A.M.; Wilson, P. Share roadmap 1: Towards a debate. Stud. Health Technol. Inform. 2007, 126, 164–173.
29. Li, M.; Yu, S.; Ren, K.; Lou, W. Securing personal health records in cloud computing: Patient-centric and fine-grained data access control in multi-owner settings. In Proceedings of the International Conference on Security and Privacy in Communication Systems, Singapore, 7–9 September 2010; pp. 89–106.
30. Caine, K.; Hanania, R. Patients want granular privacy control over health information in electronic medical records. J. Am. Med. Inform. Assoc. 2013, 20, 7–15.
31. Abouelmehdi, K.; Beni-Hessane, A.; Khaloufi, H. Big healthcare data: Preserving security and privacy. J. Big Data 2018, 5, 1.
32. Sun, W.; Cai, Z.; Li, Y.; Liu, F.; Fang, S.; Wang, G. Security and privacy in the medical internet of things: A review. Secur. Commun. Netw. 2018, 2018, 5978636.
33. Johnson, C.M.; Grandison, T. Compliance with data protection laws using hippocratic database active enforcement and auditing. IBM Syst. J. 2007, 46, 255–264.
34. Fernández-Alemán, J.L.; Señor, I.C.; Lozoya, P.Á.O.; Toval, A. Security and privacy in electronic health records: A systematic literature review. J. Biomed. Inform. 2013, 46, 541–562.
35. Eze, E.; Gleasure, R.; Heavin, C. Mobile health solutions in developing countries: A stakeholder perspective. Health Syst. 2020, 9, 179–201.
36. Peute, L.W.; Wildenbos, G.A.; Engelsma, T.; Lesselroth, B.J.; Lichtner, V.; Monkman, H.; Neal, D.; Van Velsen, L.; Jaspers, M.W.; Marcilly, R. Overcoming Challenges to Inclusive User-based Testing of Health Information Technology with Vulnerable Older Adults: Recommendations from a Human Factors Engineering Expert Inquiry. Yearb. Med. Inform. 2022, 31, 74–81.
37. Mamun, Q. A conceptual framework of personally controlled electronic health record (pcehr) system to enhance security and privacy. In Proceedings of the International Conference on Applications and Techniques in Cyber Security and Intelligence, Barcelona, Spain, 12–16 November 2017; pp. 304–314.
38. Samet, S.; Ishraque, M.T.; Sharma, A. Privacy-preserving personal health record (p3hr) a secure android application. In Proceedings of the 7th International Conference on Software and Information Engineering, Cairo, Egypt, 2–4 May 2018.

39. Wachter, S. The GDPR and the Internet of Things: A three-step transparency model. Law Innov. Technol. 2018, 10, 266–294.
40. Cavoukian, A. Privacy by design: The definitive workshop. A foreword by Ann Cavoukian, Ph. D. Identity Inf. Soc. 2010, 3, 247–251.
41. Zhang, A.; Lin, X. Towards secure and privacy-preserving data shar- ing in e-health systems via consortium blockchain. J. Med. Syst. 2018, 42, 140.
42. Kuo, T.T.; Kim, H.E.; Ohno-Machado, L. Blockchain distributed ledger technologies for biomedical and health care applications. J. Am. Med. Inform. Assoc. 2017, 24, 1211–1220.
43. Esposito, C.; Santis, A.; Tortora, G.; Chang, H.; Choo, K.K.R. Blockchain: A panacea for healthcare cloud-based data security and privacy? IEEE Cloud Comput. 2018, 5, 31–37.
44. Wang, J.; Li, M.; He, Y.; Li, H.; Xiao, K.; Wang, C. A blockchain based privacy-preserving incentive mechanism in crowdsensing applications. IEEE Access 2018, 6, 17545–17556.
45. Fan, K.; Wang, S.; Ren, Y.; Li, H.; Yang, Y. Medblock: Efficient and secure medical data sharing via blockchain. J. Med. Syst. 2018, 42, 136.
46. Griggs, K.N.; Ossipova, O.; Kohlios, C.P.; Baccarini, A.N.; Howson, E.A.; Hayajneh, T. Healthcare blockchain system using smart contracts for secure automated remote patient monitoring. J. Med. Syst. 2018, 42, 130.
47. Kayes, A.; Rahayu, W.; Dillon, T.; Chang, E.; Han, J. Context-aware access control with imprecise context characterization for cloud-based data resources. Future Gener. Comput. Syst. 2019, 93, 237–255.
48. Kayes, A.; Han, J.; Rahayu, W.; Dillon, T.; Islam, M.S.; Colman, A. A policy model and framework for context-aware access control to information resources. Comput. J. 2019, 62, 670–705.
49. Kayes, A.; Rahayu, W.; Watters, P.; Alazab, M.; Dillon, T.; Chang, E. Achieving security scalability and flexibility using fog-based context-aware access control. Future Gener. Comput. Syst. 2020, 107, 307–323.
50. Kayes, A.; Rahayu, W.; Dillon, T. An ontology-based approach to dynamic contextual role for pervasive access control. In Proceedings of the 2018 IEEE 32nd International Conference on Advanced Information Networking and Applications (AINA), Krakow, Poland, 16–18 May 2018; pp. 601–608.
51. Paul, J.; Annamalai, M.S.M.S.; Ming, W.; Al Badawi, A.; Veeravalli, B.; Aung, K.M.M. Privacy-preserving collective learning with homomorphic encryption. IEEE Access 2021, 9, 132084–132096.
52. Ikuomola, A.J.; Arowolo, O.O. Securing patient privacy in e-health cloud using homomorphic encryption and access control. Int. J. Comput. Netw. Commun. Secur. 2014, 2, 15–21.
53. Vengadapurvaja, A.; Nisha, G.; Aarthy, R.; Sasikaladevi, N. An efficient homomorphic medical image encryption algorithm for cloud storage security. Procedia Comput. Sci. 2017, 115, 643–650.
54. Alzubi, J.A.; Alzubi, O.A.; Beseiso, M.; Budati, A.K.; Shankar, K. Optimal multiple key-based homomorphic encryption with deep neural networks to secure medical data transmission and diagnosis. Expert Syst. 2022, 39, e12879.
55. Subramaniyaswamy, V.; Jagadeeswari, V.; Indragandhi, V.; Jhaveri, R.H.; Vijayakumar, V.; Kotecha, K.; Ravi, L. Somewhat homomorphic encryption: Ring learning with error algorithm for faster encryption of iot sensor signal-based edge devices. Secur. Commun. Netw. 2022, 2022, 2793998.
56. Vamsi, D.; Reddy, P. Electronic health record security in cloud: Medical data protection using homomorphic encryption schemes. In Research Anthology on Securing Medical Systems and Records; IGI Global: Hershey, PA, USA, 2022; pp. 853–877.