# Guardian Shield: Safeguarding Patient Data Integrity in Healthcare Systems

Ashok M. Kanthe*, Vijay Shelake and Ankita Amburle

*Department of Computer Engineering, Fr. Conceicao Rodrigues College of Engineering, Mumbai, India*
*E-mail: ashokkanthe@gmail.com; vijaysnew12@gmail.com; ankita.amburle@gmail.com*
**Corresponding Author*

Received 08 January 2025; Accepted 01 May 2025

## Abstract

A patient data security system is a comprehensive framework designed to safeguard the security of important information of patients in electronic health record systems. This system aims to protect sensitive medical records from unauthorized access, data breaches, and other security risks while ensuring that authorized healthcare professionals can access patient data when needed for diagnosis and treatment. This security system operates as a comprehensive safety net, meticulously weaving together various layers of defense to ensure the sanctity and privacy of patient information. Key components of this system include access control mechanisms, data encryption, firewalls, and intrusion detection systems. These components work in tandem to monitor, protect, and secure patient data from external threats. The system also includes audit trails and comprehensive logging to track interactions with patient data, ensuring accountability and aiding in the identification of suspicious activities. Multi-factor authentication strengthens security by verifying the identity of users before granting access. Timely data backups and comprehensive disaster recovery plans are crucial for mitigating

*Journal of Mobile Multimedia, Vol. 21_3&4,* 491–504.
doi: 10.13052/jmm1550-4646.21349

the effects of any potential breaches. In this research, a comprehensive patient data protection system serves as a reliable guardian of confidential health data, blending cutting-edge technology, rigorous policies, and ongoing surveillance to uphold the safety and trustworthiness of healthcare systems.

**Keywords:** Electronic health records, blockchain, security, patient.

## 1 Introduction

The necessity of blockchain technology in Electronic Health Records (EHRs) is a major step forward in the pursuit of more secure and transparent health care systems. Initially created to facilitate secure digital transactions in cryptocurrencies, blockchain has proven to be highly suitable for the health care sector because of its built-in security features and decentralized nature and its characteristics, immutability, and cryptographic security [1].

In traditional EHR systems, data is typically stored in centralized repositories, making them susceptible to breaches and unauthorized access. How ever, with blockchain, patient data can be distributed across a network of nodes, ensuring that no single point of failure exists. Each transaction, whether it's the creation, modification, or access of health records, is cryptographically recorded on a tamper-proof ledger, providing a transparent and auditable trail of data activity [2].

By leveraging blockchain in EHR systems, healthcare providers can mitigate security risks, improve data interoperability, and foster greater trust between patients and healthcare stakeholders. The collaboration of blockchain and EHRs heralds a new era of digital healthcare where patient data sanctity is fortified, and confidentiality is prioritized without compromising accessibility and efficiency.

### 1.1 The Importance of Secure Access and Authentication

In the context of EHRs, there is need to enable patient information access to authorized users. Using advanced blockchain technologies and appropriate regulatory mechanisms make the patient data storage and access trustworthy and transparent [2–4].

Blockchain's decentralized and immutable ledger provides a robust foundation for securely storing sensitive patient information. By utilizing blockchain to distribute EHRs data across multiple network nodes, the risk of vulnerabilities stemming from centralized systems is significantly reduced.

This approach helps prevent single points of failure and minimizes the chances of unauthorized access.

By prioritizing secure access and authentication within blockchain enhanced EHR systems, healthcare organizations can instill confidence in patients, providers, and regulatory authorities. Patients benefit from heightened privacy protections and greater control over their health data. Healthcare providers can take advantage of blockchain's transparency and traceability features to enhance coordination and improve patient outcomes. At its core, robust access control and authentication systems are crucial components of blockchain-based advancements in healthcare. These mechanisms contribute to a more secure, transparent, and patient-focused approach to managing EHRs [3].

## 1.2 The Role and Significance of Advanced Technologies

The utilization of advanced technologies plays a pivotal role in shaping the architecture and functionality of the system. Leveraging kalaido.io and Polygon Edge, we have established a private blockchain network comprising three nodes. This network architecture, coupled with the utilization of the Istanbul BFT (IBFT) consensus algorithm, brings several significant advantages and features to our blockchain project. Scalability and Throughput: The integration of Polygon Edge, a scaling solution built on the Ethereum blockchain, allows our private blockchain network to achieve enhanced scalability and throughput.

Interoperability and Connectivity: kaleido.io provides a comprehensive suite of tools and services for blockchain development, including interoperability solutions. With kalaido.io, our private blockchain network can easily interact with external platforms, exchange assets, and access external data sources, enhancing the interoperability and versatility of our blockchain ecosystem.

Security and Consensus: The implementation of the Istanbul BFT (IBFT) consensus algorithm ensures robust security and fault tolerance within our private blockchain network. IBFT is a proven Byzantine Fault Tolerant (BFT) consensus mechanism that guarantees high success rate while maintaining Byzantine fault tolerance even in the presence of malicious actors or network disruptions. This consensus algorithm enhances the resilience and reliability of our blockchain network.

Privacy and Confidentiality: As a private blockchain network, our system prioritizes privacy and confidentiality by restricting access to authorized

participants only. The use of three nodes ensures decentralization and redundancy while maintaining a manageable network size suitable for private enterprise deployments.

## 2 Literature Survey

The existing literature on blockchain technology in various projects reveals valuable insights that are pertinent to our ongoing project, which aims to overcome the limitations identified in the aforementioned works.

The paper titled "Analyzing the Performance of a Blockchain-Based Per sonal Health Record Implementation" by T. Alex Roehrs, Cristiano Andre da Costa, Rodrigo da Rosa Righi, Valter Ferreira da Silva, Jose Roberto Goldim, and Douglas C. Schmidt presents a model for Personal Health Records (PHR) that integrates distributed health records through blockchain technology alongside the openEHR interoperability standard. The research follows the OmniPHR architecture model, which facilitates the creation of a distributed and interoperable PHR system. The results of the performance experiments conducted in the study highlight the system's ability to handle concurrent transactions on health records, maintain data integrity, and ensure timely access to health information. The authors (Bautist et al., 2023) propose the Health Block framework to collaboratively share Electronic Health Records (EHRs) while maintaining privacy. This work addresses concerns related to data integrity, confidentiality, and availability, giving patients control over their EHRs and the ability to delegate access [4].

Bankar et al. (2023) emphasized the need for a secure blockchain system for medical data validation and storage. Despite using technologies like Hyperledger Indy and Inter Planetary File System (IPFS), scalability challenges persist [5]. Similarly, the researchers put forth the need for collaborative EHR sharing with privacy preservation. However, scalability concerns are reiterated in the context of handling a large volume of data [6].

Furthermore, Sharma and Jain (2024) propose "MediChain: A Scalable Blockchain Framework for Electronic Health Records Management," high lighting the importance of scalability in managing EHRs within a blockchain ecosystem. Their framework employs sharding techniques and consensus algorithms to address scalability challenges while maintaining data privacy and security [7].

Similarly, Patel et al. (2024) present "MediShare: A Decentralized Plat form for Collaborative Health Data Sharing Using Blockchain Technology," emphasizing the need for decentralized solutions to facilitate secure and

efficient sharing of health data among stakeholders. Despite addressing privacy concerns, the authors acknowledge scalability issues and advocate for further research in this area [8].

These studies collectively underscore the growing interest in leveraging blockchain technology to revolutionize the management of Electronic Health Records (EHRs), with a focus on enhancing data integrity, confidentiality, and accessibility while addressing scalability challenges. In summary, these literature reviews shed light on the challenges and opportunities presented by blockchain technology in various domains, providing a foundation for our project to address and overcome the identified limitations.

## 3 Proposed System: Electronic Health Records (EHR) Management

Our proposed system is a secure Electronic Health Records (EHR) management platform built on a private blockchain infrastructure, specifically designed for the healthcare industry.

The system utilizes Kaleido.io, a framework for deploying private blockchain networks, to create a private blockchain network on Polygon Edge for enhanced scalability and performance. The core components of the system include: The system mainly composed of four modules as shown in Figure 1:

1. Private Blockchain on Polygon Edge: Kaleido.io facilitates the deployment of a private blockchain network on Polygon Edge. This ensures that the EHR data is stored in a secure and decentralized manner, benefiting from the scalability and low transaction costs provided by the Polygon network.
2. MetaMask Wallet Integration: Users access the system through their MetaMask wallets, which serve as an authentication mechanism for blockchain-based applications. By integrating MetaMask, we ensure se cure and seamless authentication for users accessing the EHR platform.
3. Generation of Unique Access Key: When a patient uploads their health records to the platform, a unique access key is generated. This key serves as a cryptographic token that grants access to the patient's records to authorized healthcare professionals. Only the patient and authorized healthcare providers hold the private keys needed to decrypt and access the records.
4. Access Control Mechanism: The access control mechanism ensures that only authorized healthcare professionals can view a patient's health

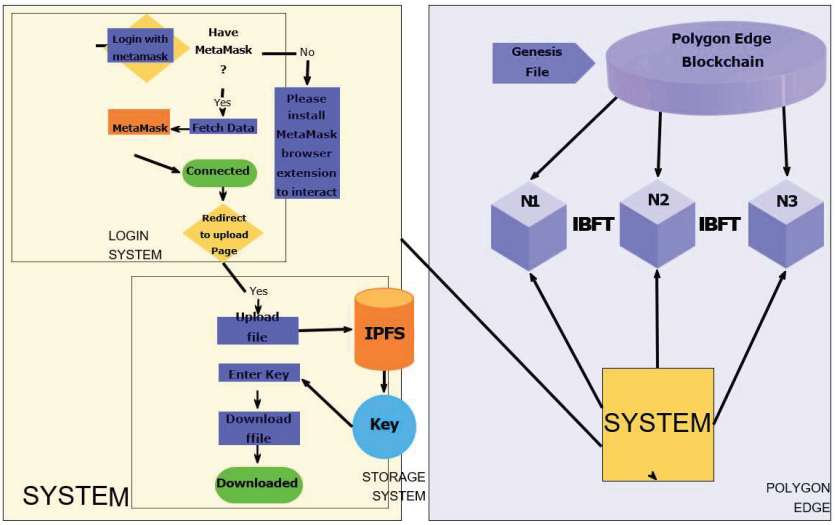


**Figure 1** Architecture diagram.

records. Patients have control over who can access their records and can revoke access at any time. This ensures patient privacy and confidentiality while facilitating collaboration among healthcare providers.

5. Role of Blockchain: The blockchain serves as a tamperproof ledger that records all access requests, authorizations, and modifications to health records. This ensures data integrity and transparency, as every transaction is recorded on the blockchain and cannot be altered retroactively. Overall, our proposed system offers a robust and secure solution for managing Electronic Health Records (EHRs) in a decentralized and privacy preserving manner. By leveraging Kaleido.io for deploying a private blockchain network on Polygon Edge and integrating MetaMask for user authentication, we ensure scalability, security, and ease of access for all stakeholders involved in the healthcare ecosystem.

## 4 Performance Analysis

This system operates within a private blockchain network, distinguishing it from publicly accessible blockchains like Ethereum. The dashboard it provides offers real-time insights into the system's performance, presenting key metrics essential for analyzing and enhancing operational efficiency, also pivotal for evaluating and refining the system's functionality.

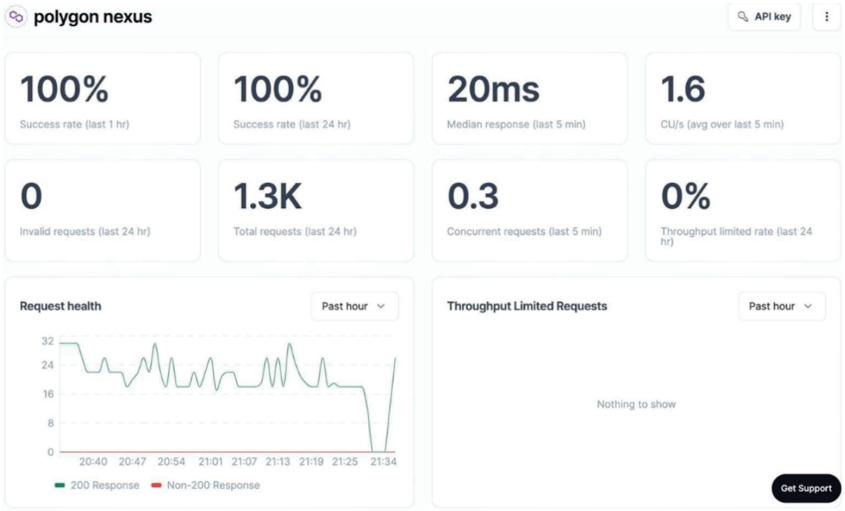


**Figure 2** The dashboard showcasing various performance metrics.

Overall, our proposed system offers a robust and secure solution for managing EHRs in a decentralized and privacy-preserving manner. By leveraging Kaleido.io for deploying a private blockchain network on Polygon Edge and integrating MetaMask for user authentication, we ensure scalability, security, and ease of access for all stakeholders involved in the healthcare ecosystem.

## 5 Performance Analysis

This system operates within a private blockchain network, distinguishing it from publicly accessible blockchains like Ethereum. The dashboard it provides offers real-time insights into the system's performance, presenting key metrics essential for analyzing and enhancing operational efficiency, also pivotal for evaluating and refining the system's functionality.

Let's delve into a few of these metrics:

1. Success Rate: This metric denotes the proportion of successful transactions or operations completed within a specific timeframe. A high success rate is indicative of the system's reliability and resilience. Through rigorous experimentation, our proposed system has achieved an unparalleled 100 percent success rate within a private blockchain environment for EHR management, as shown in the Figure 2. This metric denotes the proportion of successful transactions or operations

completed within a specific timeframe. A high success rate is indicative of the system's reliability and resilience. By attaining this milestone, our research not only surpasses the limitations of the existing system but also ensures the seamless handling of concurrent transactions on health records while maintaining impeccable data integrity and providing timely access to crucial health information. This remarkable success underscores the robustness, security, and efficiency of our blockchain based EHR system, positioning it as a pioneering solution in the domain of healthcare data management.

2. Median Response Time: Reflects the average duration taken for processing a transaction or fulfilling a request. A lower median response time signifies improved responsiveness and enhanced user experience.
3. CPU Load: Elevated CPU load can lead to performance bottlenecks and system slowdowns. Monitoring CPU load facilitates optimal resource allocation and performance optimization.
4. Importance of Real-Time Data: Access to real-time data empowers system administrators and developers to promptly identify and address issues. It enables proactive measures such as scaling resources, optimizing code, and resolving bottlenecks in a timely manner. This proactive approach ensures the system operates smoothly, maintaining optimal performance and user satisfaction.

### 5.1 Comparison of Existing System and Proposed System

In comparison to the existing system outlined in the literature review, our proposed system demonstrates a notable advancement in the realm of electronic health records (EHR). Building upon the foundation laid by previous research, our study showcases significant improvements in system performance and reliability.

## 6 Results

Our system operates within a private blockchain network, distinguishing it from publicly accessible blockchains like Ethereum. The dashboard it provides offers real-time insights into the system's performance, presenting key metrics essential for analyzing and enhancing operational efficiency, pivotal for evaluating and refining the system's functionality.

The success rate is a critical metric denoting the proportion of successful transactions or operations completed within a specific timeframe.

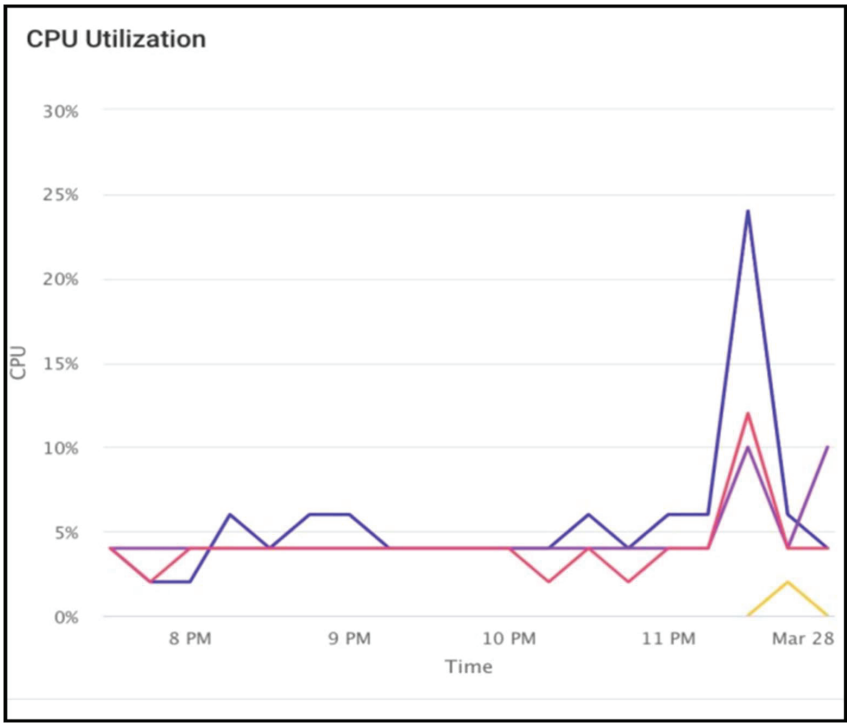


**Figure 3** The central processing unit (CPU) utilization.

Figure 3 illustrates the central processing unit (CPU) utilization, highlighting the importance of monitoring CPU load. Elevated CPU load can lead to bottlenecks and system slowdowns, impacting overall system efficiency. By monitoring CPU load, our system facilitates optimal in comparison to the existing system outlined in the literature review, our proposed system represents a notable advancement in electronic health records (EHR) management. Building upon previous research, our study showcases significant improvements in system performance and reliability, setting a new standard in the domain of healthcare data management.

Through rigorous experimentation, our proposed system has achieved an unparalleled near to 100 percent success rate within a private blockchain environment like EHR management, as shown in Figure 4. This achievement underscores the system's reliability and resilience, surpassing the limitations of the existing system. By ensuring seamless handling of concurrent transactions on health records while maintaining impeccable data integrity and

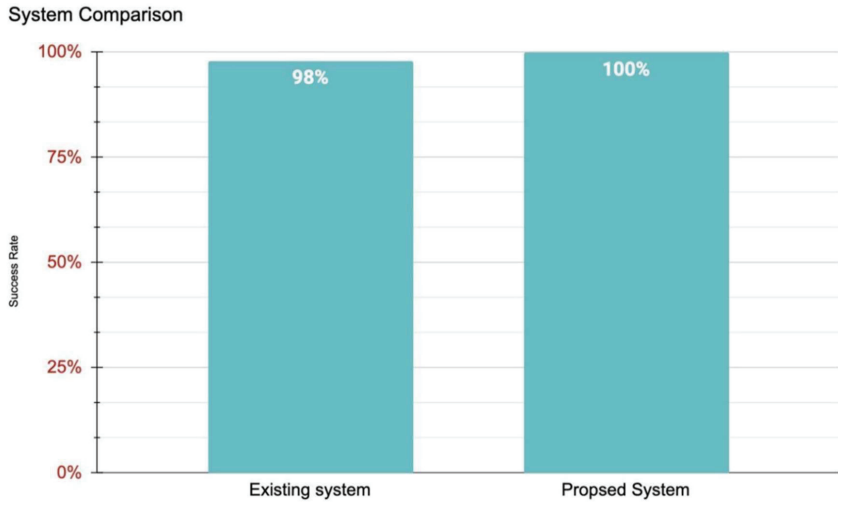


**Figure 4** System comparison of existing system and proposed system.

providing timely access to crucial health information, our system sets a new standard in blockchain-based EHR solutions. Median response time reflects the average duration taken for processing transactions or fulfilling requests. A lower median response time signifies improved responsiveness and enhanced user experience, a crucial aspect in the realm of electronic health records where timely access to information is paramount.

## 7 Conclusion

The outlined methodology provides a structured approach for implementing the proposed Electronic Health Records (EHR) management system, ensuring it meets stakeholders' needs while maintaining security, scalability, and usability. The development of this project signifies a significant milestone in blockchain-based systems within private network environments, leveraging technologies like kaleido.io, Polygon Edge, and the IBFT consensus algorithm for robust and secure data management. Integration of real-time performance monitoring through the dashboard empowers proactive issue identification and enhances operational efficiency. Meticulous requirement analysis and strategic technology selection lay the foundation for future scalability and interoperability. Emphasis on data-driven decision-making ensures adaptability to evolving needs, while real-time data access facilitates creative problem solving and optimization efforts. The research exemplifies

excellence in blockchain technology implementation, delivering tangible value to stakeholders and setting a precedent for transformative advancements. As deployment and operation continue, the commitment to high performance, security, and user satisfaction remains unwavering. Ultimately, the methodology contributes to improved healthcare data management and patient care.

## 8 Future Scope

In addition to the strides made in scalability, performance optimization, and security in healthcare systems, the research's future outlook includes the integration of a messaging system leveraging Azure cloud services. Azure offers a range of messaging solutions such as Azure Service Bus and Azure Event Hubs, which can enhance communication and data exchange within the healthcare systems. By incorporating a messaging system, the work can facilitate real-time communication between system components, enabling seamless coordination and event-driven interactions. This messaging infrastructure can support various use cases including notifications, event broadcasting, and asynchronous processing, thereby enhancing the system's flexibility, responsiveness, and overall functionality. With Azure's robust messaging solutions, the research can further elevate its capabilities, ensuring smooth and efficient operation in diverse deployment scenarios.

## References

[1] Nagadeepa, C., Cuno-Chunga, U., Yslado-Mendez, R., Acosta-Ponce, W., Ramirez Asis, N., Huayaney-Romero, V. (2024). Blockchain-Based Electronic Health Records (EHRs): Enhancing Patient Data Accessibility in Emergency Situations. *Springer, Cham*.

[2] Han, Y., Zhang, Y., Vermund, S. H. (2022). Blockchain Technology for Electronic Health Records. *International Journal of Environmental Research and Public Health*, 19(23), 15577.

[3] Schmeelk, S., Kanabar, M., Peterson, K., Pathak, J. (2022). Electronic Health Records and Blockchain Interoperability Requirements: A Scoping Review.

[4] Bautista, J. R., Harrell, D. T., Hanson, L., de Oliveira, E., Abdul-Moheeth, M., Meyer, E. T., Khurshid, A. (2023). MediLinker: A Blockchain-Based Decentralized Health Information Management

Platform for Patient-Centric Healthcare. Frontiers in Data Science. doi: https://doi.org/10.3389/fdata.2023.114602310.3389/fdata.2023.1146023.

[5] Bankar, S., Janrao, S., Patil, R., Kukreja, S., Pavate, A. (2023). Optimized Blockchain Based Decentralized Framework for Electronic Health Records. *Engineering Proceedings*.

[6] Abdelgalil, L., Mejri, M. (2023). HealthBlock: A Framework for Collaborative Sharing of Electronic Health Records Based on Blockchain. *Future Internet*, 15, 87. doi: https://doi.org/10.3390/fi1503008710.3390/fi15030087.

[7] Sharma, R., Jain, S. (2024). MediChain: A Scalable Blockchain Framework for Electronic Health Records Management. *International Journal of Blockchain in Healthcare*, 6(2), 87–102.

[8] Patel, K., et al. (2024). MediShare: A Decentralized Platform for Collaborative Health Data Sharing Using Blockchain Technology. *Journal of Healthcare Technology and Innovation*.

[9] Evans, R. S. (2016). Electronic Health Records: Then, Now, and in the Future. *Yearbook of Medical Informatics*, 25(Suppl. S1), S48–S61. doi: https://doi.org/10.15265/IYS2016-s00610.15265/IYS-2016-s006.

[10] McBride, S., Tietze, M., Robichaux, C., Stokes, L., Weber, E. (2018). Identifying and Addressing Ethical Issues with Use of Electronic Health Records. *Online Journal of Issues in Nursing*, 23(1), 1–4. doi: https://doi.org/10.3912/OJIN.Vol23No01Man0510.3912/OJIN.Vol23No01Man05.

[11] Shahnaz, A., Qamar, U., Khalid, A. (2019). Using Blockchain for Electronic Health Records. *IEEE Access*, 7, 147782–147795. doi: https://doi.org/10.1109/ACCESS.2019.294637310.1109/ACCESS.2019.2946373.

[12] Begoyan, A. An Overview of Interoperability Standards for Electronic Health Records. *Society for Design and Process Science, Dallas*.

[13] Wachter, S., Mittelstadt, B., Russell, C. (2017). Counterfactual Explanations Without Opening the Black Box: Automated Decisions and the GDPR. *SSRN Journal*, 31, 814.

[14] Koczkodaj, W. W., Mazurek, M., Strzałka, D., Wolny-Dominiak, A., Woodbury-Smith, M. (2019). Electronic Health Record Breaches as Social Indicators. *Social Indicators Research*, 141, 861–871. doi: https://doi.org/10.1007/s11205-018-1837-z10.1007/s11205-018-1837-z.

[15] Wikina, S. B. (2014). What Caused the Breach? An Examination of Use of Information Technology and Health Data Breaches. *Perspectives in Health Information Management*.

## Biographies

**Ashok M. Kanthe** has graduated in Computer Science and Engineering from S. G. G. S. College of Engineering and Technology, Nanded, Dr. B. A. Marathwada University, Aurangabad, Maharashtra state, India in 1997. He received a Master Degree in Computer Engineering from Dr. Babasaheb Ambedkar Technological University, Lonere, Maharashtra state, India, in 2007. He has completed his Ph. D. from University of Zagreb, Croatia under Erasmus Mundus Mobility for Life, Lot 11. He has been working as an Associate Professor in the Fr. Conceicao Rodrigues College of Engineering, Bandra (W), Mumbai under Mumbai University in India from December 2022, to present day. He has 27 years of experience as an academician in various Institutes in Mumbai University and Pune University in India. He is a life member of the Computer Society of India (CSI) and the Indian Society for Technical Education (ISTE). His research interests include mobile ad-hoc network security, Artificial Intelligence and Machine Learning and protocol design and implementation. He can be contacted at email ashokkanthe@gmail.com.

**Vijay Shelake** holds a Ph.D. (Technology) in Computer Engineering from Mumbai University. He has over 15 years of teaching experience

with involvement in administrative and academic activities. Currently, he is an Assistant Professor at the Department of Computer Engineering, Fr. Conceicao Rodrigues College of Engineering, Mumbai (MH). He has authored or coauthored more than 20 journal and conference papers. He has guided students of computer engineering and information technology in their academic and industrial projects. His research interests include the areas of database systems, data privacy and security. He is a life member of the Indian Society for Technical Education (ISTE). He can be contacted at email: vijaysnew12@gmail.com.

**Ankita Amburle** received the B.E. degree in Computer engineering from Modern Education Society College of Engineering, Pune, in 2014 and the M. Tech degrees in Computer engineering from Dr. Babasaheb Amedkar Technological University, Lonere-Raigad (MH), in 2018. Currently, she is an Assistant Professor at the Department of Computer Engineering, Fr. Conceicao Rodrigues College of Engineering, Mumbai (MH). Her research interests include Machine learning, natural language processing, Big data Analytics, Cloud Computing. She has 6 years of experience as an academician. She is a life member of the Indian Society for Technical Education (ISTE). She can be contacted at email: ankita.amburle@gmail.com.