Indonesian Journal of Electrical Engineering and Computer Science
Vol. 32, No. 3, December 2023, pp. 1746~1754
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v32.i3.pp1746-1754

Patient data management using blockchain technology

Vijaykumar Bidve[1], Kiran Kakade[2], Pakiriswamy Sarasu[3], Shailesh Kediya[4], Pradip Tamkhade[5], Suprakash Sudarsanan Nair[6]
[1]School of Computer Science and Information Technology, Symbiosis Skills and Professional University, Pune, India
[2]Lala Lajpatrai Institute of Management, University of Mumbai, Mumbai, India
[3]Department of Computer Science and Engineering, Kalasalingam Academy of Research and Education, Srivilliputhur, India
[4]School of Logistics and Supply Chain Management, Symbiosis Skills and Professional University, Pune, India
[5]Department of Mechanical Engineering, Marathwada Mitra Mandal's College of Engineering, Pune, India
[6]Department of Information Technology, Kalasalingam Academy of Research and Education, Srivilliputhur, India

Article Info

Article history:

Received Sep 5, 2023
Revised Sep 27, 2023
Accepted Oct 4, 2023

Keywords:

Blockchain
Decentralized
Healthcare
Interoperability
Patient data

ABSTRACT

The patient data management is an essential component of healthcare systems, the secure and efficient data processing is important for the medical data. Data security, interoperability and privacy are the key requirements of data storage systems of healthcare organizations. The electronic medical records have become a key technique to maintain patient information in hospitals due to the technology revolution. Some hospital systems are also using server-based patient detail management systems, they require considerable storage to record all of the patient's medical reports, limiting scalability. They are facing difficulties, including interoperability, security and privacy worries, cyberattacks on centralized storage, and maintaining medical policy compliance simultaneously. The blockchain technology has come up with solution having decentralized and irreversible data storage. A distributed secure ledger of blockchain is the solution, enabling safe storage and retrieval of data. The proposed work yields effectively deployed smart contracts based on the system's functions, real-time patient health monitoring. The main goal of this system is to bring the whole medical data together on a single platform, employing a secured decentralized approach to store and retrieve medical information effectively.

Corresponding Author:

Vijaykumar Bidve
School of Computer Science and Information Technology, Symbiosis Skills and Professional University
Kiwale, Pune, India
Email: vijay.bidve@gmail.com

1. INTRODUCTION

Currently, many hospitals use manual processes to handle and maintain critical data of the patients. In current systems data repositories are spread out across the organization and also the data is in the form of lots of papers. Incomplete or management-standards-incompatible information is commonly presented. The forms get lost while being moved between the departments. Thus, a comprehensive monitoring is required to ensure that no important documents are lost. Numerous copies of the same data are maintained, which results in data discrepancies. Currently, the user has to browse through multiple files to learn about the patient's history, making it difficult to remember and retrieve essential information. This results in inconvenience and wastage of time. Properly maintaining the information generated by numerous transactions takes time and effort. Since changing specific information, including patient information or a child's vaccination history, needs documentation, it might be difficult. Manual process require much work and are prone to error, which might lead to erroneous findings. This method gets difficult since obtaining information from numerous registers is difficult.

Blockchain technology has a potential to address various issues of healthcare domain including security, interoperability, privacy of data. The capabilities of blockchain technology can be utilized in enhancing healthcare data management [1], [2]. Patient data management which includes the data collection, storage, sharing patient data across healthcare practitioners is a crucial component of healthcare [3], [4]. Despite of improvements in health information exchange (HIE) and electronic health records (EHR) systems, the conventional centralized approach has resulted in data silos, security flaws, and lack of data interoperability [5], [6]. As blockchain equipped with features like decentralization, distributed ledger, it has capabilities to provide privacy, security, and openness of patient data.

The blockchain based patient data management system includes registering patients, maintaining the information in system, and automating laboratory and pharmacy invoicing [7]. The patient is provided with unique ID, the staff and patient data is automatically recorded. The user can use the ID to check doctor's and patient's information. The username and password are essential for each user to access blockchain based patient data management system. The hospital staff is also able to access data, add patient information to the system. The data processing in the system is quick as the data adequately safeguarded for authorised users only. The blockchain based patient data management system is explicitly created for multispecialty hospitals where multiple administrative and managerial activities are needed to be handled [8], [9]. A smooth flow of information is provided across the hospital to assist administration, decision making regarding patient. The fundamental activities of hospital can be managed effectively through the blockchain based patient data management system [10], [11].

The blockchain technology was initially developed for virtual currencies like Bitcoin, has now moved beyond its financial root and proved efficient for various other sectors like healthcare management. Blockchain is decentralized, immutable digital ledger to record transactions, monitoring assets inside network. Blockchain constitutes blocks including a set of data, timestamp, and a cryptographic hash. Hash creates a distinct figure for each block linking it to previous block, ensuring integrity of data. The chain in the blocks refers to the link between blocks which produces continues succession of data series. These blocks run on decentralized network called as nodes, whereas in the conventional networks the control of network is at a single point. In blockchain no need of centralized control, there is more openness and less chances of data tampering and illegal access. The timestamp imbedded in each block is used to enhance security of each block. The timestamp confirms existence of certain data in particular time period [12], [13].

After considering all the capabilities of the blockchain technology and requirements of the healthcare industry, authors decided to develop a system for patient data management using blockchain. The work focuses to enable healthcare users to have at most secured data and better control over the patient data. The study aims to highlight the potential for the users to manage patient information securely and with ease of use, transaction effectiveness, and data security. In the proposed system data collection, representation is done with the help of front-end of the application. Use of blockchain ensures that the sensitive information of patient is accessible to only the authorized users of the system.

The subsequent paper is organized in three sections. The second section contains methodology including literature review and technology used for the implementation of the system. The next section contains the results showing the outcome and ways to interact with the system. The last section gives conclusion of the work.

2. METHOD

The patient data management using blockchain is a topic of interest for many researchers. In this paper many articles are reviewed in the domain of blockchain data management, this section conducts a detailed literature review related to the applications of blockchain in healthcare data management. Mainly the work related to the patient data management using blockchain is targeted for the literature review.

Westphal and Seitz [14] examined application of blockchain technology in healthcare beyond the hypothetical concept. They conducted in-depth analysis of critical articles by categorizing them into three main primary use cases in the form of blockchain applications in healthcare. The study demonstrates growing significance of securely storing and accessing medical data. Study shows that blockchain technology guiding principles are increasingly relevant to create safe, dependable solutions for healthcare data. It also states that the hybrid system combining conventional data storage with blockchain are more efficient and cost effective than a fully blockchain data storage systems. Additionally, the author suggested automated blockchain based smart contracts for the tasks like tracking of patient data.

Bharath *et al.* [15] described that, the traditional way of maintaining patient records in medical industry is challenging and needs more memory to store it. The data stored in the form of databases is more structured and difficult to share with third party users. Authors stated that the blockchain based EHR are the more efficient way of storing health information. Blockchain is best technique to restore public confidence in the medical industry, it resolves the majority of problems related with patient data storage and retrieval.

Blockchain offers a trustworthy mechanism for exchanging patient data in a quicker and more effective way. With EHR, the time and effort required to manage patient data may be considerably reduced while achieving effective and efficient results.

Dimitrov[16] listed the advantages of blockchain in comparison with conventional healthcare database management solutions. The first advantage is decentralized administration without supervision of central management intermediary. Second, blockchain offers immutable blocks to preserve important information. Third, it provides data provenance which can be used to manage digital asset, such as patient consent. The data can only be altered by owner using cryptographic techniques. Forth, blockchain guarantees the reliability and accessibility of data. Fifth, the data is in encrypted form and can only be decoded using patients private key. There is no practical method for unauthorised users to read the data even if the network has been compromised.

Hovorushchenko *et al.* [17] described the need of blockchain based method for medical data management systems. The blockchain based system have an ability to analyse and quantify medical data for sufficiency. The required information can be added and retrieved to and from the blockchain system. The system has a choice for users to add patient's data to blockchain and release the data from blockchain in response of doctor's request. The authors developed methods to evaluate, test, validate and to check feasibility of medical data. The transactions on the medical data are simple and have sufficiency with the help of blockchain technology.

Faruk *et al.* [18] discussed that, the blockchain technology was created to address difficulties with traditional databases and other associated challenges that people were having. The research covered development of blockchain technology and a general review of software engineering. It shows that, an Ethereum based systems can store patient data in a safe and immutable blockchain network. The prototypes enable the system to add, update, and retrieve EHR data in a RESTful application programming interfaces (API) environment.

Azaria *et al.* [19] explored that, the blockchain technology's built-in security characteristics are one of its main advantages for managing patient data. Once data is recorded, it cannot be readily changed or tampered with due to blockchain's decentralized and immutable nature. This property is essential for safeguarding patient records' confidentiality and avoiding illegal access. Authors highlighted blockchain's cryptographic tools used to improve patient data security, lowering the risk of data breaches and medical identity theft.

Ekblaw *et al.* [20] stated that, the essential feature of blockchain is its ability to enable seamless and safe data sharing across various healthcare stakeholders. Data fragmentation among many providers and systems is a common problem for traditional healthcare systems. Establishing an integrated and uniform patient record accessible to authorized parties is possible with the help of blockchain's distributed ledger. The authors introduced a blockchain based system named MedRec. This system aims to increase data exchange and interoperability across healthcare providers and increases patient's authority over their records. Liang *et al.* [21] described that use of blockchain to build a decentralized infrastructure for exchanging clinical trial data, assuring parties may have confidence in one other. Authors argue that blockchain is able to facilitate the smooth interchange of patient data between healthcare stakeholders while upholding data integrity and patient consent.

Zhang *et al.* [22] discussed blockchain technology integration into healthcare systems and its hurdles. These include problems with scalability, energy use, regulatory compliance, and the requirement for standardization. These issues are discussed in along with potential solutions, and it is critical to strike a balance between decentralization and scalability.

Ichikawa *et al.* [23] stated that, the blockchain systems gives people more control over their health data. Individuals own their medical records that are recorded on the blockchain. To improve data exchange while maintaining patient autonomy, patients can allow certain healthcare providers access. Promotes the notion of "self-sovereign identity," by providing patients with the control of their medical data.

Mettler [24] described that, the healthcare data cannot be processed in real time due to the scalability of public blockchains and the resource-intensive nature of consensus processes. To handle the enormous transaction volume in healthcare applications authors underlined the necessity for scalability solutions. Regulatory and legal frameworks must also be formed to address concerns with responsibility, data ownership, and adherence to data protection rules.

Mandl *et al.* [25] created an EHR management system based on blockchain that provide control of self-data to the patients. Blockchain technology is used by the eHealth Foundation of the Estonian Government to protect patient data and preserve audit trails. These examples demonstrate practical attempts to use blockchain technology in healthcare systems. With blockchain technology, people may better manage their health information. Patients can allow access to certain medical records, ensuring that only those who need to see their private information. This patient-centred strategy improves patient privacy and helps patients and healthcare professionals develop a relationship of trust.

Kuo *et al.* [26] explored how blockchain technology might help people control their health data and select who has access to it, resulting in a more patient-driven healthcare environment. There are clear advantages of using blockchain technology in healthcare, there are also difficulties. Concerns that practitioners and researchers need to work on scalability, data protection laws, system integration, and energy usage.

Literature survey leads to the conclusion that, the conventional methods of management and maintenance of vital information in hospitals are time consuming and not efficient. Information is frequently incomplete or does not adhere to management standards. In the existing literature, authors mainly reviewed blockchain based systems but none of the system have explain the implementation in details. Also, none of the paper could explain the technical details of how the smart contracts are built, security and integrity of patient data is maintained. Hence, the authors have proposed the solution to manage patient data using blockchain technology with the help of keenly developed smart contracts and achieved data encryption using SHA-256 algorithm. The works proves its novelty in the way the smart contracts are developed and encryption is achieved with the help of SHA-256 algorithm. The SHA-256 uses hasing technique for data encryption; the authors have used the algorithm as it is for encryption. The smart contracts developed in this work are adequate and unique for effective working of the data management system. In the literature none of the researcher have provided implementation details of smart contracts for effective working. In this work the smart contracts are developed mainly for access control, ownership transfer, constructor initialization, event transparency, function modifiers, input validation, gas limitations, and testing for effective working of the blockchain based system. Additionally, this work provides transaction data encryption with the help of SHA-256 algorithm. It means, this work proves its uniqueness by providing combination of keen smart contracts for trasactions and data encryption for security. Hence, the proposed system is more effective than the work available in the literature. To improve transaction effectiveness by providing data security is the key motive of this work.

This system is designed to keep track of patient information, doctor information, and hospital information. These services are delivered in a timely and cost-effective manner, with the goal of minimizing the amount of time and resources currently required for such tasks and have a secured system. Figure 1 shows the architecture of patient data management system.

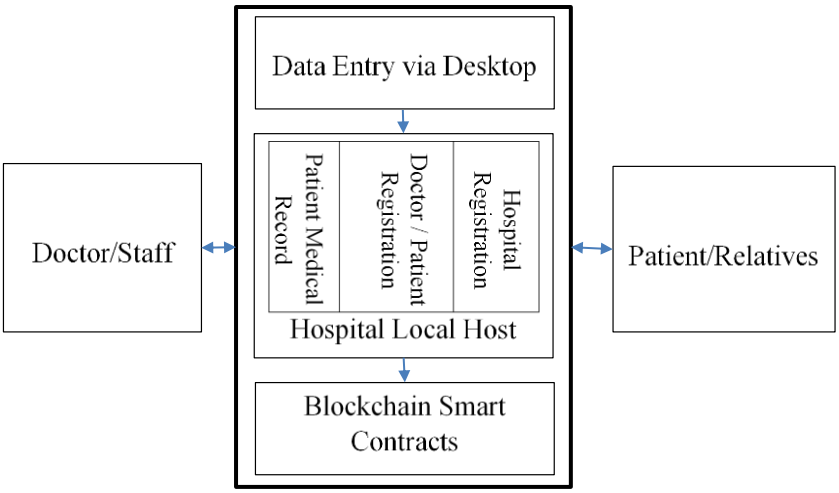

Figure 1. Architecture of patient data management system

The blockchain architecture consist of multiple components which makes blockchain unique in order to function and interact with each other. The important components of blockchain are ethereum virtual machine (EVM), minor blocks, transaction, consensus algorithm, account, and smart contract. The blockchain network contains multiple blocks including miners and few nodes do not mine but works for running the smart contracts and transactions. These nodes are called EVMs. Every node is connected to another node of network and each miner keeps record of instance of ledger. A ledger contains all blocks in the chain and EVMs hosts smart contracts which helps for business functionality.

The smart contracts are designed to provide the exact bundle of features that are needed by the primary objectives of the application to be achieved. They are minimalistic in that they provide the user of the application with just enough features to allow them to track required records. The smart contracts are central to the application's functioning and offer various methods, implementing the bare logic of how data management system function, keeping up with the perspective and specificity of patient data. The

administrative methods and operations are combined that offer rights to the users that interact with patient data management system. The ownership of this contract is transferred immediately to the initiator of the transaction. These contracts establish the foundation of the entire logic of the idea of a patient data management system. It includes functionalities that allow the admin to invite users to the chain and subsequently lets the users interact with various objects of the system. The contract is the final piece of the puzzle that provides the synchronization that is required in a patient data management system. This contract would reveal the system as follows:

- Hospital registration: the contract allows users to enter doctors' details. Only the designated owner (contract creator) can initiate registration process.
- Doctors registration: the authorized users can enter doctors' details and do the registration.
- Patient registration: the authorized users can enter patients details and do the registration.
- View patients details: presents patient details to users.
- View medical record: the contract supports access of patient's medical history.
- View patient examine details: the contract provides all examined details of the patient to the authenticated users of the system.

The smart contracts empower a streamlined and effective patient data management system. Through the deployment contract, new instances of the core contract are established, facilitating the management of users and their respective functions. Users are assigned specific roles, and they can interact with the system, creating and accessing information. Ownership and access control mechanisms are enforced using a foundational contract, ensuring that only authorized individuals can exercise critical operations. By synergistically combining these contracts, a robust and dynamic patient data management system infrastructure emerges, promoting secure and transparent interactions among the users and the system. The provided smart contracts have some security measures in place. Here's an overview of the security measures implemented in the form of smart contracts.

Access control: the ownable contract implements access control by defining the onlyOwner and onlyTxOrigin modifiers. These modifiers ensure that only the contract owner or the original initiator of a call can access certain functions. This has been done to have a role-based access control (RBAC) system for finer-grained control. This allows different roles to perform specific actions, reducing the risk of unauthorized access.

Ownership transfer: is a critical security feature. The contracts include functions like (_transferOwnership and _transferOwnershipFromOrigin) to transfer ownership securely, emitting an event to record the change. Constructor initialization: the contracts properly initialize key variables and parameters in their constructors, reducing the risk of uninitialized variables. Events for transparency: events are emitted for important actions, providing transparency and allowing external parties to monitor contract activities. Function modifiers: modifiers are used to enforce access control and reduce code duplication, which can help prevent unauthorized actions. Input validation: input validation checks have been added to ensure that function parameters meet expected criteria. For example, validation of addresses, string lengths, and numerical values to prevent invalid inputs.

Gas limitations: gas limits have been carefully considered in implementation of smart contracts to prevent functions from consuming excessive gas and becoming unresponsive. Gas limitations have been implemented keeping in mind the following things: prevention of denial-of-service (DoS) attacks, fair resource allocation for efficient use of the network's resources, discourage spam transactions prevent infinite loops, reduce contract vulnerabilities, predictable execution, network stability, resource management.

Testing and test coverage: the smart contracts have been thoroughly tested using automated testing frameworks like mocha against all major functionalities and different cases. High test coverage is kept in mind to identify and fix issues. Use of the latest solidity version: the solidity compiler is kept up-to-date to benefit from the latest security enhancements and improvements.

3. RESULTS AND DISCUSSION

The development team first provide a design for the user interface, wireframe the layout and navigation, and then begin developing the interface using ReactJS and Tailwind CSS. This is how the frontend of a project is built utilizing the sprint approach. Each sprint, the team concentrate on a certain set of features and strive to improve and refine them, such as user registration. The development team first generate a thorough specification for each contract, then use a tool like remix or truffle to write and test the code. This is how the development team builds the blockchain smart contracts for a project. The team concentrate on enhancing and perfecting a particular set of contracts during each sprint. After the contracts are complete, they may be launched on a test network like ganache to evaluate their performance and functionality.

Authors developed an application with the help of programming languages like HTML, PHP, JavaScript and MySQL database. Different access rights are provided to the different users like patients, doctors, and hospital staff. The various forms are created to collect information of doctors, patient, and patient's medical record is generated by the system as shown in Figures 2 and 3. The Figure 2 shows a form used to register and retrieve doctors' details to and from the system. The Figure 3 is used to register and retrieve patients' details to and from the system. Similar forms are created for the other operations like view patient details, view medical record and to view examine details of the patient.

Figure 2. Doctor registration form

By leveraging the frontend's capabilities, users can interact with the blockchain based system efficiently and effortlessly. The frontend's ability to extract, structure, and present essential information from the complex blockchain logs enhances the user experience, making it easier for both authorized users and customers to access pertinent details. The authorization-based system ensures that sensitive information remains secure and accessible only to relevant parties, safeguarding the integrity and privacy of the blockchain network. Customers can effortlessly access an abstracted version of data tailored to their specific needs, without the need for technical expertise or direct involvement in the blockchain.

Although the concept of a blockchain may be based on decentralization and bolstering of publicly available information, it doesn't imply the layman's understanding of "public". Information on blockchain is mainly of two types - transactional data and ledger data. Transactional data includes metadata on the transaction like recipient name, and addresses. This data is encrypted and made immutable to stop tampering of the data. Ledger data that stores all kinds of actual data that is stored on smart contracts is also encrypted, but the main difference is that this data is encrypted using public key cryptography, allowing a permissioned address or wallet to interact with the contract and decrypt the data to make sense of it. Transactional data is hashed using the SHA-256 algorithm that allows the blockchain to create a merkle tree that holds its state together. This method ensures the integrity of the entire blockchain. Hence, the first layer of data security is offered by the working of secret keys that are attached to each wallet, which is used to carry-out transactions on the blockchain. In general, this is the first layer of security at play on various blockchains. Additionally, the smart contracts so created to facilitate the system, offer certain more restrictions that allow it to be as secure as possible. The design of the smart contract allows easier administration of the entire system and its entities. Admin rights that are reserved to the creator of the system, restrict the addition of entities to the discretion of the admins. This basic yet fundamental characteristic allows any attempts by miscreants to hamper the organization of the system be unfruitful, following this, each entity type is ascribed with a role that come with specific rights that allow them to modify the blockchain. Such specific rights often include updation and shipping actions that are of immense importance to the functioning of the system, and therefore are inherently offered on the basis of the unique wallet address and ownership rights.

Figure 3. Patient registration form

4. CONCLUSION

The use of blockchain in patient data management system driven by factors such as the capacity to perform transactions in real-time at low cost, decentralized administration, immutable data, specific data generation, flexible access, data availability, and improved security and privacy. These benefits can transform patient care, cooperation, and data management. However, scalability, interoperability, and regulatory compliance must be addressed to realize blockchain's promise in healthcare fully.

ACKNOWLEDGEMENTS

We acknowledge all who directly or indirectly involved in the development of this system. We are grateful to family members, friends and colleagues who helped and guided us directly and indirectly for the development of this system, and preparation of this paper. Our special thanks to our employers for their support from the very beginning, that has come a long way, for the publication of this paper.

REFERENCES

[1] C. Woo and J. Yoo, "Exploring the determinants of blockchain acceptance for research data management," *Journal of Computer Information Systems*, vol. 63, no. 1, pp. 216–227, Apr. 2023, doi: 10.1080/08874417.2022.2049019.

[2] M. S. Minu, S. S. S. Ramesh, S. K. R. Peruru, and N. M. Roshan, "Efficient maintenance of hospital records by entrusted proof of work algorithm in block chain technology," in *EAI/Springer Innovations in Communication and Computing*, vol. Part F274, Springer International Publishing, 2023, pp. 337–351.

[3] W. J. Gordon and C. Catalini, "Blockchain technology for healthcare: facilitating the transition to patient-driven interoperability," *Computational and Structural Biotechnology Journal*, vol. 16, pp. 224–230, 2018, doi: 10.1016/j.csbj.2018.06.003.

[4] C. Pirtle and J. Ehrenfeld, "Blockchain for healthcare: the next generation of medical records?," *Journal of Medical Systems*, vol. 42, no. 9, Aug. 2018, doi: 10.1007/s10916-018-1025-3.

[5] V. Patel, "A framework for secure and decentralized sharing of medical imaging data via blockchain consensus," *Health Informatics Journal*, vol. 25, no. 4, pp. 1398–1411, Apr. 2019, doi: 10.1177/1460458218769699.

[6] A. Dubovitskaya, Z. Xu, S. Ryu, M. Schumacher, and F. Wang, "Secure and trustable electronic medical records sharing using blockchain," *AMIA annual symposium proceedings*, p. 650, 2017.

[7] G. Wood, "Ethereum: a secure decentralised generalised transaction ledger," *Ethereum project yellow paper*, vol. 151, pp. 1–32, 2014.

[8] X. Liu, Y. Hong, and J. Sun, "Blockchain-based medical data storage and sharing system," in *2022 IEEE International Conference on Advances in Electrical Engineering and Computer Applications, AEECA 2022*, Aug. 2022, pp. 62–66, doi: 10.1109/AEECA55500.2022.9918841.

[9] C. Mao and W. Golab, "Sharding techniques in the era of blockchain," in *Proceedings of the IEEE Symposium on Reliable Distributed Systems*, Sep. 2021, vol. 2021-Septe, pp. 343–344, doi: 10.1109/SRDS53918.2021.00041.
[10] A. Ruggeri, M. Fazio, A. Celesti, and M. Villari, "Blockchain-based healthcare workflows in federated hospital clouds," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 12054 LNCS, Springer International Publishing, 2020, pp. 113–121.
[11] L. Hang, E. Choi, and D. H. Kim, "A novel EMR integrity management based on a medical blockchain platform in hospital," *Electronics (Switzerland)*, vol. 8, no. 4, p. 467, Apr. 2019, doi: 10.3390/electronics8040467.
[12] Q. Huang, S. Chen, H. Zhao, and J. Wen, "Blockchain-based intelligent hospital security and data privacy construction," *Journal of Physics: Conference Series*, vol. 1187, no. 5, p. 52064, Apr. 2019, doi: 10.1088/1742-6596/1187/5/052064.
[13] F. Jamil, L. Hang, K. H. Kim, and D. H. Kim, "A novel medical blockchain model for drug supply chain integrity management in a smart hospital," *Electronics (Switzerland)*, vol. 8, no. 5, p. 505, May 2019, doi: 10.3390/electronics8050505.
[14] E. Westphal and H. Seitz, "Digital and decentralized management of patient data in healthcare using blockchain implementations," *Frontiers in Blockchain*, vol. 4, Aug. 2021, doi: 10.3389/fbloc.2021.732112.
[15] H. Bharath, N. Rahul, S. Shylash, and P. Vinny, "Patient data management using blockchain," *International Journal of Scientific and Research Publications (IJSRP)*, vol. 10, no. 7, pp. 310–316, Jul. 2020, doi: 10.29322/ijsrp.10.07.2020.p10339.
[16] D. V. Dimitrov, "Blockchain applications for healthcare data management," *Healthcare Informatics Research*, vol. 25, no. 1, pp. 51–56, 2019, doi: 10.4258/hir.2019.25.1.51.
[17] T. Hovorushchenko, A. Moskalenko, and V. Osyadlyi, "Methods of medical data management based on blockchain technologies," *Journal of Reliable Intelligent Environments*, vol. 9, no. 1, pp. 5–16, May 2023, doi: 10.1007/s40860-022-00178-1.
[18] M. J. H. Faruk, H. Shahriar, M. Valero, S. Sneha, S. I. Ahamed, and M. Rahman, "Towards blockchain-based secure data management for remote patient monitoring," in *Proceedings - 2021 IEEE International Conference on Digital Health, ICDH 2021*, Sep. 2021, pp. 299–308, doi: 10.1109/ICDH52753.2021.00054.
[19] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "MedRec: using blockchain for medical data access and permission management," in *Proceedings - 2016 2nd International Conference on Open and Big Data, OBD 2016*, Aug. 2016, pp. 25–30, doi: 10.1109/OBD.2016.11.
[20] A. Ekblaw, A. Azaria, J. D. Halamka, and A. Lippman, "A case study for blockchain in healthcare: 'MedRec' prototype for electronic health records and medical research data," *Proceedings of IEEE Open and Big Data Conference*, 2016.
[21] X. Liang, J. Zhao, S. Shetty, J. Liu, and D. Li, "Integrating blockchain for data sharing and collaboration in mobile healthcare applications," in *IEEE International Symposium on Personal, Indoor and Mobile Radio Communications, PIMRC*, Oct. 2018, vol. 2017-October, pp. 1–5, doi: 10.1109/PIMRC.2017.8292361.
[22] P. Zhang, J. White, D. C. Schmidt, G. Lenz, and S. T. Rosenbloom, "FHIRChain: applying blockchain to securely and scalably share clinical data," *Computational and Structural Biotechnology Journal*, vol. 16, pp. 267–278, 2018, doi: 10.1016/j.csbj.2018.07.004.
[23] D. Ichikawa, M. Kashiyama, T. Ueno, and T. Suzuki, "Blockchain technology for securing personal genomic data," *Journal of Biomedical Informatics*, vol. 71, pp. 122–127, 2017.
[24] M. Mettler, "Blockchain technology in healthcare: the revolution starts here," Sep. 2016, doi: 10.1109/HealthCom.2016.7749510.
[25] K. D. Mandl, I. S. Kohane, and C. A. Longhurst, "Leveraging blockchain technology to enhance EHR data sharing and consent," *Digital Medicine*, vol. 3, no. 1, p. 2016, 2016.
[26] T. T. Kuo, H. E. Kim, and L. Ohno-Machado, "Blockchain distributed ledger technologies for biomedical and health care applications," *Journal of the American Medical Informatics Association*, vol. 24, no. 6, pp. 1211–1220, Sep. 2017, doi: 10.1093/jamia/ocx068.

BIOGRAPHIES OF AUTHORS

Dr. Vijaykumar Bidve is Associate Professor at Symbiosis Skills and Professional University, Kiwale, Pune, Maharashtra, India. He Holds a Ph.D. degree in Computer Science and Engineering with specialization in Software Engineering. His research areas are Software Engineering, Machine Learning. Dr Vijaykumar has published six patents. He has published more than 40+ research articles in national and international journals. He is a life member of ISTE. He is working as an expert for various subjects. Also, he has worked as a reviewer for various conferences and journals. He can be contacted at email: vijay.bidve@gmail.com.

Dr. Kiran Kakade is Associate Professor at Lala Lajpatrai Institute of Management, University of Mumbai, India. Management science and have completed post-graduation in MBA (HR), LL.M (Law), and MCA (Master in Computer Application) from the prestigious University of Pune. His research areas include artificial intelligence in HR and Law. He has published 6 patents and over 50 research papers published in esteemed ABDC and Scopus publications. He significant contributions to academia and industry, notably at esteemed institutions like TISS, TIMSR, GNIMS, and MIT World Peace University. He can be contacted at email: kirankakade2025@gmail.com.

Dr. Pakiriswamy Sarasu is Director International and Industry relations, Professor in Computer Science Engineering Department at Kalasalingam Academy of Research and Education, Tamilnadu, India. She holds a Ph.D. Degree in Computer Science and Engineering. She did her masters in Embedded Systems Technology and Bachelors in Computer Science Engineering. Her research areas include chaotic systems, cryptography and autonomous vehicle. She played a major role in creating innovation entrepreneurial ecosystem and more than 120 startups are created under her guidance and mentorship. She is continuously involved in mentoring students and faculty members for innovation and entrepreneurship. One patent is granted for her as one of the inventors. She can be contacted at email: sarasujivat@gmail.com.

Dr. Shailesh Kediya is Associate Professor at Symbiosis Skills and Professional University, Kiwale, Pune, Maharashtra, India. He Holds a Ph.D. degree in Logistics Management. His research areas are innovative and disruptive technologies, business management. Dr Shailesh Kediya has published 2 international patents, awarded with 12 copyright and written 8 books. He has published more than 50 research articles in national and international journals. He is a member of IEEE, SEBI and NISM. He is working as an expert for various subjects. Also, he has been editor of four international journals and worked as a reviewer for various conferences and journals. He can be contacted at email: kediya.shailesh@gmail.com.

Dr. Pradip Tamkhade is Associate Professor and Dean Student Affairs at Marathwada Mitra Mandal's College of Engineering, Pune, Maharashtra, India. He Holds a Ph.D. degree in Mechanical Engineering with specialization in thermal engineering. His research areas are heat transfer and heat exchanger. Dr Pradip has published number of patents. He is working as an expert for various subjects. Also, he has worked as a reviewer for various conferences and journals. He can be contacted at email: pradiptamkhade@gmail.com.

Dr. Suprakash Sudarsanan Nair is Associate Professor at Kalasalingam Academy of Research and Education, Tamilnadu, India. He holds a Ph.D. degree in Green Cloud Computing. He did his masters in VLSI design and bachelor's in Computer Science and Engineering. His research areas include computing, security, data science, sensor fusion in autonomous vehicles. He has published many research articles in national and international journals. He has also published various patents. He is a lifetime member in ISTE and IAENG. He is the technical lead and done many projects in reducing paper waste and automation. Also, he is a technical expert for various workshops and reviewer for conferences and journals. He can be contacted at email: s.suprakash@gmail.com.