International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Smart Healthcare: Blockchain-Driven Patient Risk Classification with Machine Learning

Jyoti Sunil More*[1], Jyoti Sandesh Deshmukh[2], Deeplaxmi V. Niture[3]

Submitted: 25/01/2024 **Revised**: 03/03/2024 **Accepted**: 11/03/2024

Abstract: The development of any nation's economy depends largely on having an efficient healthcare system. This article investigates the architecture of a framework for patient risk classification in a smart healthcare system which combines blockchain technology with machine learning. The framework seeks to transform healthcare delivery by utilizing machine learning algorithms' predictive powers in conjunction with blockchain's transparency, immutability, and decentralized data storage. This study clarifies the potential to improve patient outcomes through more precise and customized risk assessments by thoroughly analyzing the opportunities and challenges. Data security, interoperability, regulatory compliance, and technological scalability are important factors to take into account. The findings of this study provide encouraging paths for enhancing patient care and public health outcomes globally, since interdisciplinary cooperation and continuous innovation propel improvements in healthcare technology.

Keywords: *Blockchain Technology, Smart healthcare system, Machine learning*

1. Introduction

One of the key effects of modernization is the development of the culture of nuclear families. The elderly patients usually stay with spouses, or alone when their children settle in the foreign countries or metros, due to employment needs. For such patients, the situation becomes worse if they get some health issues that lead to bed binding. The health of bed bound patients either at home or at hospital is always a concern for family and hospital. They require continuous monitoring if any comorbidity is present. We propose a remote monitoring methodology which will help the bed bound patients and the caretakers to do continuous monitoring and trigger appropriate actions if required. Our system will also work on the mental health of such patients. This will reduce the health risk of the patients in the short term as well as long term by deploying machine learning algorithms. It can be utilized for the elderly or disabled bed bound patients who do not have family or stay alone.

Medical care industry is becoming costlier than at any other time in this advanced age, however the quantum of patients and health issues are truly expanding. As the health of an individual is a priority among the most imperative issues nowadays, IoT could be utilized in the prosperity business as a flawless wellbeing observing infrastructure. Internet, cloud computing, AI, blockchain, IoT, etc. are some important modern technologies, which can make vital industries like Finance, Marketing, Healthcare, Insurance, etc. better, faster and more efficient. The healthcare sector has been embracing cutting-edge technologies that enable clinical process automation and the digitalization of patient records. The blockchain revolution has a huge possibility to drive the digital transformation of healthcare data, supply chain data, smart contracts, payment information, pharmaceutical applications and other areas. The sharing and archiving of healthcare data is a crucial component of healthcare systems. Private healthcare data might become more secure, scalable, and tamper-proof by being stored on the blockchain. Sharing personal information insecurely among different businesses or entities runs the risk of exposing sensitive data. Serious repercussions, such as unauthorized individuals getting access to the private medical information, result from clients not having control over their personal information. In electronic health or medical records (EHR/EMR), privacy protection, data integrity protection, and stakeholder compatibility are critical factors. Blockchain technology makes it feasible to address the challenges brought about by COVID-19, such issues with exchanging medical records, breaches of patient confidentiality, and insufficient monitoring mechanisms. Blockchain technology is ultimately required to handle issues like privacy and security, since it arises as a result of the necessity to give legitimacy to the entire system.

Apart from this, some major objectives of using blockchain in our proposed system are discussed below. The varied standards and communication patterns involved with IoT technology prevent traditional security techniques from being directly implemented. Additionally, the existence of such a vast network with so many interrelated organizations will undoubtedly suggest several complex scenarios. All

[1] *Department of Computer Engineering, Agnel Charities' Fr. C. Rodrigues Institute of Technology, Vashi, Navi Mumbai, INDIA*
[2] *Department of Computer Engineering, Pillai College of Engineering, Navi Mumbai, INDIA*
[3]*Department of Electronics and Telecommunication Engineering,COEP Technological University, Pune, INDIA*
** Corresponding Author Email: jyotim8582@gmail.com*

those devices will be very vulnerable as a result, endangering the associated users. Since physical devices may store and handle sensitive user information, cyber-security systems must provide tailored mechanisms to safeguard the collected data from the physical devices. This means that IoT systems must always offer data availability, confidentiality, and integrity. Data encryption and data redundancy, authentication, access control, and authorization procedures, can be used to prevent access to unauthorized users. However, since information providers can act dishonestly by providing false or misleading information, there may arise many situations where it is necessary to protect oneself as well as the entire system from them. In these situations, traditional security mechanisms fail to protect users from this type of threat. Therefore, it is crucial to have a fully secure solution, such as blockchain, which will offer an IoT system secure distributed solution.

To further the subject, research agendas for the suggested secure and intelligent healthcare system should give priority to a number of important areas. Research on improving data security and privacy in blockchain-driven healthcare systems should be given top priority. To protect sensitive patient data, this entails investigating decentralized identity management systems, advanced encryption techniques, and privacy-preserving strategies. Research endeavors ought to prioritize the enhancement of interoperability standards and protocols to facilitate the smooth transfer of data among diverse healthcare institutions and systems. The creation of standardized formats for data transmission and representation should be prioritized in order to enable effective communication between various platforms. Furthermore, there might be a substantial impact on patient care outcomes from the exploration of cutting-edge machine learning algorithms and methodologies for predictive analytics, illness detection, and customized therapy recommendations. Furthermore, investigating the integration of cutting-edge technologies such as edge computing and Internet of Things (IoT) devices into the healthcare setting may improve data gathering, real-time monitoring, and decision-making procedures. Finally, to tackle difficult issues and guarantee the responsible implementation of clever and safe healthcare solutions, multidisciplinary research collaborations between technologists, policymakers, and ethicists are essential. Encouraging the creation and uptake of cutting-edge technologies that enhance patient outcomes, healthcare delivery, and data security is the main objective of these research goals.

2. Related Work

The main challenge of dealing with blockchain on various platforms like IoT, machine learning, etc is interoperability. Data sharing through mechanisms including data acquisition, patient identity, data liquidity, data access and data integrity are due to the change from institution-centric to patient-centric framework for data handling (Green et al. 2018; Agbo et al. 2019; Khezr et al. 2019; Zubaydi et al. 2019; Shahnaz et al. 2019; Ali et al. 2020). There are a few issues with speed and scalability that arise when using blockchain technology in a distributed messaging system (Alla et al. 2018; Chakraborty et al. 2019; Jamil et al. 2020; Asad et al. 2019), as well as concerns with resource constraints, absence of normalization, scalability, bandwidth, security breaks, and compatibility (Azbeg et al. 2022). Traceability features in blockchain were proved to be significant while dealing with supply chains in the pharmaceutical domain (Abu-Elezz et al. 2020). The confidentiality and security of patient information are the essential worries with regards to savvy medical care because of the interoperability of numerous partners (Chakraborty et al. 2019; Aithal et al. 2021; Rakic et al. 2018; Gupta et al. 2021; Pham et al. 2018). Many blockchain frameworks, most notably BiiMED (Jabbar et al. 2020), have been created to improve interoperability and integrity surrounding EHR sharing. Through the provision of a decentralized external auditor to ensure data integrity and access, the management framework governing the exchange of EHRS among various clinical providers is regulated. Key components, applications, opportunities, and hindrances are illustrated for critical achievement measures that might assume a vital part in the reception of blockchain. The discoveries support decision-making while thinking up plans and procedures for using blockchain in the medical services domain (Bali et al. 2023).

Disseminated occasions with a distributed service platform will support resolving issues like congestion or weak links and will hurry transaction handling (Agbo et al. 2019). A healthcare security framework Multimedia data is built using blockchain (Anjum et al. 2020; Rathee et al. 2020; Khan et al. 2020; Wong et al. 2018; Wu et al. 2021). A blockchain testing environment that investigates several needs for healthcare apps is created using Hyperledger fabric (Wang 2020). Lightweight blockchain is recommended to address blockchain's issues (Dwivedi et al. 2019; Srivastava et al. 2019).

In order to reduce security risks related to remote patient monitoring, real-time patient monitoring was implemented using a private blockchain. Additionally, automated notice distribution to all patients is made easier (Griggs et al. 2018). To determine whether or not the data should be entered into the blockchain, an extra filtering mechanism can be added at the sensor level. This aids in maximizing the BC size and decreasing the quantity of coins needed for transactions (Pham et al. 2018). Adding software-defined networking (SDN), which ensures network efficacy and flexibility(Barka et al. 2021), is another way to handle these issues. SDN offers a wide range of services along with operational and security

solutions that users can utilize. Enrollment in a health programme can be made secure for both individuals and medical personnel with the help of Ethereum smart contracts. (Srivastava et al. 2019; Kazmi et al. 2020; Javed et al. 2021; Mohammed et al. 2021; Ejaz et al. 2021). It was suggested to combine IoT with healthcare monitoring and to use a security architecture based on the Hyperledger Fabric. (Jamil et al. 2020; Attia et al. 2019; Faruk et al. 2021; Srivastava et al. 2019; Rani et al. 2022). A patient agent (PA) is used in another agent-based architecture that was put out (Uddin et al. 2018) to link the blockchain and the RPM data stream.

3. Proposed System

Figure 1 depicts the proposed framework of our system for bed bound patients. Finding use cases for blockchain and machine learning in healthcare, like risk assessment and patient data management, is the first step in the framework. Making the appropriate choice in blockchain platforms, like Ethereum or Hyperledger Fabric, is essential to guaranteeing the security of data and the operation of smart contracts. A predetermined data schema is created to store demographic and medical history information about patients on the blockchain. A variety of sources provide the patient data, which is preprocessed to get rid of noise and irregularities. In order to facilitate risk assessment, pertinent parameters such as age, medical history, and lifestyle factors are derived from the data. Machine learning methods like logistic regression and decision trees are used in risk categorization. After these models have been trained and verified using labeled patient data, their performance is assessed using cross-validation.

In order to provide privacy and auditability, smart contracts are designed to run risk assessment algorithms on the blockchain in a transparent manner. Systems for managing patient permission are put in place to restrict data access for risk assessment. The execution of risk assessment smart contracts based on patient data inputs is governed by a predetermined procedure. Prioritizing integration with current healthcare systems helps to guarantee seamless data flow and interoperability. Pilot testing assesses the accuracy, scalability, and usefulness of the framework. Iterative updates to the design and functioning of the framework are driven by ongoing input received from patients and healthcare practitioners.

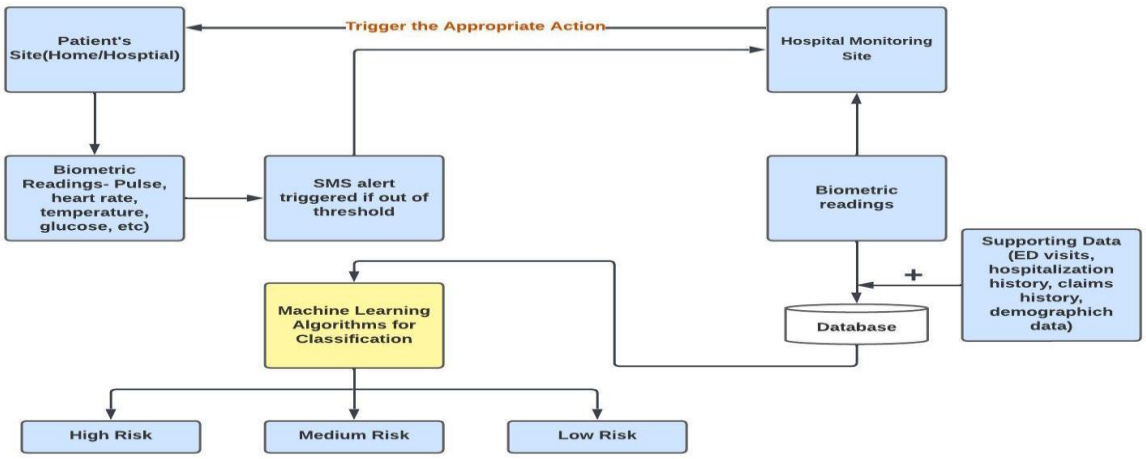

Fig. 1. Block diagram for proposed framework for Deploying IoT and Machine learning Algorithms for healthcare needs of bed bound patients

Healthcare organizations may leverage blockchain technology and machine learning to improve patient outcomes, expedite risk assessment procedures, and optimize resource allocation by implementing a complete strategy.

Initially, the required biometric data of the bed bound patient will be collected for monitoring and further analysis. This data along with some auxiliary data like demographic data will be stored in a database server, which will be exclusively used for Machine learning setup to fulfill our objectives. Typically, the significant biometric readings of the patient viz. temperature, blood pressure, oxygen levels, glucose, etc, will be recorded using IoT setup. The IoT sensors will be responsible for recording the physical status/wellbeing of the patient. All the involved sensors will record the data periodically, and will be handled by NodeMCU. The usage of NodeMCU instead of Arduino setup is preferred as it can provide the data to be directly generated and handled efficiently. In addition to this, the system can also be configured to take care of the wellbeing of patients, by providing periodical reminders for their medicine intake and will also take care of any emergencies, initiated by the patient. (E.g., in case of any unwanted situation like fall, uneasiness, etc.) If medicines are out of stock, a third party can be used to take care of the stock

management which will again need the intervention of blockchain, for supply chain management.

4. Machine Learning Setup for classification and prediction of the patients

The Machine Learning Methodology can be deployed to classify the patients' different categories as level of risk viz., high level, medium level and low level as shown in figure 2.

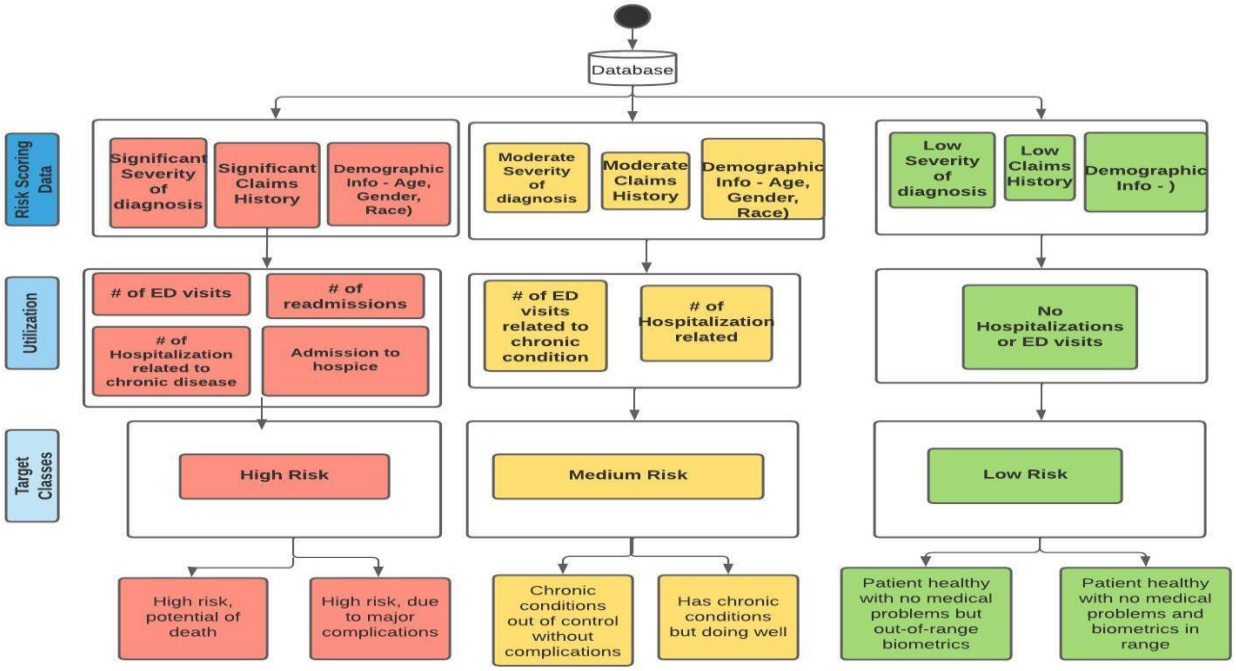

Fig. 2. The Machine Learning Methodology deployed to classify the patients in different categories

The participating features will be typically based on risk scoring data and the type and extent of utilization of medical facilities by the patients. Figure 3 illustrates the deployment of blockchain to ensure security and privacy within the integrated system, which includes IoT-monitored data analyzed through machine learning tools and algorithms. This facilitates precise classification of patients according to their risk levels.

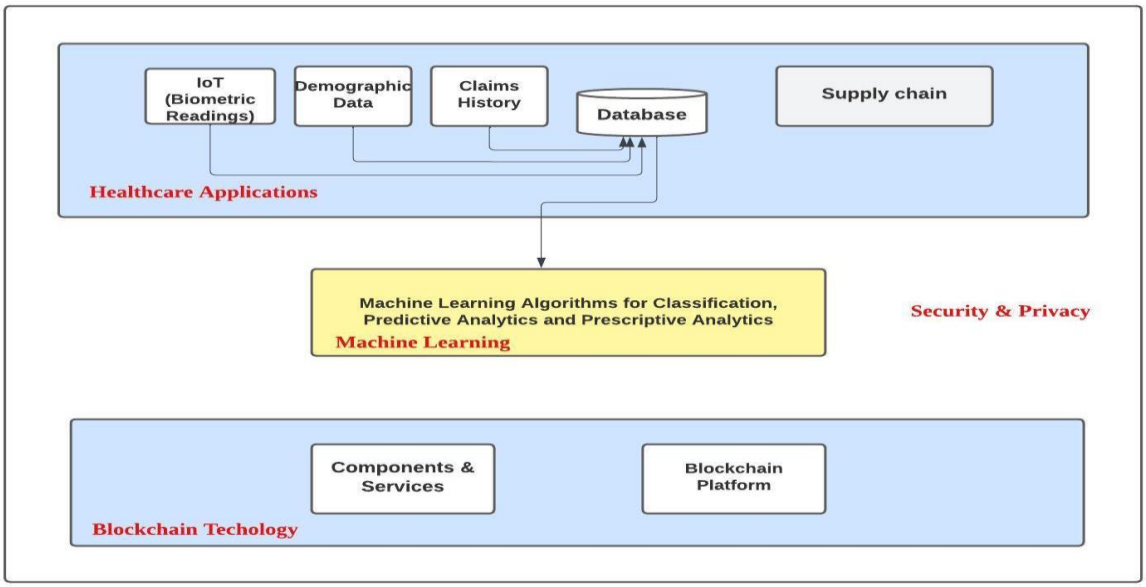

Fig. 3. The Blockchain Methodology deployed to provide security and privacy for integrated Healthcare, IoT and ML technologies.

```
contract PatientDataManagement {
        struct Patient {
        uint256 id;
        string name;
        uint8 age;
        string medicalHistory;
        // Add other relevant patient attributes
        }
mapping(uint256 => Patient) public patients;
        uint256 public patientCount;
        function addPatient(string memory _name,
uint8 _age, string memory _medicalHistory) public
{
        patientCount++;
        patients[patientCount] =
Patient(patientCount, _name, _age,
_medicalHistory);
        }
// Add functions for accessing and updating patient
data
}
```

Fig 4 a. Patient Data Management Contract

```
pragma solidity ^ 0.8.0;
import "./PatientDataManagement.sol";
contract RiskAssessment is PatientDataManagement {
        enum RiskCategory { Low, Medium, High }
        mapping(uint256 => RiskCategory) public
patientRisk;
        function assessRisk (uint256_patientId) public
returns (RiskCategory) {
        // Implement machine learning algorithm to
categorize patient risk
        // Example: dummy logic for demonstration
purposes
        if (patients[_patientId].age > 60) {
        patientRisk[_patientId] = RiskCategory.High;
        } else if (patients[_patientId].age > 30) {
        patientRisk[_patientId] = RiskCategory.Medium;
        } else {
        patientRisk[_patientId] = RiskCategory.Low;
        }
        return patientRisk[_patientId];
        }
// Add functions for accessing patient risk categories
}
```

Fig 4 b. Risk Assessment Contract

A sample code for patient data Management Contract and Risk Assessment Contract is shown in figure 4 a and 4 b respectively.

The flowchart shown in Figure 5 describes the overall system flow.

Phase1: The patient registers to the hospital monitoring system. At the monitoring site, the demographic information like gender, age, social background, etc. and also the auxiliary information like patient's medical history, ailments, comorbidities, etc. is collected during the registration process. All the IoT devices are installed as wearable devices at the patient's site. Vital signs such as blood pressure, heart rate, and temperature will be recorded and transmitted to the hospital monitoring site. In order to provide security and authorization, blockchain smart contracts can be written.

Phase2: The analytics site receives the data gathered at the monitoring site and uses it to classify the patients into low, medium, and high risk groups.

Depending on the risk category the patient will get the necessary attention by the hospital. For instance, high risk patients will be treated as high priority and will be monitored closely, with necessary care. Also these machine learning algorithms will help to predict and notify the hospitals about the number of patients who need special attention with maximum resources and thus it may help hospitals to plan the resources. By doing this segregation, optimum utilization of the hospital resources can be achieved.

Fig. 5. Flowchart of the proposed system for smart healthcare system

5. Challenges

Building a framework in a smart healthcare system with blockchain and machine learning to categorize patients into high, medium, and low risk groups presents a number of challenges. The most important reason to protect data privacy and security is that medical data is sensitive. To balance blockchain technology's transparency with the requirement for secrecy, creative encryption methods and privacy-protecting protocols are crucial. Furthermore, to address any interoperability issues that may surface during the integration of blockchain and machine learning technologies with current healthcare systems, standardization initiatives and smooth data exchange protocols would be necessary. Thirdly, access to high-quality, labeled patient data is necessary to create effective machine learning models for risk categorization. However, this data may be sparse or biased, which could make model training and validation difficult. Furthermore, careful consideration of scalability, efficiency, and auditability is required when creating smart contracts to carry out risk assessment algorithms on the blockchain. Finally, the design process becomes more complex due to regulatory compliance and ethical issues, which necessitate alignment with ethical norms and healthcare regulations. Examples of these factors include patient consent management and fair treatment. To tackle these obstacles, multidisciplinary cooperation, cutting-edge technologies, and an all-encompassing strategy for creating intelligent and safe healthcare systems are needed.

There are some important differences between the design of a blockchain-integrated machine learning framework for patient risk classification in a smart healthcare system and a traditional system. Patient data management in the conventional system often depends on outdated technologies and centralized databases, raising concerns about privacy violations, data security, and interoperability problems amongst healthcare organizations. On the other hand, blockchain-based systems have built-in benefits including

immutability, decentralized data storage, and cryptographic security, which improve data security and privacy protection. Furthermore, blockchain-integrated machine learning algorithms enable automated, data-driven risk categorization based on intricate patterns and predictive analytics, resulting in more precise and customized patient outcomes than traditional risk assessment methods, which frequently rely on manual analysis and predetermined rules. In contrast to conventional systems, the application of blockchain and machine learning brings with it difficulties with scalability, regulatory compliance, and integration complexity. Despite these difficulties, the potential advantages of machine learning and blockchain technology in terms of better security, transparency, and predictive analytics highlight the significance of using cutting-edge design techniques when creating intelligent healthcare systems to improve patient outcomes. Table 1 summarizes how the suggested system compares to the conventional system.

Table 1. Comparison of proposed system with conventional system

Feature	Traditional System	Proposed System
Confidentiality	Methods optd- end to end encryption, DB Security	High level security through BC
Availability	Traditional methods for DB Backup & recovery mechanisms	High fault tolerance & service availability
Reliability	DBS are vulnerable to manipulation & security attacks	Blocks are immutable so high level of reliability
Traceability	Detection of changes in health records or logs not guaranteed	Verified blocks can be used to keep track of origin of creation &thus help in tracking
Integrity of HER	No guarantee on integrity	Integrity is assured.
Data Sharing	No guarantee over data security	There is a safe, decentralised platform available for any information interactions.
Fraud detection	No support for fraud detection & may allow duplicate or modified transaction	BC has feature-immutability which strictly prohibits duplication or modified transactions.
Predictability	No support of predictability related to risk probability.	System provides classification based on multiple factors, which helps in risk predictability.
Load balancing	The healthcare systems don't segregate the patients hence, equal attention is given to all the patients, across the system	Due to risk accessibility, depending on the need, high risk patients are prioritized and handled separately with smart mechanisms.
Resource Utilization	The healthcare system sometimes may end up having unbalanced resource allocation.	Due to predictability of the risk bracket of the patients, the resource utilization can be optimized.

6. Conclusion

In order to provide a framework for a smart healthcare system, this research study has examined the complex junction of blockchain technology and machine learning. Significant progress can be achieved in improving patient risk classification by utilising blockchain's built-in qualities of transparency, immutability, and decentralized data storage in conjunction with machine learning algorithms' predictive powers. By offering more precise and customized risk assessments, this study has highlighted the potential to transform healthcare delivery through a thorough examination of the opportunities and problems present in such a framework. Blockchain and machine learning can be used to potentially improve patient outcomes, data security, and interoperability within the healthcare sector. However, it's also critical to acknowledge the difficulties, such as concerns about privacy, compliance with the law, and the scalability of technology. Realizing the full potential of smart healthcare systems will depend on interdisciplinary collaboration and continuous innovation as this field of study advances. In the end, the knowledge gathered from this study opens the door for further developments in

medical technology, which could have a favorable effect on patient care and public health outcomes globally.

Conflicts of interest

The authors declare no conflicts of interest.

References

[1] Gordon, W. J., & Catalini, C. (2018). Blockchain technology for healthcare: facilitating the transition to patient-driven interoperability. *Computational and structural biotechnology journal*, *16*, 224-230.

[2] Agbo, C. C., Mahmoud, Q. H., & Eklund, J. M. (2019, April). Blockchain technology in healthcare: a systematic review. In *Healthcare* (Vol. 7, No. 2, p. 56). MDPI.

[3] Alla, S., Soltanisehat, L., Tatar, U., & Keskin, O. (2018). Blockchain technology in electronic healthcare systems. In *IIE Annual Conference. Proceedings* (pp. 901-906). Institute of Industrial and Systems Engineers (IISE).

[4] Chakraborty, S., Aich, S., & Kim, H. C. (2019, February). A secure healthcare system design framework using blockchain technology. In *2019 21st International Conference on Advanced Communication Technology (ICACT)* (pp. 260-264). IEEE.

[5] Jamil, F., Ahmad, S., Iqbal, N., & Kim, D. H. (2020). Towards a remote monitoring of patient vital signs based on IoT-based blockchain integrity management platforms in smart hospitals. *Sensors*, *20*(8), 2195.

[6] Azbeg, K., Ouchetto, O., Andaloussi, S. J., & Fetjah, L. (2022). A taxonomic review of the use of IoT and blockchain in healthcare applications. *Irbm*, *43*(5), 511-519.

[7] Abu-Elezz, I., Hassan, A., Nazeemudeen, A., Househ, M., & Abd-Alrazaq, A. (2020). The benefits and threats of blockchain technology in healthcare: A scoping review. *International Journal of Medical Informatics*, *142*, 104246.

[8] Chakraborty, S., Aich, S., & Kim, H. C. (2019, February). A secure healthcare system design framework using blockchain technology. In *2019 21st International Conference on Advanced Communication Technology (ICACT)* (pp. 260-264). IEEE.

[9] Aithal, P. S., Aithal, A., & Dias, E. (2021). Blockchain technology-current status and future research opportunities in various areas of healthcare industry. *International Journal of Health Sciences and Pharmacy (IJHSP)*, *5*(1), 130-150.

[10] Jabbar, R., Fetais, N., Krichen, M., & Barkaoui, K. (2020, February). Blockchain technology for healthcare: Enhancing shared electronic health record interoperability and integrity. In *2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT)* (pp. 310-317). IEEE.

[11] Bali, S., Bali, V., Mohanty, R. P., & Gaur, D. (2023). Analysis of critical success factors for blockchain technology implementation in healthcare sector. *Benchmarking: An International Journal*, *30*(4), 1367-1399. https://doi.org/10.1108/BIJ-07-2021-0433

[12] Anjum, H. F., Rasid, S. Z. A., Khalid, H., Alam, M. M., Daud, S. M., Abas, H., ... & Yusof, M. F. (2020). Mapping research trends of blockchain technology in healthcare. *ieee Access*, *8*, 174244-174254, doi: 10.1109/ACCESS.2020.3025011.

[13] Rathee, G., Sharma, A., Saini, H., Kumar, R., & Iqbal, R. (2020). A hybrid framework for multimedia data processing in IoT-healthcare using blockchain technology. *Multimedia Tools and Applications*, *79*(15), 9711-9733. https://doi.org/10.1007/s11042-019-07835-3

[14] Khan, F. A., Asif, M., Ahmad, A., Alharbi, M., & Aljuaid, H. (2020). Blockchain technology, improvement suggestions, security challenges on smart grid and its application in healthcare for sustainable development. *Sustainable Cities and Society*, *55*, 102018.

[15] Wong, M. C., Yee, K. C., & Nøhr, C. (2018). Socio-technical considerations for the use of blockchain technology in healthcare. In *Building Continents of Knowledge in Oceans of Data: The Future of Co-Created eHealth* (pp. 636-640). IOS Press.

[16] Wu, H., Dwivedi, A. D., & Srivastava, G. (2021). Security and privacy of patient information in medical systems based on blockchain technology. *ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM)*, *17*(2s), 1-17.

[17] Wang, H. (2020). IoT based clinical sensor data management and transfer using blockchain technology. *Journal of ISMAC*, *2*(03), 154-159.

[18] Dwivedi, A. D., Malina, L., Dzurenda, P., & Srivastava, G. (2019, July). Optimized blockchain model for internet of things based healthcare applications. In *2019 42nd international conference on telecommunications and signal processing (TSP)* (pp. 135-139). IEEE. doi: 10.1109/TSP.2019.8769060.

[19] Srivastava, G., Crichigno, J., & Dhar, S. (2019, May). A light and secure healthcare blockchain for iot medical devices. In *2019 IEEE Canadian conference of electrical and computer engineering (CCECE)* (pp. 1-5). IEEE. doi: 10.1109/CCECE.2019.8861593.

[20] Griggs, K. N., Ossipova, O., Kohlios, C. P., Baccarini, A. N., Howson, E. A., & Hayajneh, T. (2018). Healthcare blockchain system using smart contracts for secure automated remote patient monitoring. *Journal of medical systems*, *42*, 1-7. doi: 10.1007/s10916-018-0982-x. PMID: 29876661.

[21] Pham, H. L., Tran, T. H., & Nakashima, Y. (2018, December). A secure remote healthcare system for hospital using blockchain smart contract. In *2018 IEEE globecom workshops (GC Wkshps)* (pp. 1-6). IEEE. doi: 10.1109/GLOCOMW.2018.8644164.

[22] Barka, E., Dahmane, S., Kerrache, C. A., Khayat, M., & Sallabi, F. (2021). STHM: A secured and trusted healthcare monitoring architecture using SDN and Blockchain. *Electronics*, *10*(15), 1787. https://doi.org/10.3390/electronics10151787

[23] Kazmi, H. S. Z., Nazeer, F., Mubarak, S., Hameed, S., Basharat, A., & Javaid, N. (2020). Trusted remote patient monitoring using blockchain-based smart contracts. In *Advances on Broad-Band Wireless Computing, Communication and Applications: Proceedings of the 14th International Conference on Broad-Band Wireless Computing, Communication and Applications (BWCCA-2019) 14* (pp. 765-776). Springer International Publishing.

[24] Javed, I. T., Alharbi, F., Bellaj, B., Margaria, T., Crespi, N., & Qureshi, K. N. (2021, June). Health-ID: A blockchain-based decentralized identity management for remote healthcare. In *Healthcare* (Vol. 9, No. 6, p. 712). MDPI. doi: 10.3390/healthcare9060712. PMID: 34200778; PMCID: PMC8230390.

[25] Mohammed, R., Alubady, R., & Sherbaz, A. (2021, March). Utilizing blockchain technology for IoT-based healthcare systems. In *Journal of Physics: Conference Series* (Vol. 1818, No. 1, p. 012111). IOP Publishing.

[26] Ejaz, M., Kumar, T., Kovacevic, I., Ylianttila, M., & Harjula, E. (2021). Health-blockedge: Blockchain-edge framework for reliable low-latency digital healthcare applications. *Sensors*, *21*(7), 2502. doi: 10.3390/s21072502. PMID: 33916700; PMCID: PMC8038371.

[27] Attia, O., Khoufi, I., Laouiti, A., & Adjih, C. (2019, June). An IoT-blockchain architecture based on hyperledger framework for health care monitoring application. In *NTMS 2019-10th IFIP International Conference on New Technologies, Mobility and Security* (pp. 1-5). IEEE Computer Society.. doi: 10.1109/NTMS.2019.8763849.

[28] Faruk, M. J. H., Shahriar, H., Valero, M., Sneha, S., Ahamed, S. I., & Rahman, M. (2021, September). Towards blockchain-based secure data management for remote patient monitoring. In *2021 IEEE international conference on digital health (ICDH)* (pp. 299-308). IEEE. doi: 10.1109/ICDH52753.2021.00054.

[29] Uddin, M. A., Stranieri, A., Gondal, I., & Balasubramanian, V. (2018). A patient agent to manage blockchains for remote patient monitoring. *Stud. Health Technol. Inform*, *254*, 105-115. PMID: 30306963

[30] Hasan, M. R., Deng, S., Sultana, N., & Hossain, M. Z. (2021). The applicability of blockchain technology in healthcare contexts to contain COVID-19 challenges. *Library Hi Tech*, *39*(3), 814-833. https://doi.org/10.1108/LHT-02-2021-0071

[31] Rakic, D. (2018, March). Blockchain Technology in Healthcare. In ICT4AWE (pp. 13-20).

[32] Khezr, S., Moniruzzaman, M., Yassine, A., & Benlamri, R. (2019). Blockchain technology in healthcare: A comprehensive review and directions for future research. *Applied sciences*, *9*(9), 1736. https://doi.org/10.3390/app9091736.

[33] Asad Ali Siyal; Aisha Zahid Junejo; Zawish, Muhammad; Kainat Ahmed; Khalil, Aiman; et al. (2019): Cryptography; Basel Vol.3, Iss.1, 3. DOI:10.3390/cryptography3010003

[34] Gupta, P., Hudnurkar, M., & Ambekar, S. (2021). Effectiveness of blockchain to solve the interoperability challenges in healthcare. *Cardiometry*, (20), 79-87.

[35] Zubaydi, H. D., Chong, Y. W., Ko, K., Hanshi, S. M., & Karuppayah, S. (2019). A review on the role of blockchain technology in the healthcare domain. *Electronics*, *8*(6), 679. https://doi.org/10.3390/electronics8060679

[36] Shahnaz, A., Qamar, U., & Khalid, A. (2019). Using blockchain for electronic health records. *IEEE access*, *7*, 147782-147795. doi: 10.1109/ACCESS.2019.2946373.

[37] Pham, H. L., Tran, T. H., & Nakashima, Y. (2018, December). A secure remote healthcare system for hospital using blockchain smart contract. In *2018 IEEE globecom workshops (GC Wkshps)* (pp. 1-6). IEEE. doi: 10.1109/GLOCOMW.2018.8644164.

[38] Srivastava, G., Parizi, R. M., Dehghantanha, A., & Choo, K. K. R. (2019, November). Data sharing and privacy for patient IoT devices using blockchain. In *International Conference on Smart City and Informatization* (pp. 334-348). Singapore: Springer Singapore. https://doi.org/10.1007/978-981-15-1301-5_27

[39] Rani, P., Kaur, P., Jain, V., Shokeen, J., & Nain, S. (2022). Blockchain-based IoT enabled health monitoring system. *The Journal of Supercomputing*, *78*(15), 17284-17308. https://doi.org/10.1007/s11227-022-04584-3

[40] Ali, M. S., Vecchio, M., Putra, G. D., Kanhere, S. S., & Antonelli, F. (2020). A decentralized peer-to-peer remote health monitoring system. *Sensors*, *20*(6), 1656. doi: 10.3390/s20061656. PMID: 32188135; PMCID: PMC7146265.