AI and Blockchain for Healthcare Data Security in Smart Cities

Anand Singh Rajawat, Pradeep Bedi, S. B. Goyal, Rabindra Nath Shaw, Ankush Ghosh, and Sambhav Aggarwal

Abstract The healthcare industry is interested in various AI and blockchain technology characteristics, such as the immutability of data stored in a blockchain. Numerous interesting IoT-based applications are being examined. IoT-based Clinical and biological research will be sped up, biomedical and healthcare data ledgers will be advanced using *Blockchain and AI*. These evaluations are based on essential Blockchain and AI technology features such as decentralized management, immutable audit trails, data authenticity, resilience, better security, and most importantly, the restoration of charterers' rights. Blockchain and AI are being used to create innovative and advanced solutions to improve the present standards of medical data handling, sharing, processing, analysis, and classification according to the outcomes. With enhanced efficiency, access control, technical development, privacy protection, and security of operational data processes, blockchain technology is transforming the IoT-based healthcare industry. In this chapter, we proposed AI and Blockchain based framework for improving the data security in the smart cities domain.

A. S. Rajawat
Department of Computer Science Engineering, Shri Vaishnav Vidyapeeth Vishwavidyalaya, Indore, India

P. Bedi
Computer Science and Engineering, Lingaya's Vidyapeeth, Faridabad, Haryana, India

S. B. Goyal
City University, Petaling Jaya, Malaysia

R. N. Shaw
Department of Electrical, Electronics and Communication Engineering, Galgotias University, Greater Noida, India
e-mail: r.n.s@ieee.org

A. Ghosh (✉)
School of Engineering and Applied Sciences, The Neotia University, Sarisha, West Bengal, India

S. Aggarwal
Department of Computer Science Engineering, Maharaja Agrasen Institute of Technology, New Delhi, India

V. Piuri et al. (eds.), *AI and IoT for Smart City Applications*, Studies in Computational Intelligence 1002, https://doi.org/10.1007/978-981-16-7498-3_12

Keyword Artificial intelligence · Blockchain · Healthcare data security · Smart city

1 Introduction

Blockchain was first developed to support Bitcoin, but it has now evolved into a technology used to operate a wide range of distributed systems. Overall, healthcare [1] can be thought of as a three-part system: (a) core service provider of medical care services including such physicians, nurses, healthcare administrations, and professionals; (b) important services associated with medical care services such as medical research and health insurance; and (c) consumers or members of the general public who require medical or health-related services. It is believed that the current healthcare system will incorporate contact-based and technology-based remote monitoring services provided by constituent service providers to encourage, maintain, or repair recipients' health [2]. The healthcare industry is becoming increasingly interested in several areas of artificial intelligence and Blockchain, such as the immutability of data stored on a blockchain. Many of the apps already available show promising results in this regard. Incorporating artificial intelligence, blockchain technology, and smart healthcare can address conventional smart healthcare's pain points in sharing information, data security, and privacy management, enhance user-centered smart healthcare systems, and establish a multiparty medical alliance chain encompassing government agencies, private companies, and persons to enhance smart healthcare's industrialization. In Fig. 1 show AI And Blockchain-based Data Security in Smart Cities.

We are starting with the top-level design, doctor management, medical records [3] record keeping, treatment optimization, social inclusion, cost savings, externally and internally regulation, medical insurance, and environmental governance, artificial intelligence and Blockchain are helping to improve the Internet of Things-based smart healthcare system. Designing at the highest level, managing medical records, and managing doctors are the primary reasons for system construction; second, in the field of smart healthcare, artificial intelligence and blockchain applications are focused primarily on intelligent contracts, which are dependent on medical records management and are confined by the system, and optimizing the application is the key to upgrading the system. The third point to make is that as the system grows and evolves, regulation, medical insurance, and environmental governance all serve as protective functions, effectively defending stakeholders' interests. The effectiveness of internal and external regulation is critical to the system's health, and health insurance and environmental governance must be encouraged at the first three levels of government. Therefore, the transaction, information, and stakeholder layers must all be present in the intelligent medical service system based on artificial intelligence and blockchain technology.

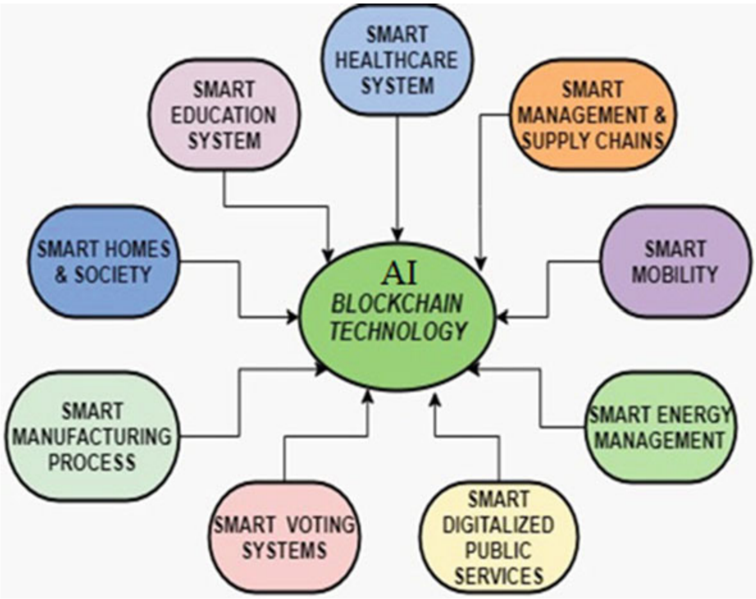

Fig. 1 AI and blockchain-based data security in smart cities

2 Related Work

Bitcoins are just one example of how blockchain technology might be used. It can be employed in a variety of areas, including healthcare. The proposed solution was based on the bitcoin technique, which satisfied the needs of information clients while also protecting patients' privacy. According to this concept, if a consumer wants to look at a patient's record, they must pay a fee in bitcoins. The disadvantage is that the patient's information could be exploited, and paying fees each time is costly. The research changed from public blockchain networks to private blockchain networks. Many people in the healthcare industry need access to the same information. Gem Health Network was founded as a blockchain-based healthcare platform [4]. This design allows information to be shared among multiple entities. The most up-to-date treatment information is readily available to avoid the usage of outdated material. It also shows all of the patent's prior interactions with doctors.

The Blockchain's Ownership The two most popular types of blockchains are permissioned and permissionless blockchains [5]. A permissioned blockchain has been created with a single or several authorities in mind. The verification procedure might be carried out by a central authority or a group of trusted pre-selected partners (consortium).

A group of individuals or several groups controls the Blockchain, and data access is limited to them [6]. A smaller number of players means more efficiency and scalability.

At the end of the day, these blockchains have a central authority [7]. Due to their large number of nodes, permissionless blockchains are completely decentralized and inefficient. Participants' prior consent is not required for the mining of transaction blocks in these blockchains. In exchange for a monetary payment, anyone can lend their computer power to network operations.

This Blockchain is public since it allows the whole public to read and publish transactions to it [8]. The system has decentralization, timestamps, communal maintenance, programmability, and tamper-proofing. Due to a shortage of blockchain applications in medical care, researchers are currently looking to combine Blockchain with other specialized information technology.

Similarly, health insurance might be simplified by removing the need to review medical records [9]. Assuring patients' rights and reducing hospital uncollected payments and management costs are all benefits of using blockchain technology in medical insurance. Table 1 represents the For smart cities, a comparative analysis of several factors for Blockchain Applications in Healthcare System and Table 2 Comparative analysis of different parameters for Blockchain Applications in Healthcare System for smart cities.

Comparative Analysis

Table 1 For smart cities, a comparative analysis of several factors for Blockchain Applications in Healthcare System

S. no.	Citation	Blockchain-based healthcare system for smart cities	Research gaps
1	Hölbl et al. [10]	DEMATEL, fuzzy set theory, and the ISM technique	All possible qualities are missing. China provided the majority of the data
2	Wang et al. [11]	Artificial systems for healthcare	The technology digitizes patients' vital signs and uses a wearable gadget
3	Wang et al. [12]	A decentralised Ethereum network connects manufacturers, distributors, GPOs, and healthcare providers	Contracts should remain secret. Changes to contract source code data fields would be necessary
4	Zheng et al. [13]	Simulation of a PBFT-based healthcare blockchain network using CTMC models	Nodes that fail to replicate are not counted. Component processing methods are not evaluated. In the future, a more detailed CTMC model will be constructed
5	Goel et al. [14]	A blockchain-based healthcare duo Healthcare authority and patient blockchains are combined to promote privacy	Health data is too big for Blockchain. A third party's access may compromise security

Table 2 Comparative analysis of different parameters for AI based appraoch Healthcare System for smart cities

S. no.	Citation	AI based approach healthcare system for smart cities	Research gaps
1	Yu et al. [15]	The usage of image-based diagnostics is increasing in fields like robotic surgery and pathology	In the absence of high-quality training data, deep networks' results are difficult to interpret by humans
2	Dorado-Díaz et al. [16]	Cardiography Using NN	The risk of inaccurate findings and the ML model's interpretability
3	Khan et al. [17]	Mobile health systems use ESMs, EMAs, CT and MRI images to measure patients' correlations between events and disease development	A lack of trained medical people to analyze AI-generated data
4	Reddy et al. [18]	Fuzzy logic-based healthcare delivery, management, and patient monitoring systems	Medical-legal considerations, as well as the risk of sampling bias
5	Noorbakhsh-Sabet et al. [19]	Epidemic forecasting, disease diagnosis, treatment efficacy, medication discovery, and clinical trials	Concerns about data security, clinical staff and patient acceptance of system outcomes

3 Artificial Intelligence (AI) and Blockchain in the Healthcare Industry

The quantity of patient data that healthcare providers and insurance companies have been sharing has increased rapidly in recent years, resulting in the establishment of data-driven healthcare models. The presence of high levels of security and access control in IoT-based healthcare services, which generate and manage tremendous amounts of personal data, is essential. There are numerous methods to enhance the efficiency and quality of smart healthcare with AI. Blockchain technology can help increase claim adjudication quality while also aiding with administrative issues related to healthcare, as medical records are accurate and interoperable with the use of Blockchain in healthcare systems. In this context, the combination of AI and Blockchain [20] can improve data security and data integrity. We could design a data management system that uses Blockchain to manage patient health data by building a shared and unchangeable data structure. Many healthcare records are scattered throughout different healthcare institutions and organizations, leaving patient data out of reach to healthcare providers when they need it most. Healthcare providers have a big problem on their hands. With the usage of AI and Blockchain for the transfer and securing of patient health records and medical data as well as its monetization for

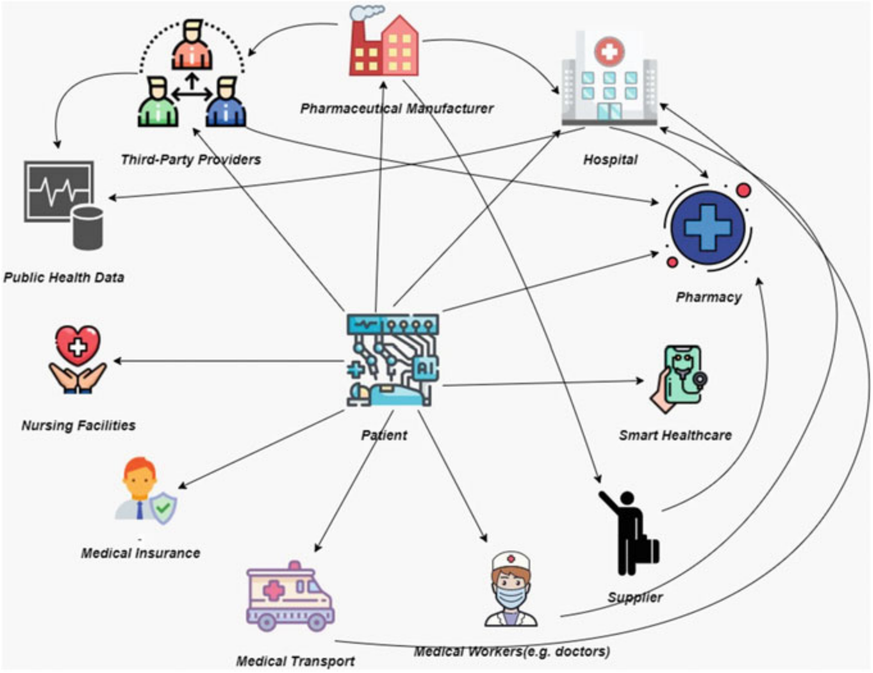

Fig. 2 Stakeholders of healthcare sector

research, smart healthcare is on the rise. In Fig. 2 show the Stakeholders of healthcare sector.

Working Principle of AI And Blockchain

This is how AI and Blockchain are implemented:

Step 1: A blockchain user requests a transaction.

Step 2: Other members are shown the request (i.e., nodes).

Step 3: The network of nodes then confirms the transaction.

Step 4: The nodes complete the transaction after approving the request.

Step 5: A new immutable block is introduced to the blockchain network.

Step 6: A new data block is formed by joining confirmed transactions. To submit data to the Blockchain, one must first log in with a public address and a private key.

AI and Blockchain [21] offer great reliability in e-health services, which may help deliver more tailored and effective treatment. Blockchain allows for secure decentralisation of patient data, using AI-based technique machine learning and deep learning, making medical records and paperwork more accessible to patients and professionals. Doctors may detect severe illnesses earlier with rapid access to health data, perhaps saving many lives. As the horrific events around COVID-19 demonstrated [22], this is critical in urban environments. COVID-19 makes a solid argument for further blockchain integration. These qualities can replace today's value networks, which lack connectedness and frictionless data interchange. To tackle the COVID-19 epidemic, several researchers used blockchain technology to help health professionals make better decisions about social distance and quarantine measures. Using technology, smart citizens' health data might be protected from theft and misuse during this outbreak. For patient ID validation, data security businesses [23] collaborated with smart cities users. Every citizen got a smartcard that linked their SHER (Standardized electronic health record) data to their blockchain identification. Changing the SEHR generates a hash that gets logged in the Blockchain. That way, the SEHR data has a permanent audit trail and cannot be purposely altered. Immutable, timestamped data logs can also be utilized to archive data in existing healthcare databases. Any change to the healthcare database is timestamped and cryptographically signed in a block. In the pharmaceutical industry, drug development and research are among the most costly activities due to escalating healthcare expenses and a drive to develop novel pharmacological cures faster. To allow the exchange of reliable information and knowledge among many people, blockchain technology may be used. Even in non-collaborative research and drug development scenarios, Blockchain can help track and manage data, consent, and adverse drug effects, to mention a few. Pharmaceutical companies rarely outsource clinical research jobs. In this scenario, Blockchain could help ensure data integrity and outcomes verification. With its distributed nature, blockchain technology is suitable for big medical data and IoT-based wearable devices. Blockchain technology can help big data technologies deliver on their promises and generate new applications based on healthcare data. When managing or keeping data, privacy and security are always concerns. To authenticate records, the Blockchain uses consensus rather than third-party permission because all participants can see data. This technology threatens information security and privacy by allowing anyone to view records. Patients can provide authorized staff members access to their data in an emergency, placing it in danger. Blockchain was developed to store and process transaction data. Its limited storage capacity has become a major healthcare data storage issue. Rapid data collection and analysis using Deep learning is used for Covid-19. Hospitalizations, covid-19 test results, X-rays, and death require a lot of storage. Fast-paced programs hate it when database growth slows record searching and information access. Using massive algorithms to secure blockchains can lead to data leakage. Algorithms can be used to bypass security and access a database. The security of patient data is critical.

This is a serious challenge in blockchain-based healthcare. As indicated previously, experts or other employees share patient data. Also, because blockchain and service providers interact, unsecured data exchange is Covid-19 raises possible Indirect and direct cybersecurity threats in healthcare networks. These include DDoS attacks [24], health data theft, and ransomware.

4 Proposed Methodology

Using private Blockchain in healthcare is a great way to preserve data while also preserving patient privacy. Private blockchains allow only a few people to access data, limiting information access [25]. Data access control on a private blockchain is stringent. Furthermore, only approved individuals or patients will access and maintain their data and medical records, held in a private centralized blockchain. It may be a feasible way to protect data. It also improved privacy and security.

Cloud data storage and analysis using AI: Insecure cloud architecture, this option is useful for data storage, sharing, and classification [26]. This gives patients access to and control over their own data. Because Blockchain only provides a limited amount of data storage, healthcare apps have issues keeping regularly generated data. Cloud storage allows the Blockchain to manage enormous amounts of data while also allowing these apps to store data.

Proof of interoperability is a consensus approach that efficiently allows healthcare apps to perform transactions based on network participants' compatibility. The Cloud Middleware will fetch information from the previous level utilizing REST services. The third level will manage the blockchain [27] network's nodes. The blockchain function is separated into various layers, improving interoperability. Figure 3 show the Proposed AI and Blockchain framework.

Multi-factor authentication [28]: Identification can be verified via MFA. To modify the information or store it in blocks or add new blocks of information, 51 percent of all participants must agree. Fraudsters can assume a verified participant's identity and manipulate data. To avoid this risk, multifactor authentication can be utilized to authenticate users. Researchers are leveraging these tools to build AI-based predictive frameworks to improve medical informatics and diagnostics. A few of the practical responsibilities addressed in the healthcare area include prescription fraud prevention, verifiable data collecting, and automatic claim settlement.

Studies have built frameworks to lower the cost of execution, storage, and preservation of data of any scale. These new frameworks are said to improve runtime, delivery, and reaction times. System interoperability, inter-institutional credential management, and data control have all been examined. Prior work on AI and blockchain [29] data management features in healthcare focused on safeguarding data privacy by limiting access to medical records. The study states that access control management [30] has received specific attention. This research focuses on critical healthcare because it protects patient privacy by improving accountability, immutability, and access control. A priori research has established AI-blockchain-based [31] frameworks for efficient, user-centric, secure/encrypted access to patient PHRs and other medical data. Interoperability, authentication, and safe data sharing are all addressed by blockchain applications.

Results

To perform the simulation using the python language and anaconda tools. This study's purpose was to assess the existing state and future possibilities of blockchain

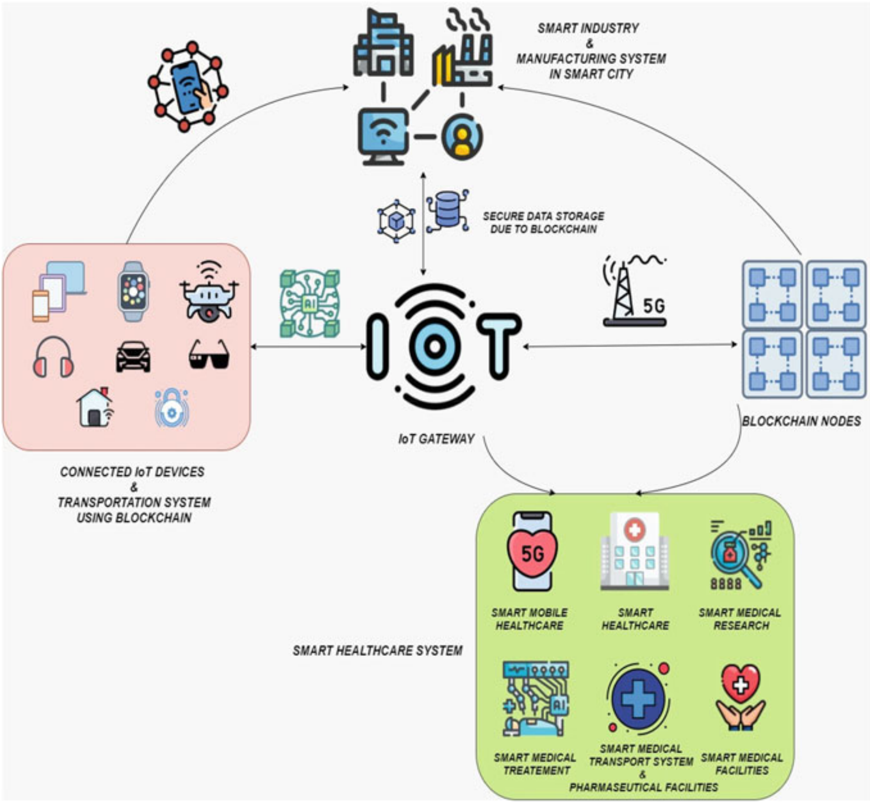

Fig. 3 Proposed AI and blockchain framework

applications in healthcare. Several factors influence the adoption of Blockchain in smart healthcare development [32]. The manner, mechanism, and degree of activity vary depending on the conditions. Blockchain is being investigated and used more in healthcare. According to current trends, Blockchain is used in healthcare for data exchange, health records, and access control, but not for supply chain management or pharmaceutical prescription management. That means a lot of Blockchain's power is unused. Blockchain is largely utilized in healthcare [33] to share EHRs. The traditional security approaches to protecting healthcare apps were inadequate in the past. Blockchain has recently offered new security approaches and procedures for healthcare applications, enabling data security and privacy for clinical, biological, and HER medical applications. Secure blockchain-based [34–36] service computing is vital for trust-free sharing services. Because the Blockchain is decentralized, data availability is not dependent on other parties [26, 37, 38].

We considered the following aspects before making our decision:

- Batch-Time-out: This is when the ordering requires a batch to be generated before it is canceled.

- Batch Size: The number of total messages and bytes in a batch. Amount OF BYTES PER BATCH—The most desired option is the total bytes per batch of serialized messages. Messages that are over the length of the maximum byte will result in batches that are too long. Components running Python and Anaconda with a Laptop with 4 GB RAM and 2.3 GHz Intel Core i3 7th Gen. the process of putting additional pieces in.

Clustered blockchain-IoT architecture: To simulate the prototype, ten IoT sensors were used. Each device generated a random number of network transactions (Figs. 4 and 5).

The blockchain implementation will raise network traffic overhead. In our experiments, we compared the network traffic overhead of conventional and clustered blockchain implementations [39–41]. Block Time: We simulated for 3 h. We found that as the number of blocks increased, so did the processing time. Most systems use a permissionless blockchain network, allowing anybody to join while remaining

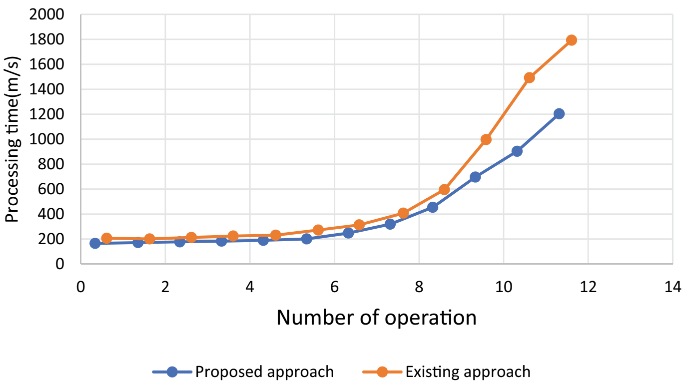

Fig. 4 Comparing processing time between the existing system and the planned blockchain system

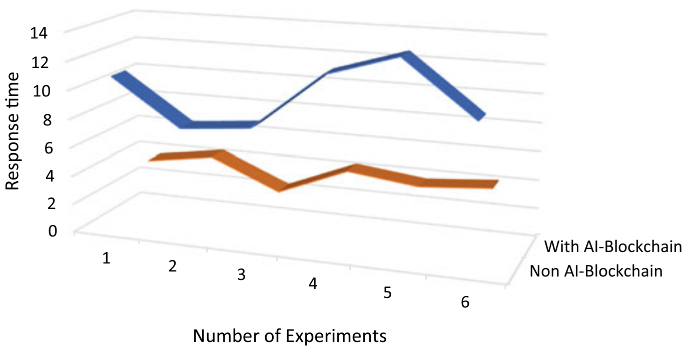

Fig. 5 Write time comparison: existing system versus planned blockchain system

anonymous. So neither the contracts nor the transaction details are secret [42–44]. To maintain privacy, the systems incentivize high-cost or high-performance mining of intelligent contracts. A transaction's cost and speed can be altered.

5 Conclusion

Data breaches, data theft or leakage, manipulation, and other security threats make healthcare data management and storage problematic. Traditional security approaches to protect healthcare apps have proven ineffective. AI and Blockchain have recently offered new security approaches and processes for healthcare applications, giving data confidentiality and privacy. When implemented appropriately, blockchain technology opens up a world of possibilities beyond bitcoin. Blockchain may eliminate central authority and thus the commission. Data can be supplied directly to machine learning algorithms. Due to its rapid expansion, Blockchain has been employed in various ways to improve medical care automation. Most AI and blockchain-related healthcare research focus on e-health record sharing. Blockchain researchers are also interested in biotechnology, pharmaceutical supply chains, and insurance. Articles on implementation are also infrequent. While blockchain technology holds great promise, more research is required to comprehend, develop, and assess it completely. To increase stakeholder trust in adopting this technology and its acceptance in healthcare, ongoing efforts are being made to address scalability, security, and privacy issues.

We will study and analyze advances in electronic devices that have expanded wireless communication system technology globally in future work. As a result, 5G and Blockchain have accelerated communication. We will study the global issue of COVID-19 that has created worry about Blockchain-based smart healthcare application issues in the edge computing environment.

References

1. Yoon H-J (2019) Blockchain technology and healthcare. Healthcare Informat Res 25(2):59. https://doi.org/10.4258/hir.2019.25.2.59
2. Tandon A et al (2020) Blockchain in healthcare: a systematic literature review, synthesizing framework and future research agenda. Comput Ind 122(103290):103290. https://doi.org/10.1016/j.compind.2020.103290
3. Ahmad K (2020) Blockchain technology and its implementations in medical and healthcare field. Int J Eng Res Technol 9(9). https://www.ijert.org/blockchain-technology-and-its-implementations-in-medical-and-healthcare-field. Accessed 20 Aug 2021
4. Du X et al (2021) Research on the application of blockchain in smart healthcare: constructing a hierarchical framework. J Healthcare Eng. https://www.hindawi.com/journals/jhe/2021/6698122/. Accessed 10 June 2021

5. Ray PP et al (2020) Blockchain for IoT-based healthcare: background, consensus, platforms, and use cases. IEEE Syst J 15(1):1–10. https://doi.org/10.1109/jsyst.2020.2963840. Accessed 27 Mar 2020
6. Vyas S et al (2019) Converging blockchain and machine learning for healthcare. IEEE Xplore. ieeexplore.ieee.org/document/8701230. Accessed 20 Aug 2021
7. Yaqoob S et al (2019) Use of blockchain in healthcare: a systematic literature review. Int J Adv Comput Sci Appl 10(5). https://doi.org/10.14569/ijacsa.2019.0100581. Accessed 21 Nov 2019
8. Nguyen DC, Ding M, Pathirana PN, Seneviratne A (2021) Blockchain and AI-based solutions to combat coronavirus (COVID-19)-like epidemics: a survey. IEEE Access 9:95730–95753. https://doi.org/10.1109/ACCESS.2021.3093633
9. Agbo C et al (2019) Blockchain technology in healthcare: a systematic review. Healthcare 7(2):56. https://www.mdpi.com/2227-9032/7/2/56/htm. https://doi.org/10.3390/healthcare7020056
10. Hölbl M et al (2018) A systematic review of the use of blockchain in healthcare. Symmetry 10(10):470. https://www.res.mdpi.com/symmetry/symmetry-10-00470/article_deploy/symmetry-10-00470-v2.pdf. https://doi.org/10.3390/sym10100470
11. Wang S et al (2018) Blockchain-powered parallel healthcare systems based on the ACP approach. IEEE Trans Comput Soc Syst 5(4):942–950. https://doi.org/10.1109/tcss.2018.2865526. Accessed 9 Sep 2019
12. Omar IA, Jayaraman R, Debe MS, Salah K, Yaqoob I, Omar M (2021) Automating procurement contracts in the healthcare supply chain using blockchain smart contracts. IEEE Access 9:37397–37409. https://doi.org/10.1109/ACCESS.2021.3062471
13. Zheng K, Liu Y, Dai C, Duan Y, Huang X (2018) Model checking PBFT consensus mechanism in healthcare blockchain network. In: 2018 9th International conference on information technology in medicine and education (ITME), 2018, pp 877–881. https://doi.org/10.1109/ITME.2018.00196
14. Goel U, Ruhl R, Zavarsky P (2019) Using healthcare authority and patient blockchains to develop a tamper-proof record tracking system. In: 2019 IEEE 5th intl conference on big data security on cloud (BigDataSecurity), IEEE Intl conference on high performance and smart computing, (HPSC) and IEEE Intl conference on intelligent data and security (IDS), 2019, pp 25–30. https://doi.org/10.1109/BigDataSecurity-HPSC-IDS.2019.00016
15. Yu Kun-Hsing et al (2018) Artificial intelligence in healthcare. Nat Biomed Eng 2(10):719–731. https://www.nature.com/articles/s41551-018-0305-z. https://doi.org/10.1038/s41551-018-0305-z
16. Dorado-Díaz P Ignacio et al (2019) Applications of artificial intelligence in cardiology. The future is already here. Revista Española de Cardiología (English Edition) 72(12):1065–1075. https://doi.org/10.1016/j.rec.2019.05.014. Accessed 12 Dec 2019
17. Faizal KZ, Alotaibi SF (2020) Applications of artificial intelligence and big data analytics in m-health: a healthcare system perspective. J Healthcare Eng. https://www.hindawi.com/journals/jhe/2020/8894694/
18. Reddy S et al (2018) Artificial intelligence-enabled healthcare delivery. J R Soc Med 112(1):22–28. https://doi.org/10.1177/0141076818815510
19. Noorbakhsh-Sabet N et al (2019) Artificial intelligence transforms the future of health care. Am J Med 132(7):795–801. https://doi.org/10.1016/j.amjmed.2019.01.017
20. Treiblmaier H et al (2020) Blockchain as a driver for smart city development: application fields and a comprehensive research agenda. Smart Cities 3(3):853–872. https://doi.org/10.3390/smartcities3030044. Accessed 12 Aug 2020
21. Angraal S et al (2017) Blockchain technology. Circul Cardiovasc Qual Outcomes 10(9). https://doi.org/10.1161/circoutcomes.117.003800
22. Chamola V, Hassija V, Gupta V, Guizani M (2020) A Comprehensive review of the COVID-19 pandemic and the role of IoT, drones, AI, blockchain, and 5G in managing its impact. IEEE Access 8:90225–90265. https://doi.org/10.1109/ACCESS.2020.2992341

23. Firouzi F et al. (2021) Harnessing the power of smart and connected health to tackle COVID-19: IoT, AI, robotics, and blockchain for a better world. In: IEEE IoT J 8(16):12826–12846. https://doi.org/10.1109/JIOT.2021.3073904
24. Tanwar S, Bhatia Q, Patel P, Kumari A, Singh PK, Hong W (2020) Machine learning adoption in blockchain-based smart applications: the challenges, and a way forward. IEEE Access 8:474–488. https://doi.org/10.1109/ACCESS.2019.2961372
25. Sun J et al (2016) Blockchain-based sharing services: what blockchain technology can contribute to smart cities. Fin Innov 2(1). https://doi.org/10.1186/s40854-016-0040-y
26. Rajawat AS, Barhanpurkar K, Goyal SB, Bedi P, Shaw RN, Ghosh A (2022) Efficient deep learning for reforming authentic content searching on big data. In: Bianchini M, Piuri V, Das S, Shaw RN (eds) Advanced computing and intelligent technologies. Lecture notes in networks and systems, vol 218. Springer, Singapore. https://doi.org/10.1007/978-981-16-2164-2_26
27. Alam T (2021) Blockchain cities: the futuristic cities driven by Blockchain, big data and internet of things. GeoJournal. https://doi.org/10.1007/s10708-021-10508-0
28. Rajawat AS, Rawat R, Barhanpurkar K, Shaw RN, Ghosh A (2021) Blockchain-based model for expanding IoT device data security. In: Bansal JC, Fung LCC, Simic M, Ghosh A (eds) Advances in applications of data-driven computing. advances in intelligent systems and computing, vol 1319. Springer, Singapore. https://doi.org/10.1007/978-981-33-6919-1_5
29. Tagde P, Tagde S, Bhattacharya T et al (2021) Blockchain and artificial intelligence technology in e-Health. Environ Sci Pollut Res. https://doi.org/10.1007/s11356-021-16223-0
30. Rajawat AS, Rawat R, Shaw RN, Ghosh A (2021) Cyber physical system fraud analysis by mobile robot. In: Bianchini M, Simic M, Ghosh A, Shaw RN (eds) Machine learning for robotics applications. Studies in computational intelligence, vol 960. Springer, Singapore. https://doi.org/10.1007/978-981-16-0598-7_4
31. Yaqoob I, Salah K, Jayaraman R et al (2021) Blockchain for healthcare data management: opportunities, challenges, and future recommendations. Neural Comput Appl. https://doi.org/10.1007/s00521-020-05519-w
32. Rajawat AS, Barhanpurkar K, Shaw RN, Ghosh A (2021) Risk detection in wireless body sensor networks for health monitoring using hybrid deep learning. In: Mekhilef S, Favorskaya M. Pandey RK, Shaw RN (eds) Innovations in electrical and electronic engineering. Lecture notes in electrical engineering, vol 756. Springer, Singapore. https://doi.org/10.1007/978-981-16-0749-3_54
33. Rejeb A, Treiblmaier H, Rejeb K et al (2021) Blockchain research in healthcare: a bibliometric review and current research trends. J Data Inf Manage 3:109–124. https://doi.org/10.1007/s42488-021-00046-2
34. Zhang G, Li T, Li Y et al (2018) Blockchain-based data sharing system for AI-powered network operations. J Commun Inf Netw 3:1–8. https://doi.org/10.1007/s41650-018-0024-3
35. Bedi P, Goyal SB, Rajawat AS, Shaw RN, Ghosh A (2022) A framework for personalizing atypical web search sessions with concept-based user profiles using selective machine learning techniques. In: Bianchini M, Piuri V, Das S, Shaw RN (eds) Advanced computing and intelligent technologies. Lecture notes in networks and systems, vol 218. Springer, Singapore. https://doi.org/10.1007/978-981-16-2164-2_23
36. Goyal SB, Bedi P, Rajawat AS, Shaw RN, Ghosh A (2022) Multi-objective fuzzy-swarm optimizer for data partitioning. In: Bianchini M, Piuri V, Das S, Shaw RN (eds) Advanced computing and intelligent technologies. Lecture notes in networks and systems, vol 218. Springer, Singapore. https://doi.org/10.1007/978-981-16-2164-2_25
37. Garg C, Namdeo A, Singhal A, Singh P, Shaw RN, Ghosh A (2022) Adaptive fuzzy logic models for the prediction of compressive strength of sustainable concrete. In: Bianchini M, Piuri V, Das S, Shaw RN (eds) Advanced computing and intelligent technologies. Lecture notes in networks and systems, vol 218. Springer, Singapore. https://doi.org/10.1007/978-981-16-2164-2_47
38. Palimkar P, Bajaj V, Mal AK, Shaw RN, Ghosh A (2022) Unique action identifier by using magnetometer, accelerometer and gyroscope: KNN approach. In: Bianchini M, Piuri V, Das S, Shaw RN (eds) Advanced computing and intelligent technologies. Lecture notes in networks and systems, vol 218. Springer, Singapore. https://doi.org/10.1007/978-981-16-2164-2_48

39. Rawat R, Mahor V, Chirgaiya S, Shaw RN, Ghosh A (2021) Analysis of darknet traffic for criminal activities detection using TF-IDF and light gradient boosted machine learning algorithm. In: Mekhilef S, Favorskaya M, Pandey RK, Shaw RN (eds) Innovations in electrical and electronic engineering. Lecture notes in electrical engineering, vol 756. Springer, Singapore. https://doi.org/10.1007/978-981-16-0749-3_53
40. Rawat R, Rajawat AS, Mahor V, Shaw RN, Ghosh A (2021) Dark web—onion hidden service discovery and crawling for profiling morphing, unstructured crime and vulnerabilities prediction. In: Mekhilef S, Favorskaya M, Pandey RK, Shaw RN (eds) Innovations in electrical and electronic engineering. Lecture notes in electrical engineering, vol 756. Springer, Singapore. https://doi.org/10.1007/978-981-16-0749-3_57
41. Paul A, Sinha S, Shaw RN, Ghosh A (2021) A neuro-fuzzy based IDS for internet-integrated WSN. In: Bansal JC, Paprzycki M, Bianchini M, Das S (eds) Computationally intelligent systems and their applications. Studies in computational intelligence, vol 950. Springer, Singapore. https://doi.org/10.1007/978-981-16-0407-2_6
42. Rawat R, Mahor V, Chirgaiya S, Shaw RN, Ghosh A (2021) Sentiment analysis at online social network for cyber-malicious post reviews using machine learning techniques. In: Bansal JC, Paprzycki M, Bianchini M, Das S (eds) Computationally intelligent systems and their applications. Studies in computational intelligence, vol 950. Springer, Singapore. https://doi.org/10.1007/978-981-16-0407-2_9
43. Kumar A, Das S, Tyagi V, Shaw RN, Ghosh A (2021) Analysis of classifier algorithms to detect anti-money laundering. In: Bansal JC, Paprzycki M, Bianchini M, Das S (eds) Computationally intelligent systems and their applications. Studies in computational intelligence, vol 950. Springer, Singapore. https://doi.org/10.1007/978-981-16-0407-2_11
44. Rawat R, Rajawat AS, Mahor V, Shaw RN, Ghosh A (2021) Surveillance robot in cyber intelligence for vulnerability detection. In: Bianchini M, Simic M, Ghosh A, Shaw RN (eds) Machine learning for robotics applications. Studies in computational intelligence, vol 960. Springer, Singapore. https://doi.org/10.1007/978-981-16-0598-7_9