Blockchain-Driven Security, Privacy and Reliability for Digital Healthcare Systems

Radhiya Sulaiman Nasser Alhabsi and Alla Salim Mohammed Almukhaini
University of Nizwa, 616 Nizwa, Sultanate of Oman
RadhiyaAlhabsi@unizwa.edu.om, 12468128@uofn.edu.om

Keywords: IoT-Blockchain Platform, Data Integrity, Smart Contracts, Sensor Data Management, Decentralized Security.

Abstract: With the integration of digital technologies in healthcare, several transformative advances have been made, including the management and sharing of patient data. Security, privacy, and system reliability are among the challenges presented by digitizing health data. Health data integrity, confidentiality, and reliability are all ensured by blockchain technology because of its decentralized, immutable nature. The purpose of this paper is to explore the potential of blockchain technology by using it to address medical imaging, diagnosis, and secure data sharing. Combining distributed ledger technology and cryptography can improve the security, privacy, and interoperability of healthcare systems. Using blockchain-driven AI models, the study illustrates how medical imaging applications can be significantly enhanced through secure, auditable, and transparent data-sharing practices, thus increasing stakeholder trust and substantially enhancing the scalability and reliability of AI-driven systems. By effectively combining blockchain's decentralized security features with advanced artificial intelligence techniques, diagnostic accuracy can be improved, patient care and clinical decision-making processes can be optimized, and strict regulatory compliance in medical imaging environments can be consistently maintained. This integrated approach also facilitates smoother collaboration among medical professionals.

1 INTRODUCTION

With the advent of digital technologies, the storage, sharing, and analysis of healthcare data have been transformed. With EHRs, telemedicine platforms, and wearable health devices, patients now have real-time access to data and can make better decisions regarding their health. Patient and healthcare provider data are increasingly digitizing and being shared across platforms, resulting in greater risks of data breaches, unauthorized access, and system failures. Digital data can be secured and managed in a decentralized, immutable, and transparent manner with blockchain technology. Healthcare has found extensive use for Blockchain's underlying features, including distributed ledger technology (DLT), cryptographic security, and smart contracts [1]. By means of blockchain technology, sensitive health data can be stored and shared in a secure, tamper-proof manner that ensures data integrity and confidentiality while allowing patients greater control over their health information. The decentralized nature of Blockchain can also mitigate the risks associated with centralized data management, where a single point of failure may compromise system reliability [2].

A crucial component of modern healthcare is imaging and diagnostics, which improve outcomes and help make better decisions for patients. An X-ray or MRI generates a huge amount of complicated data that must be interpreted immediately. Healthcare systems worldwide face substantial challenges due to a global shortage of radiologists and diagnosticians, as well as an increase in the complexity of medical imaging data. As a result of artificial intelligence, image analysis, anomaly detection, and predictive diagnosis have been transformed [3], [4]. The use of artificial intelligence in medical imaging is not without challenges, including data security, interoperability, and trustworthiness. In order for AI-driven healthcare systems to be open, privacy-conscious, and efficient, comprehensive frameworks are needed. There are a number of difficulties that blockchain technology can solve [5].

Security, transparency, and accountability have all been improved through the decentralized and immutable ledger system blockchain. Blockchain can solve a variety of healthcare problems, including

ensuring the integrity of medical records, tracing AI training, and improving interoperability. As a result of Blockchain and AI, medical imaging applications can become more scalable and reliable, as sensitive patient data can be secured, regulatory compliance can be ensured, and collaboration between institutions can be facilitated in the development of AI models [6],[7],[8],[9]. Blockchain and artificial intelligence might transform medical imaging. A blockchain-based system ensures the sharing of imaging datasets among institutions while protecting the privacy and ownership of patient data. As a result, there may also be fewer data silos and biases in AI training since it creates decentralized training settings [10]. By utilizing AI-driven diagnostic models, professionals, patients, and regulators can benefit by enhancing trust and understanding.

Medical imaging and diagnosis could be improved by Blockchain and AI, as discussed in this article. As a first step, it addresses the challenges associated with standard medical imaging workflows as well as the limitations of independent AI solutions. This section examines blockchain technology's potential to resolve these issues with a focus on the safe sharing of data, the validation of AI models, and compliance with regulatory requirements. Author [1], cutting-edge blockchain-driven artificial intelligence implementations and research are discussed in relation to medical imaging and diagnostic imaging. In addition to its technological effects, this integration has a social impact. As blockchain and artificial intelligence become more widespread, sophisticated diagnostic technologies can become more affordable, especially in impoverished areas. Additionally, they improve the accuracy, efficiency, equity, and patient-centeredness of medical imaging.

Medical imaging and diagnostics may undergo a revolution thanks to Blockchain and artificial intelligence. Through the implementation of these technologies, long-standing problems may be solved, and new opportunities may be created to improve the health ecosystem's resilience, security, and efficiency. Further research into its implications and applications will be encouraged by this study, as well as illuminating this intriguing junction. Diagnoses and treatment plans are aided by medical imaging in healthcare. Increasingly sophisticated imaging modalities and the desire to improve diagnostic accuracy have led to the implementation of AI in this field as an important facilitator of innovation. The use of artificial intelligence to analyse images, detect anomalies, and predict outcomes leads to improved diagnostic efficiency and accuracy [11]. The security, trustworthiness, and scalability of medical imaging limit its potential.

AI for medical imaging is challenging because healthcare data is delicate. Medical imaging datasets usually contain personally identifiable information, which is subject to strict privacy laws and compliance with HIPAA and GDPR [12]. Data breaches in centralized data management systems raise privacy and security concerns. Additionally, the quality and reliability of AI algorithms are strongly influenced by diversified and high-quality datasets. In the absence of transparent data infrastructures and institutional resistance to sharing private information, AI systems cannot function optimally. Having a model that is easily explainable and auditable is another critical issue. AI decision-making should be transparent so that clinicians and regulators can foster trust and accountability. In traditional AI systems, decision processes tend to be hidden within black boxes, making tracking them difficult [13], [14]. Regulatory compliance can be complicated when there is a lack of transparency in high-stakes healthcare applications. Medical imaging could benefit from blockchain technology, but its use with AI is still being explored. With Blockchain's decentralized, immutable ledger structure, patients' data can be exchanged safely, and AI models can be trained collaboratively without compromising their privacy. An AI algorithm's traceability and dependability can be improved using Blockchain by tamper-proofing training data and model validation. There are few academic publications and real-world applications on blockchain-driven artificial intelligence in medical imaging that address implementation, scalability, and interoperability.

2 LITERATURE REVIEW

There are a number of traditional components to the healthcare system, including doctors, patients, laboratories, hospitals, electronic health records, and patient information systems. Additionally, they can be used for monitoring, diagnosing, treating, conducting medical research, making decisions, and managing hospitals. The above healthcare services require key-enabling technologies to be controlled and managed.

2.1 Internet of Things-Based Smart Healthcare Systems

Additionally, it is necessary to manage the physical assets of the health care system so that their location

and number can be tracked in the event of an emergency, including oxygen cylinders, nebulizers, wheelchairs, oxygen meters, heart monitors, personal protective equipment, and surgical tools. [15], [16]. Using an IoT-based healthcare asset management application, these assets can be tracked quickly. Their discussion includes, for instance, how advanced medical facilities are required in a short amount of time to treat COVID-19 [17], [18]. A cloud-based data centre with hybrid communication, colossal medical screening, and hybrid communication capabilities is proposed to assist hospitals, rescue teams, and first aid units in healthcare monitoring. An edge-enabled IoT healthcare management system for monitoring, diagnosing, and managing patient data was presented by Author [19]. This proposal proposes a database-based system to manage and monitor medical tasks. A breach of the system is possible because of its centralized storage.

2.2 Smart Healthcare Systems Using Artificial Intelligence

Healthcare companies use intelligent and predictive services to provide precise, effective care and to streamline administrative tasks [20]. The healthcare industry generates and transmits a massive amount of data through IoT devices. Considering how much data is generated in the healthcare sector, AI technology could improve data management and data improvisation. Healthcare systems using artificial intelligence offer numerous benefits over those relying on cumbersome analytics and decision-making. It also helps clinicians make decisions based on medical data (training data) to provide valuable insights into medical diagnosis, treatment, and clinical decision support. According to [21], osteoporosis (dead bones) is usually detected by X-rays and magnetic resonance imaging (MRI). By incorporating AI-based features, the authors optimized the classification of osteoporosis patients based on ultrasound data.

Using artificial intelligence, a healthcare author [22] predicts heart attacks and cancer, as well as finds intelligent patterns in collected data. They developed a lightweight, secure and AI-based healthcare ecosystem communication scheme. Simulations were conducted to evaluate the scheme's performance, including end-to-end delays and throughput. As a result of their computation time comparison, decision trees are faster than other algorithms, and SVM is more accurate than existing algorithms [23]. An AI algorithm has been applied to sustainable development by the author [24]. Researchers have identified a number of scenarios in which AI-based question recommender systems may be useful. The study authors focused exclusively on enhancing AI-based question recommendations for both security screenings and financial services, as well as their application in healthcare. There has been much attention given to federated learning in healthcare recently for data offloading and privacy protection. The Author [25] proposed a framework based on federated learning to monitor healthcare data locally. As a result of their framework, medical professionals are also able to detect skin diseases more effectively. In addition to protecting patients' privacy, the researchers' proposed framework reduces operators' costs [26].

The author [27] also reviewed the problem of training machine learning models on the diverse data of healthcare. In this study, message queueing telemetry transport (MQTT) and decentralized algorithms were employed for brain tumour segmentation, which is referred to as federated learning. According to their results, the proposed framework is more accurate and latency-efficient in the regular operation of healthcare systems.

2.3 A Blockchain-Based Healthcare System

The author developed a system that prevents security breaches in electronic healthcare records by utilizing blockchain technology [28]. Security was provided by swarm intelligence and private blockchain technology for the IoT network. The recent COVID-19 pandemic has provided an opportunity to use blockchain technology to solve diabetes problems, according to Author [29]. As a result of the pandemic, diabetes patients were disproportionately affected by a constant monitoring system, oxygen, insulin pumps, and medical beds powered by blockchain technology. An interplanetary file system, smart contracts, and the new economy movement were used to develop a proof-of-concept model encrypting and authenticating patient data. It is impressive how fast, cheap, and efficient their system is in terms of transaction speed and fees, as well as power consumption [30].

2.4 Healthcare Technology Based on Cloud Computing

Healthcare industries are increasingly collaborating and connecting through cloud computing, edge computing, and fog computing in the Cloud [31]. The implementation of smart healthcare ecosystems is

facing a variety of challenges, such as high operational costs, privacy concerns, and centralized data storage issues. In healthcare workflows, cloud technology promotes accessibility, faster response times, better personalised care, and load balancing. Using fog and edge computing techniques, wearable devices and doctors can communicate more quickly. A wearable device that cannot communicate rapidly with medical practitioners can endanger the lives of ICU patients. Fog and edge computing enable medical devices to process their data locally, as opposed to transmitting it from a global model, making remote monitoring and patient engagement easier.

3 METHODOLOGY

The blockchain system ensures the safety and security of hospitals' EHR data by increasing their data security levels. At the Central Server, the data is stored on a blockchain, increasing its security. Using blockchain technology, data is stored in a highly secure manner thanks to a hash algorithm linking each block of data to another and a consensus mechanism connecting distributed peer-to-peer networks.

Using hashes of the previous blocks in a blockchain, it is possible to link all data blocks together in order of arrival to form a chain of blocks. Whenever data within a block is changed, the hash value will change as well. There will be an immediate indication of changes, and the original block will be retrieved as well. By hashing, changes can be flagged. A blockchain consists of several nodes whose hash values propagate from one block to another.

Blockchains are built on Ethereum platforms, as mentioned previously [14]. A Proof-of-Stake consensus mechanism has replaced Proof-of-Work, where mining nodes had to solve cryptographic puzzles to create a new block of currency. Consequently, processing costs increased due to the computational requirements for solving this problem. While Proof-of-Stake does not require solving puzzles, it is quicker and less expensive.

Using the web3.js library, we developed the blockchain interface API to connect with the Ethereum blockchain. In this library, you will find JavaScript functions related to multi-blockchains.

3.1 The Data Layer

Consensus blockchains record and share data via their block producer nodes. Blockchain technology prevents data from being altered or changed once it is recorded. Authentication and interaction with the data layer are handled by Data Sharing Modules, which enable unified data, improved authorization mechanisms, and more efficient access controls. A data layer can be accessed and interacted with by readers and writers using the application layer. Messages will be posted and received by the application layer, and the Data Sharing Module will create blockchain-compatible data structures. The Key Management Service (KMS) of Amazon Web Services manages and creates encryption keys for data storage. There is no way to expose any part of the KMS environment to the Master Key that encrypts Data Keys, which are encrypted and stored in the Blockchain.

3.2 Smart Contact

In the Smart Contract, 10 patient records are sent to mobile devices. In addition to the patient's personal information, there is information about the visit, information about laboratory tests, and information about drug orders. Solidity is the language we use to develop Ethereum's smart contracts. Patient information for a specific PID can be accessed using the mapping object, which stores patient information as a dictionary. When creating patient information, the system compares the Hash for a new visit to the Hash for the patient's most recent existing visit. The system will not be able to read new visitor information if that hash value repeats.

3.3 Application Programming Interface

ABlockchains are connected and interacted with through an Application Programming Interface (API). In the mobile application, API functions can be used to read and write patient data. With Node.js APIs, Amazon's Key Management System (AWS KMS) and Simple Storage Service (S3) are integrated, and two keys are encrypted: search hashes and encryption/decryption keys. Data that is encrypted will remain encrypted for as long as it exists without a means to decrypt it unless explicitly authorized.

A master key can be generated through the Amazon Key Management System (Amazon KMS). They are stored on an Amazon server with a very high level of security. Our application will use these keys to encrypt and decrypt data keys. In the blockchain system, patients' data is searched using a hashing key,

and API Servers and mobile applications encrypt and decrypt data using an encryption/decryption key.

3.3.1 Initialization

The initialization process involves the registration of three entities (Cloud, DO, and DU) and the publication of resources.

3.3.1.1 Registration of Cloud

Cloud, DO, and DU must register in Blockchain before becoming legitimate users or nodes. KGen, AGen, SynData, and ISave, each of which is implemented by Blockchain, are introduced before designing the registration workflow. Input null is passed to KGen(), and output KW is output; input. K_{pub} is passed to AGen(), and output Addr is output. SynData() synchronizes data from time. t_i and t_j. Inputs t_i and t_j, outputs blockdataij. It is an interface for blockchain storage that accepts addresses, signatures, private keys, storage contents, and outputs trans.

3.3.1.2 Registration of User

A two-step registration workflow is designed for DO and DU. Since DO and DU share the same registration process, we collectively refer to it as user registration.

- User->Blockchain: $URequest||t_l||t_m$. A user registers with Blockchain.
- Blockchain->User: $E(ks_2, Addr_{user}||K_{user_{w)}}||E(K_{pubU}, ks_2)||blockdata_{lm}$. K_{user_w} is generated by Blockchain, and $AGen\left(L_{pub_{user_w}}\right)$ creates $Addr_{user}$. Then, $E(ks_2, Addr_{user}||K_{user_w}||E(K_{pubU}, ks_2)||blockdata_{lm}$ is sent to the user. $Addr_{user}||K_{user_w}$ represents the data generated by Blockchain from t_l to t_m, which is decrypted by the $D(K_{priU}, Ks_2)$ and $D(ks_2, Addr_{user}||K_{user_w})$. To synchronize $blockdata_{lm}$ with the local database, the user normally calls $SynData(t_l, t_m)$.

3.3.1.3 Resource Publishing

A resource publisher uploads resources to a cloud and publishes their metadata on a blockchain. The first step in designing a registration workflow is to introduce the functions $ResUp()$ and $ISend()$ in the Blockchain. Uploading resources to the Cloud is performed by DO, which inputs and outputs resUpURL and resInfo; the $ISend()$ function initiates blockchain transactions by inputting. $K_{pri_{from}}$, $Addr_{from}$, $Addr_{to}$, index, content, and timestamp, and outputting $tran_{ID}$. In line 2, the smart contract $Tx_{reg_{resource}}$ configures the Blockchain, lines 3-8 encrypt access control permissions, lines 9 and 10 assign bresInfo, line 11 calls I_{Send}, and line 12 returns $tran_{ID}$.

3.3.2 Access Control

In cloud access control, users request cloud resources, and the Cloud determines whether users can access the resources based on permissions stored in Blockchain. Users with rights can access resources in the Cloud, and Blockchain records the access. We introduce a function called VerifyCap and an interface called IQuery before designing access control workflows. With VerifyCap(), realized by Cloud, two permission sets are checked for inclusion. If $resCAP_1$ contains $resCAP_{S_2}$, returns true; otherwise, returns false. It takes input, K_{priC}, and $resCAP_{S_2}$, and outputs true or false.

A transaction query interface is IQuery(), which is realized by Blockchain, which inputs index, $Addr_1$ and $Addr_2$, where index represents the query index value, $Addr_1$ and $Addr_2$, which represents trading parties and outputs the train.

- Cloud->User: access information for responses. A resource can only be accessed by a User if the Response access Info is true; otherwise, the Resource cannot be accessed.
- Cloud->Blockchain: $Txlog_{record}(K\_pri_{cloud_w}, Addr_{cloud}, Addr_{user}, Addr_{DO}, K_{pubC}, resInfo', timestamp)$. An access log is published in the Blockchain using $Tx_{log_{record}}$, a smart contract created by the Cloud.

3.3.3 Authorization

Direct and indirect authorizations are divided into two categories. DUs are authorized directly by the DO, whereas indirect authorizations are authorized indirectly by the granted DU:

3.3.3.1 Direct Authorization

Owners of resources directly authorize others to access their resources. Publishing resources requires direct authorization workflows.

- DU1->Cloud: $E(ks_5, auth_{flag}| |Addr_{U1}| |Addr_{DO}| |res_{Info}) || E(K_{pubC}, ks_5)$. As part of the authorization request, DU1 sends an authorization flag to Cloud, $auth\_flag$, which is the authorization key. $Addr_{U1}, Addr_{DO}$ resInfo are obtained from cloud decryption.
- Cloud->Blockchain: $hash_{resID}| |Addr_{DO}$. Cloud computes Hash(resID) to get $hash_{resID}$, and calls QFCapChain ($Addr_{DO}, Addr_{cloud}$, $hash_{resID}$).
- Blockchain->Cloud: $resCAP_S$. Cloud receives $resCAP_S$ from Blockchain
- Cloud: erifyCap($resInfo.resCAP, K_{priC}, resCAP_S$) . To ensure that DU1's permission requests are within the scope of the host's authorization, Cloud checks that $Addr_{DO}$ is the host of the Resource.
- Requests that fall outside the authorization scope are immediately terminated.
- Cloud->DO: $E(ks_6, auth_{flag}| |Addr_{U1}|| resInfo)|| E(K_{pubDO}$. A request to authorize DU1 is sent from the Cloud to the DO.
- DO->Blockchain: $Tx_{publish}(Kpri_{DO_w}, Addr_{DO}, Addr_{U1}, K_{pubC}, resIr$. Using $Tx_{publish}$, DO publishes authorization to the Blockchain. $Tx_{publish}$ is a smart contract,
- DO->DU1: h_flag . DU1 receives auth_flag from DO.

3.3.3.2 Indirect Authorization

DUs with indirect authorization provide authorization to at least five entities: DOs (resource owners), DU1s (authorizers), DU2s (requesters), Blockchains, and cloud-based technologies. Processes specific to interaction.

4 RESULTS AND DISCUSSION

A comparison of packets sent versus rounds for four models is shown in Figure 1: Medrec, Medchain, Medblock, and the Proposed Model. Each model sends more packets as rounds increase, but the Proposed Model consistently sends fewer packets, showing superior efficiency. The most packets are sent by Medrec, followed by Medchain and Medblock. As a result of the Proposed Model, the communication load is reduced, resulting in enhanced data transmission efficiency.

A comparison between the proposed framework and benchmark models is illustrated in Figure 2. Round and transaction numbers are analyzed during the analysis. In comparison with the benchmark models, the proposed method achieved a greater number of transactions. In the proposed approach, smart contracts are used to minimize delays and allow for more transactions at the sink, which leads to an improvement in transaction volume.

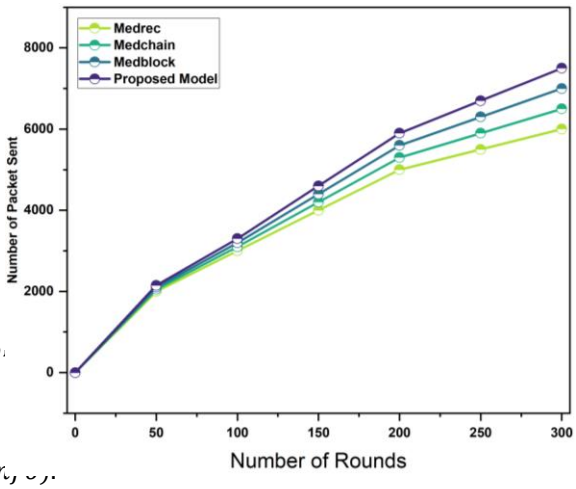

Figure 1: Communication efficiency: packets sent versus rounds.

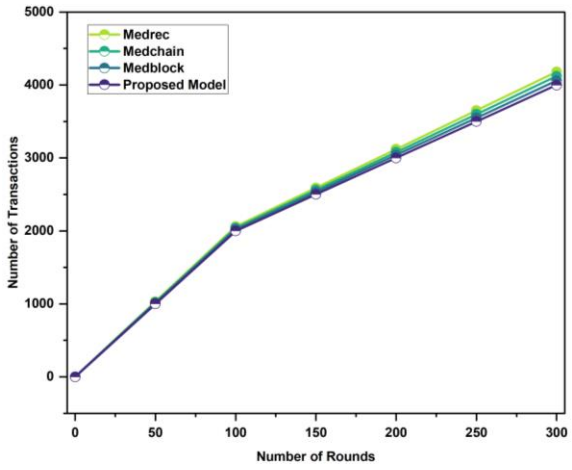

Figure 2: Number of transactions per round.

According to Figure 3, dead nodes are compared to rounds in terms of the number of dead nodes. Based on simulation results, the proposed method generates fewer dead nodes than Medrec, Medchain, and Medblock.

A summary of the simulation results, as well as the number of live nodes, can be found in Figure 4. The maximum number of live nodes observed after 300 rounds was 4000. A comparison of the proposed method with the benchmark models clearly shows that it maintains a higher number of live nodes for a given number of rounds. In this way, our framework demonstrates its superior efficiency.

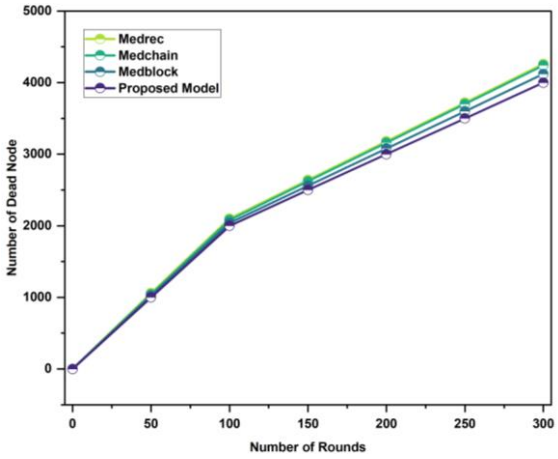

Figure 3: Number of dead nodes versus rounds.

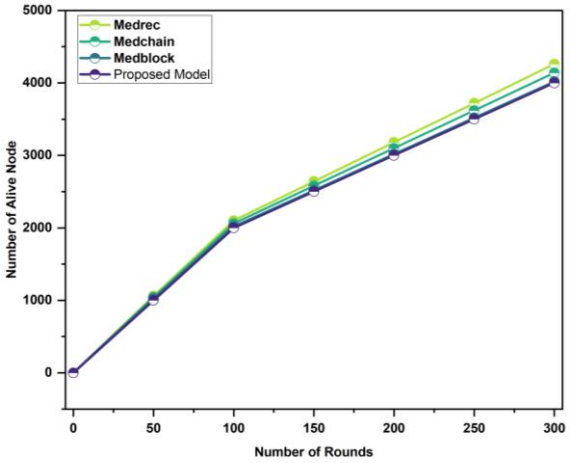

Figure 4: Number of live nodes versus rounds.

5 CONCLUSIONS

Using Blockchain technology, we developed a platform for securing, integrating, and presenting data from IoT devices. It was found that the proposed system registered devices and transmitted sensor data faster than conventional systems, based on performance evaluations. The study illustrates how medical imaging applications can be significantly enhanced through secure, auditable, and transparent data-sharing practices, thus increasing stakeholder trust and substantially enhancing the scalability and reliability of AI-driven systems. By effectively combining blockchain's decentralized security features with advanced artificial intelligence techniques, diagnostic accuracy can be improved, patient care and clinical decision-making processes can be optimized, and strict regulatory compliance in medical imaging environments can be consistently maintained. This integrated approach also facilitates smoother collaboration among medical professionals, encourages patient engagement by ensuring data ownership and consent management, and promotes innovation in personalized healthcare solutions through trustworthy and interoperable data exchanges.

REFERENCES

[1] P. Rani, S. Verma, S. P. Yadav, B. K. Rai, M. S. Naruka, and D. Kumar, "Simulation of the lightweight blockchain technique based on privacy and security for healthcare data for the cloud system," Int. J. E-Health Med. Commun. (IJEHMC), vol. 13, no. 4, pp. 1–15, 2022.

[2] A. Singh et al., "Blockchain-Based Lightweight Authentication Protocol for Next-Generation Trustworthy Internet of Vehicles Communication," IEEE Trans. Consum. Electron., vol. 70, no. 2, pp. 4898–4907, May 2024. [Online]. Available: https://doi.org/10.1109/TCE.2024.3351221.

[3] K. Devarapu, K. Rahman, A. Kamisetty, and D. Narsina, "MLOps-Driven Solutions for Real-Time Monitoring of Obesity and Its Impact on Heart Disease Risk: Enhancing Predictive Accuracy in Healthcare," Int. J. Reciprocal Symmetry Theor. Phys., vol. 6, pp. 43–55, 2019.

[4] C. R. Thompson, R. R. Talla, J. C. S. Gummadi, and A. Kamisetty, "Reinforcement Learning Techniques for Autonomous Robotics," Asian J. Appl. Sci. Eng., vol. 8, no. 1, pp. 85–96, 2019.

[5] P. K. Gade, "MLOps Pipelines for GenAI in Renewable Energy: Enhancing Environmental Efficiency and Innovation," Asia Pac. J. Energy Environ., vol. 6, no. 2, pp. 113–122, Dec. 2019. [Online]. Available: https://doi.org/10.18034/apjee.v6i2.776.

[6] R. K. Karanam et al., "Neural Networks in Algorithmic Trading for Financial Markets," Asian Account. Audit. Adv., vol. 9, no. 1, pp. 115–126, 2018.

[7] R. Mohammed et al., "Optimizing Web Performance: Front End Development Strategies for the Aviation Sector," Int. J. Reciprocal Symmetry Theor. Phys., vol. 4, pp. 38–45, 2017.

[8] D. Narsina et al., "AI-Driven Database Systems in FinTech: Enhancing Fraud Detection and Transaction Efficiency," Asian Account. Audit. Adv., vol. 10, no. 1, pp. 81–92, 2019.

[9] M. Rodriguez et al., "Oracle EBS and Digital Transformation: Aligning Technology with Business Goals," Technol. Manag. Rev., vol. 4, pp. 49–63, 2019.

[10] P. Rani, K. Ur Rehman, S. P. Yadav, and L. Hussein, "Deep Learning and AI in Behavioral Analysis for Revolutionizing Mental Healthcare," in Demystifying the Role of Natural Language Processing (NLP) in Mental Health, A. Mishra et al., Eds., IGI Global, 2025, pp. 263–282. [Online]. Available: https://doi.org/10.4018/979-8-3693-4203-9.ch014.

[11] H. P. Kommineni, "Cognitive Edge Computing: Machine Learning Strategies for IoT Data Management," Asian J. Appl. Sci. Eng., vol. 8, no. 1, pp. 97–108, Oct. 2019. [Online]. Available: https://doi.org/10.18034/ajase.v8i1.123.

[12] S. Kothapalli et al., "Code Refactoring Strategies for DevOps: Improving Software Maintainability and Scalability," ABC Res. Alert, vol. 7, no. 3, pp. 193–204, Dec. 2019. [Online]. Available: https://doi.org/10.18034/ra.v7i3.663.

[13] R. R. Kundavaram et al., "Predictive Analytics and Generative AI for Optimizing Cervical and Breast Cancer Outcomes: A Data-Centric Approach," ABC Res. Alert, vol. 6, no. 3, pp. 214–223, Dec. 2018. [Online]. Available: https://doi.org/10.18034/ra.v6i3.672

[14] P. Rani, D. S. Mohan, S. P. Yadav, G. K. Rajput, and M. A. Farouni, "Sentiment Analysis and Emotional Recognition: Enhancing Therapeutic Interventions," in Demystifying the Role of Natural Language Processing (NLP) in Mental Health, A. Mishra et al., Eds., IGI Global, 2025, pp. 283–302. [Online]. Available: https://doi.org/10.4018/979-8-3693-4203-9.ch015.

[15] E. Mezghani, E. Exposito, and K. Drira, "A Model-Driven Methodology for the Design of Autonomic and Cognitive IoT-Based Systems: Application to Healthcare," IEEE Trans. Emerg. Top. Comput. Intell., vol. 1, no. 3, pp. 224–234, Jun. 2017. [Online]. Available: https://doi.org/10.1109/TETCI.2017.2699218.

[16] M. N. Kadhim, A. H. Mutlag, D. A. Hammood, and N. B. H. Ismail, "Identification of Vehicle Logos in Deep Learning: A Comprehensive Survey," JT, vol. 7, no. 1, pp. 37–47, Mar. 2025.

[17] G. Tomasicchio, A. Ceccarelli, A. D. Matteis, and L. Spazzacampagna, "A space-based healthcare emergency management system for epidemics monitoring and response," in IET Conf. Proc., vol. 2021, no. 14, pp. 195–199, Apr. 2022. [Online]. Available: https://doi.org/10.1049/icp.2022.0571.

[18] S. Verma et al., "An automated face mask detection system using transfer learning based neural network to preventing viral infection," Expert Syst., p. e13507, 2024.

[19] A. F. Subahi, "Edge-Based IoT Medical Record System: Requirements, Recommendations and Conceptual Design," IEEE Access, vol. 7, pp. 94150–94159, 2019. [Online]. Available: https://doi.org/10.1109/ACCESS.2019.2927958

[20] M. U. Rehman et al., "A Novel Chaos-Based Privacy-Preserving Deep Learning Model for Cancer Diagnosis," IEEE Trans. Netw. Sci. Eng., vol. 9, no. 6, pp. 4322–4337, Nov. 2022. [Online]. Available: https://doi.org/10.1109/TNSE.2022.3199235.

[21] D. Miranda, R. Olivares, R. Munoz, and J.-G. Minonzio, "Improvement of Patient Classification Using Feature Selection Applied to Bidirectional Axial Transmission," IEEE Trans. Ultrason. Ferroelectr. Freq. Control, vol. 69, no. 9, pp. 2663–2671, Sep. 2022. [Online]. Available: https://doi.org/10.1109/TUFFC.2022.3195477.

[22] M. Wazid, J. Singh, A. K. Das, S. Shetty, M. K. Khan, and J. J. P. C. Rodrigues, "ASCP-IoMT: AI-Enabled Lightweight Secure Communication Protocol for Internet of Medical Things," IEEE Access, vol. 10, pp. 57990–58004, 2022. [Online]. Available: https://doi.org/10.1109/ACCESS.2022.3179418.

[23] G. Ansari, P. Rani, and V. Kumar, "A novel technique of mixed gas identification based on the group method of data handling (GMDH) on time-dependent MOX gas sensor data," in Proc. Int. Conf. Recent Trends Comput. (ICRTC 2022), Springer, 2023, pp. 641–654.

[24] C. M. Parra, M. Gupta, and D. Dennehy, "Likelihood of Questioning AI-Based Recommendations Due to Perceived Racial/Gender Bias," IEEE Trans. Technol. Soc., vol. 3, no. 1, pp. 41–45, Mar. 2022. [Online]. Available: https://doi.org/10.1109/TTS.2021.3120303

[25] H. Elayan, M. Aloqaily, and M. Guizani, "Sustainability of Healthcare Data Analysis IoT-Based Systems Using Deep Federated Learning," IEEE Internet Things J., vol. 9, no. 10, pp. 7338–7346, May 2022. [Online]. Available: https://doi.org/10.1109/JIOT.2021.3103635.

[26] P. Rani, S. P. Yadav, P. N. Singh, and M. Almusawi, "Real-World Case Studies: Transforming Mental Healthcare With Natural Language Processing," in Demystifying the Role of Natural Language Processing (NLP) in Mental Health, A. Mishra et al., Eds., IGI Global, 2025, pp. 303–324. [Online]. Available: https://doi.org/10.4018/979-8-3693-4203-9.ch016.

[27] B. C. Tedeschini et al., "Decentralized Federated Learning for Healthcare Networks: A Case Study on Tumor Segmentation," IEEE Access, vol. 10, pp. 8693–8708, 2022. [Online]. Available: https://doi.org/10.1109/ACCESS.2022.3141913.

[28] N. A. Kadhim, A. A. Obed, A. J. Abid, A. L. Saleh, and R. J. Hassoon, "A Systematic Review for Reconfiguring Photovoltaic Arrays under Conditions of Partial Shading," EETJ, vol. 1, no. 1, pp. 20–34, Jun. 2024.

[29] G. Subramanian and A. Sreekantan Thampy, "Implementation of Blockchain Consortium to Prioritize Diabetes Patients' Healthcare in Pandemic Situations," IEEE Access, vol. 9, pp. 162459–162475, 2021. [Online]. Available: https://doi.org/10.1109/ACCESS.2021.3132302.

[30] P. Rani, U. C. Garjola, and H. Abbas, "A Predictive IoT and Cloud Framework for Smart Healthcare Monitoring Using Integrated Deep Learning Model," NJF Intell. Eng. J., vol. 1, no. 1, pp. 53–65, 2024.

[31] V. K. Prasad, M. D. Bhavsar, and S. Tanwar, "Influence of Montoring: Fog and Edge Computing," Scalable Comput. Pract. Exp., vol. 20, no. 2, pp. 365–376, May 2019. [Online]. Available: https://doi.org/10.12694/scpe.v20i2.1533.