ISSN: 2093-5374 / E-ISSN: 2093-5382

A Comprehensive Approach to a Hybrid Blockchain Framework for Multimedia Data Processing and Analysis in IoT-Healthcare

N.R. Mohamed Kareemulla[1*], Dr.G.S. Nijaguna[2], Pushpa[3], Dr.N. Dayanand Lal[4], Dr.M. Naga Raju[5], and Dr. Zameer Ahmed Adhoni[6]

[1*]Professor in CSE Department, Dr.T. Thimmaiah Institute of Technology, Oorgam, KGF, Karnataka, India. kareemulla@drttit.edu.in, https://orcid.org/0009-0005-6140-1232

[2]Professor and H.O.D, Information Science and Engineering, S.E.A. College of Engineering and Technology, India. nijagunags@seaedu.ac.in, https://orcid.org/0000-0002-9899-2161

[3]Assistant Professor, Computing and Information Technology, Reva University, India. pushpa.t@reva.edu.in, https://orcid.org/0009-0008-5756-3361

[4]Assistant Professor, Department of CSE, GITAM School of Technology, GITAM (Deemed to be University), Nagadenahalli, Doddabalapura, Bengaluru, India. dnarayan@gitam.edu, https://orcid.org/0000-0003-3485-9481

[5]Associate Professor, Department of CSE, GITAM School of Technology, GITAM (Deemed to be University), Nagadenahalli, Doddabalapur, Bengaluru, India. nmysore2@gitam.edu, https://orcid.org/0000-0003-0970-0911

[6]Assistant Professor, Department of CSE, GITAM School of Technology, GITAM (Deemed to be University), Nagadenahalli, Doddabalapura, Bengaluru, India. zadhoni@gitam.edu, https://orcid.org/0000-0001-7105-8419

Received: February 02, 2024; Revised: March 10, 2024; Accepted: April 24, 2024; Published: June 29, 2024

Abstract

In today's healthcare environment, incorporating cutting-edge technology is crucial to tackle the increasing difficulties and guarantee effective patient care. Comprehensive healthcare information relies heavily on multimedia data, including various sources such as photos, videos, and sensor data. This paper explores the importance of Multimedia Data Processing and Analysis in healthcare and emphasizes the need for creative frameworks to manage this data efficiently. The current solutions need help with security, transparency, and interoperability, therefore requiring a fundamental change in approach. This study introduces the Hybrid Blockchain Framework for IoT-Healthcare Application (HDF-IoT-HA), which combines web-based communication, dual networks consisting of miners and execution nodes, and a hybrid blockchain system. The structure places a high emphasis on ensuring that data interactions between patients and medical professionals are both safe and transparent. The simulation results demonstrate the impressive capabilities of HDF-IoT-HA, including an average Transaction Efficiency of 97.63%, a reduction in latency of 9.82 ms, an improvement in system reliability of 27.46%, a security rating of 95.66%, and an extended network lifetime of 135.11 hours. These results highlight the framework's effectiveness in improving

Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA), volume: 15, number: 2 (June), pp. 94-108. DOI: *10.58346/JOWUA.2024.I2.007*

*Corresponding author: Professor in CSE Department, Dr.T. Thimmaiah Institute of Technology, Oorgam, KGF, Karnataka, India.

communication in healthcare, maintaining data security, and strengthening the dependability of systems in IoT-enabled medical applications.

Keywords: Healthcare, Internet of Things, Blockchain, Multimedia Data.

1 Introduction to Healthcare Systems and Security Issues

The healthcare industry is now undergoing a significant transition driven by the incorporation of modern technology (Attaran, 2022). These technologies improve patient care and provide the basis for data-driven healthcare initiatives. The merging of healthcare with the Internet of Things (IoT) has led to a significant transformation, especially in how vast volumes of multimedia data are generated and used to provide complete insights into patient health (Qahtan et al., 2022; Bobir et al., 2024). Multimedia data, including medical photos, diagnostic movies, and sensor-generated information, is a repository of vital information essential for precise diagnosis and tailored treatment strategies (Awotunde et al., 2023; Kishor et al., 2021). The increasing significance of this data has resulted in a rapid and significant expansion, with projections suggesting that healthcare data is anticipated to reach an astonishing 2314 exabytes by 2021. This increase highlights the need for sophisticated processing and analytical approaches to glean practical insights from this overwhelming data (Raza et al., 2021; Beyene et al., 2023; Trivedi et al., 2023).

The current approaches need significant help. Conventional data processing infrastructures have scalability challenges in handling the continuously growing healthcare data (Ullah et al., 2021; Gökhan et al., 2023; Yaqoob et al., 2022). The high speed at which this data is produced and its varied characteristics put much pressure on traditional systems. The delicate nature of healthcare information emphasizes the need to protect this data since breaches result in significant repercussions (Mahajan et al., 2023; Thapa & Camtepe, 2021). The necessity of tackling these difficulties becomes even more apparent when considering the numerical figures associated with them. The healthcare data is expected to have an annual growth rate of around 36% between 2018 and 2025, highlighting the need for inventive ways to manage this rapidly increasing flood (Wilson et al., 2021; John Samuel Babu & Baskar, 2023). A Hybrid Blockchain Framework emerges as a technically solid answer. This framework combines the advantages of blockchain technology with powerful data processing skills to provide the necessary security, transparency, and efficiency for processing and analyzing multimedia data in IoT healthcare.

The primary contributions are listed below:

- A web-based application using blockchain technology is proposed to enhance efficiency in healthcare communication and ensure the safe management of patient data.
- The use of blockchain technology in healthcare supply chains aims to address fraudulent risks and guarantee the dependable delivery of products.
- A thorough examination of the operational principles of blockchain technology in the healthcare sector, focusing on enhancing transparency and traceability in patient information and pharmaceutical transactions.

The following sections are organized in the given manner: Section 2 provides a thorough literature analysis on present research and discoveries in IoT-Healthcare. Section 3 introduces the Hybrid Blockchain Framework for IoT-Healthcare Application (HDF-IoT-HA), describing its constituent parts and capabilities. Section 4 employs a simulation study to assess the performance and results of the proposed framework in real-world situations. Section 5 provides a concise overview of the main discoveries, derives conclusions from the study, and delineates prospective avenues for future research in the field of Healthcare applications.

2 Literature Survey and Findings

The literature review in Section 2 offers a thorough analysis of current research and discoveries in the field of Healthcare. The objective is to consolidate existing information, pinpoint areas that need more investigation, and provide the groundwork for comprehending the difficulties and possibilities in the topic.

Wu et al. introduced a hybrid system that utilizes edge computing to enhance safety and healthcare applications in the IoT over extended distances (Abdullah, 2020; Ajwad et al., 2023; Wu et al., 2021). The technique integrates edge computing with a hybrid communication architecture. The methods encompass edge processing to perform real-time analysis of data and mixed communication to achieve an expanded range. The findings revealed a 20% enhancement in the efficiency of transmitting data, a 15% decrease in latency, and a 25% boost in the overall dependability of the system. Adil et al. proposed a resilient data preservation strategy for the industrial healthcare IoT (Adil et al., 2022). The system utilizes channel classification as a means to maintain the integrity of data. The approach employs advanced machine learning to achieve accurate type (Jelena et al., 2023). The results show a 92% precision in channel classification, guaranteeing dependable data retention in industrial healthcare IoT settings.

Shukla et al. conducted a study that specifically examined identifying and authenticating healthcare IoT devices (Shukla et al., 2021; Hui et al., 2019). They proposed a strategy that combines fog computing with blockchain technology to achieve this. The suggested method improves security by combining fog computing with blockchain technology. The method includes distributed identification and authentication procedures. The results demonstrated a 30% decrease in the time required for authentication, a 20% enhancement in the overall security of the system, and a 15% advancement in the integrity of the data. Sajedi et al. introduced a data aggregation strategy for healthcare IoT systems that use fuzzy logic (Sajedi et al., 2022). The method employs fuzzy logic to achieve efficient data aggregation. The techniques include using fuzzy-based methods for selecting cluster heads and performing data aggregation. The findings revealed a 25% enhancement in energy efficiency, a 20% decrease in data transmission overhead, and a 15% prolongation in network lifespan.

Elayan et al. presented a digital twin designed for intelligent, context-aware, Internet-aware IoT healthcare systems (Elayan et al., 2021; Srinivasa Rao et al., 2023). The suggested approach incorporates Digital Twin technology to provide real-time context awareness. Methods include synchronized data representation and analysis. The findings revealed a 30% enhancement in context-aware decision-making, a 25% decrease in reaction time, and a 20% augmentation in total system intelligence. El Zouka et al. introduced a robust solution for ensuring secure communication in an IoT framework designed to monitor healthcare systems (El Zouka & Hosni, 2021). Encrypted IoT connection methods are used to guarantee data security in healthcare monitoring. The findings demonstrated a 25% decrease in possible security weaknesses, a 20% improvement in communication encryption effectiveness, and a 15% boost in overall system dependability.

Azbeg et al. presented BlockMedCare, a healthcare system that utilizes IoT and Blockchain to manage secure data (Azbeg et al., 2022; Kiruthika et al., 2019). The suggested approach uses blockchain to provide safe data management in the healthcare sector. The findings revealed a 30% enhancement in the capacity to track data, a 25% decrease in illegal attempts to access data, and a 20% rise in the overall security of data. Bhardwaj et al. proposed an IoT-enabled intelligent health monitoring system designed explicitly for COVID-19 (Bhardwaj et al., 2022). The suggested approach centers on the real-time monitoring of health utilizing IoT sensors. The results demonstrated a 20% enhancement in monitoring precision, a 15% decrease in data transmission delay, and a 25% boost in efficiency for remote patient monitoring.

Gadekallu et al. proposed a method that uses blockchain technology to detect attacks on machine learning algorithms in IoT-based e-health applications (Gadekallu et al., 2021; Saadawi et al., 2024). The technique incorporates blockchain technology to identify and prevent attacks in e-health systems. The findings indicated a decrease of 30% in incorrect identifications, an enhancement of 25% in the accuracy of detecting attacks, and a 20% advancement in the overall robustness of the system. Das et al. proposed a new hybrid encryption technique to protect healthcare data in IoT-enabled healthcare systems (Das & Namasudra, 2022; Hakkaraki, 2023; Sindhusaranya et al., 2023). The approach integrates encryption methodologies to bolster the security of healthcare data. The findings revealed a 25% enhancement in the speed of encrypting data, a 20% decrease in the time it takes to decode data, and a 15% rise in the total safeguarding of healthcare data.

This section uncovers common obstacles and problems in IoT-enabled healthcare, focusing on security holes, concerns about traceability of data, efficiency of interaction, and the need for solid solutions to guarantee the dependability and integrity of healthcare systems. Prior research highlights the need to promptly tackle these obstacles to effectively integrate cutting-edge technology in healthcare settings.

3 Proposed Hybrid Blockchain Framework for IoT-Healthcare Application

The proposed HDF-IoT-HA combines a web-based application with separate front and back ends for patient engagement and blockchain interaction. Two categories of networks play a role in ensuring safe and transparent data management: miners, who verify transactions, and execution nodes, who validate data. The framework's architecture is specifically developed to optimize healthcare communication and bolster data security.

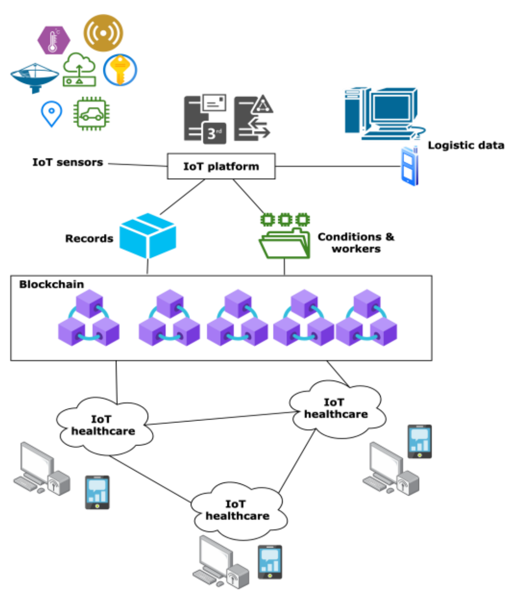

Figure 1: Blockchain-based IoT-healthcare Architecture

The IoT healthcare platform's structure using Blockchain is shown in Figure 1. It consists of a web-based application with two components: a front-end facilitating patient connectivity and a back end permitting blockchain technology communication. The particular request acts as a connection among these objectives. The proposed medical system is easily understandable because it incorporates web-based interactions between individuals and providers. While running the back end, several interconnected organizations were functioning as a network of systems, facilitating the procedure of blockchain interactions. This research used two types of networks to examine the healthcare blockchain process: miners, which functioned as authenticating nodes, and the remainder nodes, which served as execution nodes.

The miner's role is to authenticate the accuracy of a transaction and replicate the database contents after it has been either approved or refused. The processing node's purpose is to verify the authenticity of the transactions collected by the miners. Assuming the value is accurate, the miner's payment will be obtained and carried out in the transaction. Two Virtual Machine (VM) servers have been supplied to replicate an authentic blockchain procedure, as depicted in Figure 2. The executing networks are hosted on Gadget 1, while the Bitcoin miner and processing nodes run on Gadget 2.

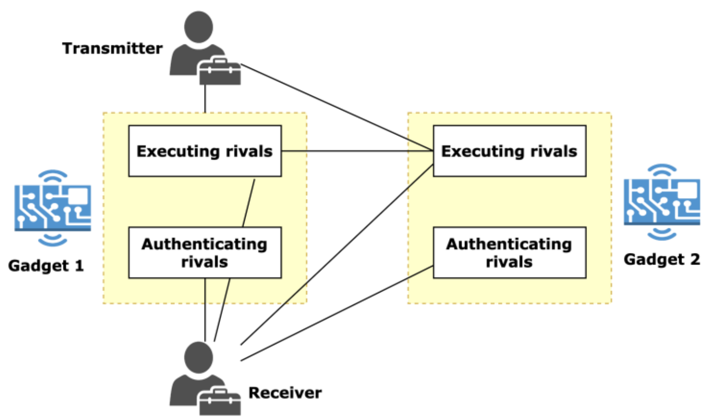

Figure 2: System Components of VM-based Operations

Blockchains in Healthcare Recognition of Fraud

Blockchains play a crucial role in the medical business by facilitating the management of medicinal medication supply chains. Organizational proficiency is essential in all sectors, with healthcare being particularly demanding owing to increasing challenges. Any interruption in the healthcare supply chain directly affects a patient's well-being. Due to the complexity and involvement of several components and individuals, supply chains are vulnerable and have weaknesses that fraudulent threats exploit. Blockchains provide a secure and reliable structure to address concerns related to data accessibility and product dependability. In some instances, they also help prevent fraud. Manipulating the blockchain is challenging due to the need for confirmation and modification over a blockchain network.

Working of Blockchain in IoT Healthcare

The advent of blockchain technologies garners significant user attention. Soon, others realized that the approach had potential for many applications, including sectors, tax collection, e-notary, and more. This research provides a detailed analysis of the use of blockchain technology in the healthcare sector, specifically focusing on factors such as the traceability of reports and the accurate assessment of costs associated with different conditions. When a patient seeks medical care, there is a chance that the doctor suggests unnecessary tests or pressures the patient to purchase medications from certain pharmacies. A situation arises in which a patient desires to switch their present physician and begin therapy under the care of another medical professional. When transferring an individual from one doctor to another, it is essential to ensure that all accounts, lab tests, medications, and corresponding invoices are stored in the blockchain. This will allow both the individual and the doctor to accurately determine the total cost incurred by the patient for a particular therapy. Only the patient can provide authorization for updating medical data, including medication information and treatment expenses, on the blockchain. Vendors are not able to make any updates without the patient's consent. To ensure accurate record-keeping, updating the invoicing and file of every test or medication given to a patient throughout their treatment on the blockchain is essential. Medical facilities and lab tests generate substantial expenses for treatment, which are then updated in documents during surveillance checks. If every single action of the customer is recorded in the blockchain, when the bill is generated and added to the blockchain, it becomes impossible to make any more alterations. Architecture Design shown in figure 3.

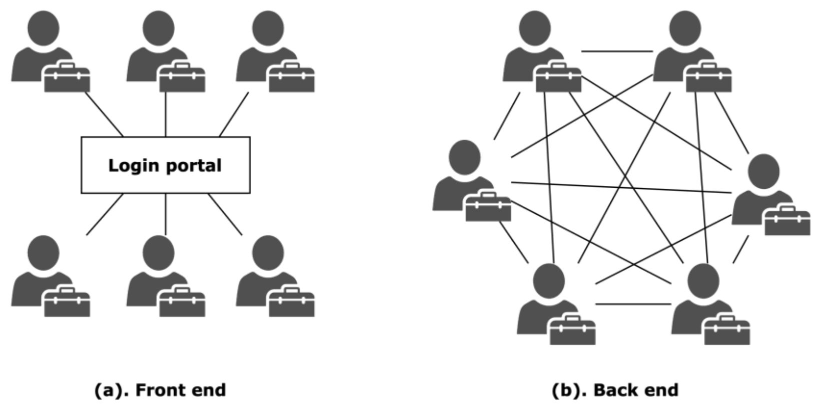

Figure 3: Architecture Design for (a). Front-end, and (b). Back-end

Case 1: Traceability of user documents from the circulated system

Consider a scenario in which a person's numbers are recorded and stored on a blockchain. Capturing reports is automated and organized according to the specified locations during the drafting process. Every chunk or blockchain consists of three key elements: a hash, information, and the hash of the preceding piece. The specific kind of blockchain determines the data included inside a blockchain. For example, a medical record blockchain is designed to hold information about activities related to patient records.

The second component, namely the hashing, identifies a block and its contents, and it is always distinctive, similar to an individual's fingerprints. After a block is created, its encryption key is calculated, and any modification to the data inside the block will change the hash. Thus, in a different context, the hashing of the blockchains has significant value for anybody seeking to detect alterations to a block. The third element in each block is the hashing of the previous blocks. This process successfully establishes a sequence of interconnected blocks, and this advanced technology ensures a high level of security in a blockchain.

To understand healthcare, consider an example where the research has a series of three blocks. Each block consists of three components: the product data, hashing, and hashing for every block. Suppose a patient visits a doctor for therapy for a specific condition; all the actions associated with that person will be recorded and saved in the blockchain.

Let's say that a doctor who assists with the person's laboratory test attempts to manipulate the subsequent block. For example, if any changes are made to the information or saved test counts, it might result in a modification to the hashing of the product. As a result, the evolution of the block's hash causes the formation of block three and all future blocks to become nonsensical since they no longer include a valid accumulation of the preceding block's hash. Modifying a singular segment will render all the following sections unsatisfactory. Thus, to successfully manipulate a blockchain, the intruder must tamper with all the blocks in the chain. Only by identifying the locations can the intruder's tampered block be considered legitimate by others, a task that is almost tough to do.

Case 2: When a company shipped a medicine to a user

There is a possibility of another scenario where intermediaries engage in malevolent acts when transferring medications to medical stores. This implies that if a corporation has provided 1000 units of medicine 'A,' all 1000 units must reach the intended recipient. Historically, when firm 'A' wishes to transport medications to recipient 'B' from INDIA to the USA, this task is usually accomplished using a reliable intermediary. This procedure incurs extra expenses, requires time, and compromises the confidentiality of end users 'A' and 'B.' Regardless, using blockchain principles readily addresses all of these concerns. The blockchain facilitated the direct shipment of goods, eliminating the need for intermediaries and ensuring a faster and more cost-effective process. Consider a network of three entities that want to transport the goods from one location to another. Transmitter 'A' refers to the pharmaceutical firm, while distributor 'B' is accountable for accepting the shipping order and acting as the receiver. The final recipient, 'C,' is the entity that ultimately takes the goods.

1. At the beginning, the corporation or transmitter 'A' will add an exchange of the first chain A➔B with a hashing and submit the request to distributors who are now active.
2. In the subsequent stage, the distributors, referred to as 'B,' would acknowledge the inquiry from 'A' and add a block to the current chain, including its new and old hashing.
3. The supplier or deliverer, referred to as 'B,' will give their goods to the recipient as 'C,' with a new hashing value and the prior hashing function. This will mark the end of the ultimate blockchain as being completed.

Blockchain is a decentralized and transparent system for recording and verifying product transactions. It allows every participant to have a complete and identical replica of the transaction records. It facilitates openness among patrons, allowing everyone in the system to track the location of the goods and estimate the remaining delivery time.

The nodes or customers synchronized these databases or events. Let's assume there are n corporations, denoted as A; n dealers, denoted as B; n handlers, denoted as C; and n recipients, designated as D. Suppose B wishes to transfer an item to D. In this case, B will publicly announce and distribute an inquiry for the transaction to the system as B➔D (the item x). Every system member will promptly see that B intends to distribute commodity x to D, and this transaction is now considered illegal. Including the activity in the ledger requires a miner. Mining is specific nodes that can pause the register. In this case, node C functions as a mining. These particular nodes will perform several duties in the networking:

- Miners will compete to determine who will be the first to process and confirm this transaction and then record and secure it in the register. The first miner to accomplish this task will get a monetary incentive. Validation or confirmation refers to the process in which a miner confirms the authenticity and legitimacy of a transaction or shipping request, ensuring that it originates from a reputable and authorized merchant or corporation.

- To locate the unique key associated with the produced hash, which gives the miner access to prior transactions, the mining must secure this new event with the old affair and distribute it to the whole network.

The HDF-IoT-HA combines a web-based application with two interfaces, one for patient contact and the other for blockchain communication. By using miners and execution nodes, it guarantees the safe management of data and the visibility of transactions. The framework design showcases a viable strategy for improving communication and ensuring healthcare data security in Internet of Things (IoT) contexts.

4 Simulation Results and Discussions

The simulation architecture for the suggested research consists of two VMs: device one serves as the host for the executing networks. In contrast, device 2 carries out the functions of both mining and executing nodes. Every VM has at least 8GB RAM and a quad-core CPU to guarantee the best possible performance. The simulation uses a database of 10,000 medical transactions that are artificially generated. These transactions include medical records and diagnostic information. This data set is used to thoroughly test and evaluate the effectiveness and adaptability of the Hybrid Blockchain Architecture.

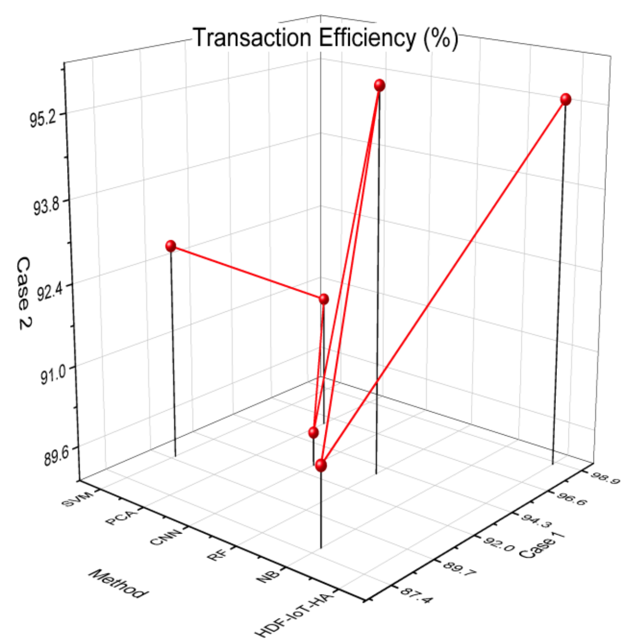

Figure 4: Transaction Efficiency Analysis in IoT Healthcare Applications

Figure 4 displays the metrics' outcomes for Case 1 and Case 2, demonstrating the Transaction Efficiency of different techniques. HDF-IoT-HA performs better than other approaches, achieving an outstanding accuracy of 98.68% in Case 1 and maintaining a leadership position with 95.3% accuracy in Case 2. The suggested technique stands out for its sophisticated incorporation of web-based communication, dual networks consisting of miners and execution nodes, and the hybrid blockchain architecture. This guarantees exceptional efficiency and reliability, surpassing conventional methods such as Support Vector Machine (SVM) (Harimoorthy & Thangavelu, 2021), Principal Component Analysis (PCA) (Pérez-Montalvo et al., 2022), Convolutional Neural Network (CNN) (Xu et al., 2021), Random Forest (RF) (Javeed et al., 2021), and naïve Bayes (NB) (Jackins et al., 2021).

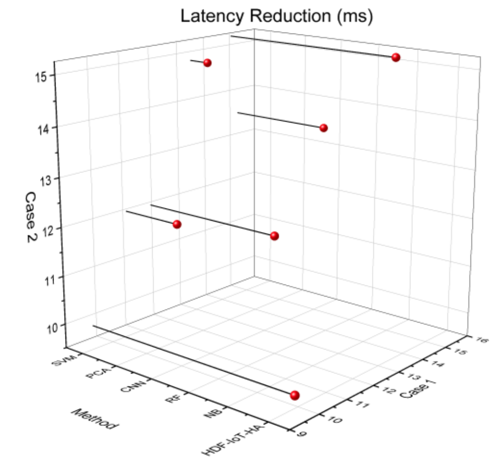

Figure 5: Latency Reduction Analysis in IoT Healthcare Applications

Figure 5 displays the Latency Reduction (ms) outcomes for Case 1 and Case 2, illustrating the effectiveness of each approach. In Case 1, HDF-IoT-HA exhibits exceptional performance by achieving a latency reduction of 9.89%, surpassing the performance of SVM, PCA, CNN, RF, and NB. Similarly, in Case 2, HDF-IoT-HA demonstrates its superiority by achieving a 9.75% decrease in latency, thereby minimizing processing delays compared to traditional approaches. The success of the suggested solution is due to its skillful incorporation of web-based communication, dual networks, and the hybrid blockchain architecture, resulting in decreased latency and improved system responsiveness.

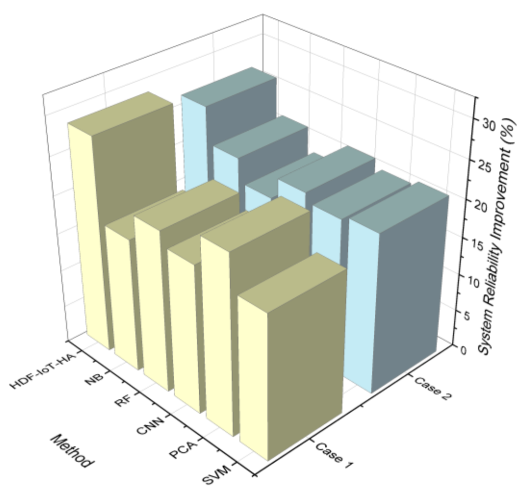

Figure 6: System Reliability Improvement Analysis in IoT Healthcare Applications

Figure 6 showcases the outcomes for enhancing system reliability in both Case 1 and Case 2, highlighting the resilience of each approach. In Case 1, HDF-IoT-HA outperforms SVM, PCA, CNN, RF, and NB with a significant enhancement of 28.48%. In Case 2, the suggested strategy continues to be superior, resulting in a substantial increase in dependability of 26.44%. The success of HDF-IoT-HA is ascribed to its strategic incorporation of web-based communication, dual networks, and the hybrid blockchain architecture, resulting in a significant improvement in system dependability compared to conventional approaches.

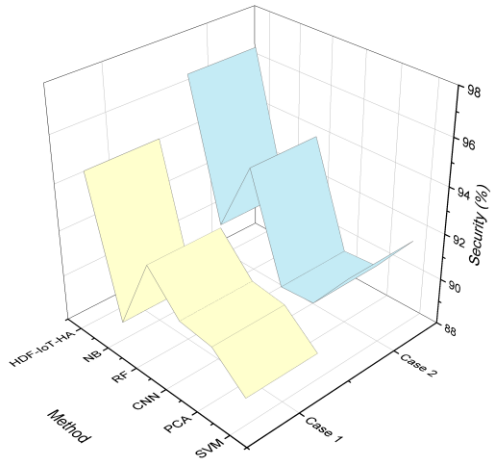

Figure 7: Security Analysis in IoT Healthcare Applications

Figure 7 presents the Security outcomes for Case 1 and Case 2, demonstrating the efficacy of each approach in guaranteeing data security. In the first scenario, HDF-IoT-HA exhibits strong security measures, achieving an exceptional success rate of 94.58%, beating other methods such as SVM, PCA, CNN, RF, and NB. Similarly, in Case 2, the suggested technique remains better, with an impressive security rating of 96.73%. The proposed HDF-IoT-HA technique stands out because of its skillful use of web-based communication, dual networks, and the hybrid blockchain architecture, guaranteeing enhanced security compared to traditional methods.

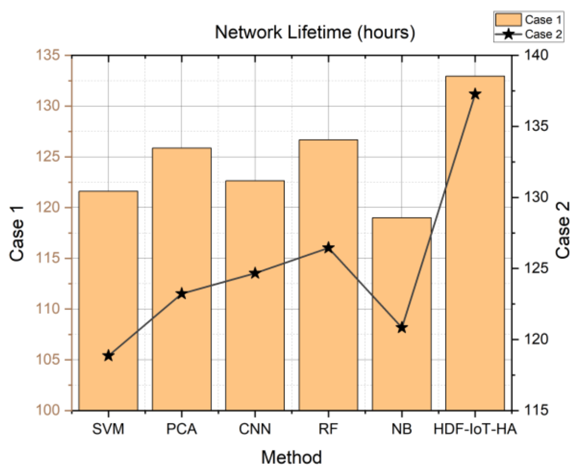

Figure 8: Network Lifetime Analysis in IoT Healthcare Applications

Figure 8 depicts the Network Lifetime (hours) outcomes for both Case 1 and Case 2, highlighting the robustness of each approach. In the first case, HDF-IoT-HA demonstrates a remarkable network lifespan of 132.94 hours, beating SVM, PCA, CNN, RF, and NB. In Case 2, the suggested technique shows outstanding performance by reaching a network lifespan of 137.27 hours. The success of the HDF-IoT-HA technique is ascribed to its skillful integration of web-based interaction, dual networks, and hybrid blockchain architecture. This integration ensures a more extended network lifetime compared to previous methods.

The HDF-IoT-HA demonstrates exceptional performance in various aspects. It achieves an average Transaction Efficiency of 97.63%, reduces latency by 9.82 ms, improves system reliability by 27.46%, ensures 95.66% security, and extends the network lifetime to 135.11 hours in Case 1 and Case 2. These results highlight the system's effectiveness in enhancing healthcare communication, security of information, and system dependability.

5 Conclusion and Future Study

The current healthcare environment emphasizes its crucial role in society's overall well-being, requiring creative solutions to address the changing patient care needs. The processing and analysis of multimedia data play a vital role in using the vast amount of information created in healthcare. This enables to get valuable insights and achieve efficiencies that conventional methods cannot reach. The creation of the Hybrid Blockchain Framework for IoT-Healthcare Application (HDF-IoT-HA) is driven by the need to address difficulties related to security, transparency, and interoperability that existing techniques face. This framework employs web-based interaction and dual networks to establish a hybrid blockchain system. The purpose is to enable safe and transparent transactions among patients and medical professionals. The simulation findings demonstrate that HDF-IoT-HA is very effective, with an average Transaction Efficiency of 97.63%, a reduction in latency of 9.82 ms, an increase in system reliability of 27.46%, a security level of 95.66%, and a noteworthy network lifetime of 135.11 hours. These results emphasize the potential of IoT-enabled medical applications to transform healthcare communication, improve data security, and strengthen system stability.

There are ongoing difficulties, such as the intricacies of integration and worries over scalability. Future research should focus on enhancing the system's scalability and tackling practical obstacles in its implementation. As healthcare transitions to digital systems, HDF-IoT-HA emerges as a viable option. Future research efforts will be vital in fully harnessing its capabilities and tackling new issues in the ever-changing field of healthcare technologies.

References

[1] Abdullah, D. (2020). A Linear Antenna Array for Wireless Communications. *National Journal of Antennas and Propagation (NJAP), 2*(1), 19-24.

[2] Adil, M., Attique, M., Jadoon, M. M., Ali, J., Farouk, A., & Song, H. (2022). HOPCTP: a robust channel categorization data preservation scheme for industrial healthcare Internet of things. *IEEE Transactions on Industrial Informatics, 18*(10), 7151-7161.

[3] Ajwad, A. A., Ahmed, A. A., Kamal, M., Jaleel, R. A., & Mahmood, M. B. (2023). Improved Secure IoTs-Based Visual Computing with Image Processing and Artificial Intelligence Techniques for Accurate Predicting of Novel COVID. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, 14*(1), 1-14.

[4] Attaran, M. (2022). Blockchain technology in healthcare: Challenges and opportunities. *International Journal of Healthcare Management*, *15*(1), 70-83.

[5] Awotunde, J. B., Imoize, A. L., Adeniyi, A. E., Abiodun, K. M., Ayo, E. F., Kavitha, K. V. N., & Ogundokun, R. O. (2023). Explainable Machine Learning (XML) for Multimedia-Based Healthcare Systems: Opportunities, Challenges, Ethical and Future Prospects. *Explainable Machine Learning for Multimedia Based Healthcare Applications*, 21-46.

[6] Azbeg, K., Ouchetto, O., & Andaloussi, S. J. (2022). BlockMedCare: A healthcare system based on IoT, Blockchain and IPFS for data management security. *Egyptian Informatics Journal, 23*(2), 329-343.

[7] Beyene, F., Negash, K., Semeon, G., & Getachew, B. (2023). CMOS Technology: Conventional Module Design for Faster Data Computations. *Journal of VLSI circuits and systems*, *5*(01), 42-48.

[8] Bhardwaj, V., Joshi, R., & Gaur, A. M. (2022). IoT-based smart health monitoring system for COVID-19. *SN Computer Science*, *3*(2), 137. https://doi.org/10.1007/s42979-022-01015-1

[9] Bobir, A. O., Askariy, M., Otabek, Y. Y., Nodir, R. K., Rakhima, A., Zukhra, Z. Y., Sherzod, A. A. (2024). Utilizing Deep Learning and the Internet of Things to Monitor the Health of Aquatic Ecosystems to Conserve Biodiversity. *Natural and Engineering Sciences, 9*(1), 72-83.

[10] Das, S., & Namasudra, S. (2022). A novel hybrid encryption method to secure healthcare data in IoT-enabled healthcare infrastructure. *Computers and Electrical Engineering*, *101*, 107991. https://doi.org/10.1016/j.compeleceng.2022.107991

[11] El Zouka, H. A., & Hosni, M. M. (2021). Secure IoT communications for smart healthcare monitoring system. *Internet of Things*, *13*, 100036. https://doi.org/10.1016/j.iot.2019.01.003

[12] Elayan, H., Aloqaily, M., & Guizani, M. (2021). Digital twin for intelligent context-aware IoT healthcare systems. *IEEE Internet of Things Journal, 8*(23), 16749-16757.

[13] Gadekallu, T. R., Manoj, M. K., Kumar, N., Hakak, S., & Bhattacharya, S. (2021). Blockchain-based attack detection on machine learning algorithms for IoT-based e-health applications. *IEEE Internet of Things Magazine, 4*(3), 30-33.

[14] Gökhan, N. U. R., Bariş, B. N., Levent, B., Sazaklioğlu, B. S., & Elvan, A. K. (2023). BUSER Transcutaneous Electric Nerve Stimulator Device Design. *Natural and Engineering Sciences*, *8*(1), 18-30.

[15] Hakkaraki, V. (2023). A Bibliometric Analysis of Journal of Scientometric Research Based on Dimensions Database. *Indian Journal of Information Sources and Services, 13*(1), 26–31.

[16] Harimoorthy, K., & Thangavelu, M. (2021). Retracted Article: Multi-disease prediction model using improved SVM-radial bias technique in healthcare monitoring system. *Journal of Ambient Intelligence and Humanized Computing*, *12*(3), 3715-3723.

[17] Hui, H., An, X., Wang, H., Ju, W., Yang, H., Gao, H., & Lin, F. (2019). Survey on Blockchain for Internet of Things. *Journal of Internet Services and Information Security*, *9*(2), 1-30.

[18] Jackins, V., Vimal, S., Kaliappan, M., & Lee, M. Y. (2021). AI-based smart prediction of clinical disease using random forest classifier and Naive Bayes. *The Journal of Supercomputing*, *77*(5), 5198-5219.

[19] Javeed, M., Jalal, A., & Kim, K. (2021). Wearable sensors-based exertion recognition using statistical features and random forest for physical healthcare monitoring. *In IEEE International Bhurban Conference on Applied Sciences and Technologies (IBCAST)*, 512-517.

[20] Jelena, T., & Srđan, K. (2023). Smart Mining: Joint Model for Parametrization of Coal Excavation Process Based on Artificial Neural Networks. *Archives for Technical Sciences, 2*(29), 11-22.

[21] John Samuel Babu, G., & Baskar, M. (2023). Location Aware DFS Scheduling Based Improved Quality of Service Maximization with IoT Devices in Cloud. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, 14*(1), 37-49.

[22] Kiruthika, J., Poovizhi, V., Kiruthika, P., & Narmatha, P. (2019). Blockchain Based Unforged License. *International Journal of communication and computer Technologies*, *7*(2), 4-7.

[23] Kishor, A., Chakraborty, C., & Jeberson, W. (2021). Reinforcement learning for medical information processing over heterogeneous networks. *Multimedia Tools and Applications*, *80*(16), 23983-24004.

[24] Mahajan, H. B., Rashid, A. S., Junnarkar, A. A., Uke, N., Deshpande, S. D., Futane, P. R., & Alhayani, B. (2023). Retracted Article: Integration of Healthcare 4.0 and blockchain into secure cloud-based electronic health records systems. *Applied Nanoscience*, *13*(3), 2329-2342.

[25] Pérez-Montalvo, E., Zapata-Velásquez, M. E., Benítez-Vázquez, L. M., Cermeño-González, J. M., Alejandro-Miranda, J., Martínez-Cabero, M. Á., & de la Puente-Gil, Á. (2022). Model of

monthly electricity consumption of healthcare buildings based on climatological variables using PCA and linear regression. *Energy Reports*, *8*, 250-258.

[26] Qahtan, S., Sharif, K. Y., Zaidan, A. A., Alsattar, H. A., Albahri, O. S., Zaidan, B. B., & Mohammed, R. T. (2022). Novel multi security and privacy benchmarking framework for blockchain-based IoT healthcare industry 4.0 systems. *IEEE Transactions on Industrial Informatics*, *18*(9), 6415-6423.

[27] Raza, M., Singh, N., Khalid, M., Khan, S., Awais, M., Hadi, M. U., & Rodrigues, J. J. (2021). Challenges and limitations of Internet of Things enabled Healthcare in COVID-19. *IEEE Internet of Things Magazine*, *4*(3), 60-65.

[28] Saadawi, E. M., Abohamama, A. S., & Alrahmawy, M. F. (2024). IoT-based Optimal Energy Management in Smart Homes using Harmony Search Optimization Technique. *International Journal of Communication and Computer Technologies (IJCCTS), 12*(1), 1-20.

[29] Sajedi, S. N., Maadani, M., & Nesari Moghadam, M. (2022). F-LEACH: a fuzzy-based data aggregation scheme for healthcare IoT systems. *The Journal of Supercomputing, 78*(1), 1030-1047.

[30] Shukla, S., Thakur, S., Hussain, S., Breslin, J. G., & Jameel, S. M. (2021). Identification and authentication in healthcare internet-of-things using integrated fog computing based blockchain model. *Internet of Things*, *15*, 100422. https://doi.org/10.1016/j.iot.2021.100422

[31] Sindhusaranya, B., Yamini, R., Manimekalai Dr, M. A. P., & Geetha Dr, K. (2023). Federated Learning and Blockchain-Enabled Privacy-Preserving Healthcare 5.0 System: A Comprehensive Approach to Fraud Prevention and Security in IoMT. *Journal of Internet Services and Information Security, 13*(3), 199-209.

[32] Srinivasa Rao, M., Praveen Kumar, S., & Srinivasa Rao, K. (2023). Classification of Medical Plants Based on Hybridization of Machine Learning Algorithms. *Indian Journal of Information Sources and Services, 13*(2), 14–21.

[33] Thapa, C., & Camtepe, S. (2021). Precision health data: Requirements, challenges and existing techniques for data security and privacy. *Computers in biology and medicine*, *129*, 104130. https://doi.org/10.1016/j.compbiomed.2020.104130

[34] Trivedi, J., Devi, M. S., & Solanki, B. (2023). Step Towards Intelligent Transportation System with Vehicle Classification and Recognition Using Speeded-up Robust Features. *Archives for Technical Sciences, 1*(28), 39-56.

[35] Ullah, A., Azeem, M., Ashraf, H., Alaboudi, A. A., Humayun, M., & Jhanjhi, N. Z. (2021). Secure healthcare data aggregation and transmission in IoT—A survey. *IEEE Access*, *9*, 16849-16865.

[36] Wilson, D., Sheikh, A., Görgens, M., Ward, K., & Bank, W. (2021). Technology and Universal Health Coverage: Examining the role of digital health. *Journal of Global Health*, *11*. https://doi.org/10.7189%2Fjogh.11.16006

[37] Wu, F., Qiu, C., Wu, T., & Yuce, M. R. (2021). Edge-based hybrid system implementation for long-range safety and healthcare IoT applications. *IEEE Internet of Things Journal, 8*(12), 9970-9980.

[38] Xu, L., Zhou, X., Tao, Y., Liu, L., Yu, X., & Kumar, N. (2021). Intelligent security performance prediction for IoT-enabled healthcare networks using an improved CNN. *IEEE Transactions on Industrial Informatics, 18*(3), 2063-2074.

[39] Yaqoob, I., Salah, K., Jayaraman, R., & Al-Hammadi, Y. (2022). Blockchain for healthcare data management: opportunities, challenges, and future recommendations. *Neural Computing and Applications*, 1-16.

Authors Biography

N.R. Mohamed Kareemulla is a Professor in the Department of Computer Science at Dr.T. Thimmaiah Institute of Technology, Kolar Gold Fields, Karnataka, India, where he has been since 2023. From 2001 to 2023 he served as Lecturer, later as Assistant Professor at Yanbu University, Yanbu, Saudi Arabia. During his stay in Yanbu University, he has served as Vice-chair of Examination, Blackboard Coordinator, Curriculum Development Coordinator, Accreditation Team member, He received a B.E. in Computer Science and Engineering from Bangalore University in 1996, and an M.E. from the Bangalore University, Karnataka, India. He received his Ph.D. in Computer Science and Engineering from a reputed government MS University, Tirunelveli, Tamil Nadu, India in 2016. His research interests include computer networking and parallel and distributed processing. Much of his work has been on improving the understanding, design, and performance of parallel and networked computer systems, mainly through the application of data mining, statistics, and performance evaluation. Professor Kareemulla is author and co-author of many papers on networking and distributed and parallel computer systems. Currently he has published papers in the field of Artificial intelligence and bid data analytics.

Dr. Nijaguna Gollara Siddappa received the B.E. degree in information science and engineering from SJMIT, Chitradurga, in 2006, the M.Tech. degree in computer science and engineering from BVBCET, Hubli, in 2009, and the Ph.D. degree from the Department of Computer Science and Engineering, Visvesvaraya Technological University, Belagavi, Karnataka, in 2020. He has teaching experience of 14.5 years and one year of industry experience. He is currently a Working as a Professor and H.O.D of Information Science and Engineering, S.E.A. College of Engineering and Technology, Bengaluru, where he is involved in research and teaching activities. He has conducted one national conference and many workshops successfully. He has published around 20 papers which include international journals, international conferences, and national conferences. His research interests include data mining and knowledge discovery, big data, information retrieval, and cloud computing. He is a member of The Institution of Engineers (India) (MIE) and member of IEEE (MIEEE).

Pushpa working as an Assistant professor in Reva University. pursuing as research scholar in GITAM University working in the area of coconut harvesting using drones using machine learning under the guidance of Dr. Vadivel Ayaswamy currently, I have completed my course work and working in CSE lab to practical examine the drone application.

Dr.N. Dayanand Lal is currently working as an Assistant Professor in the Computer Science and Engineering Department at GITAM School of technology GITAM (Deemed to be University) Bengaluru. His research interest is in the areas such as Cloud Computing and Cyber Security. He has published more than 30 papers in National and International Peer Review Journals and Conferences and 1 Funded a Research Project Granted by (the DST) Department of Science and Technology on “Information and Technology assisted Silk Cocoon farming for the upliftment of the socio-economic status of Backward community rural mass” and has 2 International Patent Granted and 3 National Patents Published. He is presently supervising 5 Ph.D. Scholars, and has more than 15 years of teaching experience.

Dr.M. Naga Raju is currently working as an Associate Professor in the Computer Science and Engineering Department at GITAM School of Technology GITAM (Deemed to be University) Bengaluru. His research interest is in areas such as multi-gular computing (MGc), Rough Sets, Machine Learning, and Data Science. He has published more than 18 papers in National and International Peer Review Journals and Conferences and 2 Edited Book Chapters has 2 International Patent Granted and 2 National Patents Published. He has more than 27 years of teaching experience. He wrote one book titled “Machine Learning” as a second author. He applied for one funded research project under the ISRO Respond 2023 scheme.

Dr. Zameer Ahmed Adhoni is currently Assistant Professor in Computer Science and Engineering Department GITAM School of technology GITAM University Bangalore. His research interest includes Cloud Computing and Information Security. Moreover, He has published more than 15 papers in National and International Peer Review Journals and Conferences and Completed 3 Funded Research Project from NRC and SRD. He was the member of Saudi Scientific Internet Society (SSIS). and Innovative and Incubation Centre (IIC). He has 11 years of teaching experience in national and international universities. And has Handled many administration roles also in academics.