ISSN: 2182-2069 / E-ISSN: 2182-2077

Privacy-enhancing Blockchain Solutions for the Healthcare Sector: Efficient Message Sharing and Robust Big Data Protection

Dr. Mehak Saini[1*], Dr. Himanshi[2], and Dr. Sanju Saini[3]

[1*]Software Engineer, Aditya Softech, Murthal, Sonipat, Haryana, India.
19001903006mehak@dcrustm.org, https://orcid.org/0000-0001-8060-3968

[2]Assistant Professor, Deenbandhu Chhotu Ram University of Science and Technology, Murthal Sonipat Haryana, India. himanshi.ece@dcrustm.org, https://orcid.org/0000-0002-8516-4148

[3]Professor, Deenbandhu Chhotu Ram University of Science & Technology, Murthal, Sonipat, Haryana, India. sanjusaini.ee@dcrustm.org, https://orcid.org/0000-0003-1390-4861

Received: December 19, 2023; Revised: February 07, 2024; Accepted: March 09, 2024; Published: May 30, 2024

Abstract

Electronic Medical Records (EMRs) play a crucial role in patient care, physician diagnoses, and the advancement of healthcare technology. Researchers have been studying the use of a distributed medical blockchain (BC) system to address the issue of isolated data within centralized healthcare service platforms. Many significant problems persist, including protecting patients' private details, exchanging data across different institutions, and enhancing medical services and effectiveness. This study presents a Blockchain-based Healthcare Privacy Protection Model (BC-HCPPM) for maintaining anonymity in a medical BC system. Initially, the research used an integrated encoder to secure the original EMRs cryptographically. This obscures the confidential data in EMRs to safeguard the patient's privacy and security. A lightweight message-sharing strategy with a (t, n)-threshold is introduced. The EMRs are correlated with a set of n distinct abbreviated portions and are rebuilt using a minimum of t portions. The stored EMR shares use their indexes to create interconnected blocks, forming a BC. To get an EMR from the BC nodes, approved data consumers or institutions must request at least t copies of the EMR. Thus, the medical BC technology streamlines the sharing procedure between institutions and provides adequate safeguards for EMRs. The simulation findings demonstrate that the suggested scheme surpasses comparable literature regarding power usage and storing space efficiency. The medical BC system exhibits excellent stability by implementing the proposed message-sharing method.

Keywords: Blockchain, Healthcare, Big Data, Privacy, Message Sharing.

Journal of Internet Services and Information Security (JISIS), volume: 14, number: 2 (May), pp. 85-97.
DOI: *10.58346/JISIS.2024.I2.006*

*Corresponding author: Software Engineer, Aditya softech, Murthal, Sonipat, Haryana, India.

1 Overview of Blockchain and Healthcare Applications

Electronic Medical Records (EMRs) are crucial in healthcare. Due to the growing need for cross-institution communication, big data processing, and enhancement of medical quality, the present integrated medical service structure cannot match the fast progress of contemporary healthcare. Blockchain (BC) technologies have been used to address conventional systems' vulnerabilities, leading to a decentralized medical BC network (Guo & Yu, 2022). They provide a globally applicable redactable blockchain strategy in this research that is independent of consensus algorithms and blockchain kinds (Jung, 2022). To safeguard the confidentiality of users and prevent the disclosure of private data, it is essential to encrypt EMRs before they are uploaded to the medical BC network (Thilagavathy et al., 2023). Conventional data encryption systems must be improved because of their complexity and expensive information processing. Therefore, it is crucial to investigate methods that protect privacy using a low-complexity message exchange system. Processing large volumes of health information in the medical BC system has significant challenges due to the complex task of satisfying efficiency, system privacy, and effectiveness criteria. To provide a safe and practical solution for ITS, this article (Mada & Abdulatif, 2023) proposes a paradigm based on blockchain technology. Additionally, it facilitates autonomous vehicle collaboration via the use of smart contracts, which establish mutual confidence.

A cloud-based medical system enhances effectiveness and lowers costs compared to a conventional healthcare system. It is essential to acknowledge that the architecture still has several limitations (Wu et al., 2022).

1. Cloud servers are necessary for large-scale intelligent medical devices due to their need for extensive computation and storage capability (Jangjou & Sohrabi, 2022). Given that cloud storage and processing might be considered somewhat centralized, any disruption or assault on cloud servers could potentially impact all users.
2. Medical information is very confidential and requires robust security measures. Cloud servers have the potential to compromise user privacy to gain economic advantages. For example, users authorize qualified healthcare professionals to access their health information. However, cloud service companies disclose users' individualized EMR for medical study and medication marketing without obtaining the user's consent to enhance their advantages.
3. In a healthcare disagreement, the end-user has concerns that the initial EMR saved to the cloud has been tampered with, leading to a lack of confidence in the third party involved. Distributing data preserved in the cloud across several systems while adhering to specific authentication standards is challenging (Singh et al., 2022).

Implementing a medical BC system offers a potential solution to address the isolated data in centralized systems. Like the Bitcoin network, the BC provides a publicly accessible, verifiable, and unchangeable record that ensures the safety and openness of transaction execution. Patients access their EMRs via the medical BC structure, allowing them to get ongoing and traceable treatment. The cross-institutional exchange of EMRs would be facilitated by the participation of several medical centers in this medical BC structure, eliminating the need for patients to create multiple EMRs at various medical facilities (Lee et al., 2022).

The following sections are arranged in the following manner: Section 2 illustrates the background of healthcare applications' privacy and security methods. Section 3 proposes a Blockchain-based Healthcare Privacy Protection Model (BC-HCPPM) for enhancing privacy in the healthcare sector using

blockchain. Section 4 indicates the software results of the proposed method, which are compared with the existing models. Section 5 shows the conclusion and future scope of the research.

2 Related Research and Findings

This section examines previous studies about the conventional intelligent medical system, the use of BC in-network situations, and the implementation of competent medical care using BC technology.

To safeguard personal medical information stored on partially authorized cloud servers, Attribute-Based Encryption (ABE) establishes precise access control (Jiang et al., 2022). Introduced a new patient-centric architecture that utilizes ABE technologies to secure users' EMR data, enabling fine-grained and scalable data access management (Wu et al., 2024). Offered a solution to address the issue of exposing access rules in classical Ciphertext-Policy Attribute-Based Encryption (CP-ABE) by concealing the particular and sensitive values of attributes inside the access policy (Wang et al., 2023). Analyzed and discovered a significant volume of duplicated EMR data stored in the cloud (Benil & Jasper, 2023). To minimize storage expenses on cloud servers, a method was developed to enable the removal of redundant data and, thus, decrease storage costs. Introduced CINEMA, a robust and privacy-preserving central diagnostic system for online treatment (Shen et al., 2023). This framework allows users to perform query activities on cloud servers without decoding their personal information. It does this via quick, secure permutations and comparison techniques. CINEMA needs cloud servers with robust computational and storage capabilities to accommodate simultaneous online queries from millions of consumers (Haleem et al., 2022; Stojanovic et al., 2020).

Introduced a Decentralized Trust Managing Structure (DTMS) that utilizes BC methods (Arshad et al., 2023). This system aims to assess the reliability of vehicles in untrusted situations by continuously updating and sharing trust data among every vehicle in the framework. They enhanced the process of distributed agreement by introducing a novel consensus method to contend for updated confidence among all Road Side Units (RSU). Used smart agreements for storing and disseminating vehicle data, resulting in streamlined and automatic data handling (Philip & Saravanaguru, 2022). Introduced a privacy-preserving and effective data-gathering system in a smart grid based on BC technology (Akgün et al., 2023). The system divides users into groups for optimum planning while safeguarding individual privacy. Within every group, a user is chosen as a miner responsible for aggregating the information and appending it to a private chain specific to that group. Using five distinct datasets including varying numbers of images, this research developed and compared a model for leaf classification. They (Camgözlü & Kutlu, 2023) use four distinct pre-trained models—VGG16, InceptionV3, MobileNet, and DenseNet—to achieve this goal.

Recent research has shown that BC technology has great potential for ensuring the confidentiality and privacy of private medical data. Several research endeavors focus on illustrating the benefits of BC-based intelligent health systems and proposing designs. However, they need more detailed application specifics. Several studies examine managing access to Internet of Things (IoT) consumer data (Abounassar et al., 2022). Yet, they fail to adequately address the issue of confidentiality for EMRs created by physicians.

Some schemes have been developed to use the BC system to empower people to manage their EMRs, which hospitals in intelligent medical systems traditionally hold. Introduced a technique called Medical Block Chain (MBC) that focuses on safeguarding the privacy of medical information from the user's perspective (Malik et al., 2023). Within the MBC system, individuals use encryption techniques to secure confidential health information, which is then stored on a BC that requires permission for access.

Access to data stored on MBC is restricted to people with the correct password. Individuals must provide passwords when exchanging medical information, which enables a rudimentary access control system and increases the risk of password leakage. MBC does not have mechanisms for updating passwords and keys. MBC is susceptible to replay assaults and offline vocabulary assaults (Sharma et al., 2024). This research (Varshavardhini & Rajesh, 2023) introduces FSS-FWNN, an intelligent feature subset selection method for large data categorization (Trivedi et al., 2023). To efficiently manage massive data, the FSSFWNN method makes use of the Hadoop Ecosystem tool. This research (Rosa et al., 2024) suggests a Machine Learning-based Intelligent Database Management Systems (ML-IDMS) technique. This invention combines the skills of Machine Learning with DBMS, improving flexibility and decision-making capacities.

Apart from the issues above, challenges persist in crucial management and adaptable revocation. Thus, the research introduces BC-HCPPM, a system that facilitates precise access control for big data and incorporates the handling of keys and flexible cancellation via separate vital operations.

3 Proposed Blockchain-based Healthcare Privacy Protection Model

This section proposes a privacy-preserving method for EMRs in decentralized medical blockchain systems. The technique is based on sharing confidential data and is designed to be lightweight.

3.1. System architecture

Figure 1 illustrates each of the elements of BC-HCPPM.

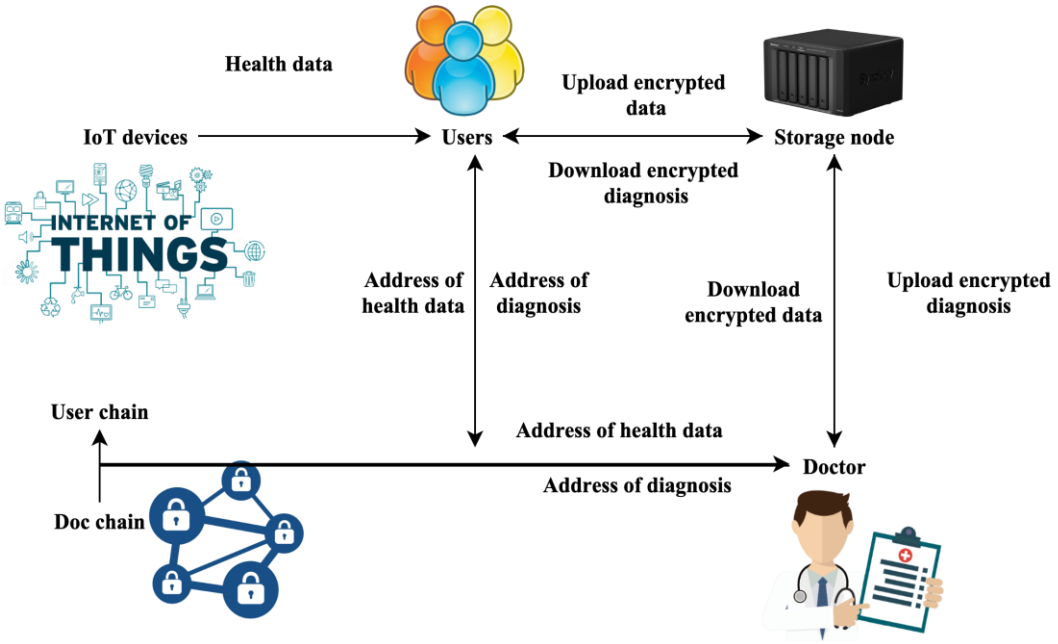

Figure 1: The system architecture of BC-HCPPM

- **IoT Devices**

These sensors can either be worn on the body or implanted within the body. IoT devices track many health metrics of users, including weight, heartbeat, energy expended, sleep habits, blood glucose stages, and more. Each IoT device is assigned a single user node as its administration node. They transmit

diverse health-related information gathered to the user nodes. IoT devices have attributes such as mobility, energy efficiency, customization, and constrained computational and storage capacities. They do not have direct participation in the BC.

- **User Nodes**

Each user U_x represents the administration of one or more IoT devices, which can collect, secure, and transmit data from these devices to a storing node. Several lightweight client nodes exist that retain the block headings of the Userchain (UC). These nodes are limited to generating and publishing events. Some customer nodes, called core client nodes, possess robust computational and storing capacity. Core client nodes can create, distribute, authenticate, and support lightweight client nodes in their search for transactions. They can extract fresh Ublocks (UB) and incorporate new client transactions into a newly formed UB. Client nodes can perform data extraction on Docchain (DC) but cannot add activities to the DC.

- **Doctor Nodes**

Each D_x is a licensed medical professional working in a hospital and an artificial intelligence health analyzer employed by an intelligent medical service. They can provide uninterrupted diagnostics using consumers' IoT data. Every hospital and company inside BC-HCPPM collectively become a consortium, whereby the consortia's regulations govern the actions of all physician nodes. Physician nodes with proper authorization can access and get UC data and create DC activities. Physician nodes cannot append events to DC.

- **Accounting Node**

The system includes a unique node that the group implements. It can authenticate the accuracy and validity of transactions originating from physician nodes. During every time duration, every bookkeeping node chooses a leader. The leader collects established activities from physician nodes in the group and creates a new Dblock (DB), which is then appended to the DC.

- **Storage Nodes**

The data from consumers' IoT devices and physicians' diagnoses are stored together in a distributed way, with both sets of information being fully protected. This study assumes that every storing node is built, administered, and operated by a group of healthcare suppliers, such as institutions. It employs a content referencing mechanism in which the location is generated from the file's contents. Every file is transformed into an encrypted string, which is distinct and serves as a unique identifier for the file. The saved file was accessed using the file's hashing phrase on UC or DC. It enables the efficient distribution of large amounts of information.

- **Userchain**

This is a publicly accessible BC that is used for the publication of data submitted by users. Individuals can participate in UC by accessing and reviewing activities, initiating activities, and engaging in mining activities at their convenience. UC is comprised of a sequence of UB and expands progressively. Every UB includes the preceding UB cryptographic hash and the activities created by users.

- **Docchain**

The BC is a cooperation that is used for the dissemination of physicians' diagnoses. Diagnosis activities can only be produced by physician nodes approved by the collaboration. Such transactions are then uploaded to DC by accounting networks. The data on DC is accessible to anybody. DC comprises a sequence of DB that progressively expands as time passes. Each DB contains the preceding DB cryptographic hash and the transactions created by physicians.

3.2. Privacy-enhancing Framework

The system developed a lightweight (t, n)-threshold messaging sharing method to enhance the safety and efficiency of the EMR sharing network. This technique ensures anonymity in the medical BC system. The research is deliberating on the procedures for storing and retrieving EMR shares. The architecture primarily consisted of two key components: the generation and retention of EMR shares and the retrieval while employing EMRs. Figure 2 shows the privacy-enhancing model of BC-HCPPM.

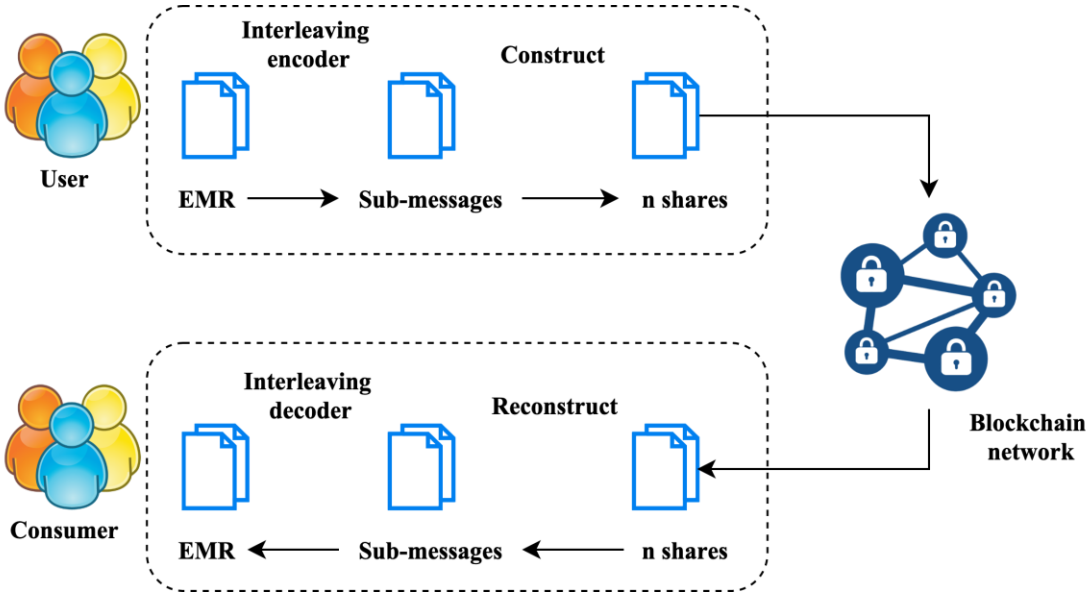

Figure 2: Privacy enhancing model of BC-HCPPM

3.2.1. Creation and Storage

The primary actors responsible for generating the initial EMRs are the patient's doctor and the medical practitioner. To safeguard the private data and preserve the integrity of the initial EMRs, they opt to upload and keep encrypted shares instead of unencrypted EMRs on the distributed ledger nodes.

EMR integrating encoding involves encoding the initial EMRs into a sequence of sub-messages using an integrating encoder. The initial EMRs, consisting of l bits, are divided into l/t groups, where every grouping has t bits. Here, t is a positive integer less than or equal to n. The research consistently append a sequence of $(t - (l \bmod t))$ zeros to the end of the l-bit string R. Next; it transforms them into t sub-messages $\{x_1, x_2, \cdots, x_t\}$ having a size of l/t. The adversary's ability to gain multiple shares is rendered meaningless due to the integrating encoder's destruction of the semantic meaning of each share. This is achieved by dividing and reassembling the initial data.

The EMRs $\{x_1, x_2, \cdots, x_t\}$ will be transformed into n distinct shares, denoted as s_x (where x = 1, 2,..., n), using Equation (1) throughout the manufacturing process of the EMR shares.

$$s_x = \begin{cases} s_1 + s_2 + \cdots + s_{i-1} + ix_i + x_{i+1} + \cdots + x_t mod\ p & if\ 1 \le i \le t \\ \frac{s_1}{i+1-t} + \frac{s_2}{i+2-t} + \cdots + \frac{s_t}{i+t-t} & else \end{cases} \quad (1)$$

Let p be the most significant prime number less than or equal to $2(l/t)$. The magnitude of s_x is consistently less than the ceiling value of l divided by t of p. By reducing the amount of shares l/t compared to the size l of the initial message, the message splitting scheme becomes more compact and significantly enhances data processing performance. The building of EMRs involves encrypting t sub-messages into n shares, improving individual users' security.

Rights are stored at BC nodes. The original EMRs are transformed into n shares by integrating the encoder and constructing shares. Each share will be distributed across various BC nodes and kept inside their internal storage. The indices will be downloaded into the medical BC network. Like the transaction confirmation process in BC, the index of the shares and the accompanying IDs of the block networks are merged and shared with the medical BC system, including all the BC node locations, for confirmation.

Confirmation of EMRs and creation of a new block: Once a node acquires the authority to generate a new block via the consensus method, it will keep track of the indices of EMR shares and their corresponding storage locations in the medical BC system. Given the immutability of data contained in the blocks, the BC servers cannot refute their responsibility for storing the appropriate EMR shares.

To enhance effectiveness, the intelligent contract includes the integration of EMRs' interleaving encoded and building procedures and EMRs' reconstructing and integrating decoding operations. Implementing this trade agreement is a preventive measure against harmful customers or opponents' intentional destruction of EMRs. BC technologies enhance the transparency and credibility of the EMRs' information. Every EMR functions as an activity that can be documented in the medical BC network. This documentation is authenticated by a globally verified or end-to-end provable open BC auditing trail.

4 Simulation Results

This section focuses on conducting experiments to verify the efficacy and practicality of BC-HCPPM. An operational version of BC-HCPPM has been developed to assess its effectiveness and performance. The user node is emulated using a smartphone with a 64-bit 8-core CPU processor running at a maximum frequency of 2.45 GHz. The experiment is conducted using the Android 7.1.1 system. The Java programming language is employed for prototyping IoT transactions and critical transactions. The performance of user chain mining networks and physician nodes is evaluated on a 64-bit Windows 7 operational system running on an Intel Core i7 processor with a clock speed of 3.60 GHz. UC and DC are implemented using the Python programming language.

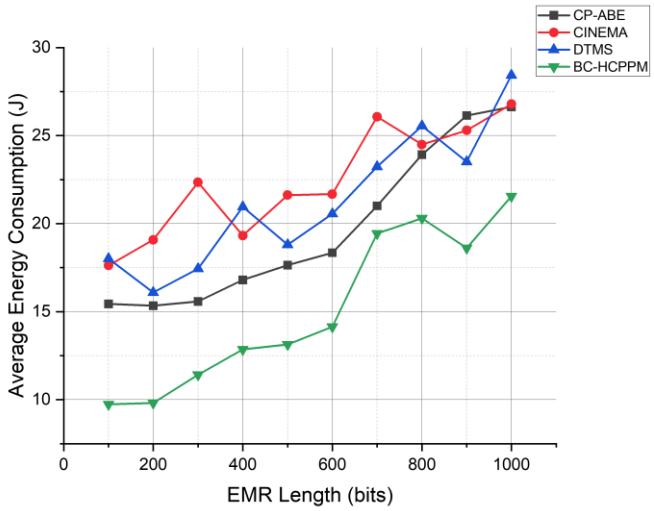

Figure 3: Average energy consumption analysis

Figure 3 depicts the mean energy consumption (measured in joules) for various EMR durations using four distinct methods: CP-ABE, CINEMA, DTMS, and BC-HCPPM. The mean results are calculated for each approach using different EMR durations. BC-HCPPM consistently beats other approaches regarding energy usage and overall EMR durations. When the length of an EMR is 1000 bits, BC-HCPPM shows a significant decrease in energy use (21.55 J) compared to CP-ABE (26.63 J), CINEMA (26.79 J), and DTMS (28.43 J). The exceptional performance of BC-HCPPM is assured by its lightweight privacy-preserving method and effective message-sharing method, resulting in decreased energy consumption and improved overall system efficiency.

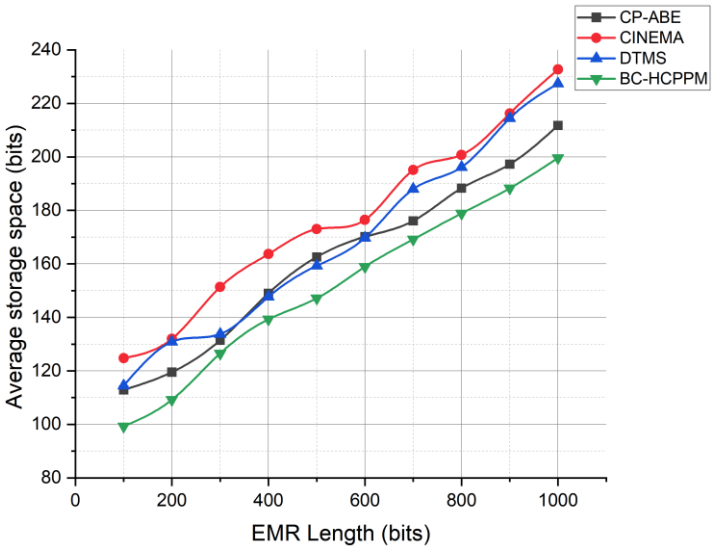

Figure 4: Average storage space analysis

Figure 4 displays the results of the mean storage capacity (measured in bits) for different durations of EMR employing CP-ABE, CINEMA, DTMS, and BC-HCPPM. The calculated averages demonstrate the storage needs of each approach for varying EMR durations. The BC-HCPPM constantly exhibits exceptional efficiency in storage capacity for all lengths of EMR. With an EMR length of 1000 bits,

BC-HCPPM only needs 199.56 bits of storage, outperforming CP-ABE (211.73 bits), CINEMA (232.68 bits), and DTMS (227.37 bits). The efficiency of BC-HCPPM is assured by its integrated encoder and lightweight message-sharing mechanism, which decrease storage requirements while preserving data integrity.

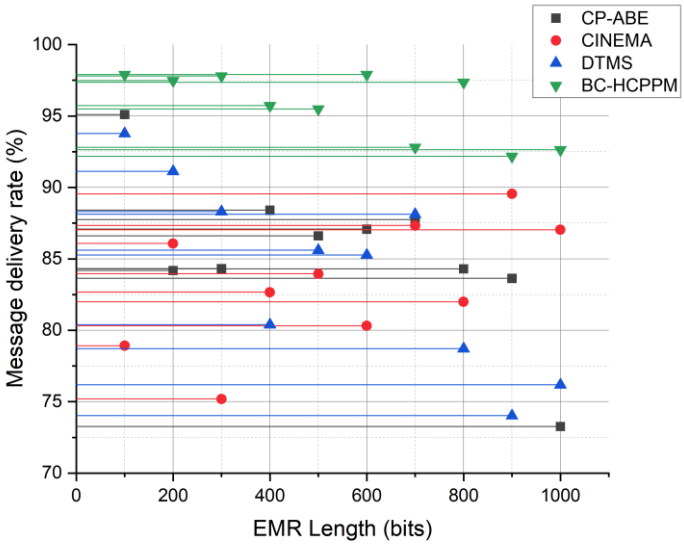

Figure 5: Message delivery rate analysis

Figure 5 illustrates the percentage of message delivery rates for different durations of EMR in CP-ABE, CINEMA, DTMS, and BC-HCPPM. The delivery rates are calculated as mean values, representing the efficiency of each technique in guaranteeing successful message delivery. The message transmission rate of BC-HCPPM routinely surpasses that of other systems. BC-HCPPM has a significantly superior delivery rate (92.63%) compared to CP-ABE (73.26%), CINEMA (87.03%), and DTMS (76.18%) at an EMR length of 1000 bits. The exceptional performance is credited to BC-HCPPM's (t, n)-threshold lightweight message-sharing system, which improves data reconstruction efficiency and promotes message delivery's reliability and effectiveness.

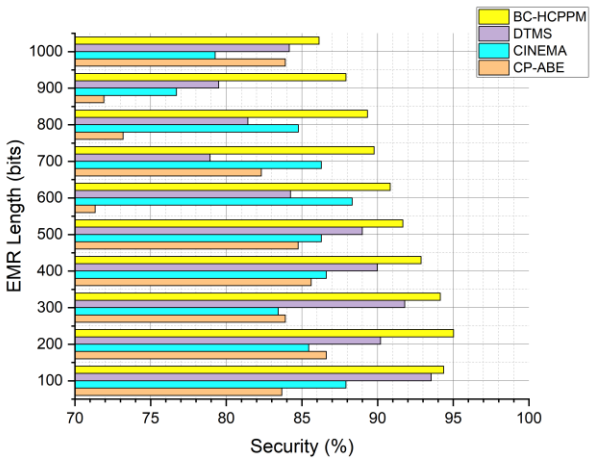

Figure 6: Security analysis

Figure 6 displays the security percentages for various EMR durations using CP-ABE, CINEMA, DTMS, and BC-HCPPM. The calculated averages indicate the security levels of each approach for

different EMR durations. BC-HCPPM routinely demonstrates greater security efficacy in comparison to other methodologies. BC-HCPPM outperforms CP-ABE, CINEMA, and DTMS regarding security percentage, achieving a remarkable 86.13% at an EMR length of 1000 bits. The BC-HCPPM guarantees strong security using privacy-preserving techniques such as the interleaving encoder, lightweight message sharing, and BC creation.

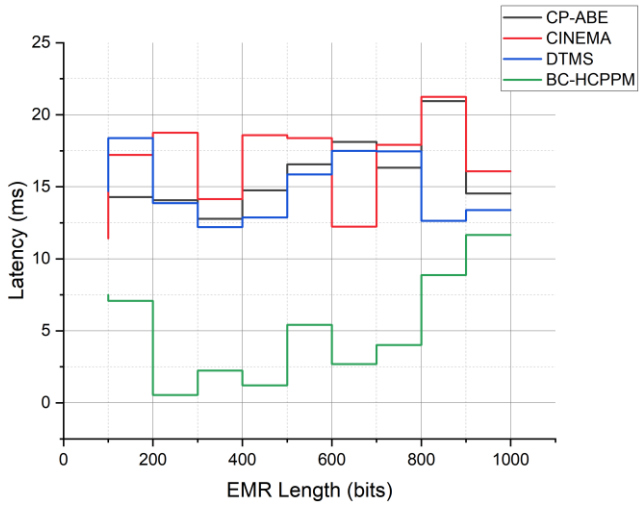

Figure 7: Latency analysis

Figure 7 presents the latency findings (in milliseconds) for different durations of EMR utilizing CP-ABE, CINEMA, DTMS, and BC-HCPPM. Latency is calculated by determining the mean duration for message transmission over various EMR durations for each technique. The BC-HCPPM approach routinely surpasses other methods in reducing latency. BC-HCPPM has notably reduced latency (11.66 ms) in comparison to CP-ABE (14.53 ms), CINEMA (16.08 ms), and DTMS (13.38 ms) at an EMR length of 1000 bits. The exceptional performance of BC-HCPPM is credited to its effective message-sharing scheme, integrated encoder, and BC design. These factors work together to decrease latency in healthcare BC communication significantly.

The BC-HCPPM presented displays exceptional performance in all aspects: it achieves a lower average energy consumption of 9.74 J, uses a smaller storage space of 99.23 bits, accomplishes a higher message delivery rate of 97.89%, provides strong security with a rate of 94.37%, and demonstrates decreased latency of 7.51 ms. The results highlight the effectiveness of BC-HCPPM in achieving a balance between privacy, security, and effectiveness in healthcare BC systems. It is a robust and efficient option for exchanging data between institutions, outperforming other studied techniques.

5 Conclusion and Outcomes

This study presents a privacy-preserving cross-institution EMR sharing strategy. The approach is built on BC technology and a lightweight (t, n)-threshold messaging sharing method. The integrated encoding method was used to obfuscate the semantic significance of the initial EMRs and conceal the clients' and healthcare facilities' private data. The (t, n)-threshold messaging sharing system first fragmented the encoding EMRs into n shorter stakes, resulting in enhanced data processing performance. The BC nodes maintained the shares instead of the initial EMRs. During the EMR retrieval procedure, clients must first identify the BC networks that have shares of the specific EMR they are interested in. They then proceed to request all the relevant shares. The initial EMR might be recreated using a minimum of $t(1 < t \leq$

n) shares. This method can potentially enhance data security and the efficiency of data exchange across organizations and data consumers. The research conducted a series of tests to assess the effectiveness of the suggested approach. The simulation findings demonstrated a substantial reduction in energy usage and storage requirements compared to conventional methods.

There are various ways in which the approach might be further enhanced. Initially, the research will endeavor to develop a more streamlined message exchange system to enhance the effectiveness of processing EMR data in the following endeavors. The study will investigate integrating BC technology and mobile edge computing in medical service systems to improve efficiency, considering the significant growth of data terminals. The current scheme needs an effective method for retrieving EMRs. The research will develop an innovative index structure for storing and retrieving EMR sharing. This can significantly enhance the experience for consumers and medical centers.

References

[1] Abounassar, E.M., El-Kafrawy, P., & Abd El-Latif, A.A. (2022). Security and interoperability issues with internet of things (IoT) in healthcare industry: A survey. *Security and Privacy Preserving for IoT and 5G Networks: Techniques, Challenges, and New Directions*, 159-189.

[2] Akgün, M., Soykan, E.U., & Soykan, G. (2023). A privacy-preserving scheme for smart grid using trusted execution environment. *IEEE Access, 11*, 9182-9196.

[3] Arshad, Q.U.A., Khan, W.Z., Azam, F., Khan, M.K., Yu, H., & Zikria, Y.B. (2023). Blockchain-based decentralized trust management in IoT: systems, requirements and challenges. *Complex & Intelligent Systems, 9*(6), 6155-6176.

[4] Benil, T., & Jasper, J. (2023). Blockchain based secure medical data outsourcing with data deduplication in cloud environment. *Computer Communications, 209*, 1-13.

[5] Camgözlü, Y., & Kutlu, Y. (2023). Leaf Image Classification Based on Pre-trained Convolutional Neural Network Models. *Natural and Engineering Sciences, 8*(3), 214-232.

[6] Guo, H., & Yu, X. (2022). A survey on blockchain technology and its security. *Blockchain: research and applications, 3*(2), 100067. https://doi.org/10.1016/j.bcra.2022.100067

[7] Haleem, A., Javaid, M., Singh, R. P., & Suman, R. (2022). Medical 4.0 technologies for healthcare: Features, capabilities, and applications. *Internet of Things and Cyber-Physical Systems, 2*, 12-30.

[8] Jangjou, M., & Sohrabi, M.K. (2022). A comprehensive survey on security challenges in different network layers in cloud computing. *Archives of Computational Methods in Engineering, 29*(6), 3587-3608.

[9] Jiang, Y., Xu, X., & Xiao, F. (2022). Attribute-based encryption with blockchain protection scheme for electronic health records. *IEEE Transactions on Network and Service Management, 19*(4), 3884-3895.

[10] Jung, S.W. (2022). Universal Redactable Blockchain. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA), 13*(4), 81-93.

[11] Lee, J.S., Chew, C.J., Liu, J.Y., Chen, Y.C., & Tsai, K.Y. (2022). Medical blockchain: Data sharing and privacy preserving of EHR based on smart contract. *Journal of Information Security and Applications, 65*, 103117. https://doi.org/10.1016/j.jisa.2022.103117

[12] Mada, A., & Abdulatif, A. (2023). Intelligent Transport System based Blockchain to Preventing Routing Attacks. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA), 14*(1), 126-143.

[13] Malik, H., Anees, T., Faheem, M., Chaudhry, M.U., Ali, A., & Asghar, M.N. (2023). Blockchain and Internet of Things in smart cities and drug supply management: Open issues, opportunities, and future directions. *Internet of things*, 100860. https://doi.org/10.1016/j.iot.2023.100860

[14] Philip, A.O., & Saravanaguru, R.K. (2022). Smart contract based digital evidence management framework over blockchain for vehicle accident investigation in IoV era. *Journal of King Saud University-Computer and Information Sciences*, *34*(7), 4031-4046.

[15] Rosa, C., Wayky, A.L.N., Jesús, M.V., Carlos, M.A.S., Alcides, M.O., & César, A.F.T. (2024). Integrating Novel Machine Learning for Big Data Analytics and IoT Technology in Intelligent Database Management Systems. *Journal of Internet Services and Information Security, 14*(1), 206-218.

[16] Sharma, A., Kaur, S., & Singh, M. (2024). A secure blockchain framework for the internet of medical things. *Transactions on Emerging Telecommunications Technologies*, *35*(1), e4917. https://doi.org/10.1002/ett.4917

[17] Shen, G., Fu, Z., Gui, Y., Susilo, W., & Zhang, M. (2023). Efficient and privacy-preserving online diagnosis scheme based on federated learning in e-healthcare system. *Information Sciences*, 119261.

[18] Singh, S., Rathore, S., Alfarraj, O., Tolba, A., & Yoon, B. (2022). A framework for privacy-preservation of IoT healthcare data using Federated Learning and blockchain technology. *Future Generation Computer Systems*, *129*, 380-388.

[19] Stojanovic, L., Figun, L., & Trivan, J. (2020). Risk Management on Medjedja Dam on Tailing Storage Facility, Omarska Mine Prijedor. *Arhiv za tehničke nauke, 1*(22), 11–20.

[20] Thilagavathy, R., Renjith, P.N., Lalitha, R.V.S., Murthy, M.Y.B., Sucharitha, Y., & Narayanan, S.L. (2023). A novel framework paradigm for EMR management cloud system authentication using blockchain security network. *Soft Computing*, 1-9.

[21] Trivedi, J., Devi, M. S., & Solanki, B. (2023). Step Towards Intelligent Transportation System with Vehicle Classification and Recognition Using Speeded-up Robust Features. *Arhiv za tehničke nauke, 1*(28), 39-56.

[22] Varshavardhini, S., & Rajesh, A. (2023). An Efficient Feature Subset Selection with Fuzzy Wavelet Neural Network for Data Mining in Big Data Environment. *Journal of Internet Services and Information Security*, *13*(2), 233-248.

[23] Wang, H., Liang, J., Ding, Y., Tang, S., & Wang, Y. (2023). Ciphertext-policy attribute-based encryption supporting policy-hiding and cloud auditing in smart health. *Computer Standards & Interfaces*, *84*, 103696. https://doi.org/10.1016/j.csi.2022.103696.

[24] Wu, S., Zhang, A., Gao, Y., & Xie, X. (2024). Patient-centric medical service matching with fine-grained access control and dynamic user management. *Computer Standards & Interfaces*, *89*, 103833. https://doi.org/10.1016/j.csi.2024.103833

[25] Wu, Z., Xuan, S., Xie, J., Lin, C., & Lu, C. (2022). How to ensure the confidentiality of electronic medical records on the cloud: A technical perspective. *Computers in biology and medicine*, *147*, 105726. https://doi.org/10.1016/j.compbiomed.2022.105726

Authors Details

Dr. Mehak Saini completed her Ph.D. in Wireless Communication Systems from D.C.R. University of Sci. and Tech., Murthal, India, with a thesis titled "Performance Enhancement of MIMO Systems in Wireless Communication." Prior to her doctoral studies, she served as an Assistant Professor in the School of Electrical and Electronics Engineering at L.P.U., Jalandhar. Mehak also brings valuable experience in software engineering to her research pursuits. Her research interests encompass MIMO Wireless Communication Systems, Machine Learning, and Deep Learning.

Dr. Himanshi received the B. Tech. degree in ECE from Kurukshetra University and M.E. in Microelectronics from BITS Hyderabad. She received Ph.D. degree in Electronics and Communication Engineering from Deenbandhu Chhotu Ram University of Science & Technology, Murthal, Sonepat, Haryana, India in 2018. Currently, she is working as Assistant Professor in Electronics and Communication Engineering Department of Deenbandhu Chhotu Ram University of science and technology, Murthal, Sonipat. Her areas of research are High speed networks, Networks' Survivability, Restoration and Protection options in Optical Networks.

Dr. Sanju Saini received the B. Tech. degree in Electrical Engineering and M. Tech.in Electrical Engineering with specialization in Control System from NIT, Kurukshetra. She received Ph.D. degree in Electrical Engineering from Deenbandhu Chhotu Ram University of Science & Technology, Murthal, Sonepat, Haryana, India in 2016. Currently, she is working as Professor in Electrical Engineering Department of Deenbandhu Chhotu Ram University of science and technology, Murthal, Sonipat. She has more than 50 technical research papers to her credit and has twice won the best paper presentation award. Her areas of research are fault diagnosis in Power system, machine learning and deep learning.