Received: October 22, 2022. Revised: December 16, 2022. 572

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

Fully Decentralized Block Chain with Proxy Re-Encryption Algorithm for Healthcare Security

Parag Rastogi[1]* Devendra Singh[1] Sarabjeet Singh Bedi[2]

[1]*IFTM University, Moradabad, India*
[2]*MJP Rohilkhand University, Bareilly, India*
* Corresponding author's Email: parag0305@gmail.com

Abstract: The medical technology is being evolved for enhancing the healthcare information related to medication, diseases, medical images etc., by using Electronic Healthcare Recording (EHR). The details such as gender, age, and weight of patients are sensitive, and require protection against unauthorized access. Therefore, providing a robust security for medical data is indeed a challenge. The present research work proposed a Fully Decentralized Block chain (FDBC) model with the Proxy Re-Encryption Algorithm (PReA) with an Ethereum smart contract. The proposed FDBC-PReA allows the data to be visible only for the owner and the smart contract as the model is implemented in an Ethereum based test bed. Each time when the data is transformed, the data loss is obtained for the incorrect data which is taken care by the decentralized BC. The fully decentralized BC stores and checks whether each of the entity shares or accesses the real time data. The proposed FDBC-PReA Ethereum smart contracts, and proxy re-encryption algorithms are executed with a faster rate that consumed average block time of 5.48s, which is lesser when compared to average block times of Smart-Contract Ethereum Distributed Ledger-14s, Searchable Encryption-48.125s, and Decentralized Security Architecture-Software Defined Networking (SDN)-10s.

Keywords: Electronic healthcare recording, Ethereum smart contracts, Fully decentralized block chain, Proxy re-encryption algorithm, Healthcare information.

1. Introduction

The Block Chain (BC) technology has allowed to create the decentralized public record in a network over the computer systems [1-3]. The data is called as the 'block' as it is linked together in the form of 'chain' which makes it a single list consisting of digital information [4-7]. There are block-chain applications in healthcare, which are helpful in data exchange to protect the health information [8, 9]. The block chain has an advantage in medical field as it eliminates cost issues, but at the same time it can cause data overload [10-12]. Yet, the BC is associated with reconciling both of the properties that are compatible for real time applications [13-15]. The health records are shared and preserved by performing necessary tasks in the healthcare systems [16]. The health monitoring shows loss in the high security levels that affects negatively for the protection of large health records [17-19]. The loss of data integrity has led with the serious implication shows loss in the patient's life [20]. This is necessary for providing the security for the EHR as it consists of privative or sensitive information [21]. The block chain technologies are considered in recent years as an adaptive approach when compared to the existing techniques [22]. The management of medical data from the medical institutions does not guarantee the patient data reliability and integrity [23]. The risk factors like hacking, data loss, and data authentication from unauthorized users, personal privacy leakages, and lack of security etc., From all the distinct medical institutions, the medical data obtained are gathered in such a way that the data present is very much vulnerable to cyber threats [24]. Thus, in the proposed work, the block chain technology is used that provides advantage as it addresses the problems related to security and cloud

system [25, 26]. The research contribution is that the proposed FDBC-PReA smart contracts and proxy re-encryption algorithms enhance the computational time and execution time of the patients' data and do not reverse the process of hashing as explained below:

- The proposed scheme is a combination of FDBC-proxy re-encryption with fully decentralized block chain model establishes dynamic smart contracts among trusted third parties' involvement. The FDBC model allows the data to be visible only for the owner and the smart contract, as the model is implemented in an Ethereum based test bed. Each time, when the data is transformed, the data loss from the incorrect data is entered into the work stream, which will be monitored by the decentralized BC.
- The stored data is checked by the fully decentralized BC if each entity access or share the real time data. The hospital's corresponding financial transactions are managed based on the agreed smart contract automatically, in the BC.

The present section explains about the existing models involved in providing security to healthcare based on the BC is as follows:

Mehedi [27] developed a block chain-based security system for IoT infrastructure management based on Ethereum transactions. Storing EHR data as a whole in block chain was hard due to the price and size of the block chain. Therefore, an Elliptic Curve Cryptosystems (ECC) was utilized for providing health data sharing securely in cloud computing. The developed model utilized an EHR system from various attacks based on the security using an Automated Validation approach of Internet Security Protocols and Applications (AVISPA). Yet, the developed model showed difficulty for set of simulations for realistic protocol testing that failed to provide a secured protocol for cloud-assisted EHR systems in BC. Rathore [28] developed a BC that was based on decentralized IoT networks in a security based architecture. The decentralized approach was designed to provide security based Software Defined Networking (SDN) for IoT-based BC. The developed model has an advantage in the IoT network to detect the network attacks effectively. However, it used longer time of 8 to 14 seconds to reach its normal system state. Kim [29] designed a protocol for cloud assisted EHR for providing security using the BC. The block chain technology developed showed data integrity for controlling and accessing for the log transactions. The cloud servers have the ability to store the EHR's patient data showed security for managing the transactions. The developed model showed realistic simulation to test the protocol which provided security to the cloud in the BC.

Chelladurai [30] developed a BC based EHR automated system for health data. The developed model was aimed at exchange of health information for building smart e-health systems. The health data based model was launched as it was immutable for creation of patient log by using the modified Merkle Tree data structure. The model provided rapid security to the stored health records. The model updated the health information, medical records among distinct providers. Yet, the developed model required a new Merkle tree data model for ensuring the integrity of content. Abunadi [31] developed a block chain security framework (BSF) that securely stored and effectively kept the EHRs. The model was safe and proficient as it acquired medical information proficiently from the patients, doctors, and insurance agents for protecting data of patient. The BSF-HER showed the lightweight EHR which considered less time when compared with the existing models. Yet, the BC provided with security was only provided with the healthcare domain.

The research paper structure is as shown below: The section 2 includes the proposed method that involves the steps involved in it. The section 3 discusses the results and discussions. The section 4 is the conclusion for the research work.

2. Materials and methods

The proposed FDBC-PReA method consists of the following implementation steps that adds the individual features. The proposed FDBC-PReA explanation method is shown in Fig. 1.

2.1 Dataset description

The Health Service Executive (HSE) is a dataset used in the research which is important to provide personal and health care social services to make the public funds for the people residing in the Ireland region. The dataset consists of information about the inpatients, the outpatients and all the lists of each department in the hospital from Ireland that has been considered in the research. The waiting lists of the outpatients and inpatients of the day will be managed by the National Treatment Purchase Fund (NTPF). The medical centres are registered well in detail regarding the patient' data that describes the data as well. The medical centres privately participate inside the BC that are registered by the network administrators. The HSE generates for identifying the data and store them in the medical centres. The medical centres view the HSE for each of the patients.

The medical data is uploaded through the server and views the HSE stored to serve the cloud. The transaction information is shared and stored in the cloud server.

2.2 Decryption

The present research work is as shown in Fig. 1 that constitutes of communication entities that perform Smart Contract System (SCS) to access and control data encryption and for storing them in the IPFS. The entities present for data encryption are as follows:

2.2.1. Data owner (DO)

It is the initial point present in the system and the DO is used for data upload or sharing to perform the proper agreement and communication, which is posed by the Multi-Party Authority (MPA). The MPA registers the hash of the data and locates the address on the block chain. This hash function will help the data to perform encryption using the symmetric key algorithm. The key algorithm is utilized to send the P2P decentralized database with another encrypted key together with the public key sharing a wallet among the DO and MPA based on the multi-signature. Thus, the hash function will create SCS that has components to address the data. The DO will perform re-encryption from the public key present in the DR and thus send its private key to send for the proxy servers.

2.2.2. Data requester (DR)

The requester contacts SCS for encrypting and accessing the data so that suitable data can be provided. The validation is provided by the requester to valid for the data and access them for receiving the proxy for the data obtained from the SCS. The data obtained is now downloaded once the requester could encrypt the data and hash the file. Thus, the decryption process is performed using a symmetric key during the data retrieval process using the private key for decrypting data and asymmetric key.

2.2.3. IPFS

At this stage, the data will be held in a P2P decentralized database to share them among multiple users. The encrypted data with the symmetric key will be uploaded and can be used further for the process of encryption using the public key. The data requested from the database will be provided for the process of encryption with the symmetric key.

2.2.4. Proposed FDBC-PReA

In the proposed FDBC-PReA method, a proxy re-encryption algorithm has been used to perform Compute Intensive Task (CIT). As CIT operations based on SCS are an expensive approach for Ethereum block chain models, proxy re-encryption has been used to acquire the data and to perform the complicated functions. This acts as a medium for data sharing mainly among the DR and DO which manages the reputation system for the smart contracts by the proxy servers. The reputation of the smart contract will be based upon the response to the queries coming under the smart contract. The same hash will result in distinct values and the reputation for them goes lower. The proxy servers will be having their unique location or address to which the accessed token will be shared and with the requester. Fig. 1 shows the Model structure of Proxy re-encryption process.

The PRE scheme performs mainly two types of functions known as KeyGen and ReKeyGen that deal with cipher texts and messages. The KeyGen produces public and secret keys in spairs and encryption and decryption of public and secret keys. The PRE scheme defines the functions for

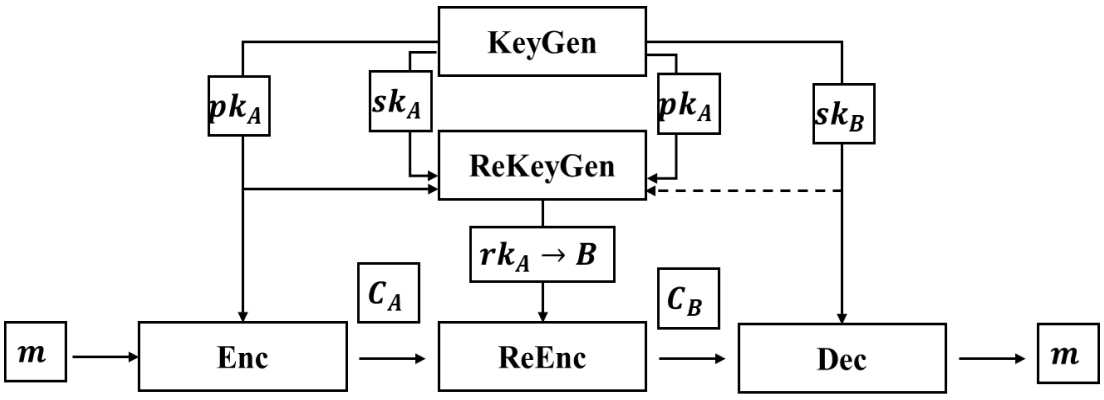

Figure. 1 Proxy re-encryption process

supporting the functionality of re-encryption. The ReKeyGen produces the re-encryption key between users as they use the key for cipher text transformation. The pre scheme defines the functions, which supports for the re-encryption between the users. The ReEnc uses the transform of the key that converts original cipher text for one user that can be retrieved by using the secret key. The general syntax of the proxy re-encryption technique is represented in Eq. (1).

$$(KeyGen, ReKeyGen, Enc, ReEnc, Dec) \quad (1)$$

Where, the input security parameter is specified as n and the output generated from the algorithm is stated as $KeyGen$. The public/secret key pairs (pk_A, sk_A) for a user A is mathematically stated in Eq. (2).

$$KeyGen(n) \rightarrow (pk_A, sk_A) \quad (2)$$

In addition, the public/secret key pairs for the users A and B are indicated as (pk_A, sk_A) and (pk_B, sk_B) . In PReA algorithm, the re-encryption key generation $ReKeyGen$ is mathematically stated in Eq. (3). Here, the ReKeyGen generates an output as a re-encryption key $rK_A \rightarrow B$.

$$ReKeyGen((pk_A, sk_A, pk_B, sk_B) \rightarrow rk_A \rightarrow B \quad (3)$$

The public key pk_A and the message $m \epsilon M$ is used for performing encryption Enc, as represented in the Eq. (4). In addition, the re-encryption $ReEnc$ is performed that generates and encrypts the output as a cipher text $C_A \epsilon C$, as mentioned in Eq. (5).

$$Enc(pk_A, m) \rightarrow C_A \quad (4)$$

$$ReEnc(rkA \rightarrow B, cA) \rightarrow cB \quad (5)$$

The input uses re-encryption key $rkA \rightarrow B$, where the cipher text is denoted as $C_A \epsilon C$. The re-encryption algorithm generates ReEnc, which is an output for the second cipher text $C_B \epsilon C$ or the error symbol $\perp$ that states C_A is invalid. Here, the user decrypts the cipher text by using the secret key $\mathrm{Dec}(sk_A, C_A)$.

The input of the secret key is represented as sk_A and a ciphertext $C_A \epsilon C$ that considers the decryption algorithm. Dec output with a message that shows the error symbol $\perp$ where $m \epsilon M$ that indicated C_A as an invalid value. The cipher text spaces and plain text are represented as M and C respectively. The PReA approach is intended for proxy re-encryption rather for fast re-encryption. The PReA performs the process of re-encryption that executes encryption mechanism, but is not as efficient as the encrypt-decrypt approach. The decentralized block chain network does not allow unauthorized users. Each of the member in the network is having an exact same copy of the data that is the distributed ledger form. In case, the ledger member is corrupted or altered, the security is prioritized over the performances. When the block chain network scales up more than the network size, it is secured and the performances slows down. As each member of the node validates all data are added at the ledger. The members are added to a decentralized network that provides safety. The model members will add a new record that is associated with particular patients and will allow recording the data among the providers. Thus, new information will be received through an automated process, for the process of verification. The evolution participants and the records are kept engaged and informed. The FDBC consists of records called as blocks that are used to record transactions across computers, in which the data is not altered retroactively without the subsequent block alterations so that any involved block cannot be altered retroactively, without the alteration of all subsequent blocks. Thus, the block chain is proven to be Fully connected BC chain model and named as FDBC. The Block chain-based MPA is used for the IPFS encrypted data access to the address of the requester to perform the process of validation. If the proxy server is receiving the shared data from the requester, then ensure the privacy, integrity, and confidentiality of the data. The proxy server will get the key encrypted from the DO and these data are downloaded from the database which was decentralized including the symmetric and encrypted key. Then, after the completion of the process, the proxy server will be having the key, which is used for data re-encryption to send it to the requester.

2.2.5. MPA

The MPA will play the role of co-owner that consists of steps like access control mechanisms to perform. The MPA will manage to access the data which was shared with the DO to avoid malicious acts. The DO uses the multi-signature technology that requires a key for the process of MPA. The process will require $m\ of\ n$ keys that have 2 keys among the 3 total keys. The keys are adjustable in the process based upon the scenario. Even though the MPA does not involve the entities in the process, they required enough keys for verification that needs to access the

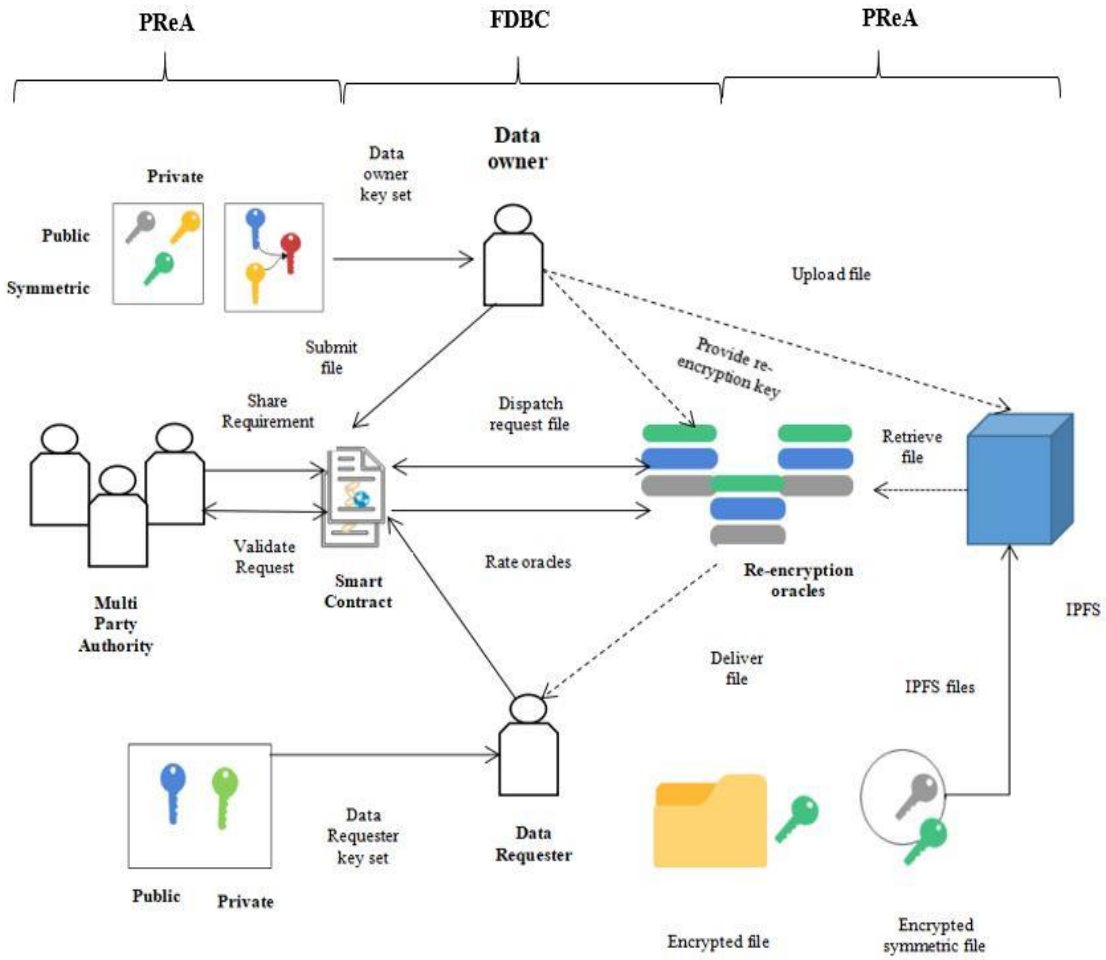

Figure. 2 Block diagram of the proposed FDBC-PReA method

data which was requested by the DR. If the highly confidential organization wants to share information (sensitive) with an agent, then the agent will be the DO but it is not mandatory to acquire the control of data. The keys that are given for access will be given to the wallet of the account from where the supervisor will know the person whom the rights have been for securely accessing. Thus the MPA technology has to be built for securing sensitive data from external attacks.

The contracts usually consist of the record ownership metadata, information related to the data integrity, and permission. The proposed FDBC-PReA system will perform block chain transactions to carry out the graphical signed instruction using cryptography for managing few properties which are explained in the next section.

2.3 SCS for healthcare

The smart contracts have been designed for distinct medical works to make access among the distinct entities of healthcare medical ecosystems.

The smart contract will help to store the data in the BC technology which has all the conditions to manage and access the data. Thus, it can be viewed that the stakeholders are used for the proposed FDBC-PReA scheme to perform different activities. The doctors and patients can interact better and thus data authorization gets embedded for smart contracts. The centralized entity will approve the operation and manage directly through the process of the smart contract which reduces the managing process and administration cost. This present research uses the medical record data for local database storage and maintains the performances through economic viability for the hash element data present in the block chain.

2.3.1. The data transactions signed with the private key of owners

The log patient provides the relationship smoothly through the smart contracts using Ethereum BC consists of the medical record viewed the data retrieval instructions and permissions. The external server execution improved the data integrity by protecting against tampering that includes the cartographic hash function. The providers will add a new record that is present with the patients that allow

the record sharing among the providers. The new information will be received from the party gives an automated notification among the cases to verify the record has been accepted or not rejected. In this way, record evolution takes place as it keeps the information engaging. The system prioritizes the offer by designing the aggregated contract that is referred for all the patient-provider relationships with references checks for the medical history before any update.

2.3.2. Manage identity verification

The present research uses public-key cryptography for managing the identity verification by using the DNS implementation for mapping the existed and accepted ID includes the social security number for the user Ethereum address. Once the block chain confirms permission through the authentication server from the database then the algorithm should sync to handle the off-chain data to exchange the database among the provider. The use of smart contracts is supported through the block chain which enables automating the track up to the state transitions for a certain level. The block chain is referred and the permissions are confirmed through the database server to sync the algorithm for handling the off-chain data exchange performed among the database and its provider. The block chain will support smart contract usage which has enabled tracking the certain transition states. The states can be related to the birth of a new record of the population. The log patient-provider will generate a relationship through the smart contracts on the Ethereum block chain to associate for viewing the data against tampering and medical record to overcome those retrieval instructions and also viewing permissions for performing an external server. Thus a cryptography-based hash function is used for recording the reports on the block chain to confirm the process of data integrity.

The system will prominently use the offering and designates the contract to aggregate all the patient-provider relationships as references and provides a single point to check the medical history updates.

2.3.3. The process to file and issue medical prescriptions

There is a various medical workflow that involves various medical steps to design and develop through the BC smart contract system. The main issues, that are included in the medical prescription for treating the diseases, are them being complex and treating them with the suitable procedure for the patients' surgery is critical. The doctor will prescribe the medical things and the medicines that are required for the surgery patients. The pharmacy will access these prescriptions through the smart contract in the Ethereum BC by granting the permissions from the patient as well as the doctor. The prescription is accessed by the pharmacy and then will issue a medicine that has the expiry data for the dosage when it is ready for the patient. The proposed FDBC-PReA method uses SCS features to organize them generally with a satisfaction which provides suggestions from doctors to the drug centres. The doctors will spend the required time explaining the medicine for requests that speaks generally about the drug stores once the patient visit for the treatment. The laboratories are used for reducing the printing expenses, patient's mail, fax that results with singular suppliers. The patients and the lab accesses from the healthcare BC from where the instalments are taken into account for the protection. The counsel information will be transferred to the process that claims from the pharmaceutical organization for information selection to use contemplates. The emergency clinics and the specialists get access to restore the information embed on the patients at not costs will decrease work and costs authoritatively.

2.3.4. Recommendation and refer the patients

The patient submits automatically for a request that is having a condition with the doctor through SCS. The doctor can consider the request from the user and revert with a recommendation for the specialization of necessary care is required. The patient information such as patient history, reports of the EHR and history for the treatment need to be considered. The patient record will be maintained by the database from where the specific rules need to be applied to access the record up to the extent and govern the smart contracts using the Ethereum BC. The patient will submit the request for medical treatment and thus sends an application for a specialist via the strict structure agreement. The doctor will now understand the demand and will revert for a recommendation from where the patients will be traded simply for providing care to the specialists. The patient data will be regarded as the treatment and should be reported for the EHR.

2.3.5. Data flow for healthcare reimbursement

The main objective is to perform reimbursement for the process improving in the field of health care and the physicians quickly work without putting it hold on the treatment for the patients and waiting for the payer for responding. Automated smart contracts are executed and for monitoring the entire process.

The ultimate aim is to reduce the error because of manually putting effort and responding to the request before the authorization process. The medical policy for the smart contract is given to the payer to determine the information obtained by the Ethereum block chain based on the request. The authorized data will be re-obtained once returned from the provider immediately. The pharmacies, laboratories, specialists and still more stakeholders will be considered from where the patient is delegated to access and verified the authorized insurance in real-time.

2.3.6. Providing drug and medical device

The medical device manufacturers are provided with the drug for simpler and cost-effective alternated clinical trials for recruitment that often needs considerable expenses for taking the patient contact information so that the data will be independently obtained from the providers and thereafter executing the marketing campaigns. The main objective of the research is to run the clinical trial which is related with the smart contracts based on Ethereum network which results safe medicines increased interest of the public with respect to the medical field. Thus, the present research work will handle the metadata under the protocol registration and perform the study details such as enrolment through smart contracts, screening process through the proposed FDBC-PReA method. The organization will send a message for each of the selected patients starting from the reader to their medical prescription to find the results from the laboratory. The patient will allow for access and form a company bill to process through the smart contracts, providing them the received fees, and also to report with appropriate results for testing the patients.

3. Result and discussion

The proposed FDBC-PReA is used in the research work is used for computing in a system containing Intel Core i9 operating with 3GHz processor having 128 GB memory and Windows 10 (64 bit) operating system, wherein the coding is implemented in Python 3.7.

3.1 Performance measures

The parametric measures are evaluated for the proposed FDBC-PReA that solved the problem of block chain technology using the verifiable secure hash technique. The performances are as follows:

I. Block chain memory size

Memory unit is the amount of data that can be stored in the storage unit of block chain.

II. Average block time

Block time, which defines the time each block takes to mine data, which is expressed as shown in Eq. (6).

$$Block\ Generation\ time = \frac{Blocksize}{Average\ transaction\ speed} \quad (6)$$

III. Total execution time (secs)

The total time taken by the block to initiate independent values, which is expressed in the Eq. (7).

$$Total\ Execuation\ Time = I \times CPI \times T \quad (7)$$

From the above Eq. (7), I is the number of instructions in the program. CPI is the average number of cycles per instruction, and T is the clock cycle time.

3.2 Quantitative analysis

Table 1 shows the performances that are evaluated for the FDBC-PReA Ethereum smart contracts showed improvement in re-encryption obtained in terms of block generation, chain memory, and total execution time. In the table 1 as the blocks become bigger, the memory is taken up by the node. In case the blocks are too big, the nodes are running out of the memory and will fail. Therefore, without the PReA Ethereum encryption algorithm the model runs out of the memory and enough memory downloads the block chains where the costs involved is running shrink the nodes in the network. Similarly, the total execution time without PReA Ethereum encryption algorithm which takes attackers a lot of time and processing power to break. Whereas, the proposed FDBC-PReA Ethereum smart contracts block numbers are ranging between 50 to 500 when the block numbers are changing the block chain memory increases because of safer data storing. There is a linear variation from one block to another where the generation time is also varied.

Table 3 shows analysis of distinct parameters such as block chain memory size, total execution time, and block generation time for various keys such as FCBC-Elliptic Curve Cryptosystems, FCBC- Smart Contract system, and FDBC-PReA Encryption with FDBC. The block chain memory is increasing up to 0.2850 Mb where the block generation time is

Table 1. Quantitative analysis of the proposed FDBC-PReA Ethereum smart contracts, and proxy re-encryption evaluated for block generation time

Number Of Blocks	Block Generation Time(secs)	Block Chain Memory Size(Mb) without PReA Ethereum Encryption algorithm	Block Chain Memory Size(Mb) with PReA Ethereum Encryption algorithm
50	1	0.3833	0.2833
100	2	0.3835	0.2835
150	3	0.3836	0.2836
200	4	0.3838	0.2838
250	5	0.3839	0.2839
300	6	0.3842	0.2842
350	6	0.3842	0.2842
400	8	0.3844	0.2844
450	9	0.3848	0.2848
500	10	0.385	0.285

Table 2. Quantitative analysis for the proposed FDBC-PReA Ethereum smart contracts for performing proxy re-encryption evaluated in terms of blocks time execution (secs)

Number Of Blocks	Total Execution Time(secs) without PReA Ethereum Encryption algorithm	Total Execution Time(secs) with PReA Ethereum Encryption algorithm
50	69	59
100	71	61
150	72	62
200	72	62
250	73	63
300	74	64
350	75	65
400	80	70
450	81	71
500	89	79

increased up to 9.9747s. The block generation time is increased as there is increase in the number of blocks. The proposed FDBC-PReA Ethereum in smart contacts and proxy re-encryption is concerned as shown in the Fig. 2. The results of the proposed FDBC-PReA Ethereum smart contracts, and proxy re-encryption algorithm, are represented in Fig. 3. The total execution of time by the system is increasing as the block numbers are also increased. The blocks are ranging from 50 to 500 where the execution time is varied from 59 to 79 seconds of time. The Table 2 shows proposed FDBC-PReA Ethereum smart contracts method results in terms of various blocks for execution time. The total execution time for obtained for the proposed method is shown in the Fig. 4. The Fig. 5 shows the graphical representation for the proposed FDBC-PReA Ethereum smart contracts, proxy re-encryption algorithms with respect to total execution time.

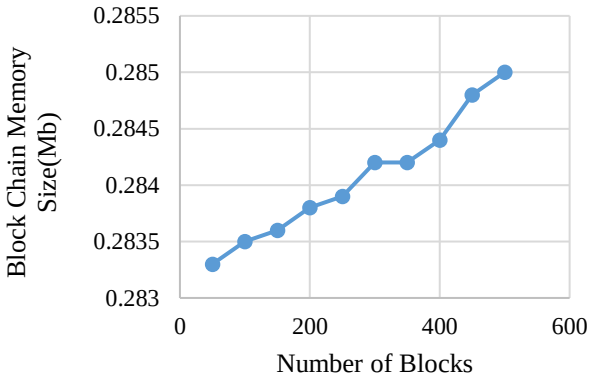

Figure. 3 The proposed FDBC-PReA ethereum smart contracts, and proxy re-encryption algorithms with respect to block chain memory

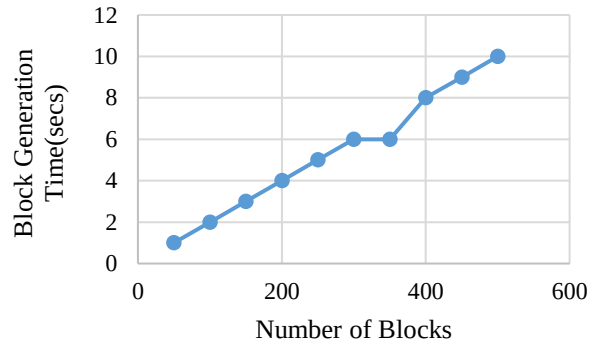

Figure. 4 The proposed FDBC-PReA ethereum smart contracts for proxy re-encryption for graphical representation to the algorithms with respect to block generation

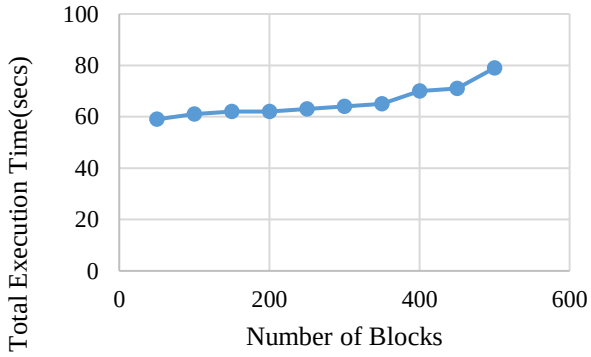

Figure. 5 The graphical representation for the proposed FDBC-PReA Ethereum smart contracts, and proxy re-encryption algorithms with respect to total execution time (s)

Table 3. Analysis of distinct parameters such as block chain memory size, total execution time, and block generation time for various keys with FDBC

Encryption Key	Block Chain Memory Size	Total Execution Time(secs)	Block Generation Time(secs)
FCBC-Elliptic Curve Cryptosystems	0.45	89	100
FCBC- Smart Contract system	0.356	80	90
FDBC- PReA Encryption	0.285	79	80

3.3 Comparative analysis

The performance results obtained by the proposed FDBC-PReA model are compared with the existing models' results, which are validated in terms of average block time (s) as seen in Table 3. In this study, the proposed FDBC-PReA model does not require the proxy for transferring the cipher text into a new one. This process significantly reduces the operation and computation time, while allowing a new user to access the files. The proposed FDBC-PReA obtains an average block time for the Ethereum smart contracts. The proxy re-encryption algorithms showed 5.48s execution time with faster execution compared to the existing models that are used to store the confidential information in the BC.

Mehedi [27] presented a Smart-Contract Ethereum Distributed Ledger model that failed to process the data exchange among nodes, which increased its block average time. Rathore [28] developed a SDN based model that decentralized security. The model consumed longer time of 10 to 14 seconds which recovered from its normal state. Kim [29] used a Searchable Encryption and ECC model for performing simulation realistically that showed improvement for simulations. The developed existing model required improvement in security that showed efficiency improvable for the HER in the cloud. The Modified Merkle Tree data structure developed by Chelladurai and Pandian [30] attained total execution time of 100s, because of its rapid process. The BSF-HER developed by Abunadi [31] obtained 4.5 s of average block time consumed by the BC for 300 number of blocks. The model showed improvement in terms of time but the number of blocks consumed were less. Therefore, the proposed FDBC-PReA Ethereum smart contracts, and proxy re-encryption algorithm, showed improvement in terms of block execution time. The proxy re-encryption algorithms used hashing technique that improved computational time among the patient's data as the attacker was unable for process reverse hashing. The computation costs for the proposed scheme is with the related schemes that computes the multiplication and performs bilinear pairing with an exponential function. It is with addition to the bilinear pairing for exponential function. which is having multiplication and bilinear pairing with hash function. The application provider has computed with the hash function and the patient computes the hash function for performing the encryption. Thus, better efficiency is obtained for the proposed compared to the existing

Table 4. Comparative analysis

Authors	Dataset	Methodology	Number of blocks	Average block time (s)	Total Execution Time (s)	Computation cost	Communication Cost
Mehedi [27]	Electronic Health records	SC Ethereum Distributed Ledger	500	14	-	-	-
Rathore [28]		Decentralized Security - SDN	500	10	69	0.8878n + 0.4438ms	-
Kim [29]		ECC	500	5.88	74.02	0.5109 ms	512 bits
Chelladurai and Pandian [30]		Modified Merkle Tree data structure	500	-	100	-	-
Abunadi [31]		Block-chain security framework- electronic health record (BSF-HER)	300	4.5	-	-	-
Proposed FDBC-PReA method		Ethereum smart contract algorithm	500	5.48	65.54	0.4932 ms	512 bits

models, when the hash functions are used. Further, the communication costs are compared at the time of authentication phase for the proposed system that showed relative encryption for ECC encryption, identity hash function and message code authentication. The proposed scheme transmitted the messages that consisted of hash function used for performing encryption.

The smart contracts of Ethereum and the proxy re-encryption algorithm is used as a verifiable key that matches the password based on the authentication received from the results showed improvement in terms of execution time. The comparative analysis also showed that the proposed FDBC-PReA Ethereum smart contracts, and proxy re-encryption algorithms estimated the key generation time when the model completed execution in 65.54 s for real time hardware. Thus, the computational cost was lowered and thus the proposed FDBC-PReA research obtained better results when compared to the existing SDN and ECC systems.

4. Conclusion

The proposed FDBC-PReA research has implemented a system for data management and shares the requirements based on a medical perspective. Block chain technology is used for providing security, privacy, availability and also to control the access of the EHR data to be checked. The main objective of using the BC will be outlined with the proposed FDBC-PReA technique to improve the healthcare process for outgoing patients. The BC will help the patients in health care in many ways like reduces the transaction cost and uses the smart contract that are embedded in the protocols simplifies the procedure in reducing the burdens from the administrative to remove those intermediaries. The BC will make an aim to improve the data collection and use them to share the data from the patients to the researchers that intermediately has the sub-processor in the data. The proposed FDBC-PReA research uses BC technology to create a healthcare system economically effective for all kinds of people that are secure, scalable, decentralization and accessible. The patients are now ready to exchange their records safe and free with hospital doctors as well as research organizations to maintain the privacy of their medical data. Thus, current healthcare security issues, like legacy networks, unstructured data difficulties, and privacy concerns, are solved. The hospital's corresponding financial transactions are automatically managed based on the agreed smart contract in the BC, by using the proposed method. The proposed FDBC-PReA Ethereum smart contracts executed at a faster rate, as it needed 5.48s of average block time for 500 blocks, which is faster than the Modified Merkle Tree data structure that took 100s of total execution time and the Block-chain security framework- electronic health record (BSF-HER), which took 4.5s of block chain time for 300 blocks. Thus, the computational cost, computation time is lowered and the proposed FDBC-PReA research obtains better results compared with the existing SDN and ECC systems. Therefore, the proposed model is applicable for real time hospital's corresponding financial transactions would be managed based on the agreed smart contract automatically, in the BC securely. However, the realistic simulations for testing the protocol was aimed and developed. Yet, the practical simulations available, would further help to develop a secured protocol for cloud assisted EHR using the BC. As a future work, the FDBC-PReA can be validated in terms of security properties: secrecy, anonymity and authentication.

Conflicts of Interest

The authors declare no conflict of interest.

Author Contributions

The paper background work, conceptualization, methodology have been done by 3rd Author. Dataset collection, implementation, result analysis and comparison, preparing and editing draft, visualization have been done by first author. The supervision, review of work and project administration, have been done by second author.

References

[1] J. Sun, X. Yao, S. Wang, and Y. Wu, "Blockchain-Based Secure Storage and Access Scheme for Electronic Medical Records in IPFS", *IEEE Access*, Vol. 8, pp. 59389-59401, 2020.

[2] S. Tanwar, K. Parekh, and R. Evans, "Blockchain-Based Electronic Healthcare Record System for Healthcare 4.0 Applications", *Journal of Information Security and Applications*, Vol. 50, p. 102407, 2020.

[3] Khatoon, "A blockchain-based smart contract system for healthcare management", *Electronics*, Vol. 9, No. 1, p. 94, 2020.

[4] H. Shu, P. Qi, Y. Huang, F. Chen, D. Xie, and L. Sun, "An Efficient Certificateless Aggregate Signature Scheme for Blockchain-Based

Medical Cyber Physical Systems", *Sensors*, Vol. 20, No. 5, p. 1521, 2020.

[5] R. Haque, H. Sarwar, S. R. Kabir, R. Forhat, M. J. Sadeq, M. Akhtaruzzaman, and N. Haque, "Blockchain-Based Information Security of Electronic Medical Records (EMR) in a Healthcare Communication System", *Intelligent Computing and Innovation on Data Science*, Vol. 118, pp. 641-650, 2020.

[6] T. Li, D. H. Shih, C. C. Wang, C. L. Chen, and C. C. Lee, "A Blockchain Based Data Aggregation and Group Authentication Scheme for Electronic Medical System", *IEEE Access*, Vol. 8, pp. 173904-173917.

[7] Q. Xia, E. B. Sifah, A. Smahi, S. Amofa, and X. Zhang, "BBDS: Blockchain-Based Data Sharing for Electronic Medical Records in Cloud Environments", *Information*, Vol. 8, No. 2, pp. 44, 2017.

[8] F. Hussein, N. A. Kumar, G. R. Gonzalez, E. Abdulhay, J. M. R. Tavares, and V. H. C. D. Albuquerque, "A Medical Records Managing and Securing Blockchain Based System Supported by a Genetic Algorithm and Discrete Wavelet Transform", *Cognitive Systems Research*, Vol. 52, pp. 1-11, 2018.

[9] S. K. Kim and J. H. Huh, "Artificial Neural Network Blockchain Techniques for Healthcare System: Focusing on the Personal Health Records", *Electronics*, Vol. 9, No. 5, p. 763, 2020.

[10] R. Rajput, Q. Li, and M. T. Ahvanooey, "A Blockchain-Based Secret-Data Sharing Framework for Personal Health Records in Emergency Condition", *Healthcare*, Vol. 9, No. 2, p. 206, 2021.

[11] Arunkumar and G. Kousalya, "Blockchain-Based Decentralized and Secure Lightweight E-Health System for Electronic Health Records", *Intelligent Systems, Technologies and Applications*, Vol. 1148, pp. 273-289, 2021.

[12] A. K. G. Escamilla, A. H. E. Hassani, and E. Andres, "Classification models for heart disease prediction using feature selection and PCA", *Informatics in Medicine Unlocked*, p. 00330, 2020.

[13] J. E. Dalton, M. B. Rothberg, N. V. Dawson, N. I. Krieger, D. A. Zidar, and A. T. Perzynski, "Failure of Traditional Risk Factors to Adequately Predict Cardiovascular Events in Older populations", *Journal of the American Geriatrics Society*, Vol. 68, No. 4, pp. 754-761.

[14] Gupta, R. Kumar, H. S. Arora, and B. Raman, "MIFH: A machine intelligence framework for heart disease diagnosis", *IEEE Access*, Vol. 8, pp. 14659-1467, 2019.

[15] G. Magesh and P. Swarnalatha, "Optimal feature selection through a cluster-based DT learning (CDTL) in heart disease prediction", *Evolutionary Intelligence*, pp. 1-11, 2020.

[16] Swain, P. Ballal, V. Dolase, B. Dash, and Santhappan, "An Efficient Heart Disease Prediction System Using Machine Learning", *In Machine Learning and Information Processing*, pp. 39-50, 2020.

[17] S. Sajeev, A. Maeder, S. Champion, A. Beleigoli, C. Ton, X. Kong, and M. Shu, "Deep Learning to Improve Heart Disease Risk Prediction", In: *Proc. of Machine Learning and Medical Engineering for Cardiovascular Health and Intravascular Imaging and Computer assisted Stenting*, pp. 96-103, 2015.

[18] R. Venkatesh, C. Balasubramanian, and M. Kaliappan, "Development of Big Data Predictive Analytics Model for Disease Prediction using Machine learning Technique", *Journal of Medical Systems*, Vol. 43, No. 8, pp. 272, 2019.

[19] R. T. Selvi and I. Muthulakshmi, "An optimal artificial neural network based big data application for heart disease diagnosis and classification model", *Journal of Ambient Intelligence and Humanized Computing*, Vol. 12, pp. 6129-6139, 2021.

[20] H. Das, B. Naik, H. S. Behera, S. Jaiswal, P. Mahato, and M. Rout, "Biomedical data analysis using neuro-fuzzy model with post-feature reduction", *Journal of King Saud University-Computer and Information Sciences*, 2020.

[21] M. A. Lakhan, A. N. Mohammed, S. Rashid, T. Kadry, K. H. Panityakul, K. H. Abdulkareem, and T. Thinnukool, "Smart-contract aware ethereum and client-fog-cloud healthcare system", *Sensors*, Vol. 21, No. 12, p. 4093, 2021.

[22] M. M. Pai, R. Ganiga, R. M. Pai, and R. K. Sinha, "Standard electronic health record (EHR) framework for Indian healthcare system", *Health Services and Outcomes Research Methodology*, Vol. 21, No. 3, pp. 339-362, 2021.

[23] M. T. Riaz, A. A. A. Sanad, S. Ahmad, M. A. Akbar, L. A. Suwaidan, H. A. A. A. Shaikh, and H. S. A. Sagri, "A wireless controlled intelligent healthcare system for diplegia patients", *Mathematical Biosciences and Engineering*, Vol. 19, No. 1, pp. 456-472, 2022.

[24] Imamalieva, "Recent Challenges of Big Data Application in Healthcare System", In: *Proc. of International Conference on Multidimensional*

Research and Innovative Technological Analyses, pp. 121-124, 2022.

[25] G. Ahmed and F. Piccialli, "A deep-learning-based smart healthcare system for patient's discomfort detection at the edge of Internet of things", *IEEE Internet of Things Journal*, Vol. 8, No. 13, pp. 10318-10326, 2021.

[26] Y. Chen, S. Ding, Z. Xu, H. Zheng, and S. Yang, "Blockchain-Based Medical Records Secure Storage and Medical Service Framework", *Journal of Medical Systems*, Vol. 43, pp. 1-9, 2019.

[27] S. T. Mehedi, A. A. M. Shamim, and M. B. A. Miah, "Blockchain-Based Security Management of IoT Infrastructure with Ethereum Transactions", *Iran Journal of Computer Science*, Vol. 2, No. 3, pp. 189-195, 2019.

[28] S. Rathore, B. W. Kwon, and J. H. Park, "BlockSecIoTNet: Blockchain-Based Decentralized Security Architecture for Iot Network", *Journal of Network and Computer Applications*, Vol. 143, pp. 167-177, 2019.

[29] M. Kim, S. Yu, J. Lee, Y. Park, and Y. Park, "Design of Secure Protocol for Cloud-Assisted Electronic Health Record System Using Blockchain", *Sensors*, Vol. 20, No. 10, p. 2913, 2020.

[30] U. Chelladurai and S. Pandian, "A novel blockchain based electronic health record automation system for healthcare", *Journal of Ambient Intelligence and Humanized Computing*, Vol. 13, No. 1, pp. 693-703, 2022.

[31] A. Abunadi and R. L. Kumar, "BSF-EHR: blockchain security framework for electronic health records of patients", *Sensors*, Vol. 21, No. 8, p. 2865, 2021.