International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Electronic Health Record Sharing in Cloud Computing with Privacy and Security Preservation Using Blockchain Technology

Divya Singh[1], Dr. D. Nagaraju[2], Dr. B. Rama Mohan[3], Sathish Bojjawar[4], Sreedhar Burada[5], Dr. Solleti Phani Kumar[6], Dr. Ravi Kumar[7], Dr. R. Sundar[8]

Submitted: 27/05/2023 **Revised**: 08/07/2023 **Accepted**: 26/07/2023

Abstract: Nowadays, electronic health records are an important system in cloud computing technology. Different types of algorithms are fostered various components by means of image based encryption for medical care applications. Although more security protocols were created among them without a doubt, not many procedures were proficient and hearty for the speedy recovery of reports from the cloud yet numerous conventions endure by reason of less security, privacy, and respectability. Existing techniques depended on encrypting the record in view of the key generation centre. To overcome the security issues a novel optimized Whale based Cryptographic Blockchain (WBCB) technique is proposed. Moreover, public cloud system is utilized to develop the technique efficiently. Here, the MATLAB platform is used for the implementation process. Furthermore, the developed technique is compared with conventional techniques such as encryption time, decryption time, etc.

Keywords: *security protocols, Cryptographic Blockchain, public cloud system, encryption time, decryption time*

1. Introduction

In the modern day, healthcare information sharing and its maintenance are one of the major tasks in cloud computing systems [1]. Moreover, many of the organizations and business entities are fascinated with the digital cryptocurrency by using blockchain innovation. Moreover, blockchain is the decentralized ledger technology, which is efficiently protecting healthcare information from third party users [2]. The main goal of blockchain technology is the transmission process to be transparent and verifiable. In a modern era, transactions are securely protected without any third party interruption [3]. Several sectors and organizations are effectively utilize the business, banking sector, defence sectors, electronic computing system, etc [4]. Moreover, these all are incorporated with the smart technology Machine Learning (ML), Internet of Things (IoT) and Artificial Intelligence (AI). The basic model of crypto system is shown in fig.1. [5]

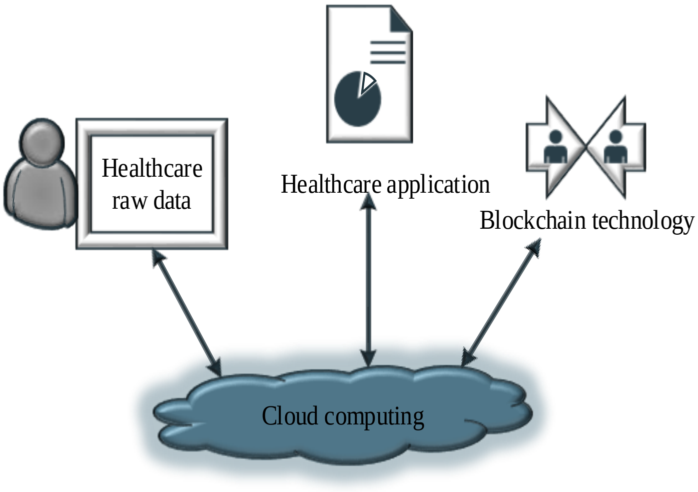

Fig.1 Basics of public crypto system

Furthermore, the utilization of blockchain innovation in the medical services industry has been upgraded the straightforwardness as well as interchanges among the patients and medical services suppliers [6]. Here, the

[1]*Assistant Professor, Electronics and Communication Engineering, GLA University,*
Mathura, India
[1]*Divya.singh@gla.ac.in*
[2]*Professor, Department of CSE, Sri Venkatesa Perumal College of Engineering and Technology, Puttur, Andhra Pradesh, India*
[2]*raj2dasari@gmail.com*
[3]*Department of CSE Hyderabad Institute of Technology and Management, Hyderabad.*
[3]*ramamohan.cse@hitam.org*
[4]*Associate Professor, EIE Dept,CVR College of Engineering*
[4]*satishbojjawar@cvr.ac.in, 9701188826*
[5]*Assistant Professor, Dept. of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur Dist., Andhra Pradesh - 522502, India.*
[5]*sreedharburada1@gmail.com*
[6]*Assistant Professor, Dept.of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur Dist., Andhra Pradesh - 522502, India.*
[6]*Email: phanikumar.solleti@gmail.com*
[7]*Associate Professor, Department of ECE, Jaypee University of Engineering and Technology,*
Guna - 473226.
[7]*ravi.kumar6@gmail.com*
[8]*Assistant Professor, Computer science and Engineering, Madanapalle Institute of Technology & Science.Ap.*
[8]*drsundarr@mits.ac.in*

healthcare records are developed based on the complexity and size of the each information, which is stored into the cloud system. [7], However, the enhanced given healthcare records are used in various sectors and it has various attributes such as names and identifiers, and their accessibility in various organizations [8]. Besides, healthcare services are having strong security because it is the essential phase to preserve patient data safe from forestall crimes. From this case, the healthcare data accessed by third party users are then the patient information cannot be utilized with individual data of patients being displayed to anybody with contact. The protection of patients' information is fundamental to effectual medical services the board [9]. These types of issues and performance can be tackled by utilizing the blockchain model helped by healthcare Industry 4.0 is to guarantee the reliability of information as well as forestall altering disappointment at a particular sector [10]. Consequently, Data Integrity (DI) technique is to detect accurate diagnosis and maintain the unique identifier system [11]. Here, the DI system is very important to prevent injury during quick medical treatments. However, all developed strategies can prove the drug discovery, insurance claim, etc [12]. In addition, blockchain technology allows the healthcare management system to transmit patient records over the blockchain network [13]. As EHR frequently contains patients' delicate clinical data, it becomes fundamental to guarantee the classification and appropriate mystery of the re-appropriated EHRs [14]. Besides, in the cloud-helped EHR stockpiling model, the patients never again have direct command over their rethought EHRs, which may likewise cause serious honesty and secrecy-related security issues [15]. As of now, the medical care industry sees that the arising changeless blockchain innovation appropriately accomplishes the fundamental security needs for fostering a safe cloud helped EHR stockpiling structure [16].

In past, DangueCBC [17], blockchain-based E-health system [18], access management strategy for cloud storage system [19] and fine-grained searchable encryption method [20] several techniques are implemented to address such issues. But, still, now accurate solutions are not proposed to address the cloud-based problems. Therefore, the present article introduced a novel optimized blockchain-based neural framework to enhance security and privacy systems efficiently. Moreover, the developed work's contribution is summarized in below,

- Primarily, electronic healthcare data is taken from cloud storage system and trained to that data in a proposed system.
- Hereafter, a novel efficient WbCB framework is structured with the suitable parameter to protect the data from the external users or third parties.
- Consequently, the proposed system can convert the original plaintext into the ciphertext for their security purpose during the data transmission.
- Then, verify the secret key the ciphertext is turned into the original plaintext.
- After finishing the analysis software performance and Implementation of this work is done with the help of Python framework.
- Consequently, the effectiveness of proposed method is compared with other techniques in terms of efficiency, communication overhead, encryption time, decryption time, running time, reliability and confidential measure.

Finally, the entire sections of this article is directly demonstrated at last of the introduction part. Recent related literatures are reviewed and concluded in section II. After that, the basic system their problems are explained in section-III. Section IV demonstrated that the proposed model and its detailed explanations and its process. Then, the simulation and comparison outcomes are illustrated in section V result and discussion. Finally, the article is concluded with section VI conclusion.

2. Related works

Current related works based on security and privacy of blockchain with cloud computing for medical data is summarized below, Nowadays, wireless mobile technology, telemedicine systems, wearable technologies are rapidly turned up in the modern medicine world. Here, telemedicine information systems (TMIS) are very proficient healthcare management systems. Therefore, Salman shamshad *et al.*[21] has proposed a blockchain-based new e-health information sharing and storing system. This technology is only applicable to the telemedicine environment. Moreover, anonymity and security are controlled by safety desires.

Nagasubramanian *et al.*[22] has introduced a keyless signature infrastructure-based blockchain technology. Here, the healthcare information is termed as resource standards of the interoperability system. Moreover, all type of healthcare information is managed by the seven international Medicare organization standards. This proposed technology is ensuring confirmation as well as offers more integrity to health information. Consequently, the validation of the proposed techniques is compared with traditional techniques.

In modern years, cloud computing-based electronic healthcare record sharing strategies are having several conveniences. Nonetheless, centralization techniques are exposed to data privacy and security preservation. Thus, Yong *et al.*[23] has proposed a blockchain-based security preserving protocol to secure electronic medical information from third parties. Here, data providers and data owners are the main contributors to the entire system's performance. Any one of the contributors can destroy the system the whole system is collapsed.

Lately, cloud storage administration has generally drawn in the medical care industry and hospitalization. Moreover, health care managements are step by step rethinking the enormous scope of electronic medical care records on the cloud computing system. These specific cloud computing-based electronic medical care records are design works with high versatility, adaptability, minimal expense tasks, and accessibility to rethink the electronic medical care records. Therefore, Rahul Mishra *et al.*[24] has developed the blockchain-based DS chain model was created across the electronic medical care records. Here, every cloud transaction is noted to this model properly.

Focal administration of electronic clinical frameworks faces a significant test since it needs more trust in a solitary element that cannot viably shield records from unapproved access or assaults. This test makes it hard to offer a few types of assistance in focal electronic clinical frameworks, for example, record search and confirmation, even though they are required. Besides, Alrebdi *et al.*[25] has introduced Searchable as well as Verifiable Blockchain-based E-health care records (SVBE). Furthermore, the system provides a lot of services such as verification, preservation, and search.

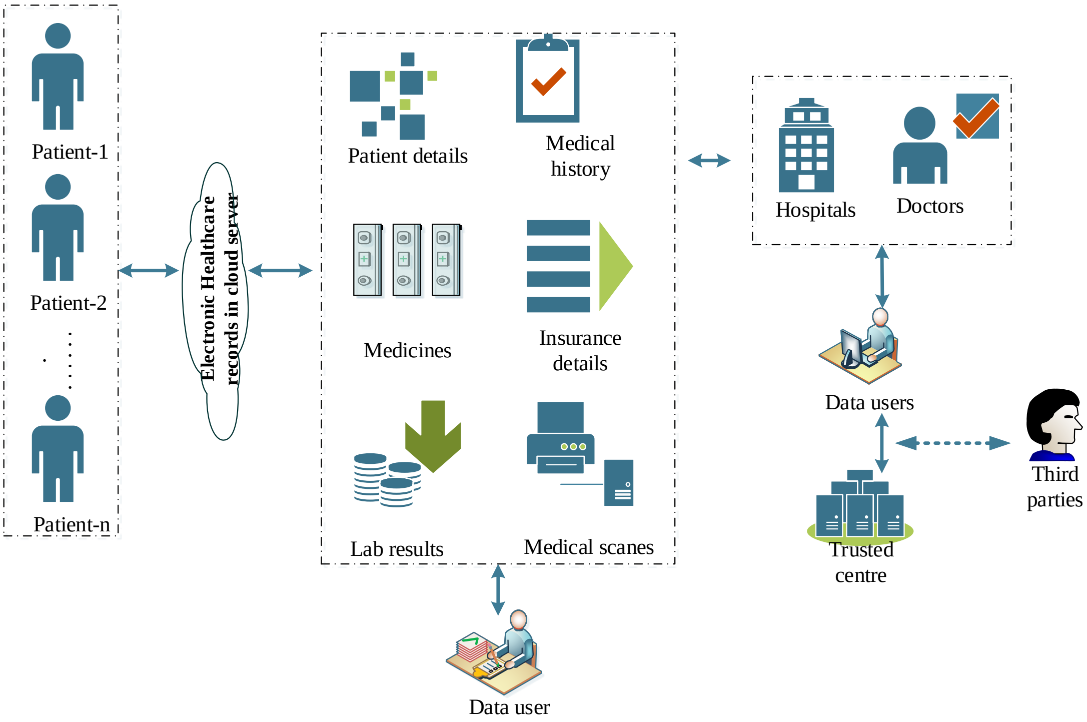

Fig.2 Healthcare application and their security

3. System Model and Problem Statement

This section explains the system model for the modern blockchain-based cloud computing technology. Moreover, e-health applications can contain a lot of medical servers as well as storage systems between the medical departments and medical practitioners [26]. In addition, electronic healthcare records include all types of medical details of their particular patients [27]. Here, data security can be classified into two categories such as consortium and secretive blockchain modules [28]. Every hospital patient's records are preserved in the blockchain modules under the creation of the new keywords. Moreover, the newly generated keywords are protected from the consortium blockchain module. System model for healthcare application is shown in fig. 2.

Here, the data owner is that individual in the framework who is accountable for the entire framework [29]. To develop the administrations from data owners every patient healthcare information and patient requirements are enrolled themselves from the data owner [30]. Furthermore, data user has the obligation of creating private keys also open for these substances. At whatever point, patient healthcare information needs to attain more electronic healthcare records of a specific patient. In general, all the patients are registering their details before meeting the doctors [31]. That details are stored in the cloud server and after meeting the doctor those details are also stored in the cloud server. In all cases, cloud storage of patient healthcare information is very important and more sensitive. Therefore, these types of data must be protected while the transferring process. For these issues, several models are executed previously. But, all techniques are having so many drawbacks. Hence, the current article has proposed to design the efficient security-based blockchain strategy to protect the information from third parties or external users or hackers..

4. Proposed Methodology

Nowadays, the digital performance of cloud computing-based blockchain technologies is the most important examination to enhance the security system during the data transmission periods. In the past lot of blockchain technologies are developed to achieve higher security. However, so many security issues are still now found in their cloud computing technology. To overcome such issues a novel whale-based Cryptographic Blockchain (WbCB) algorithm is developed to protect the cloud-based healthcare information during the data transmission periods. Here, data owners of the cloud computing servers are only assessable for their cloud storage information. In addition, the proposed WbCB scheme was designed in the public cloud system. The proposed architecture is detailed in fig.3.

Moreover, the proposed framework should guarantee the privacy and security of patient healthcare records. As a result, the framework needs to spread over the severe principles to ensure the healthcare information is honest and confidential also, the developed WbCB framework wants to predict the admittance of the healthcare records by any unapproved elements. Consequently, the framework has a higher ability to search the files or patients despite the encryption process. However, the developed technique should offer the efficient capacity to confirm the records by any external related or third party substance. Here, the proposed strategy should accomplish elite execution and low expenses concerning price, storage, and latency to be appropriate reception in the clinical area.

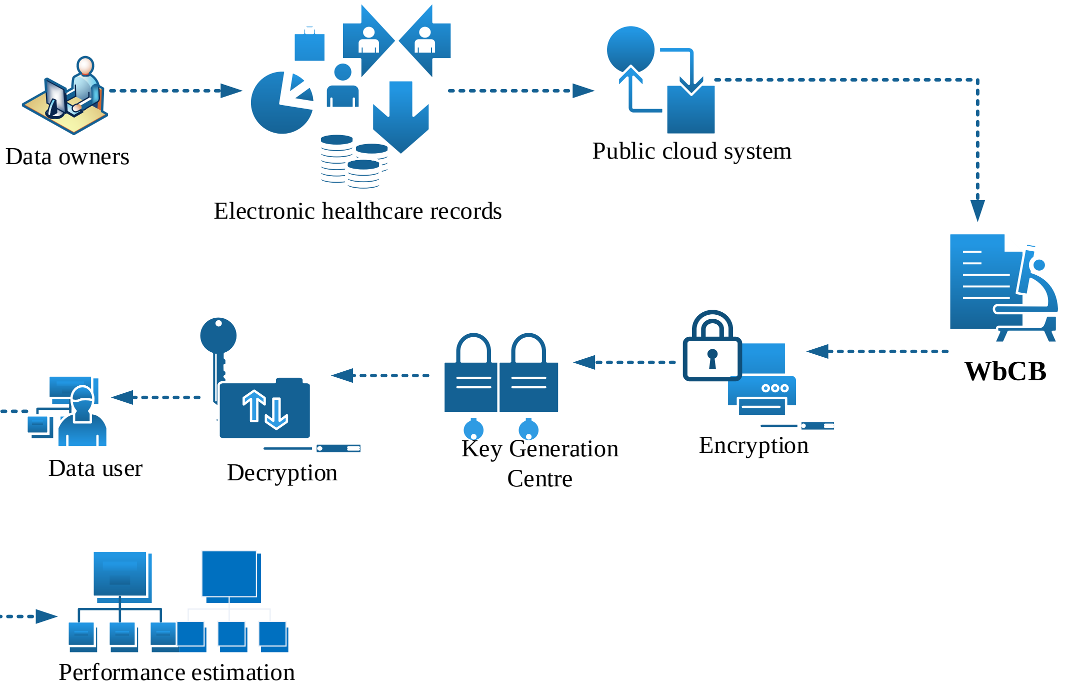

Fig. 3 Proposed WBCB model

4.1 Flow of the proposed WbCB technique

In this study, security is the most important performance, which is responsible for all cloud computing technology. Here, the proposed technique is initially takes the electronics healthcare records. Moreover, the combination of Cryptographic Blockchain technologies and wolf optimization is executed to invert the advance novel model. Consequently, the fitness function of the proposed approach is to enhance the privacy and security of the entire system. Moreover, the proposed technique is performed based on the key generation process. Initially, select the cryptographic hash function with respect to security parameter of the of the cloud computing system. Here, the proposed public could system can select the three has function that is represented in following Eqn.(1), (2), (3),

$$H'_a = (g' \times g') \times \{0,1\}$$

$$H'_b = (g' \times g') \times \{0,1\}$$

$$H'_c = (g' \times g') \times \{0,1\}$$

Where, H'_a, H'_b, H'_c is denoted as cryptographic hash function, g' is the public cyclic group, after, this selection of hash function then find the master public key to keep the medical data is secure using below mentioned Eqn.(4),

$$x'' = pq \tag{4}$$

Where, p represented as cyclic group generator and security parameter is represented as q. moreover, master key is of the public cloud system is encrypted with suitable parameters. At last, master is protected and the system parameters are distributed with data owners only. Master key and attributes are efficiently generating the private key both encrypt and decrypt the electronic healthcare records. Here, initially collect the system parameters (s'_p), identity of the cloud server system (c'_s), master key parameter (x''). Consequently, randomly choose the any one of the value here, value is represented as medical record and estimate the value using eqn.(5)'

$$R(c'_s) = H'\{s'_p * x'' * h(c'_s)\} \tag{5}$$

Where, $R(c'_s)$ is random value, $h(c'_s)$ is represented as hash value of the identity cloud server system. Then, key generation centre is to create the server partial private key to authenticate the cloud server with the secure path using eqn.(6),

$$P_r(k) = R(c'_s) + h(c'_s) \,.\, x'' \tag{6}$$

In cloud based medical services framework, a few measures of patient's medical care data are gathered from the cloud data set. Here, datasets are sored into the cloud database that contains patient’s entire health details everything. By the by, this cloud data set has nonattendance of security as well as medical care subtleties are misused through the outside client, and that implies outsiders. This problem may influence the patients' treatment cycle at the starting stage. So, the WO algorithm is incorporated with the cryptographic mechanism to provide the security of electronic healthcare data. Here, user details that mean patient healthcare information and electronics medical records are updated in the public cloud system. Then the patient details are protected using following eqn.(7)

$$E_{n+1} = E_{kn} + \frac{(bn - a_n)}{bm - a_n} \tag{7}$$

Where, performance of the electronic healthcare data observing performance is denoted as E_{n+1} . Consequently, performance of the electronic healthcare data observing performance is denoted as a_n . Here, individual patients and group of patients are shared the information to the cloud server that transmission can assess the data. So again clouds database is protected using following eqn.(8),

$$a_n = \frac{a_n + E_{n+1}}{\phi} \tag{8}$$

Where, ϕ is denoted as unit time of the entire system. Additionally, it can give a more profundity highlight the space for implanting. A combined arrangement with the proposed encryption can assist with reinforcing assault flexibility and disarray. Performing inserting with a solitary layer can cause higher-deceivability detectable quality and effect picture quality post-inserting. Then again, implanting with a more elevated level coefficient can be more compelling at the expense of expanded calculation, which can't be reasonable for contemporary continuous application requests. Consequently, private key is having 256 bits based in this subkey is generated. Then, it is separated in final keys as well as pre key based on 64 bits using eqn. (9)

$$P_k = \left(P_{(k-4)} \oplus P_{(p-1)}\lambda, \lambda \oplus p_r(k)\right) \tag{9}$$

Where, λ is denoted as original patient information of data bits, pre keys of the data in the mapped interface is denoted as P_q also this can be expressed as input data. In this proposed method medical care information is coordinated firmly in the cloud server framework. On the off chance that the information is encoded, outsiders can't adjust the genuine medical care information of the patient. Subsequently, to affirm the security in conveying the evidence information, the fitness function of the WO is updated to protect the data from unauthorized users. Besides, suggested system security analysis is displayed in algorithm.2.

Algorithm:2Electronics healthcare data security and privacy using WbCB

```
Start
    Input: plaintext
    Initialize the collected Electronics healthcare dataset
    Update system parameters ( $s'_p$ ), identity of the cloud server system ( $c'_s$ ), master key parameter ( $x''$ )
    For (cloud server identity $c'_s$
    Partial private key
            Perform (data owner. Data user, server)
    While (public key) Do
    {
        $P_k = \left(P_{(k-4)} \oplus P_{(p-1)}\lambda, \lambda \oplus p_r(k)\right)$
    }
    While (criteria) Do
    Data transferring process
    Optimization parameters
    Stored data from cloud server
        Condition verified stop the process
    Else
            Repeat
    // security level verification
        If (key matching)
            data reached without any collapse
    else
            Hacked
    End if
        End if
    // Decryption
        Inverse performance
        encrypted key calculation
        Best solution
stop
    Output: secure data
```

These administrations deal with the protection, classification, discernibility, and personality of the blockchain. In the blockchain, enrolment is applied just to the approval blockchain. In this proposed work, approved blockchain are utilized to permit explicit entertainers for doing exchanges and approve the organization. The part encryption administrations in the blockchain convey the hash work and the advanced mark to permit the expansion of new information in the blockchain. Involving the hash work in each marked square can frequently shield the record from different changes by any specialist or assailant. Any data changes to be made in the record are performed by a registered hash close by the recently registered hash and put away in the record.

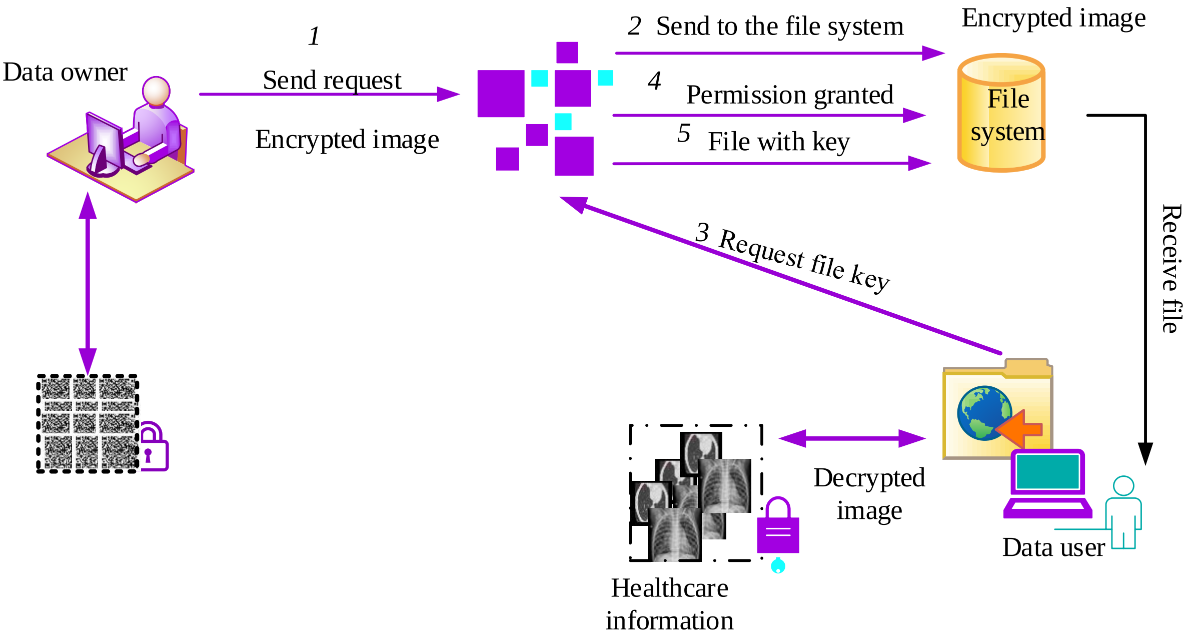

Fig. 5 Flow chart for proposed technique

Another ciphertext is registered for each time another exchange is added to the record. Advanced marks affirm that the beneficiary gets the exchanges without halfway parts changing or misshaping the con- tents of the exchanges. Additionally, affirm that the exchanges produced using shippers endorsed with private keys are not done by frauds. Moreover, work flow of the developed approach is demonstrated in fig. 5.

5. Result and discussion

The proposed technique implementation is done on the MATLAB platform for securing the electronics healthcare records based on the software performance. To avoid the third part assess control was blocked with the help of proposed blockchain technology. Moreover, to prove the effectiveness of the proposed approach is compared with existing techniques in terms of performance metrics.

5.1 case study

In this segment, the proposed WbCB technique considers information dividing between data Owner, Cloud-User and information put away in the cloud as the primary issue to create a new strategy. Be that as it may, information put away in the cloud additionally resolves the issue of debasement and information misfortune because of equipment disappointments, programming bugs and human blunders in the cloud. The motivation behind the new strategy is to keep the touchy data of the patients and emergency clinic in the cloud as a safe way, and not to be investigated by other outside clients, and not making any progressions in information to ruin their mix-up. Overall performance proposed technique is illustrated in fig.6.

In our proposed work, electronic healthcare records are to be put away in the cloud. It contains both the patient's general information such as the name of patients, contact details, ID number, and so forth and medical clinic sensitive data such as the name of the emergency clinic, patient ID and so on. Consequently, to check assuming the information is accurately put away in the cloud, there need to check the honesty of the information in the cloud. The method for tackling this issue is to scramble the information with reasonable catchphrases before putting it away in the cloud and confirm the respectability of the encoded record by creating a signature. Consequently, it makes the entire common records incapable to seen by other outer clients. The job of blockchain in distributed storage gets client information in the wording of an extra degree of safety utilizing blockchain usefulness such as open/private encryption key, a hashing capacity, and exchange records. The beginning of blockchain utilizes a cryptographically marked transaction to work in each square. Where the verification of a transaction is approved and assessed for every weak spot. This interaction affirms the inflexibility of information with the created hash. To give blockchain security, cryptographic is utilized for blockchain exchanges as far as a square of keys like public and private keys for the whole exchange. After finishing the exchanges, the information is put away in a decentralized structure. By this, assuming aggressors or programmers attempt to hack it, they have no data or thoughts regarding the usefulness of the blockchain that gets reports in the blockchain. At whatever point a patient attempts to recuperate information, the information is first approved, and if changes are made to the information, the changed information is taken out from the organization by the excavator and made as one more excess duplicate close to the first squares.

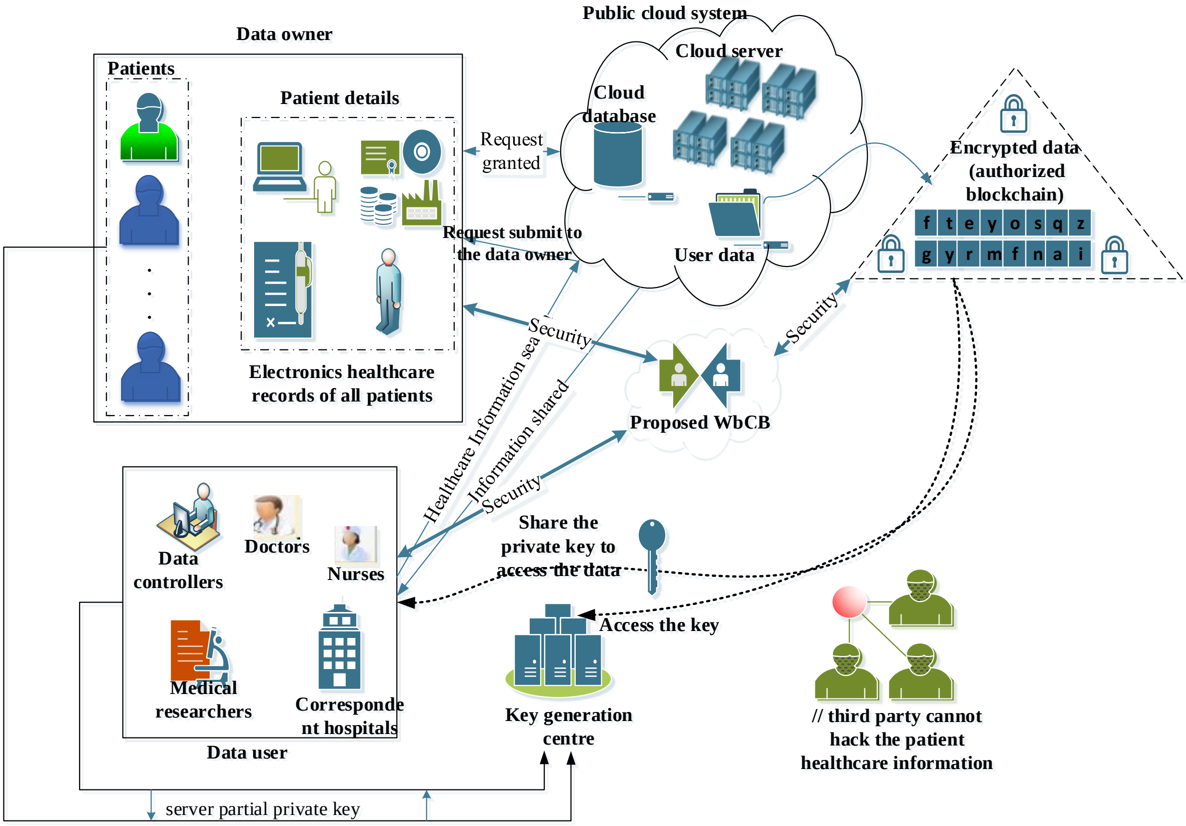

Fig. 6 Overall Process of proposed model

5.2 Performance estimation

The performance of the developed WbCB algorithm is measured based on the security of cloud computing channels. So, the cloud computing channels are differentiated from the other security modules. Therefore, Provable Data Possession (PDP) strategy [32], multicopy PDP (MPDP) technique and Secure Authentication Module (SAM) [33] were compared with developed model for numerous matrices like efficiency, communication overhead, encryption time, decryption time, running time, reliability and confidential measure. Moreover, several classifications are assessable for the past few decades. But here, the outcome estimations are observed from the various blockchain based cloud computing technologies.

5.2.1 Efficiency

The efficiency of the proposed WbCB framework is analysed based on the two types of complex aspects such as computational complexity, communication complexity, and storage complexity. Here, computational complexity is to create the cryptographic ciphertext and perform the healthcare records in the cloud storage system. Increasing the number of healthcare records is more efficient and attained the safety auditing from the public key. Then, communication complexity is to transfer the access as well as ciphertext from the data used to the data owner. Finally, storage complexity is estimated based on the key assessment such as the private key, the public key, and secret key.

Table.1 Performance comparison of Efficiency

No of records	Efficiency			
	PDP	MPDP	SAM	Proposed WbCB
25	70	65.5	75	92

50	70.5	66	80	93.9
75	71	67	80.7	94
100	75	68	80.87	96
125	79	70	81	97.5

Moreover, proposed method efficiency is compared with various existing techniques such as PDP, MPDP and SAM. In this comparison PDP method has attained efficiency measure 79%, MPDP method has achieves 70% efficiency measure and SAM method has attained 81% efficiency for125 electronics healthcare records. Furthermore, comparison values and representation are demonstrated in table.1 and fig.7.

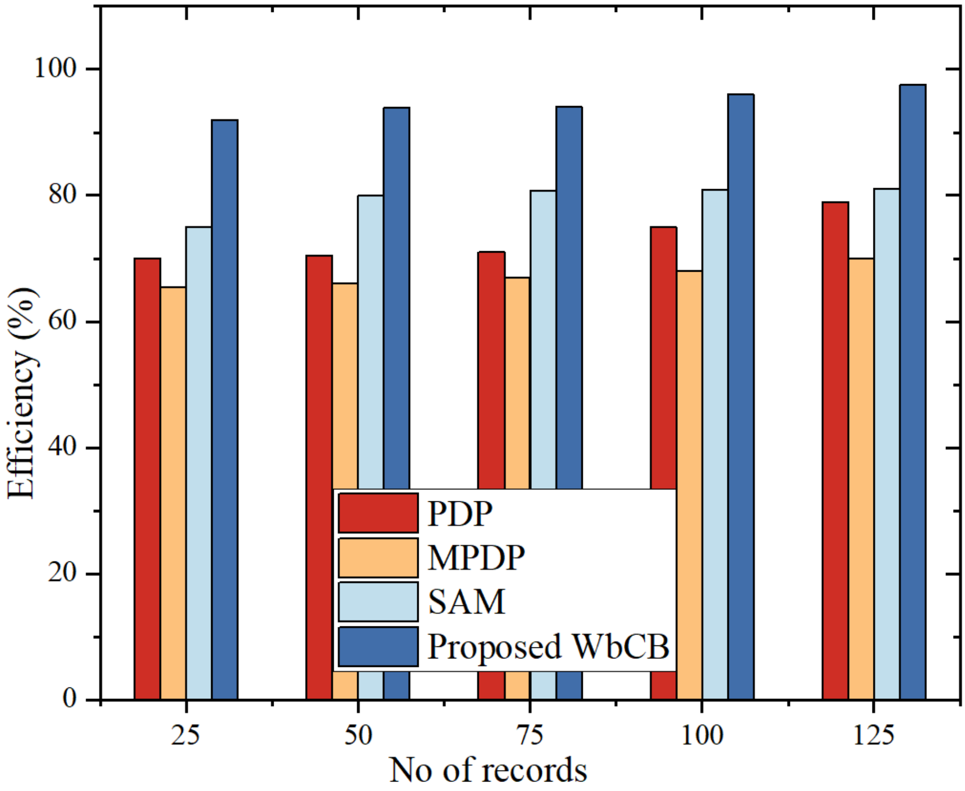

Fig. 7 validation of efficiency

Table.2 Performance comparison of Encryption time

No of records	Encryption time (ms)			
	PDP	MPDP	SAM	Proposed WbCB
25	0.06	0.67	0.17	0.014
50	0.065	0.69	0.26	0.016
75	0.068	0.75	0.29	0.018
100	0.07	0.79	0.3	0.02
125	0.08	0.85	0.43	0.022

Consequently, the developed technique that is WbCB has attained 97.5% efficiency measure for125 electronics healthcare records. When compared to other methods, proposed method attained high efficiency based on the complexity.

5.2.2 Encryption time

In a cryptographic blockchain technology encryption is the most important parameter for encoding healthcare information. Moreover, this encryption process is to convert the original cloud storage electronic healthcare record from the ciphertext formats. The time taken to the conversion process is called encryption time. Here, original cloud storage electronic healthcare records are termed as plaintext and alternative format is termed as ciphertext. Based on the proposed WbCB algorithm is generally utilizes the encryption key to finding the overall throughput.

Moreover, proposed method encryption time is compared with various existing techniques like PDP, MPDP and SAM. Consequently, PDP technique has achieved 0.08 ms, MPDP technique has got 0.85 ms and at last, SAM procedure has attained 0.43 ms for125 electronics healthcare records is demonstrates in table.2 and fig.8.

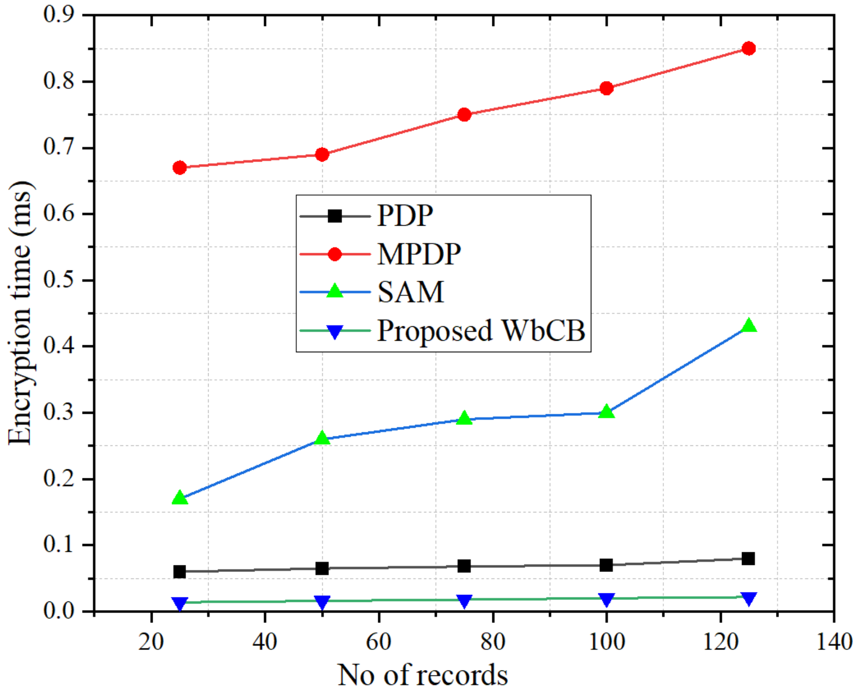

Fig.8 Validation of Encryption time

The encryption time of the proposed technique takes lower time (0.022 ms) for the purpose of encryption of entire test cases.

5.2.3 Decryption time

Decryption time is the time taken to convert the ciphertext to plaintext. On other hand converted cloud storage electronic healthcare records are turned into the original formats. Commonly this process is called a reverse operation of the encryption process. Here, the decryption process uses a secret key to assess the healthcare information from the cloud storage databases.

Table.3 Performance comparison of Decryption time

No of records	Decryption time (ms)			
	PDP	MPDP	SAM	Proposed WbCB
25	1.3	5.63	4	0.011
50	1.5	5.65	4.5	0.014
75	1.8	5.68	5.4	0.015
100	1.9	5.7	5.9	0.02
125	2.7	6.1	6.2	0.022

From the comparison shows that the conventional PDP (2.7 ms) MPDP (6.1 ms) and SAM (6.2 ms) for125 electronics healthcare records. Nonetheless, the proposed WbCB framework has attained 0.022 ms and described in fig.9 and table.3.

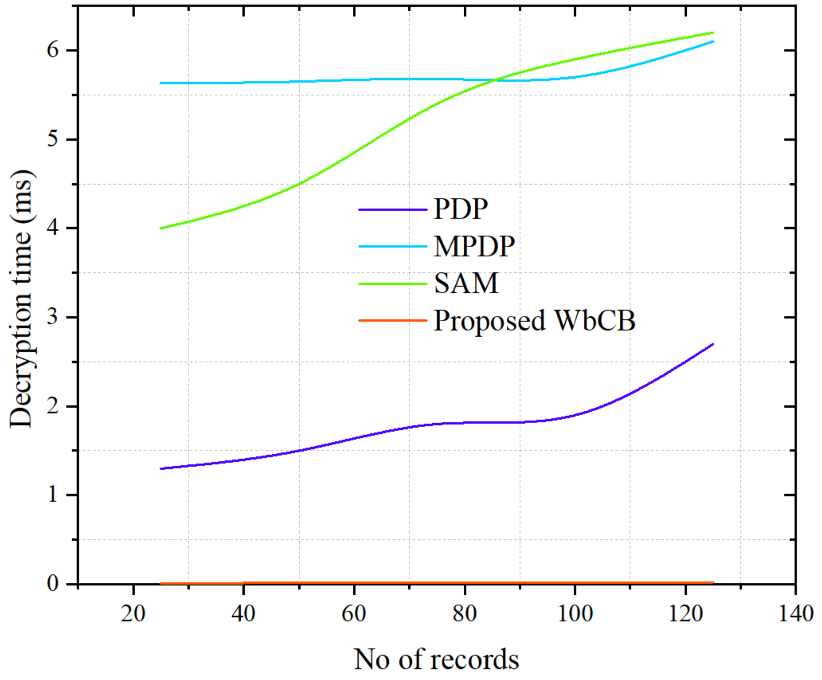

Fig. 9 validation of Decryption time

Table.4 Running time validation

No of records	Running time (s)			
	PDP	MPDP	SAM	Proposed WbCB
25	2	0.8	2.5	0.1
50	2.1	0.83	2.6	0.14
75	2.5	0.86	2.9	0.17
100	2.7	0.87	3	0.18
125	2.9	0.9	3.5	0.2

5.2. 4 Running time

The cloud service provider takes some time to retrieve the data user data processing time. After, implementation of the proposed framework the running time is the challenging response, to increase the electronic healthcare record size also running time increase simultaneously. Here, the total time duration of various file sizes can changes within few milliseconds (ms).

Generally, running time of the proposed approach is takes low when compared to other methods. Here, proposed method computation time is compared with various existing techniques like PDP, MPDP and SAM. Moreover, finest result is described in table.4 and fig.10.

In this comparison PDP method has attained running time 2.9 s , MPDP method has achieves 0.9 s of running time and SAM method has attained 3.5 s of running n time for computation time for125 electronics healthcare records. Consequently, the developed WbCB method has attained 0.2s of running time for125 electronics healthcare records.

5.2.5 Confidential score

The confidential score is efficiently calculated based on the cloud storage of electronic healthcare records. The proposed WbCB framework has provided a complete successful confidentiality measure with providing trust and integrity while transferring the electronic healthcare records from the cloud storage database.

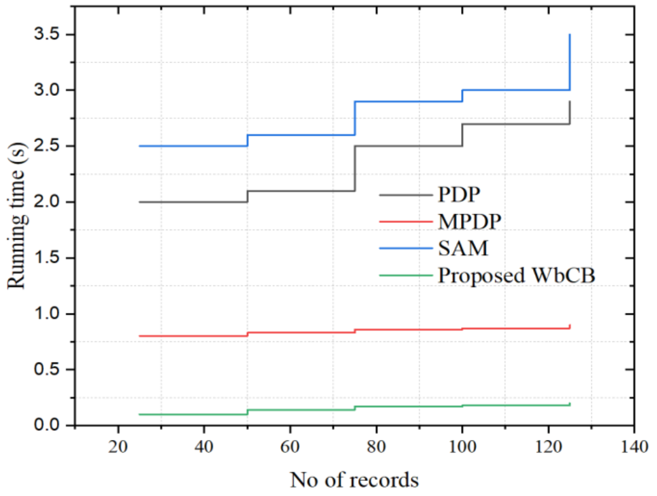

Fig. 10 validation of Running time

Table.5 Performance comparison of Confidential rate

No of records	Confidential rate (%)			
	PDP	MPDP	SAM	Proposed WbCB
25	74.5	84.6	73.2	99.23
50	74.2	84.3	73	98.3
75	74	84	72.9	98.1
100	73.9	83.9	71	97.6
125	73.6	83.6	70	97.1

Consequently, the proposed WbCB technique confidentiality measure is compare with existing techniques such as PDP, MPDP and SAM. Moreover, the validation, the PDP has attained the confidentiality measure as73.6%, MPDP is getting 83.6% of confidentiality measure and SAM has attained a confidentiality measure as 70% for125 electronics healthcare records.

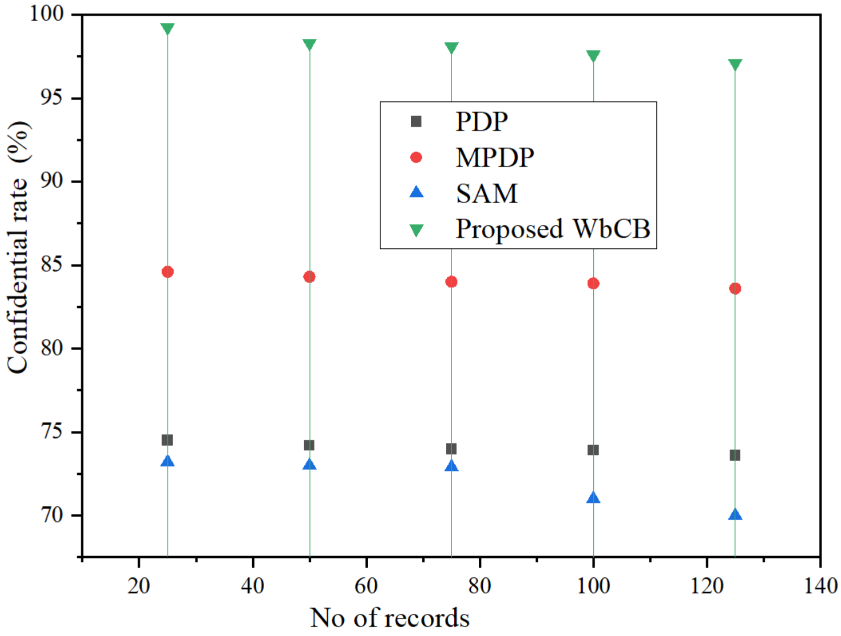

Fig. 11 validation of confidential rate

Moreover, the proposed strategy achieved confidentiality measure as 17ms for125 electronics healthcare records. Therefore, other recent techniques are attained less confidential rate but the proposed model attained higher confidential measure to execute the entire process. Moreover, the finest result and described in table.5 and fig.11.

Table.6 Performance comparison of Computational overhead

No of records	Computational overhead (s)			
	PDP	MPDP	SAM	Proposed WbCB
25	25	53	61	12
50	22	56	62	11
75	20	57	65	11
100	18	61	67	10
125	17	62	67	10

5.2.6 Computational overhead

Computational overhead of the proposed WbCB strategy is to provide the high security to assess the key management system. Moreover, the proposed framework is divided into multiple security channels with low communication cost. Here, the electronic healthcare information is securely with the help of low latency response. In addition, the secured healthcare records are effectively met the healthcare related data processing system.

The computational overhead in proposed methodology was more effective that is shown in table.6 and attained greater optimization than others. Here, in fig.6.1, the comparative analysis with other proposed method has been made and found out that the WbCB technology has attained 10s computational overhead. Consequently, PDP (17s), MPDP (62S) and SAM (67s) attained respectively. Here, the best computational overhead has been obtained as compared to other conventional methods that are demonstrated in table.6 and fig. 12.

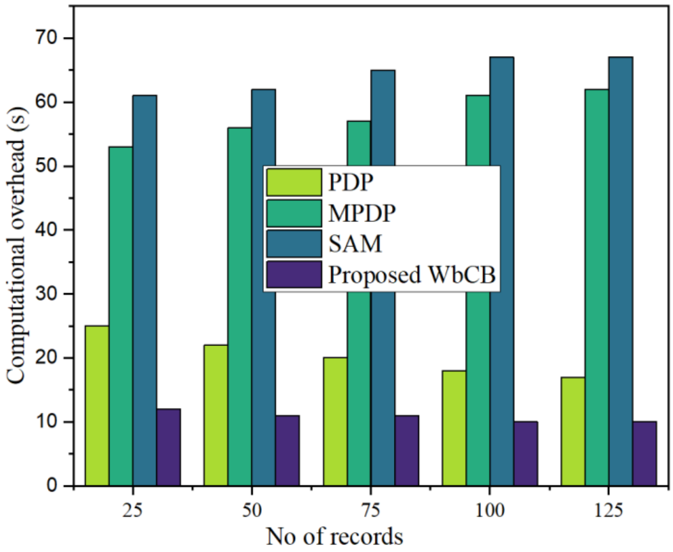

Fig.12 validation of Computational overhead

5.2.7 Reliability

Reliability is attained by the presented WbCB procedure and compared with the ordinary strategies. As the quantity of healthcare records expands, the unwavering quality is pretty much steady in both the prior and proposed methods. Moreover, the proposed Blockchain innovation is secure as it is decentralized and appropriated. There is no weak link, which makes it a lot harder to ruin. Here, failure of one node the entire framework can't influence different parts. Hence, that one failure hub got disconnected; the record is still promptly accessible to any remaining members in the organization. This protects the trustworthiness of the record and results in a common, changeless record of truth.

Table.7 Performance comparison of Reliability

No of records	Reliability (%)			
	PDP	MPDP	SAM	Proposed WbCB
25	78	62	87	98.5
50	74.8	61	85.56	97
75	72.75	56	81.08	96.06
100	69.47	57	79.67	94.78
125	64.56	53	76.8	92.5

In this comparison PDP method has attained 64.565 of reliability, MPDP method has achieves 53% of reliability and SAM method has attained 76.8 % s of reliability for125 electronics healthcare records. Consequently, the developed WbCB methodhas attained 92.5% of reliability for125 electronics healthcare records, that is demonstrated in table.7 and fig. 13.

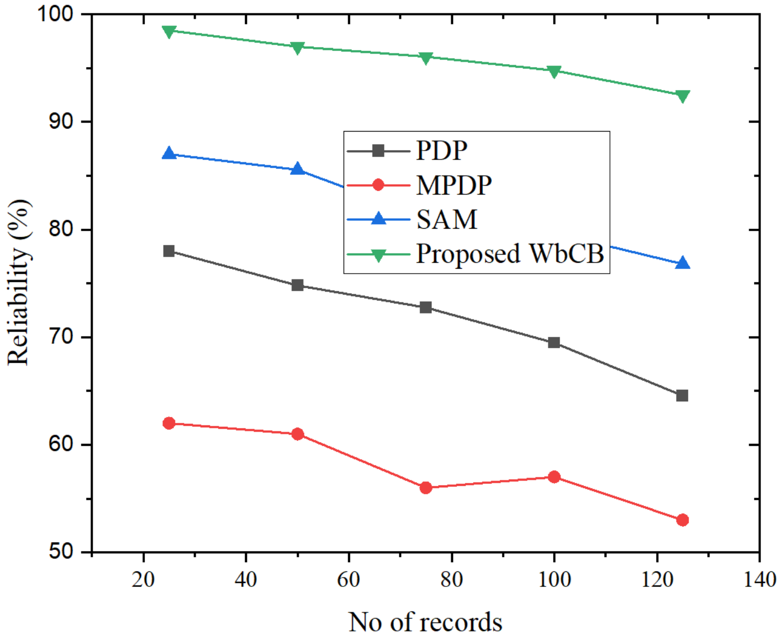

Fig.13 validation of Reliability

5.3 Discussion

The proposed blockchain algorithms are examined and effectiveness are analysed for securing the electronic healthcare records. Moreover, the developed work has explained with existing approaches that includes several blockchain methods. This approach has utilized various hospital related electronic healthcare records. In addition, key creation concept can avoid the third party asses in the cloud storage system. Therefore, the proposed technique features are only visible to the medical doctors and who are having secret key authentication key.

6. Conclusion

Cloud computing is the internet data storing and managing technology over the public cloud services. Moreover, it is the software based infrastructure applications linked through the cloud computing technology. Currently, lot of security threats are available in the Cloud computing technology. Therefore, in this paper a novel WbCB framework is proposed to diminish the security related problems. Moreover, healthcare system is embedded with blockchain based cloud computing framework. In addition, the developed model is utilizes the cryptographic blockchain algorithm to control the security problems. From the results, the duration of the projected approach can be enhanced and can attain high efficiency during the data transmission. Moreover, the encryption as well as decryption time is reduced as 0.014 ms and 0.01 ms, while compared with existing security methods.

Reference

[1] Mansour, Romany Fouad, et al. "Artificial Intelligence and Internet of Things Enabled Disease Diagnosis Model for Smart Healthcare Systems." IEEE Access 9 (2021): 45137-45146.

[2] Anuradha, M., et al. "IoT enabled cancer prediction system to enhance the authentication and security using cloud computing." Microprocessors and Microsystems 80 (2021): 103301.

[3] Sharma, Dilip Kumar, et al. "The aspect of vast data management problem in healthcare sector and implementation of cloud computing technique." Materials Today: Proceedings (2021).

[4] Yang, Zheming, Bing Liang, and Wen Ji. "An Intelligent end-edge-cloud architecture for visual iot assisted healthcare systems." IEEE Internet of Things Journal (2021).

[5] Dhasarathan, Chandramohan, et al. "A bio-inspired privacy-preserving framework for healthcare systems." The Journal of Supercomputing (2021): 1-36.

[6] Dutta, Arijit, et al. "Enhancing mist assisted cloud computing toward secure and scalable architecture for smart healthcare." Advances in Communication and Computational Technology. Springer, Singapore, 2021. 1515-1526.

[7] Denis, R., and P. Madhubala. "Hybrid data encryption model integrating multi-objective adaptive genetic algorithm for secure medical data communication over cloud-based healthcare systems." Multimedia Tools and Applications 80.14 (2021): 21165-21202.

[8] Dutta, Arijit, et al. "Enhancing mist assisted cloud computing toward secure and scalable architecture for smart healthcare." Advances in Communication and Computational Technology. Springer, Singapore, 2021. 1515-1526.

[9] Vyas, S., & Bhargava, D. (2021). Scalable Smart Health Systems. In Smart Health Systems (pp. 49-59). Springer, Singapore.

[10] Hensh, Falguni, Mayank Gupta, and Manisha J. Nene. "Mist-Edge-Cloud (MEC) Computing: An Integrated Computing Architecture." 2021 Second International Conference on Electronics and Sustainable Communication Systems (ICESC). IEEE, 2021.

[11] Das, Jaydeep, Soumya K. Ghosh, and RajkumarBuyya. "Geospatial Edge-Fog Computing: A Systematic Review, Taxonomy, and Future Directions." Mobile Edge Computing (2021): 47-69.

[12] Saha, L., Tripathy, H. K., &Sahoo, L. (2021). Business Intelligence Influenced Customer Relationship Management in Telecommunication Industry and Its Security Challenges. Privacy and Security Issues in Big Data: An Analytical View on Business Intelligence, 175-188.

[13] Viloria, Amelec, et al. "Design of a network with sensor-cloud technology applied to traffic accident prevention." Proceedings of International Conference on Recent Trends in Machine Learning, IoT, Smart Cities and Applications. Springer, Singapore, 2021.

[14] Abdul Haseeb-ur-rehman, Rana M., et al. "Sensor Cloud Frameworks: State-of-the-Art, Taxonomy, and Research Issues." IEEE Sensors Journal (2021).

[15] Hong, Hanshu, and Zhixin Sun. "A flexible attribute based data access management scheme for sensor-cloud system." Journal of Systems Architecture 119 (2021): 102234.

[16] Muhammad, G., Alshehri, F., Karray, F., El Saddik, A., Alsulaiman, M., & Falk, T. H. (2021). A comprehensive survey on multimodal medical signals fusion for smart healthcare systems. Information Fusion, 76, 355-375.

[17] Chowhan, Biky, Rashmi Mandal, and Pawan Kumar Sharma. "DengueCBC: Dengue EHR Transmission Using Secure Consortium Blockchain-Enabled Platform." Data Management, Analytics and Innovation. Springer, Singapore, 2021. 87-106.

[18] Huang, Haiping, et al. "Blockchain-based eHealth system for auditable EHRs manipulation in cloud environments." Journal of Parallel and Distributed Computing 148 (2021): 46-57.

[19] Nagarajan, Sivakumar. "Flexible Access Control Mechanism for Cloud stored EHR using Consortium Blockchain." (2021).

[20] Gupta, Brij B., et al. "Blockchain-assisted secure fine-grained searchable encryption for a cloud-based healthcare cyber-physical system." IEEE/CAA Journal of AutomaticaSinica (2021).

[21] Shamshad, Salman, et al. "A secure blockchain-based e-health records storage and sharing scheme." Journal of Information Security and Applications 55 (2020): 102590.

[22] Nagasubramanian, G., Sakthivel, R.K., Patan, R. et al. Securing e-health records using keyless signature infrastructure blockchain technology in the cloud. Neural Comput&Applic**32,** 639–647 (2020).

[23] Wang, Yong, et al. "Cloud-assisted EHR sharing with security and privacy preservation via consortium blockchain." IEEE Access 7 (2019): 136704-136719.

[24] Mishra, Rahul, et al. "DS-Chain: A secure and auditable multi-cloud assisted EHR storage model on efficient deletableblockchain." Journal of Industrial Information Integration (2022): 100315.

[25] Alrebdi, N., Alabdulatif, A., Iwendi, C. et al. SVBE: searchable and verifiable blockchain-based electronic medical records system. Sci Rep**12,** 266 (2022). https://doi.org/10.1038/s41598-021-04124-8

[26] Zutshi, Aneesh, Antonio Grilo, and TaherehNodehi. "The value proposition of blockchain technologies and its impact on Digital Platforms." Computers & Industrial Engineering 155 (2021): 107187.

[27] Alfa, Abraham Ayegba, et al. "Blockchain technology in IoT systems: current trends, methodology, problems, applications, and future directions." Journal of Reliable Intelligent Environments 7.2 (2021): 115-143.

[28] Banerji, Diptiman, et al. "Application potential of Blockchain technologies in the travel and tourism industry." Blockchain Applications in IoT Ecosystem. Springer, Cham, 2021. 289-299.

[29] Kotamraju, Siva Kumar, et al. "Implementation patterns of secured internet of things environment using advanced blockchain technologies." Materials Today: Proceedings (2021).

[30] Mahbub, Mobasshir. "Blockchain Technologies for Securing IoT Infrastructure: IoT-Blockchain Architectonics." Blockchain Applications in IoT Ecosystem. Springer, Cham, 2021. 187-202.

[31] Kuznetsov, Alexandr, et al. "Performance Analysis of Cryptographic Hash Functions Suitable for Use in Blockchain." International Journal of Computer Network & Information Security 13.2 (2021).

[32] Jayaraman, Indumathi, and Amala Stanislaus Panneerselvam. "A novel privacy preserving digital forensic readiness provable data possession technique for health care data in cloud." Journal of Ambient Intelligence and Humanized Computing 12.5 (2021): 4911-4924.

[33] Zhou, Lei, et al. "Multicopy provable data possession scheme supporting data dynamics for cloud-based Electronic Medical Record system." Information Sciences 545 (2021): 254-276.

[34] Dr. V. Arthi. (2020). A Novel Channel Estimation Technique in MIMO-OFDM Mobile Communication Systems. International Journal of New Practices in Management and Engineering, 9(02), 08 - 14. https://doi.org/10.17762/ijnpme.v9i02.84

[35] hukla, A., Juneja, V., Singh, S., Prajapati, U., Gupta, A., & Dhabliya, D. (2022). Role of hybrid optimization in improving performance of sentiment classification system. Paper presented at the PDGC 2022 - 2022 7th International Conference on Parallel, Distributed and Grid Computing, 541-546. doi:10.1109/PDGC56933.2022.10053333 Retrieved from www.scopus.com