Journal of Information Systems Engineering and Management
2025, 10(48s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Securing Electronic Health Record in Edge Computing Environment using Block Chain Technology

Jagdish Kapadnis[1*], Prasad Lahare[2], Vivek Waghmare[3], Satish Bhadane[4], Chetan Patil[5], Sandeep Jadhav[6]

[1*,2,4,5]PVG's College of Engineering & SSD IOM, Nashik,India, [1]jagdishkapadnis@gmail.com, [2]prasadlahare7@gmail.com, [3]dr.vnwaghmare@gmail.com, [4]satishbhadane@gmail.com, [5]chetanhpatil@gmail.com
[6]Sanghavi College of Engineering, Nashik, India [6]sandeeprjadhav093@gmail.com

ARTICLE INFO

Received: 20 Dec 2024

Revised: 15 Feb 2025

Accepted: 24 Feb 2025

ABSTRACT

Electronic medical record (EMR) is of prime importance in the medical field. A huge amount of physical information has been generated by using different electronic devices, such as wearable devices and mobile devices, and different medical reports generated by laboratories. Edge computing is used for processing and storage of data at the edge of the network, at the same time, data fusion is needed as physical information is collected from different electronic devices in different formats. Privacy of data is most confidential as it contains tailored information about each patient. Block chain technology is the emerging solution to protect the healthcare record. In block chain technology, there is rapid development, especially in edge computing, before uploading the data. This paper mainly focused on securing EMR on the cloud, so for securing the data, here proposed block chain technology. Block chain technology is applied for storing patient's medical information, which is distributed in several different blocks. As medical information is distributed in no of blocks, patient's privacy is maintained. To securely store EMRs, the suggested approach makes use of Inter-Planetary File System (IPFS), Edwards-curve Digital Signature Algorithm (EdDSA), Rivest Shamir and Adleman (RSA), and Advanced Encryption Standard (AES) techniques.

Keywords: Edge computing, Electronic medical record, Block chain technology.

1 Introduction

In today's world, a large amount of electronic devices are used in the medical field, and those devices generate a huge amount of medical information known as EMR. An EMR electronically maintains data of each patient's medical history, such as laboratory reports, X-ray reports, prescriptions, previous test records, and many other health-related documents of the patient's. This data is most confidential, it should be known to the patient and his doctor. In a proactive health recommendation system, the medical information that was collected from different electronic wearable devices is compared with the EMR, which is already available on the server, and after comparing the overall data, the system will recommend the treatment to patients. All the EMR are stored on servers and need to be secured, so EMR faces many issues of security, privacy, automation, storage [1], etc. During data storage and data transmission during the network, data should be secure, and its privacy should be maintained. To maintain privacy and security, block chain technology is the emerging technology for securing and protecting EMR. Data is communicated over the network; it will continuously be at risk as attackers and intruders may be present over the internet [1]. In the age of Artificial intelligence and edge computing not only information is important but how that information is collected at edge from different sources and most of the information is timely important if it is not used in time it will be no further use [2]. Further for the health recommender system, it is most important that information be timely collected and sent to the further health recommender system to recommend the medical treatment for the patient. So this is very sensitive information. It must be secure and protected, so block chain technology with AI is a solution for advanced techniques to provide security for such data.

1.1 Related Work

In the healthcare industry, edge computing is prime computing paradigm where all the resources are distributed in a manner and all the devices are connected through the Internet [3].

The electronic devices that are used in healthcare industry generate massive amounts of EMR at the edge of the network. This collected EMR is stored and transferred wherever it requires. In traditional systems, data is stored in a centralized location, so that may create threats for the system. Securing data decentralized system must be a challenging task in an edge computing environment; thus, blockchain technology is the most suitable and reliable technique for protecting edge computing [3]. The main characteristics of blockchain technology are that it works as a distributed ledger and can be used for secure data storing, exchange, and sharing in an unsecured environment. In blockchain, transactions are managed as a chain, and all blocks are interconnected. Using the crypto graphical method, all data blocks are secured and distributed, and a new block directly interacts with an old block through a chain. Proof of work (PoW) [4] is the method through which a new block is merged with the current block by adding a hash value to the current block. Also in health delivery system, a huge amount of IoT (Internet of things) devices are being used and this devices generates waste amount of data and in real time IoT systems must prioritize security to possibility of malicious attacks [5], errors. All the electronic devices including health detectors, network monitors, and other wireless devices, are energy-constrained [6] Treats of malicious nodes might reduce network lifetime, and data might be leaked. In an edge computing environment, all the devices are placed in a distributed manner, and the aim is to make devices communicate with a physical environment that makes computation closer to the edge and allows the devices less constraints to communicate [7]. The proposed health recommendation system provides dynamic, flexible, and privacy preservation structure [8]. After computing data at the edge stored centrally, for data sharing, block chain technology plays an important role in data management, data sharing, and storing [9]. A major challenge in EMR is seamless collection of data, analysis, and exchange of the information with assured security and privacy on a real-time basis with complete medical information. Decentralized EMR requires real-time, on-demand data sharing infrastructure for smooth, transparent, cost-effective and easy operation [10–11]. In addition to this, due to huge amount of advanced technology used in medical field, keeping records of EMR is challenge and it can be achieved through cloud computing, security and privacy [12–13] maintained by block chain technology. Artificial intelligence and machine learning can primarily help doctors to take primary decisions. Various health care services can take advantage of AI and blockchain along with wireless body area network (WBAN) [14]. Block chain can be visible and private [15] and hide every patient's personal information using various algorithms for securing users data. By this, it gives patients confidence for sharing and storing personal information and enhances privacy and confidentiality. Block chain technology intention is not to store information but only restrict to authorizing [16–17] some persons on sensitive transactions. In edge computing environment, smart devices are computerized programs that manage access control for storing and transmitting [18] data across numerous organizations.

2 Overview of Block Chain and Proposed Scheme

Here briefly explained how block chain technology is used to secure EMR in health recommendation application.

2.1 Need of Block chain in Healthcare

Electronic health records contain sensitive individual patient's information; the basic need of such systems should be fast and secure access for health-related services. So block chain technology is a secure ledger that provides various solutions for sharing medical information. The advantages are as follows:
1. Maintain Patients Record: All type of Patients medical information is automatically kept in a sequence as appear on block chain, including outpatient, inpatient and wearable device test. Physicians review every record and provide medical care.
2. Automatic Data Verification: The blockchain provides the facility to validate the statement without intervention of central authority.
3. Secure storage of medical information: In blockchain, medical data is stored in the form of hash chain in distributed fashion, which is tempered-free and entire system functions smoothly.
4. Effective and efficient data sharing: Blockchain provides effective interoperability by providing reliable, scalable storage and sharing medical information to all the institutions through API-based application.

2.2 Proposed Scheme

The proposed model uses blockchain-based model in edge computing environment to share EMR and corresponding diagnosis reports among patients and doctors. This paper utilizes different cryptographic encryption on health documents and stores encrypted documents in IPFS. This system make sure to enhance the security while transferring the documents over the web and ensure the automation between the patient and the doctor.

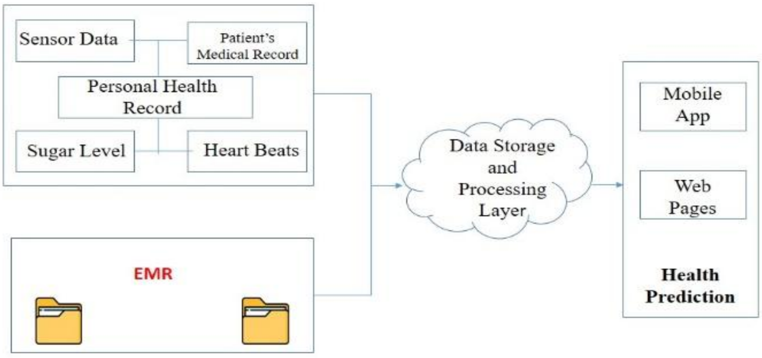

Figure 1. Patient's Health data collected from multiple sources monitoring and disease predictions

In the proposed system model, all the devices are connected to the patient's body, and devices are connected [19] through the internet through the edge. The following scheme consists of various entities such as patients, doctors, hospitals, IPFS, and blockchain networks.

1. Patients: Initially, the patient initiated communication with the doctor; this is the step through which the system is initiated. Every patient has separate credentials through which he/she logged into the system. After logging into the system, all the subsequent reports get uploaded into the system. Also, all diagnosis reports are uploaded into the system.
2. Hospitals: Which are responsible for registering and maintaining records of the patients and doctors in the blockchain environment, as well as it is the responsibility of hospitals to upload EMR into the system.

3. Doctor: doctors produce a diagnosis report for the patient, depending upon his/her EMR, and at the same time upload the data through the blockchain network.
4. IPFS: It is a centralized but distributed system where data is stored on the cloud [20]. The basic aim is to store the EMR and all the related information of patients.
5. The blockchain technology: Through this network, all medical information of patients is secured.

3. Methodology

This proposed model uses the basic characteristics of blockchain network with various features of AES, RSA, EdDSA and ECDSA RSA uses security level 80 bits, and all use security level128 bits. All the algorithms which are used are highly secured and computationally very efficient algorithms. RSA used to encrypt the AES key. A highly safe and effective signature method is EdDSA. Its resistance to quantum assaults, quick verification, simplicity of implementation, and compact signatures have all contributed to its selection. In the end, the simplicity, speed, and compact signatures of ECDSA make it the preferred method for signing the transactions. This allows for effective and safe communication and sharing of data across various healthcare stakeholders. There are seven stages to the proposed work: registration, login, diagnosis report download, examination report upload, diagnosis report generation, diagnosis report upload, and diagnosis report download. Different smart contracts are used to implement each of these stages. The user submits an inquiry to the hospital to finish the registration procedure in the suggested plan. After that, the user is given credentials to get into the system and gets admitted in the hospital based on the accuracy of the personal information they submitted. Here, a smart contract is utilized to enquire about the user's health concerns and validate credentials of users. The smart contract provides the user information about the relevant physicians based on the health conditions they have specified. In order to exchange medical records and interact with a physician, the user upload the reports to proposed system. Uploaded report is encrypted through AES-128 and key of uploaded report is encrypted through RSA-1024. Then these encrypted files are combined and using EdDSA algorithm and these files are digitally signed. EMR for the patient is created using an algorithm, and it is subsequently posted to the IPFS. Since the hash can be used to get the original information from the IPFS, it is utilized as the data to start a transaction, retrieved from IPFS hash. Then the transaction is subsequently forwarded to the hospital, where it is uploaded to the hospital's consortium blockchain network and digitally signed through the ECDSA method with a validator's private key. The proposed model uses access point’s consensus mechanism to reduce complex mining process. Doctors get notification after successfully uploading the EMR report to the blockchain and generate hash value. Same hash value through which the signed file is retrieved from IPFS. After digital signature verification using EdDSA algorithm, the doctor’s private key used to decrypt the encrypted AES key. Finally, the AES key used to deliver the original EMR of patient. After analysis of the EMR report by the doctor, the doctor will prepare a diagnosis report and upload it through the proposed system. Next, using the earlier AES key diagnosis report, it is encrypted by the same key, which is used to encrypt the EMR, and it is uploaded to the IPFS. For creating a transaction, data is obtained from the hash that was returned by the IPFS. Subsequently, the ECDSA method uses the doctor's private key for digitally sign the transaction, which is subsequently published on blockchain. Next diagnosis reports will be successfully uploaded on IPFS, and the patient will get a notification along with an associated transaction hash.

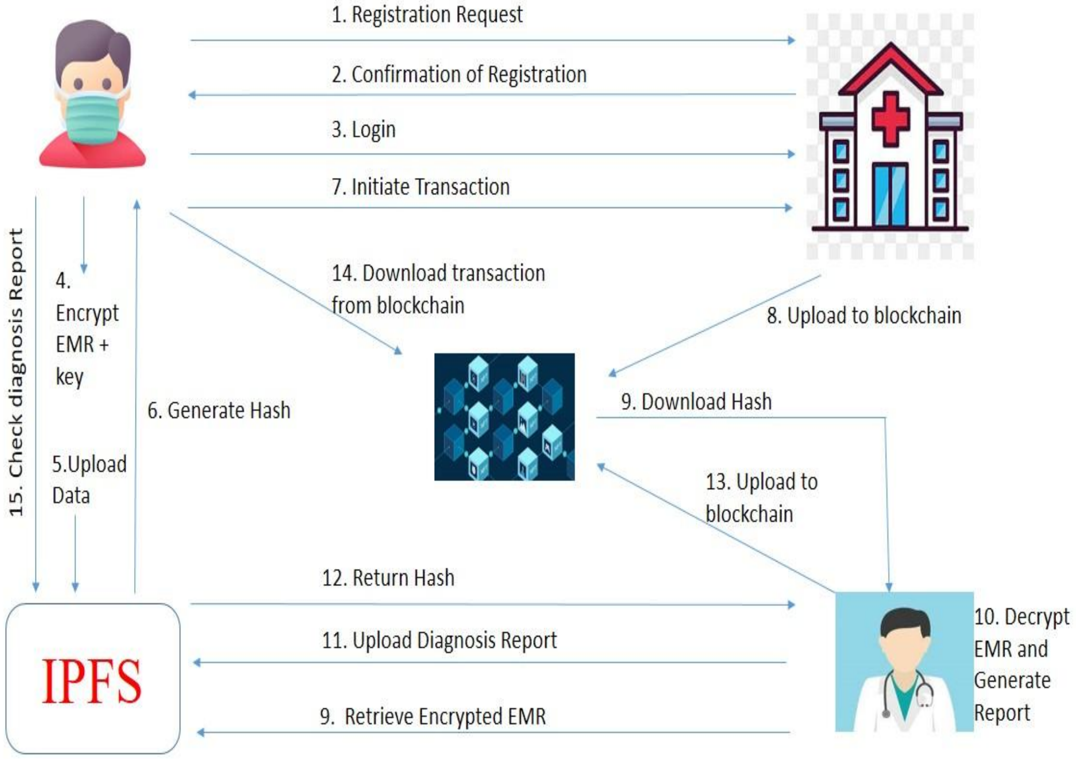

Figure 2. Working of proposed model for sharing secure EMR records

The working of the proposed model is as follows:

During registration step, user submits a registration request with personal data on IPFS through hospital 2) the user is verified at the beginning of the second phase, and a legitimate user name and password are provided. 3) In the third step, the user logs in to the system with their login credentials and requests information on health-related concerns or issues that have been identified by various smart electronic devices. 4) The user is allowed to submit medical reports to the system during the fourth phase. The reports are encrypted using an AES symmetric key, which is further encrypted using an RSA key. 5) A digital file was signed using the EdDSA technique to create the patient's EMR and upload it to IPFS. 6) The hash value is returned in the sixth step and is then utilized to obtain the file. 7) In the seventh phase, the hospital receives the same hash value. 8) Group nodes have the authority to verify transactions in the eighth phase, upload data to the blockchain, and alert the physician. 9) Doctors get the IPFS hash from the transaction after it has been posted to the blockchain network. 10) The EMR is retrieved from the IPFS by a smart contract at this phase, which also involves the doctor generating a diagnosis report after analyzing the EMR, The AES key is used to decrypt medical report, which is then returned to the doctor via the use of the doctor's RSA private key. 11) In this phase, Doctor upload patient's diagnosis report to the IPFS by encrypting it with the same AES key using recommended technique. 12) IPFS returns hash for the encrypted diagnostic report. 13) With use of the doctor's private key and ECDSA method, a signed transaction is created using hash and IPFS gives as data. After that, it uploaded to blockchain via a smart contract. Then user is being informed that the diagnosis report has been uploaded and hash is given back. 14) In the fourteenth step, the user interface retrieves the IPFS hash from the blockchain networks via a smart contract. 15) Lastly, the hash is used by the smart contract to acquire the user's encrypted diagnosis report from the IPFS when that happens, the patient receives it when it has been decoded using the AES key

Table 1. Contains lists the notations used in this work along with an explanation of each.

Notation	Description	Notation	Description
Hash_EMR	IPFS returned hash of EMR	AES_key	AES Symmetric Key
valid()	Verify validity of data	notification_reci()	Received notifications
Diag()	Diagnosis of patient report	health_issue	Patients medical issues
key_{encrp}	Encrypted key	pub_{key1}	Public key used in RSA
$diag_{encrp}$	Diagnosis encrypted report	$priv_{key1}$	Private key used in RSA
med_{report}	Patient Medical Report	pub_{key2}	EdDSA as a public key
send_to_hospital()	Send the details to hospital	$priv_{key2}$	EdDSA as a Private key
Hash()	Hash function	pub_{key3} and $priv_{key3}$	Validator public and private key
Encryt_AES()	Encrypt file	ts1	Timestamp of EMR
$Sign_{EdDSA}()$	Digitally sign data using EdDSA algorithm	ts2	Timestamp of Diagnosis
HDG	Hash of encrypted diagnosis	Wait()	Wait for notification
registration	Patient Registration	S_k	Validator Signature
authenticity()	Check authenticity of data	Verify()	Verify digital signature
medRencrp	Medical record encrypt	Notifydoc()	Notify the doctor
$List_{Doc}$	List of doctors	detail_user	Details of user
ID_{useri}	User ID i	Upload_to_CDSF()	Upload the file to CDSF
ID_{doctj}	Doctor ID I	Get_hash()	Fetch hash return by CDSF
HEi	i^{th} Patient Data	tx_{emr}	Transaction of EMR upload
HDj	j^{th} Doctor's diagnosis	tx_{Diag}	Signed transaction while uploading diagnosis Report
S_i	Signature of the ith User	error()	Different error
S_j	Signature of the jth doctor	Merge()	Merge two file
Decrypt()	Decrypt any encrypted file	Retrive()	Retrieve file

A number of smart contracts, which are explained below, are used to carry out the various stages of the proposed scheme.

Login Phase

Patients must provide accurate information throughout the login process. A blockchain-based smart contract will then confirm the information. The patient has already registered with the system, and their login information has been checked. After successful login, the system will ask the patient questions regarding their health and send them a list of doctors along with ECDSA and RSA public keys. The Suggested system's login algorithm is indicated by Algorithm 1.

```
Algorithm1: Login()
Input: Detail$_{user}$_login_credentials
Output: List$_{doc}$
Start
  if (authenticity(login_credentials ) = =TRUE)
        GET health_issue
        return List$_{Doc}$
  else
        error()
End
```

Algorithm 1. Indicate Login Algorithm

Registration Phase

The patient must provide their personal information using a blockchain-based system throughout the registration procedure. The information is validity will then be confirmed by the suggested mechanism. If so, the user will register with the system, and the patient will obtain unique keys and login credentials for additional communication. The suggested system's registration procedure is indicated by Algorithm 2.

```
Algorithm2: Registration()
Input: Detail$_{user}$
Output: login_credentials
Start
if(valid(details_user) = = TRUE)
     if(registered_user) = = TRUE)
          error()
     else
          return login_credentials
else
     error()
End
```

Algorithm 2. Indicate Registration procedure

EMR Generation Phase

The user submits a medical record, which can be any document that details the patient's health. Using the doctor's RSA public key, AES key is used to encrypt. The patient's EdDSA private key is used to produce and digitally sign the EMR. The hash is then returned after the file is submitted to the system. The transaction to generate EMRs at the hospital is started with this hash. Algorithm 03 suggested approach is used for EMR production.

```
Algorithm3: EMR_Genration()
```

Input: medreport,AES_key, $pub_{key1,}$ S_k

Output: tx_{emr}

```
Start
    medRencrp = Encryt_AES(AES_key, $med_{report}$)
    $key_{encrp =}$ Encryt_RSA(AES_key, $priv_{key1}$ )
    data = Merge(medRencrp, $key_{encrp)}$
    Si = $Sign_{EdDSA}$($S_{k,}$ Data)
    EMR= Merge(si,data)
    if( EMR != NULL)
        if(validity(EMR)= = True)
            Upload_to_CDSF()
            Hash_EMR = Get_hash(EMR)
            Generate $ts_1$
            SET HEi = H(IDui,$ts_{1,}$ Hash_EMR)
            SET $tx_{emr}$ = {HEi,IDui,$ts_{1,}$Hash_EMR}
            send_to_hospital($tx_{emr}$)
            Return $tx_{emr}$
        else
            error()
    else
        error()
    End
```

Algorithm 3. The suggested approach is used for EMR production

EMR Upload Phase

A digitally signed transaction is validated by authority using their private key and the ECDSA technique. The transaction is then uploaded to the hospital's coalition blockchain network, and the doctor gets an alert notification. Uploaded EMR procedure is shown by Algorithm 04.

Algorithm4: EMR_Upload()

Input: tx_{emr}

Output: uploaded status of report

```
Start
    Retrieve(IDui, Hash_EMR,) from $tx_{emr}$
    if(validity(IDui && authenticity(sj)) = =TRUE)
        SET $S_k$ = $Sign_{EdDSA}$($S_{k,}$ $tx_{emr}$)
        SET $tx_{emr}$ = ($S_{k,}$ $tx_{emr}$)
        Upload_to_Blockchain($tx_{emr}$ )
        $Notify_{doctor}$()
    else
        error()
End
```

Algorithm 04. Uploaded EMR procedure

Download EMR phase

During the EMR download phase, the doctor receives notification that their EMR has been uploaded to the blockchain network. They next get the signed hash value from blockchain and verify the validator's signature. If a genuine signature is found, a hash is used to obtain the associated sign file from IPFS. At the doctor's end, the digital signature of the user is confirmed. To decode the AES symmetric key, files are combined using the doctor's RSA private key. Here, encrypted EMR is decrypted and returned to the doctor after the AES symmetric key has been retrieved. Algorithm 5 shows the EMR is downloading.

Algorithm5: EMR_Download()

Input: S_k, pub_{key2}, pub_{key3}

Output: med_{report}

```
Start
if(notification_recieved() = = TRUE)
    verify($pub_{key3}$, $S_k$)
    if(authenticity($S_k$) = = FALSE)
        error()
    Retrieve(EMR)
    Verify($pub_{key2}$,Si)
    if(authenticity(Si) = = TRUE)
        Retrieve($key_{encrp}$ )
        SET key=  Decrypt($S_k$, $key_{encrp}$)
        if($med_{report}$ != NULL)
            Return $med_{report}$
        else
            error()
    else
        error()
else
    wait()
end
```

Algorithm 05. Download EMR procedure

Diagnosis Report Upload

Here in this project, a diagnosis report is prepared along with the EMR by the doctor and uploaded to the proposed system. After that, the diagnostic report is uploaded to IPFS and encrypted using the key that was used to encrypt EMR. Following that, IPFS gives the file application a hash. Every doctor working at the hospital has the authority to verify transactions, mine blockchain blocks, and post signed transactions to the blockchain network. Algorithm 6 indicates the Diagnosis Report upload procedure.

Algorithm6: Diagnosis_upload()

Input: Diag, AES_key and S_k

Output: $tx_{Diagnosis}$

```
Start
$diag_{encrp}$ = Encrypt(AES_key, Dia Diag)
if($diag_{encrp}$ != Null)
```

```
    upload_to_CDSF($diag_{encrp}$)
    HDG = Get_hash($diag_{encrp}$ )
    Generate ts2
    SET Sj= $Sign_{EdDSA}(S_{k,}H(ID_{doctj}$ , ts2, HDj))
    SET HDj = Hash($ID_{doctj}$, ts2, HDj, $S_j$))
    SET $tx_{Diagnosis}$= ($ID_{doctj,}$ ts2, HDj $S_{j,}$ HDG)
    Upload_to_Blockchain($tx_{Diagnosis}$)
     notification_reci()
     Return $tx_{Diagnosis}$
else
     error()
end
```

Algorithm 06. The Diagnosis Report upload procedure

Diagnosis Report Download phase

In this phase, the user gets notified that a diagnosis report is uploaded, a blockchain-based smart node retrieves the diagnosis report transaction from the blockchain, and the doctor's signature is authenticated. If the signature valid, it will retrieve an encrypted report from IPFS. The diagnosis report is decrypted before uploading to the EMR. Algorithm 07 indicates the diagnosis report download process.

```
Algorithm7: Diagnosis_download()
Input: $tx_{emr}$ and AES_key
Output: Diag

Start
if(notification_reci () = = TRUE)
    verify ($pub_{key3,}$ $priv_{key3}$ )
    if(authenticity($S_k$ ) = = FALSE)
        error()
  if (valid(HDG ) = = TRUE)
    Retrieve($diag_{encrp}$)
    SET Diag = Decrypt(AES_key, $diag_{encrp}$)
    if ( valid (Diag) = = TRUE)
        return Diag
     else
        error()
   else
      error()
else
    wait()
end
```

Algorithm 07. The Diagnosis Report upload procedure

Results

The performance of the proposed model has been evaluated in terms of effectiveness as well as efficiency. Here various evaluation metrics (throughput, processing time, and latency and communication time) are considered for block chain networks. High transaction throughput is expected for an energy-efficient blockchain network.

Experimental Setup

The proposed model uses Ethereum. The Ethereum, which is an open-source blockchain-based network. It will work on different elements, such as in the front end, where it will use React Native; for the backend, it requires Node-JS. In hardware configuration it uses HP Intel i7, 16GB RAM, 128GB SSD with Windows 11. In Ethereum, to accommodate the number of transactions, the block structure needs to be designed first.

Blocks Capacity selection

The capacity of the block is totally decided, and here it is 32 bytes each; the block header length of the current timestamp is 4 bytes; AES symmetric encryption (128 bit) is used; and also 1024 bit RSA is used to encrypt the AES key. Digitally signed data uploaded into the system using a 512-bit EdDSA signature and 512-bit ECDSA signature is used to digitally sign the transaction before uploading to the blockchain.

Analysis of processing time

Table 2 along with figure 3 shows various comparison analyses of the latency required for processing various EMRs after applying various cryptographic algorithms to different EMRs.

Table 2 Comparison chart of processing time required for Different EMRs

Metric	Model-I (Centralized Cloud)	Model-II (Basic Blockchain)	Proposed Blockchain Model
Processing Time for Patient EMR Transaction (50 records)	160.52 ms	236.56 ms	112.23 ms
Processing Time for Diagnosis Report Transaction (50 records)	4.95 ms	18.18 ms	2.08 ms
Processing Time for Patient EMR Transaction (100 records)	340.56 ms	520.23 ms	202.27 ms
Processing Time for Diagnosis Report Transaction (100 records)	1.98 ms	22.13 ms	3.19 ms

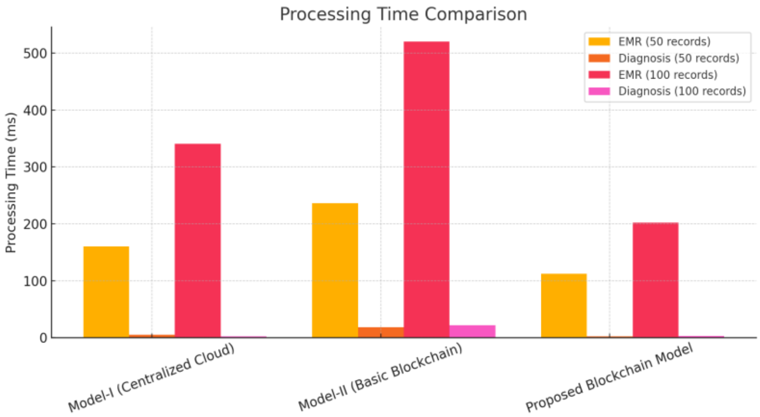

Figure 03 Indicates comparison analyses of the latency required for processing different EMRs

Blockchain Scalability and Energy Efficiency

Blockchain adoption in healthcare often faces challenges related to scalability and energy consumption indicated in table 04 and graphical representation is shown in figure 04. The proposed model, Optimizes mining using an Access Points Consensus Mechanism, reducing computational overhead. By Use of smart contracts it reduce redundant computations.

Table 04 Shows Comparison of Transaction Efficiency

Blockchain Model	Average Transactions Per Second	Energy Consumption Per Transaction
Ethereum (Standard)	15 TPS	High
Hyper ledger Fabric	20 TPS	Moderate
Proposed Model	35 TPS	Low (Optimized with Edge Processing)

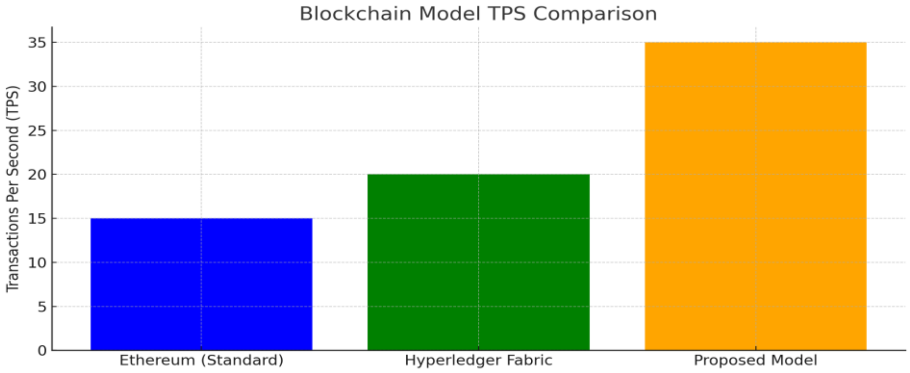

Figure 04 shows uses of scalability and energy consumption.

Conclusion

The proposed method, underscores the crucial role of EMR in modern healthcare, emphasizing the significant amount of sensitive data generated by various electronic devices. Here it highlights the necessity of effective data storage at the edge of networks through edge computing, which enables the integration of diverse data formats. Also, it identifies privacy and security as paramount concerns for patient data, as it contains highly confidential information. To address these challenges, it proposed to use of blockchain technology, a robust solution for securing EMR. By leveraging blockchain, patient data can be divided into smaller batches, enhancing privacy while facilitating efficient data management. Here, the suggested approach incorporates advanced techniques such as IPFS, Edwards-curve Digital Signature Algorithm (EdDSA), Rivest Shamir and Adleman (RSA), and Advanced Encryption Standard (AES) to secure storage and transmission of EMRs. Ultimately, this integration of edge computing and blockchain technology not only protects patient information but also supports timely health recommendations, ensuring that critical data is both accessible and secure. The findings emphasize the potential of these technologies to enhance the overall effectiveness of healthcare systems while safeguarding patient privacy.

References

[1] S. Datta and S. Namasudra, "Blockchain-based smart contract model for securing healthcare transactions by using consumer electronics and mobile edge computing," *IEEE Trans. Consum. Electron.*, 2024. doi: 10.1109/TCE.2024.3357115.

[2] Munir, E. Blasch, J. Kwon, J. Kong, and A. Aved, "Artificial Intelligence and Data Fusion at the Edge," IEEE A&E SYSTEMS MAGAZINE, pp. 62-78, Jully, 2021. DOI: 10.1109/MAES.2020.3043072.

[3] S. Wang, Z. Liu, H. Wang, and J. Wang, "Ensuring security in edge computing through effective blockchain node detection," *Journal of Cloud Computing*, vol. 12, no. 1, pp. 1-14, 2023, doi: 10.1186/s13677-023-00466-y.

[4] K. N. Mishra, V. Bhattacharjee, S. Saket, and S. P. Mishra, "Security provisions in smart edge computing devices using blockchain and machine learning algorithms: a novel approach," in *Cluster Computing*, 2022. doi.org/10.1007/s10586-022-03813-x

[5] M. M. Rashid, J. Platos, P. Choi, Y. Huh, S. H. Lee, and K. R. Kwon, "Ensuring privacy and security of IoT networks utilizing blockchain and federated learning," in *Proc. 10th Int. Conf. Future Internet of Things and Cloud (FiCloud)*, Busan, Republic of Korea, 2023.

[6] P. Zhang, Y. Wang, N. Kumar, C. Jiang, and G. Shi, "A security- and privacy-preserving approach based on data disturbance for collaborative edge computing in social IoT systems," *IEEE Trans. Comput. Social Syst.*, vol. 9, no. 1, pp. 97-108, Feb. 2022.

[7] M. Hagan, F. Siddiqui, and S. Sezer, "Enhancing security and privacy of next-generation edge computing technologies," in 2019 17th International Conference on Privacy, Security and Trust (PST), 2019, doi: 10.1109/PST47121.2019.8949052.

[8] X. Tang, C. Guo, K.-K. R. Choo, and Y. Liu, "An efficient and dynamic privacy-preserving federated learning system for edge computing," *IEEE Trans. Inf. Forensics Security*, vol. 19, pp. 207-220, 2024.

[9] M. Pandey, R. Agarwal, S. K. Shukla, and N. K. Verma, "Security of healthcare data using blockchain: A survey," *Preprint*, Mar. 2021. Available: https://www.researchgate.net/publication/350341688

[10] R. Zhang, R. Xue, and L. Liu, "Security and privacy for healthcare blockchains," *arXiv preprint arXiv: 2106.06136, v1*, 11 Jun. 2021.

[11] S. Chenthara, K. Ahmed, H. Wang, F. Whittaker, and Z. Chen, "Healthchain: A novel framework on privacy preservation of electronic health records using blockchain technology," *PLoS ONE*, vol. 15, no. 12, e0243043, Dec. 2020. doi: 10.1371/journal.pone.0243043.

[12] H. Bodur and I. F. T. Al Yaseen, "An improved blockchain-based secure medical record sharing scheme," *Cluster Computing*, 2024. doi: 10.1007/s10586-024-04414-6.

[13] Z. Sun, D. Han, D. Li, X. Wang, C.-C. Chang, and Z. Wu, "A blockchain-based secure storage scheme for medical information," *J. Wireless Commun. Network*, no. 40, 2022. doi: 10.1186/s13638-022-02122-6.

[14] M. Alshehri, "Blockchain-assisted cyber security in medical things using artificial intelligence," *Eng. Rev. Appl.*, vol. 31, no. 2, pp. 708–728, Nov. 2022. doi: 10.3934/era.202303.

[15] Haleem, M. Javaid, R. P. Singh, R. Suman, and S. Rab, "Blockchain technology applications in healthcare: An overview," *Int. J. Intell. Networks*, vol. 2, pp. 130–139, 2021.

[16] T. T. Thwin and S. Vasupongayya, "Blockchain-based access control model to preserve privacy for personal health record systems," *Security and Communication Networks*, Article ID 8315614, 15 pages, 2019. doi: 10.1155/2019/8315614.

[17] Y. Himeur, A. Sayed, A. Alsalemi, F. Bensaali, A. Amira, I. Varlamis, M. Eirinaki, C. Sardianos, and G. Dimitrakopoulos, "Blockchain-based recommender systems: Applications, challenges and future opportunities," *Comput. Sci. Rev.*, vol. 43, Article 100439, 2022.

[18] S. Niddo and K. B. Sudeep, "Data security in healthcare system using blockchain," *Int. J. Res. Eng. Sci. Manag.*, vol. 5, no. 6, pp. 1-6, Jun. 2022.

[19] V. Upadrista, S. Nazir, and H. Tianfield, "Secure data sharing with blockchain for remote health monitoring applications: A review," *J. Reliab. Intell. Environ.*, vol. 9, pp. 349–368, 2023. doi: 10.1007/s40860-023-00204-w.

[20] H. Taherdoost, "Privacy and security of blockchain in healthcare: Applications, challenges, and future perspectives," *Sci.*, vol. 5, no. 41, 2023. doi: 10.3390/sci5040041.

[21] G. Li, Z.-P. Fan, Q. Zhao, and M. Sun, "Blockchain technology application in an e-commerce supply chain: Privacy protection and sales mode selection," *IEEE Trans. Eng. Manag.*, vol. 71, 2024.