Journal of Harbin Engineering University
ISSN: 1006-7043
Vol 44 No. 11
November 2023

Performance Evaluation of a Secure System for Electronic Health Records (EHRs) using ECIES Algorithm and Blockchain Technology

Priyanka Sharma[1*], Dr. Tapas Kumar[2], Dr. S S Tyagi[3]

[1*]SCA, MRIIRS, Sector 43 faridabad, 0000-0002-5661-4875
priyankasharmaiitd2@gmail.com
[2]SET, MRIIRS, Sector 43 Faridabad
tapaskumar.set@mriu.edu.in
[3]Director of University, IMT, Greater Noida
shyamtyagi@hotmail.com

Abstract

This study develops a robust and efficient system to protect distributed electronic health records (EHRs) and provide authorized users with reliable access. The registration process lets users choose secure, unique usernames as system identifiers. Then, authorized users can access their EHRs to improve healthcare delivery and decision-making. User authentication, data integrity, and data privacy are crucial for a reliable and secure healthcare ecosystem, according to this research. Enhanced cryptographic security protects user privacy and data integrity, according to the study. The proposed research addresses essential features like decentralized access, identity management, user authentication, data integrity, and data privacy, which is consistent with previous studies. The result of the proposed blockchain + ECIES model outperforms blockchain + IPFS and centralized storage systems, as the proposed approach performs well, especially for larger files. However, the proposed study's focus on cryptographic security makes it more comprehensive and effective at securing healthcare data. In conclusion, healthcare professionals can securely access and interact with EHRs using blockchain, the cloud, and strong cryptography.

Keywords: Electronic health records (EHRs), Blockchain and Cloud Technology, User Authentication, Security, Elliptic Curve Integrated Encryption Scheme

1. Introduction

The advent of cutting-edge information technology has profoundly impacted many sectors, including healthcare. EHRs have become an integral part of today's healthcare systems because of the way they track and share patients' medical histories. The use of blockchain technology to improve healthcare and electronic health records has gained popularity in recent years [1-3]. EHRs are used to store a patient's entire health information, such as their medical history, diagnosis, treatments, and test results. They make healthcare procedures more efficient, improve clinical decision-making, and increase patient care coordination among a variety of providers of healthcare. Existing EHR systems, on the other hand, present significant obstacles, such as susceptibilities to data breaches, difficulty in exchanging information among various systems, and the necessity of protecting patient privacy.

The distributed and trustworthy nature of blockchain has shown great promise in the e-health industry, especially in the areas of safe EHR exchange and data access management among diverse medical institutions [4-6]. The decentralized and tamper-proof nature of Blockchain technology has huge implications for the future of EHR systems. Blockchain safeguards medical records by utilizing cryptographic algorithms and decentralized consensus methods. An immutable chain formed by each block's record of a transaction or change ensures the privacy of the data and prevents tampering [7]. Furthermore, blockchain promotes interoperability by providing common data formats and smart contracts, which allow for the unhindered transfer of information across various healthcare providers and systems. To be more precise, a blockchain is a decentralized database that stores a growing list of documents called blocks that are linked and safeguarded using hash functions [8]. By streamlining healthcare delivery and enhancing patient outcomes, blockchain technology has the potential to radically alter the healthcare sector. Fig. 1 depicts the Cloud-assisted EHR framework.

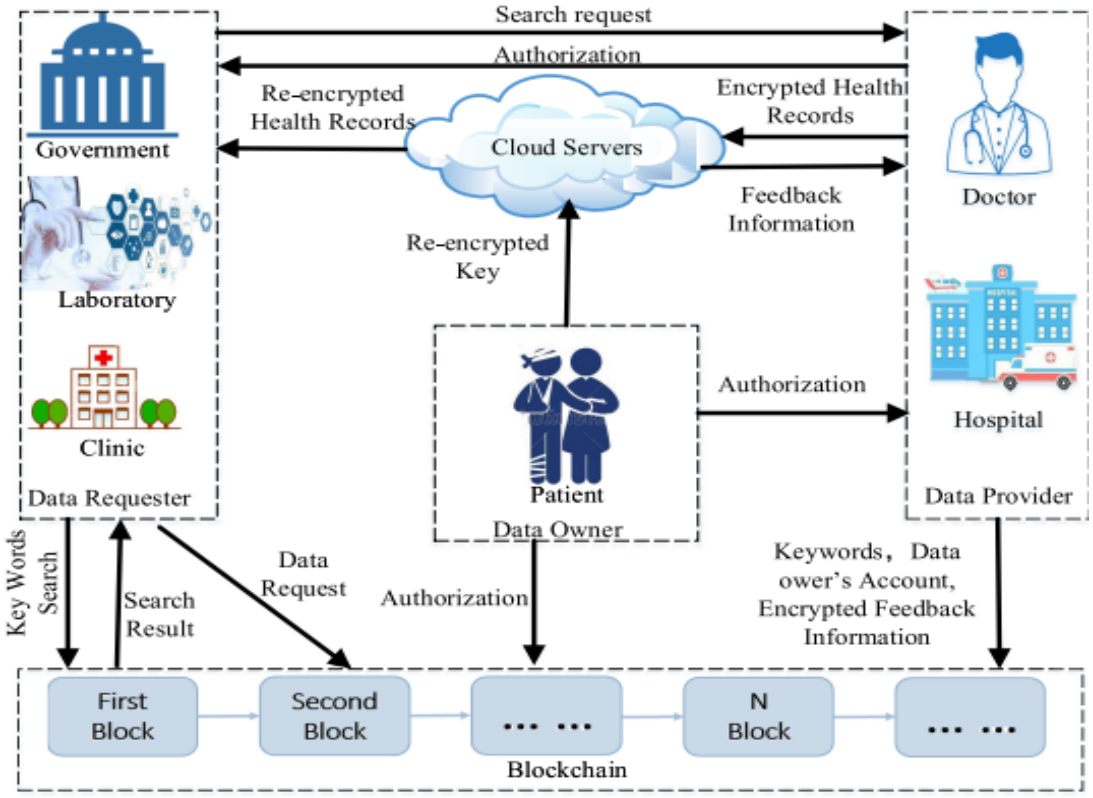

Fig. 1. Cloud-assisted EHR framework [9]

The introduction of cutting-edge technology like cloud computing and the internet of medical devices has brought about substantial shifts in the healthcare sector, which has subsequently experienced tremendous growth [10,11]. Blockchain's immutability and the scalability of the cloud make it a natural fit for EHR systems. With the scalable infrastructure made possible by cloud computing, healthcare institutions can effectively manage and process the ever-increasing amounts of EHR data. Safe and convenient access to patient data from any location has a significant impact on healthcare practitioners' ability to make quick, well-informed decisions. Using cloud technology Smartphones and wearable sensors have made it possible for patients to track their health data, which can then be stored and shared safely on the cloud. This paves the way for faster analysis of patient data and quicker responses to medical emergencies, all thanks to easier access to up-to-date medical records. Improved healthcare delivery and financial benefits for patients are realized through the combination of EHRs and cloud settings, which permits remote patient monitoring and the provision of ambulatory care in the home.

The implementation of e-health applications has been limited by the security risks associated with EHR storage on cloud systems. Safely exchanging medical records in the cloud via mobile devices is a significant challenge to data security. Without patients' knowledge or permission, unauthorized parties may acquire harmful access to EHRs, jeopardizing the confidentiality, availability, and integrity of patient information stored in the cloud. When a patient receives care from various providers, their medical records may be stored in different places across different cloud services, making it difficult for the patient to keep track of everything. To combat these issues and guarantee safe and confidential mobile cloud EHRs sharing systems, effective access control solutions are required [12,13].

Common methods of protecting sensitive data while sharing EHRs rely on the complete confidence of data owners in cloud servers to handle all authentication and access control. Since the cloud server in a mobile cloud is transparent and inquisitive, this presumption no longer holds water. While it does its job honestly, processing data requests, it may also collect user data without their knowledge or consent, which raises severe privacy and security concerns. Additionally, traditional access control solutions rely heavily on a lone cloud server as the primary entry point, which poses a serious security risk for e-health networks [14]. The development of an EHR architecture utilizing blockchain and cloud technologies provides a strong and safe answer to these problems. Data security and

integrity may be assured via decentralized and tamper-proof data storage techniques by incorporating blockchain into the EHR architecture [15]. The cryptographic methods and distributed consensus algorithms used in blockchain technology create a layer of trust that greatly diminishes the chances of hacking and other forms of data abuse. In addition, the utilization of cloud computing offers a scalable and adaptable infrastructure for the storage and management of huge amounts of EHR data, which makes it possible for various healthcare systems to seamlessly interchange data and interact with one another [16].

Some of the original thoughts and data presented in this study are as follows:

1. The study's contribution is a blockchain-based electronic health record (EHR) platform. Blockchain's distributed and unalterable nature is leveraged in this integration to improve data security, authenticity, and privacy. It makes it such that electronic health record transactions can't be altered so that sensitive patient data is protected from prying eyes.
2. The authors acknowledge cloud computing's significance in handling EHR data's massive size. The study's application of cloud computing resources improves the EHR framework's scalability and availability. This paves the way for more effective EHR data storage, processing, and retrieval within healthcare organizations, all of which contribute to quicker and better decision-making.
3. Using an EHR framework, the study proposes standardized data formats as well as smart contracts to solve the problem of healthcare system interoperability. The study's use of blockchain and cloud computing leads to the efficient sharing of patient information across healthcare providers, hence improving the quality of care provided to patients and lowering costs.
4. Patient autonomy and informed consent are highlighted as critical components of the EHR system. Patient autonomy is improved because of the study's use of blockchain technology, which provides both transparency and encryption. As a result, patients can protect their privacy while yet allowing their healthcare practitioners to share their data for study or therapy.

Altogether, the healthcare system stands to benefit greatly from an EHR framework that is designed with blockchain as well as cloud technologies in mind. This framework has the potential to improve electronic health record security, interoperability, along with privacy by combining the decentralized and safe features of blockchain technology with the expansion of cloud computing. Enhanced healthcare delivery and consumer satisfaction can result from the integration of such technologies, which not only protect the validity of EHR transactions additionally give patients more say over their medical records.

The paper is structured as follows: Section 2 provides a comprehensive review of the literature. Section 3 presents the background study conducted for this research. Section 4 defines the problem space and highlights the important research questions. Section 5 describes the research procedures followed to learn more about and examine the issue at hand. Results and discussions, digging deeper into the results and their consequences, are presented in Section 6. Finally, the report finishes in Section 7 by exploring possible future areas for further research and summarizing the important findings revealed.

2. Literature of review

This section provides a summary of the research and development performed by various writers in blockchain and cloud based EHR framework design.

Abunadi et al., (2021) [17] examined the implications for privacy and security for smart houses and towns when using EHR data. Finding a happy medium between patient confidentiality, data availability, and open communication with healthcare providers was a central focus of the research. The research suggested a blockchain security framework (BSF) to address these problems by leveraging the transactional and decentralized features of blockchain technology. The author asserts that their technology safely archives EHRs in a way that allows for convenient access by healthcare providers, consumers, and insurance companies despite jeopardizing the privacy of any of the information. The research employs simulations to show how well the framework secures EHR data and how well it satisfies the security requirements of major stakeholders in the field of medicine.

Tanwar et al., (2020) [18] suggested a framework and a procedure for protecting EHR-held patient data. This research proposes adopting a blockchain-based decentralized network to make the exchange of EHRs more resilient and less reliant on a central authority. Immutable ledger technology is used, which

ensures the ledger cannot be altered in any way. The performance of the system is measured using a caliper, and its settings, which include the block size, the block generation time, and the endorsement policy, are all subject to experimentation. According to the analysis, the suggested approach is 1.75 times more efficient and cuts latency by 1.5 times. These results further prove the broad application of blockchain technology and highlight its potential to revolutionize healthcare systems.

Kim et al., (2020) [19] provided a safe protocol for EHR systems that utilize the cloud utilizing blockchain technology. The blockchain-based log transactions in their scheme guarantee data integrity and access control, while the cloud server safely stores and manages patients' electronic health records. The study utilizes elliptic curve cryptosystems (ECC) and cloud computing to ensure the privacy of shared medical records. They show that their proposed EHR system successfully prevents numerous assaults and offers safe mutual authentication using informal security analysis, AVISPA simulation, and BAN logic analysis. The findings revealed that the suggested system is secure and efficient enough for widespread use in healthcare settings by comparing it to other current methods in terms of compute overhead, communication overhead, and security features.

Agbo et al., (2019) [20] highlighted the potential benefits of adopting blockchain technology in healthcare, while also admitting the sluggish progress that has been made due to the early stage of development and the overwhelming focus on cryptocurrency-based solutions. The authors analyze the current literature on blockchain-based healthcare applications and discover two prevalent frameworks. For the convenience of scholars and practitioners in health informatics, this study provides comparisons of these frameworks against the needs of healthcare application developers. Based on the findings, the Hyperledger Fabric blockchain technology provides more robust functionality for the creation of healthcare apps.

Rahman et al., (2019) [21] suggested a new design for a secure EHR management system that uses blockchain technology. The authors of the study warned that EHR data stored in the cloud might be compromised in the event of a security incident. With a wrapper layer known as the blockchain handshake, the proposed technology combines the pre-existing cloud based EHR management platform with the publicly accessible blockchain network, rendering it difficult to make unauthorized changes to patient records. The concept's viability was shown by the implementation of a prototype. The method proposed in this study has the potential to solve the security problems associated with EHR administration.

Ying et al., (2018) [22] determined the issue of transmitting sensitive EHR data over the Internet safely. EHR contains both medical records and private information, making secure data transfer challenging. The study came up with the idea of using ciphertext-policy attribute-based encryption (CP-ABE), a cryptographic method that permits both granular access control and one-to-many encryption. Privacy might be compromised since CP-ABE's access policy is not encrypted. The authors designed a policy preserving EHR system to solve this problem. They came up with an algorithm to conceal the policy of access while yet permitting recovery of concealed characteristics using the access matrix. Their study of essential tasks including element insertion, lookup, and recovery showed that the approach had little effect on performance. The suggested system was shown to be selectively secure in the security analysis using the q-BDHE assumption.

Ramani et al., (2018) [23] provide a safe and effective method for healthcare providers and patients to share information. This study deal with the issue of keeping private patient information safe in cyberspace in the context of intelligent healthcare networks. To ensure the data is secure, this study proposes a decentralized method based on blockchain technology. The proposed system restricts access to patients' medical records to just those who have been granted permission. The system's integrity is guaranteed, and the scheme is tested for vulnerabilities and proven secure. The suggested system's viability is proven via an Ethereum-based implementation.

Vora et al., (2018) [24] emphasized the necessity for EHR security due to the rising frequency with which patients' private information is breached. A solution that strikes a compromise between data protection and accessibility is needed because current security strategies for EHRs frequently result in limited patient access to data. The study suggested a Blockchain-based architecture for the decentralized and secure storage and maintenance of EHRs, which would allow for more convenient and safe access by patients, providers, and third parties without compromising the confidentiality of patients' personal information. The purpose of this study

is to examine how their approach satisfies the concerns of all parties involved in Healthcare 4.0 while maintaining confidentiality and privacy.

Xia et al., (2017) [25] suggested MeDShare, a blockchain-based platform for the secure exchange of medical records. MeDShare enables provenance, auditing, and governance of massive data in cloud repositories through collaboration between data stewards. All data transfers and actions are recorded in an immutable log that may be monitored for malicious usage by the system. Data usage is monitored and restricted via access controls and smart contracts. When compared to other leading cloud service providers' data-sharing options, MeDShare performs admirably. MeDShare allows data stewards to achieve data provenance and auditing while securely sharing sensitive medical data with minimum risk to patient privacy.

Liang et al., (2017) [26] recommend a distributed and authenticated blockchain system centered on individual users as a means of exchanging medical records. The solution prioritizes user anonymity via a channel creation scheme and enhances identity management via membership services powered by blockchain technology. With the use of a smartphone app, patients may compile their health records from a variety of sources and then upload them to the cloud, where they can be accessed by their doctors and insurance companies. Each record has a verifiable proof of integrity and validity that is kept in the cloud and linked to the blockchain. Large amounts of individual health data gathered via mobile platforms are processed and stored in batches using a tree-based data processing and batching approach for scalability and speed.

3. Background study

Several significant developments have occurred in the storage of EHRs, including a move toward mobile cloud settings. To improve communication between patients and doctors, this method incorporates mobile devices and cloud computing. The advantages of this new paradigm include minimal operational expenses, high flexibility, and increased access to EHRs. While this has many benefits, it also raises questions about the safety of e-health systems' data and networks. This study seeks to address these issues by proposing an innovative framework for secure EHR sharing among mobile users in the cloud. The framework integrates blockchain and the decentralized IPFS file system into a portable cloud environment. Using smart contracts, create a reliable access control method for sharing EHRs online. Using Ethereum's blockchain and a mobile app hosted on the Amazon cloud, the authors demonstrate a prototype implementation of the suggested architecture. The empirical findings show that the suggested method provides a dependable way of data exchange on mobile clouds while protecting confidential health information from unauthorized access. Performance gains from a lightweight access control scheme are highlighted in the assessment and security analysis. When compared to traditional methods of data sharing, these advantages include reduced network latency and increased security and privacy [27].

4. Problem Formulation

Whenever the patient receives medical services from the medical facility, the services are documented in the EHR. After being registered by the network administrator, the hospitals could then join the private blockchain and become part of the network's decentralized database. The medical centers are responsible for the generation of EHR and the storage of this information on cloud servers, which are then shared with other medical facilities. When one medical center views the patient's EHR from another medical center, that medical center will upload a log of data from the patient's EHR to the blockchain in the form of a transaction. The EHR data is sent from the medical center to a cloud server, which then delivers the EHR to any other medical facilities that have requested it using a pre-shared secret key.

5. Research Methodology

In this section, the author has proposed a design of an EHR framework based on blockchain and cloud using the ECIES algorithm.

5.1 Techniques Used.

(i) Blockchain-Based EHR System

The blockchain is a square chain that stores data. The procedure is designed to apply timestamps to more recent archives to render it difficult to backdate or otherwise modify the data that is stored inside those archives. Money, assets, contracts, and so on might all be transferred securely over the Blockchain without the need for a central authority or bank to act as a middleman. There is a high barrier to entry when it comes to altering data that has been stored in a Blockchain [28]. The Blockchain system makes it possible to share data without having to replicate it. This decentralized ledger improves transparency, trust, and information safety. These components form the backbone of

the Blockchain's overall design. Blockchain enables the capture, rather than duplication, of complicated data. This record provides transparency, trust, and data security. Blockchain frameworks are software solutions that reduce the time and effort required to create and launch blockchain applications [29]. As demonstrated in Fig. 2, the primary obstacles facing any blockchain system are limited computer resources, storage space, and scalability.

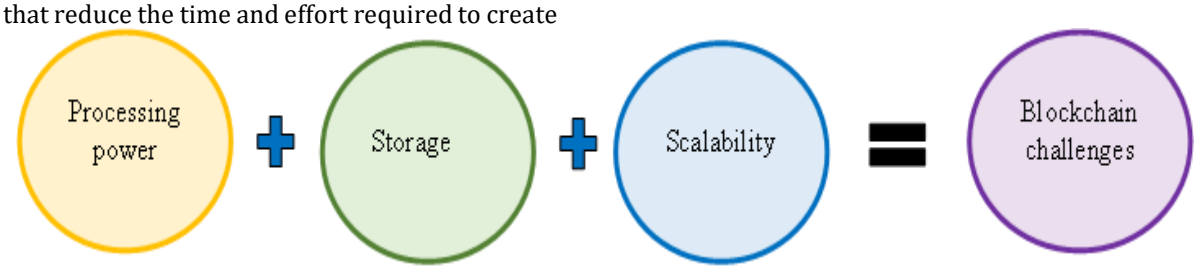

Fig. 2. Blockchain computational complexity [29].

The creation of a confidentiality and security system for electronic health records is the primary problem of EHR. This is necessary so that many parties with an interest can access the data. A blockchain-based platform is also very ideal to prevent illegal access to or use of the patient's information.

(ii) Cloud-Assisted EHR System

The cloud service chosen should be reliable and have enough storage and processing power. Patient EHRs are stored and controlled by a server in the cloud, which also allows for secure data transfer and storage. Data from EHRs are transferred from one hospital to another using a cloud server and a pre-shared secret key. Healthcare providers, clinics, and patients could access blockchain-connected data via cloud computing (CC). With DCN technology, transmission guidelines, and network sharing mechanisms, cloud computing constructs a robust data center to deliver low-cost, highly reliable, and environmentally friendly services to customers [30]. The most common applications of CC systems are those involving virtualization, encryption, decryption, and online services. A key management system is also part of this, as it allows for the safe and secure storing of keys in the cloud. Currently, signatures made possible by public key infrastructure are utilized to keep data in the cloud safe. Cloud computing provides an opportunity for eHealth systems to expand the range of services they provide. However, there are several security and privacy concerns associated with transferring patients' medical records to the Cloud. The risks of keeping EHRs on the servers of untrusted Cloud service providers are analyzed. Several suggestions are made for healthcare providers to follow to protect patient privacy and streamline the process. Also covered are issues of security that Cloud service companies must address in their system.

(iii) ECIES

The ECIES is the go-to method for secure communication using elliptic curves. The term "integrated" refers to the fact that this technique is a hybrid, making use of a public-key mechanism to transmit a session key to be utilized with a symmetric cipher. ECIES ensures data secrecy using symmetric-key encryption algorithms. The message authentication code (MAC) safeguards data integrity. Utilizing elliptic curves to create an encryption key (kENC) and a MAC key (kMAC). The ECIES technique is comparable to the one-way transfer of Diffie Hellman keys except that one side employs a fixed long-term rather than an ephemeral one. A message and its corresponding key are both necessary for ECIES encryption.

In the first step, prime numbers are selected at random from the available options. After that, the public key (U) might well be estimated. For the ciphertext to be cracked, U, c, and rare are all essential. Temporary Diffie-Hellman keys (T) require U's agreement. The message encryption takes place at position c. r is used to protect against adaptive chosen ciphertext attacks. Since U is a point on an elliptic curve, it may be compressed to save bandwidth. Below are the ECIES encryption and decryption algorithms:

➢ **ECIES Encryption**

Let Message → m, recipient's public key → Y and Ciphertext → c.

i. Generate a random ephemeral private key (k) ∈ R (1...q-1)

ii. Compute the k (U) = [k]G

iii. Compute the shared secret point (T) = [k]Y

iv. Derive symmetric encryption key (k1) and MAC key (k2) from T using a key derivation function KD (T, 1)

v. Encrypt m: c = E (k1, m) using a symmetric encryption algorithm (e.g., AES)

vi. Compute the MAC (r) = MAC (k2, c) using a MAC algorithm (e.g., HMAC-SHA256)

vii. Output the ciphertext (U, c, r)

➢ **ECIES Decryption**

Ciphertext → (U, c, r), recipient's private key → x
Decrypted message →m.

i. Compute the shared secret point (T) = [x]U

ii. Derive symmetric encryption key (k1) and MAC key (k2) from T using the same key derivation function KD (T, 1) as in encryption.

iii. Verify the MAC: Computer = MAC (k2, c) and compare it with the received MAC value r- If r ≠ r', then output "Invalid Ciphertext"

iv. Decrypt the message: m = D (k1, c) using the same symmetric encryption algorithm as in the encryption

v. Output the decrypted message m.

5.2 Proposed methodology

This section provides a comprehensive overview of a blockchain and cloud-based EHR system that depends on regional EHR-sharing medical centers to increase the safety and efficacy of medical data storage and exchange. Patients, healthcare institutions, cloud servers, and system administrators all play roles in the EHR system. The following is a comprehensive breakdown of each organization:

Firstly, the patient's medical history and the hospital's services are recorded in the EHR. The healthcare facilities that would use the private blockchain are registered with the network administrator. EHR is created and stored on a cloud server for easy access by other hospitals. Data from EHRs is sent from a medical center to a cloud server, where it is stored until it is requested by another medical facility using a secret key. They add a record of that transaction to the blockchain when hospitals and clinics review patients' medical records from other facilities. The proposed methodology is illustrated in Fig. 3.

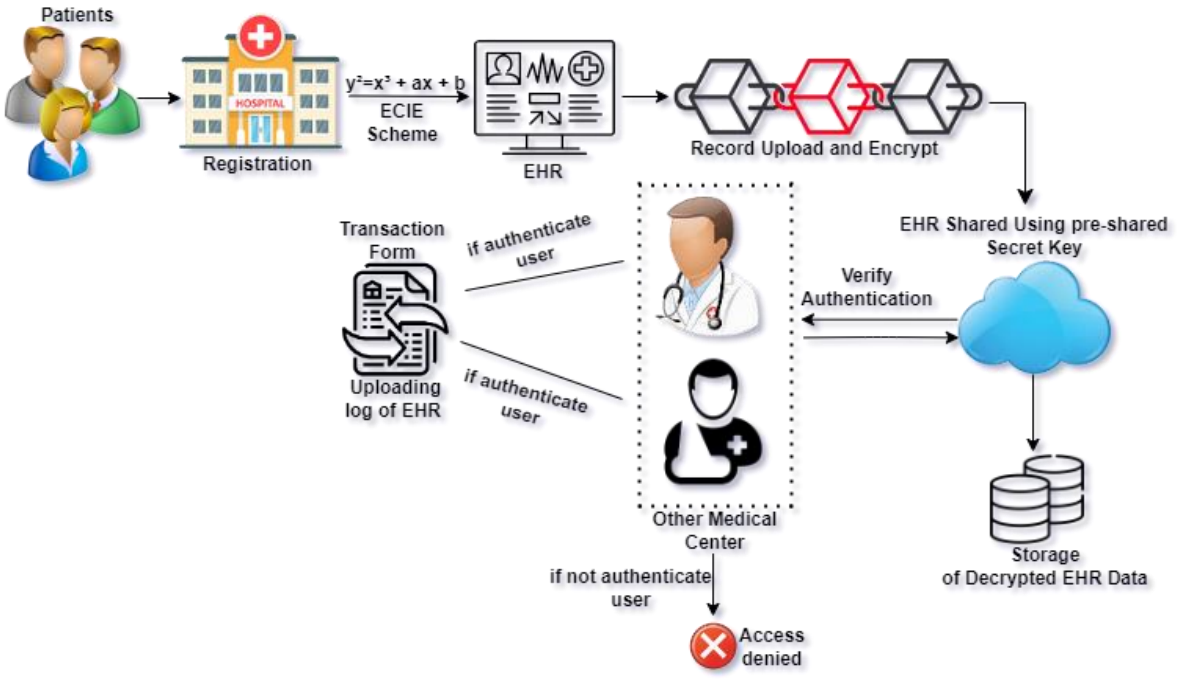

Fig. 3. Proposed Methodology

5.3 Proposed algorithm

ALGORITHM: Blockchain & Cloud-based EHR Framework

Start

Phase I**:** Set performance evaluation parameters.

→ Processing time (T_process)

→ Security level (S_lvl)

→ Scalability (Scl)

→ Data integrity (D_int)

→ Privacy preservation (P_priv)

Phase II**:** Establishing an identity with the support of a network administrator:

Step 1: Let P be the patient's identity.

Step 2: Let D be the doctor's identity.

Phase III**:** Verify identities using the ECIES algorithm:

Step 3: Let Kpd be the shared public key between P and D

Phase IV**:** Patient sends necessary information for EHR:

Step 4: Let EHRp be the EHR for the patient.

Step 5: Let SKp be the session key for encrypting the EHR.

Step 6: EHRp = Send (EHR_info, SKp)

Phase V**:** Medical center uploads EHR to the blockchain and encrypts EHRs of valid patients:

Step 7: Let EHRb be the EHR uploaded to the blockchain.

Step 8: EHRb = Upload (EHRp)

Step 9: EHRb_enc = Encrypt (EHRb)

Phase VI**:** Send encrypted EHR to the cloud server:

Step 10: Let CS be the cloud server.

Step 11: CS_receive(EHRb_enc)

Phase VII**:** Cloud server transmits EHR to other medical centers:

Step 12: Let MC be the receiving medical center.

Step 13: Let SKmc be the pre-shared secret key with MC.

Step 14: EHRmc = Transmit (EHRb_enc, SKmc)

Phase VIII**:** Cloud server decrypts EHR data and stores it in the database:

Step 15: Database_store(EHRb_dec)

Step 16: EHRb_dec = Decrypt (EHRb_enc)

Phase IX**:** Cloud server encrypts medical center's EHR data and sends it to the receiving medical facility:

Step 17: Let EHRmc be the medical center's EHR data.

Step 18: EHRmc_enc = Encrypt (EHRmc, SKmc)

Step 19: MC_receive(EHRmc_enc)

Phase IX**:** Medical center uploads log transaction to the blockchain:

Step 20: Let T be the log transaction.

Step 21: Let P' be the disguised patient's identity.

Step 22: Let D' be the disguised medical center's identity.

Step 23: Let Sig be the signature.

Step 24: Let TS be the timestamp.

Step 25: T = Upload_Log(P', D', Sig, TS)

Phase IX**:** Performance Evaluation:

Step 26: Calculate processing time:

T_process = End_time - Start_time

Step 27: Evaluate security level:

S_lvl = Security_Function()

Step 28: Measure scalability:

Scl = Scalability_Function()

Step 29: Verify data integrity:

D_int = Data_Integrity_Function()

Step 30: Preserve privacy:

P_priv = Privacy_Preservation_Function()

Phase X**:** Return performance evaluation parameters:

Step 31: Return (T_process, S_lvl, Scl, D_int, P_priv)

End

6. Result and Discussion

During registration, the user is prompted to choose a username, which should be unique and not already registered by another user. This username will be used as an identifier to differentiate the user from others within the system. Fig. 4 illustrates how a password protects a user's account and ensures that only those authorized can access their electronic health records.

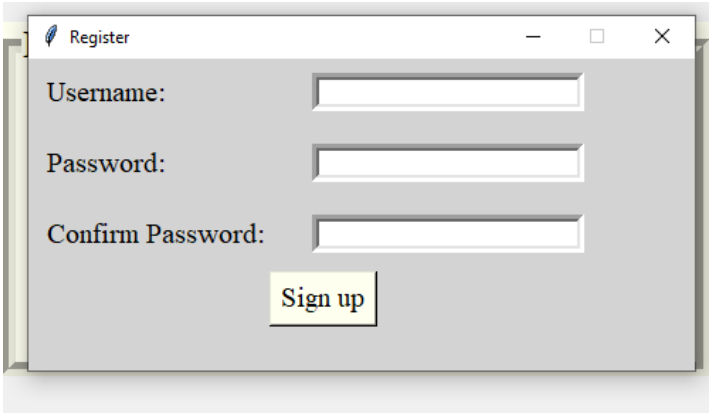

Fig. 4. User Registration

With the registration completed, the user gains the ability to log in to the system using their registered credentials as shown in Fig. 5. Upon logging in, they will be granted access to the EHRs of the patients they are authorized to view. This allows them to review and interact with the EHRs stored on the cloud, facilitating efficient healthcare delivery and decision-making processes.

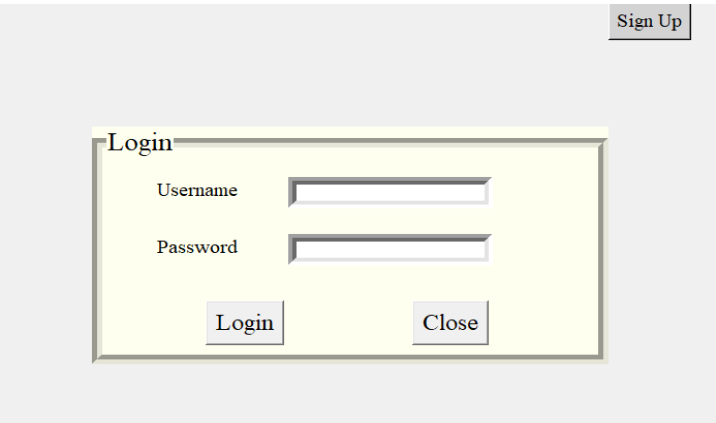

Fig. 5. User Login

After successful login, the administrator of the cloud EHRs checks the user's identity and permissions before granting access. The user's cloud account initiates a transaction by providing the patient's address to access the corresponding EHRs. The cloud EHRs manager retrieves the requested EHRs, verifying user permissions and compliance with privacy regulations as shown in Fig. 6. Authorized users can then view, analyze, or perform actions on the accessed EHRs. This secure process, utilizing blockchain and cloud technology, enables controlled access to EHRs while maintaining data privacy and security.

Fig. 6. Unauthorized access

With authorized access to the EHR data on the cloud, the user can leverage the available features and functionalities provided by the EHR framework as shown in Fig. 7. This may include the ability to update patient records, input new data, generate reports, collaborate with other healthcare professionals, and contribute to the overall management and analysis of patient information.

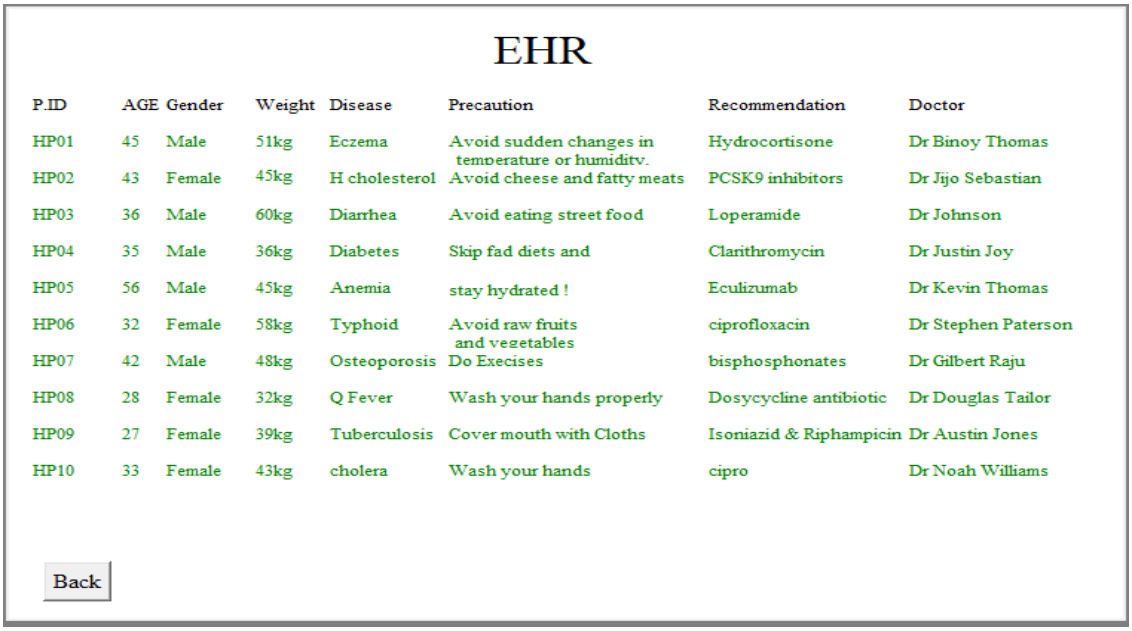

Fig. 7. Access to EHR data

Fig. 8 demonstrates the processing time taken by each authentication scheme. Comparing the three-user authentication ways, it is evident that the smart contract-based scheme consistently had the shortest processing time among the three, indicating its efficiency in user authentication. The non-authenticated scheme performed slightly slower than the smart contract-based scheme but demonstrated faster processing times compared to the ECIES-based scheme. The ECIES-based scheme had the longest processing time, which can be attributed to the complexity of the encryption and decryption processes involved and resulted in higher security and privacy.

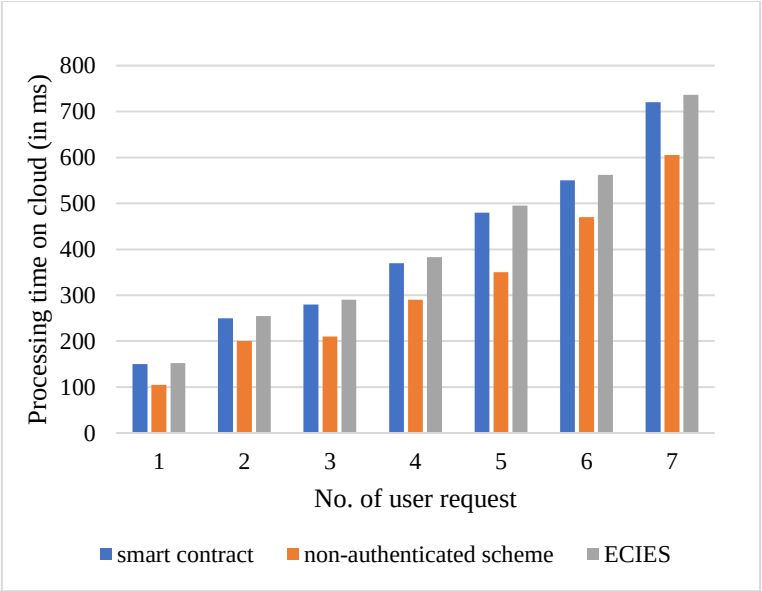

Fig. 8. Processing time v/s user request

Fig. 9 shows that the time consumption for each storage technique increases as the file size increases. The proposed blockchain-ECIES-based storage approach outperforms both blockchain-IPFS-based and centralized storage systems in terms of time consumption, and this holds over a wide range of file sizes. When compared to the other two approaches, centralized storage always takes more time. While both the blockchain-based and blockchain-ECIES-based approaches show comparable tendencies, the blockchain-ECIES-based approach typically requires less time to complete tasks. When comparing blockchain-based and blockchain-ECIES-based techniques, the time difference increases as file sizes grow. From these findings, it appears that the blockchain-ECIES-based storage method is faster than both the blockchain-based and centralized storage methods, especially for bigger file sizes.

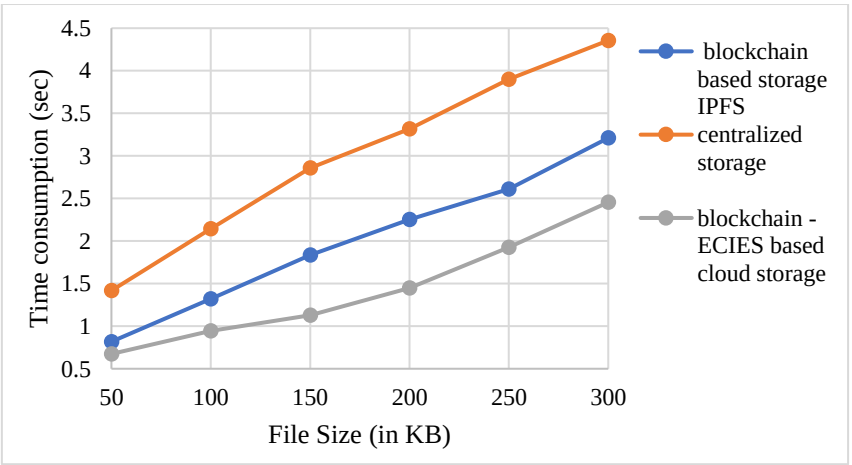

Fig. 9. File size v/s Time consumption

6.1 Comparative analysis

In consideration of the numerous studies that are presented in Table 1, a comparison analysis was performed, it could be summarized from Table 1 that the studies focus on important aspects such as

identity management, user authentication, data integrity, and data privacy. The main objective of this study is the development of systems that provide trustworthy access to distributed data while protecting its confidentiality and security. The decentralized access features are considered by all studies including the proposed study except the study proposed in [21], allowing multiple participants to access and contribute to the system. Identity management is considered a crucial aspect in the considered studies as well as in the proposed study. They emphasize the need for proper identification and management of user identities. However, the study proposed by [22] does not specifically address identity management. User authentication, data integrity, and data privacy are fundamental concerns that are addressed in all studies. The suggested research stands out from the rest since it is the only one that directly addresses the issue of improved cryptographic security.

Table 1. Comparison Table

Features	**Authors of the study**					
	Ying et al., (2018) [21]	Ramani et al., (2018) [22]	Xia et al., (2017) [24]	Liang et al., (2017) [25]	Nguyen et al., (2019) [26]	Proposed Study
Decentralized access	×	✓	✓	✓	✓	✓
Identity Management	✓	×	✓	×	✓	✓
User authentication	✓	✓	✓	×	✓	✓
Data Integrity	✓	✓	✓	✓	✓	✓
Data privacy	✓	✓	✓	✓	✓	✓
Enhanced cryptography security	×	×	×	×	×	✓

The present study examines several crucial elements that have been addressed by previous scholars, encompassing decentralized accessibility, identity management, user authentication, data integrity, and data confidentiality. Furthermore, the proposed research is distinctive in its focus on enhancing cryptographic security, a subject that is overlooked by other scholars. This demonstrates that, in comparison to prior research, the proposed study offers a more comprehensive and enhanced methodology.

7. Conclusion and future scope

In summary, this study's work on cryptographic security enhances its efficacy in safeguarding healthcare data compared to previous research. During the registration process, users have the option to select unique and secure usernames, which function as their identification within the system. Subsequently, authorized users are provided access to the Electronic Health Records (EHRs) they are permitted to view, facilitating the provision of medical care and informed decision-making based on reliable information. The system's security measures are based on three fundamental principles: user authentication, data integrity, and data privacy. Several studies have identified authentication of users, data integrity, and data privacy as the three fundamental pillars for establishing a reliable and secure healthcare ecosystem. The proposed research distinguishes itself through its focus on utilizing advanced cryptographic security measures. This additional layer enhances user privacy and data integrity, providing a notable advantage. The utilization of blockchain, cloud computing, and strong cryptography facilitates the secure access and interaction of healthcare professionals with electronic health records (EHRs). This innovative data protection and confidentiality strategy benefits both the healthcare industry and patients. Continuous research will be necessary to ensure the security of healthcare information systems in light of technological advancements.

References

1. Kuo TT, Kim HE, Ohno-Machado L. Blockchain distributed ledger technologies for biomedical and health care applications. Journal of the American Medical Informatics Association. 2017 Nov 1;24(6):1211-20. Available from: https://doi.org/10.1093/jamia/ocx068
2. Mettler M. Blockchain technology in healthcare: The revolution starts here. In 2016 IEEE 18th international conference on e-health networking, applications and services (Healthcom) 2016 Sep 14 (pp. 1-3). IEEE. Available from: https://doi.org/10.1109/HealthCom.2016.7749510
3. Gordon WJ, Catalini C. Blockchain technology for healthcare: facilitating the transition to patient-driven interoperability. Computational and structural biotechnology journal. 2018 Jan 1;16:224-30. Available from: https://doi.org/10.1016/j.csbj.2018.06.003
4. Dubovitskaya A, Xu Z, Ryu S, Schumacher M, Wang F. Secure and trustable electronic medical records sharing using blockchain. InAMIA annual symposium proceedings 2017 (Vol. 2017, p. 650). American Medical Informatics Association.
5. Hölbl M, Kompara M, Kamišalić A, Nemec Zlatolas L. A systematic review of the use of blockchain in healthcare. Symmetry. 2018 Oct 10;10(10):470. Available from: https://doi.org/10.3390/sym10100470
6. Jiang S, Cao J, Wu H, Yang Y, Ma M, He J. Blochie: a blockchain-based platform for healthcare information exchange. In2018 ieee international conference on smart computing (smartcomp) 2018 Jun 18 (pp. 49-56). IEEE. Available from: https://doi.org/10.1109/SMARTCOMP.2018.00073
7. Hasanova H, Tufail M, Baek UJ, Park JT, Kim MS. A novel blockchain-enabled heart disease prediction mechanism using machine learning. Computers and Electrical Engineering. 2022 Jul 1;101:108086. Available from: https://doi.org/10.1016/j.compeleceng.2022.108086
8. Ntantogian C, Veroni E, Karopoulos G, Xenakis C. A survey of voice and communication protection solutions against wiretapping. Computers & Electrical Engineering. 2019 Jul 1;77:163-78. Available from: https://doi.org/10.1016/j.compeleceng.2019.05.008
9. Wang Y, Zhang A, Zhang P, Wang H. Cloud-assisted EHR sharing with security and privacy preservation via consortium blockchain. Ieee Access. 2019 Sep 23;7:136704-19. Available from: https://doi.org/10.1109/ACCESS.2019.2943153
10. Lo'ai AT, Mehmood R, Benkhlifa E, Song H. Mobile cloud computing model and big data analysis for healthcare applications. IEEE Access. 2016 Sep 26;4:6171-80. Available from: https://doi.org/10.1109/ACCESS.2016.2613278
11. Islam SR, Kwak D, Kabir MH, Hossain M, Kwak KS. The internet of things for health care: a comprehensive survey. IEEE access. 2015 Jun 1;3:678-708. Available from: https://doi.org/10.1109/ACCESS.2015.2437951
12. Esposito C, De Santis A, Tortora G, Chang H, Choo KK. Blockchain: A panacea for healthcare cloud-based data security and privacy?. IEEE cloud computing. 2018 Mar 28;5(1):31-7. Available from: https://doi.org/10.1109/MCC.2018.011791712
13. Ying Z, Wei L, Li Q, Liu X, Cui J. A lightweight policy preserving EHR sharing scheme in the cloud. IEEE Access. 2018 Sep 19;6:53698-708. Available from: https://doi.org/10.1109/ACCESS.2018.2871170
14. Hathaliya JJ, Tanwar S, Tyagi S, Kumar N. Securing electronics healthcare records in healthcare 4.0: A biometric-based approach. Computers & Electrical Engineering. 2019 Jun 1;76:398-410. Available from: https://doi.org/10.1016/j.compeleceng.2019.04.017
15. Sharma P, Borah MD, Namasudra S. Improving security of medical big data by using Blockchain technology. Computers & Electrical Engineering. 2021 Dec 1;96:107529. Available from: https://doi.org/10.1016/j.compeleceng.2021.107529
16. Abunadi I, Kumar RL. BSF-EHR: blockchain security framework for electronic health records of patients. Sensors. 2021 Apr 19;21(8):2865. Available from: https://doi.org/10.3390/s21082865
17. Tanwar S, Parekh K, Evans R. Blockchain-based electronic healthcare record system for healthcare 4.0 applications. Journal of Information Security and Applications. 2020 Feb 1;50:102407. Available from: https://doi.org/10.1016/j.jisa.2019.102407

18. Kim M, Yu S, Lee J, Park Y, Park Y. Design of secure protocol for cloud-assisted electronic health record system using blockchain. Sensors. 2020 May 21;20(10):2913. Available from: https://doi.org/10.3390/s20102913
19. Agbo CC, Mahmoud QH. Comparison of blockchain frameworks for healthcare applications. Internet Technology Letters. 2019 Sep;2(5):e122. Available from: https://doi.org/10.1002/itl2.122
20. Rahman MS, Khalil I, Mahawaga Arachchige PC, Bouras A, Yi X. A novel architecture for tamper proof electronic health record management system using blockchain wrapper. InProceedings of the 2019 ACM international symposium on blockchain and secure critical infrastructure 2019 Jul 2 (pp. 97-105). Available from: https://doi.org/10.1145/3327960.3332392
21. Ying Z, Wei L, Li Q, Liu X, Cui J. A lightweight policy preserving EHR sharing scheme in the cloud. IEEE Access. 2018 Sep 19;6:53698-708. Available from: https://doi.org/10.1109/ACCESS.2018.2871170
22. Ramani V, Kumar T, Bracken A, Liyanage M, Ylianttila M. Secure and efficient data accessibility in blockchain based healthcare systems. In2018 IEEE Global Communications Conference (GLOBECOM) 2018 Dec 9 (pp. 206-212). IEEE. Available from: https://doi.org/10.1109/GLOCOM.2018.8647221
23. Vora J, Nayyar A, Tanwar S, Tyagi S, Kumar N, Obaidat MS, Rodrigues JJ. BHEEM: A blockchain-based framework for securing electronic health records. In2018 IEEE Globecom Workshops (GC Wkshps) 2018 Dec 9 (pp. 1-6). IEEE. Available from: https://doi.org/10.1109/GLOCOMW.2018.8644088
24. Xia QI, Sifah EB, Asamoah KO, Gao J, Du X, Guizani M. MeDShare: Trust-less medical data sharing among cloud service providers via blockchain. IEEE access. 2017 Jul 24;5:14757-67. Available from: https://doi.org/10.1109/ACCESS.2017.2730843
25. Liang X, Zhao J, Shetty S, Liu J, Li D. Integrating blockchain for data sharing and collaboration in mobile healthcare applications. In2017 IEEE 28th annual international symposium on personal, indoor, and mobile radio communications (PIMRC) 2017 Oct 8 (pp. 1-5). IEEE. Available from: https://doi.org/10.1109/PIMRC.2017.8292361
26. Nguyen DC, Pathirana PN, Ding M, Seneviratne A. Blockchain for secure ehrs sharing of mobile cloud-based e-health systems. IEEE access. 2019 May 17;7:66792-806. Available from: https://doi.org/10.1109/ACCESS.2019.2917555
27. Sharma S, Mishra A, Singhai D. Secure cloud storage architecture for digital medical record in cloud environment using blockchain. InProceedings of the International Conference on Innovative Computing & Communications (ICICC) 2020 Apr 1. Available from: https://dx.doi.org/10.2139/ssrn.3565922
28. Quasim MT, Khan MA, Algarni F, Alharthy A, Alshmrani GM. Blockchain frameworks. Decentralised Internet of Things: A Blockchain Perspective. 2020:75-89. Available from: https://doi.org/10.1007/978-3-030-38677-1_4
29. Kocabas O, Soyata T, Aktas MK. Emerging security mechanisms for medical cyber physical systems. IEEE/ACM transactions on computational biology and bioinformatics. 2016 Jan 22;13(3):401-16. Available from: https://doi.org/10.1109/TCBB.2016.2520933
30. Li H, Yang C, Liu J. A novel security media cloud framework. Computers & Electrical Engineering. 2019 Mar 1;74:605-15. Available from: https://doi.org/10.1016/j.compeleceng.2018.07.022