International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING

ISSN:2147-6799 www.ijisae.org Original Research Paper

A Hybrid Algorithm for Encrypting Electronic Health Record Using Blockchain in a Cloud Computing Environment

Ebtisam Ali Abdullah[1], Anwar Al Shamiri and Abdualmajed A. G. Al-Khulaidi[*,3]

Submitted: 05/05/2024 **Revised**: 18/06/2024 **Accepted**: 25/06/2024

Abstract: Emerging technologies, such as eHealth, are revolutionizing healthcare systems by providing high-quality services and improving health outcomes for a diverse range of patients. The core of eHealth is the safe and effective management of electronic health records (EHRs) using advanced information and communication technologies (ICTs).Traditional and cloud-based electronic health systems often lack adequate privacy protection and secure storage, posing critical issues in healthcare provision.The problem addressed in this paper is the security threats faced by EHRs stored in cloud systems, including data privacy, integrity, and confidentiality. The study aims to enhance EHR security and management in cloud systems by proposing a new encryption model and implementing an encryption model .This paper introduces SC2M-EHR-B, a secure cloud computing model for electronic health records (EHRs) using blockchain technology. The SC2M-EHR-B model combines blockchain to secure and share medical records, enhancing security, and provide a patient control over their medical data, more over the model make use of the cloud computing to store medical records.

This paper also proposed a hybrid algorithm consisting of two (AES and Blowfish) algorithms to encrypt the electronic health record using blockchain. The performance of the hybrid algorithm, measured using the BlockSim blockchain simulator, showed better results. The results showed better performance for the hybrid algorithm. Also, the results successfully demonstrates the effectiveness of the proposed model in and enhancing security , ensuring secure storage and sharing of medical records, at a lower communication cost .

The importance of this paper lies in providing high-quality medical services, increasing patient confidence and satisfaction, and improving patients' ability to monitor their medical records.

Keywords: *Electronic health records, Blockchain Cloud Computing, BlockSim blockchain simulator .*

1. Introduction

The sharing of Electronic Medical Records (EMRs) is crucial for improving healthcare services, reducing costs[1], and accelerating biomedical discoveries. EMRs contain highly sensitive private information for clinical diagnosis and treatment[2]. However, medical data is often scattered across various institutions with non-uniform data standards, leading to low interoperability and centralized storage vulnerabilities[3] [4] [5] .

Challenges in healthcare data sharing include privacy, security, and interoperability concerns. To address these issues, a secure data sharing infrastructure is required[6] [7]. Blockchain technology offers a solution by ensuring data integrity, reliability, and security, while empowering patients with control over their personal health data[8].

Blockchain's decentralized architecture eliminates the need for centralized trust, enhancing privacy and security. It also facilitates healthcare data supervision for patients and various actors in the medical field. Blockchain-oriented techniques, such as multi-signature, anonymous messaging encryption, and anonymous negotiable energy trading, can further protect privacy and enhance security in specific applications[9, 10].

Cloud computing has significantly improved the healthcare industry by offering faster and easier access to medical information while maintaining data integrity and confidentiality with the HIPAA(Health Insurance Portability and Accountability Act) standard[11] [12].

This technology allows patients to access their medical records from anywhere in the world, contributing to personalized healthcare. However, increased security and privacy measures are necessary to ensure the safe management of cloud computing in healthcare [13].

Healthcare information systems involve patients and medical professionals, such as physicians, nurses, and pharmacists, working together to provide medical services. Healthcare organizations are adopting electronic health systems to enhance efficiency and collaboration among healthcare providers. Cloud computing offers numerous benefits, including scalable medical data storage, easy remote access, data sharing between authorized units, and real-time updates for improved patient treatment[14] [15] [16].

Cloud computing can be categorized into four groups: disease management and treatment services, management activities and supply support, health knowledge

[1,2,3] *Sana'a University, Yemen*
ORCID ID : 0009-0003-7448-7229
** Corresponding Author Email: alkhulaidi@su.edu.ye*
[1] *ibt.alselwi@su.edu.ye*
[2] *anwarsaif@su.edu.ye*
[1] *Information Technology,* [2] *Information Systems,* [3] *Software Engineering*

infrastructure, and safe confidentiality issues . The patient's medical data, when outsourced and stored in the cloud, is known as the Electronic Health Record (EHR) [17]. EHRs are a part of the Electronic Medical Record, created and owned by the patient, and shared among healthcare organizations[14].

To ensure data security and patient privacy, EHR systems developers must classify patient information into personal identifiable information, medical data, and data type (text or images). Highly sensitive data, such as medical information or patient private information, must be kept confidential and not accessible to unauthorized users. Encrypting EHR data and implementing access control measures help protect data from unauthorized access, misuse, and modification[17].

In summary, cloud computing in healthcare offers significant benefits, including improved medical data storage, remote access, data sharing, and real-time updates. However, it also introduces security and privacy concerns. Proper classification and encryption of patient data, along with access control measures, are crucial for ensuring data confidentiality and patient privacy in EHR systems. Healthcare providers can leverage the cloud computing environment to store, process, and share huge amounts of medical data with insurance companies and medical research agents in a cost-effective way[17].

The integration of blockchain in healthcare occurs in four stages. First, healthcare providers directly connect to the blockchain and transmit patient data to the network via API. Smart contracts execute incoming transactions, and blocks are created and chained through the immutable ledger. Transactions are committed and uniquely identifiable, and clinical data is analyzed for new insights. If the patient chooses to share their identity, they can share their private key with the healthcare provider for access to their data. The database of blocks stores only non-identifiable patient data, ensuring confidentiality[18] .

Blockchain technology is a secure and exciting development in the field of Distributed Ledger Technology. Cryptography techniques, such as private and public keys, hashing, and digital signatures, are used to ensure security and privacy in the blockchain network. The four main concerns for any network are confidentiality, integrity, authentication, and non-repudiation[19] [10].Blockchain technology provides interoperability, immutability, and auditable history of data, making it ideal for the healthcare industry, where data security and privacy are of the utmost importance[20] [21, 22] [23]. The technology uses encryption and hashing techniques to ensure that stored data remains immutable and secure. Digital signatures and hashing techniques are used to secure data, such as electronic medical records, from manipulation and unauthorized access. Blockchain technology's decentralized nature and encryption techniques provide better security compared to other existing technologies. The technology ensures secure communication between nodes, giving users complete authority over their information[19] [24]. Overall, blockchain technology offers significant improvements in data security and privacy, making it a valuable tool for various industries, including healthcare[10].

2. Related Work

Numerous studies have explored combining cloud computing and blockchain technologies to secure electronic health records. Despite blockchain technology's strong security, its restricted storage capacity poses a problem. To address this, records are generally encrypted and stored in a cloud computing environment that provides abundant storage space. There are many studies on electronic health record encryption, including:

In studies [25] [26] utilized only the RSA algorithm for EHR encryption in cloud and blockchain environments, but this may not be sufficiently secure due to RSA implementation vulnerabilities and limitations. RSA encryption's security is heavily dependent on key length; shorter keys are more susceptible to brute-force attacks. Weak key generation due to predictable or non-random sources can result in insecure keys, making encryption easier to break. Padding oracle attacks exploit vulnerabilities in RSA padding schemes, potentially allowing attackers to decrypt data or extract plaintext information. Timing attacks can reveal private keys or plaintext data by measuring cryptographic operation times. Implementation bugs, such as coding errors, logic flaws, or inadequate testing, can lead to exploitable vulnerabilities. Proper key management, including secure storage and handling of private keys, is essential for RSA implementation security. Blockchain technology, while offering tamper-evident and transparent storage, is not immune to security risks like smart contract vulnerabilities, consensus algorithm flaws, and network attacks. A multi-layered security approach is recommended, incorporating RSA encryption, authentication, access control, secure key management, regulatory compliance, and blockchain security best practices. Regular security assessments, updates, and audits are crucial for identifying and addressing potential vulnerabilities in RSA implementations.

The paper in [27] introduced a blockchain cloud storage solution addressing genetic prediction and dynamic files' challenges. The strategy involves a file allocation model, node load analysis, storage response time evaluation, and load prediction analysis. A genetic algorithm is used to allocate files to nodes efficiently. Experiments confirm the strategy's superior performance, with faster access speed, higher efficiency, and a balanced load. Future work focuses on optimizing the genetic algorithm's cost, refining the algorithm process, and designing a faster population evolution method for improved cloud storage strategy stability and efficiency.

In studies [28] [29] used only ABE encryption for EHRs in cloud and blockchain environments, offering fine-grained access control and flexible policies but with implementation vulnerabilities and limitations. Key management complexity can compromise encryption security, especially in large attribute and user scenarios. Policy complexity can lead to unintended access or security vulnerabilities due to misconfigurations or errors. Trust assumptions about the key and policy-enforcing authority can undermine ABE system security if compromised. Performance overhead can impact system scalability and responsiveness, particularly in resource-constrained environments. Side-channel attacks can reveal sensitive information about attribute-based keys or plaintext data. Implementation bugs, such as coding errors or inadequate testing, can lead to exploitable vulnerabilities. Blockchain technology's security vulnerabilities can impact EHR confidentiality and integrity, requiring a multi-layered security approach.

The study in [30] used AES and RSA encryption for EHRs in a cloud environment without blockchain, offering strong security with potential vulnerabilities. Key management weaknesses can compromise encryption security, requiring secure key generation, storage, rotation, and revocation. Cryptographic protocol design must be carefully considered to prevent security vulnerabilities or unintended behaviors. Implementation weaknesses in RSA or AES can be exploited, with common vulnerabilities including random number generation, key lengths, padding oracle attacks, timing attacks, or bugs. Insufficient authentication and access control can lead to unauthorized access, requiring secure mechanisms for user and system access. Data leakage can compromise encrypted EHRs, necessitating secure data transmission, storage, and processing.

Authors in [31] used AES and RSA encryption for EHRs in a cloud and blockchain environment on Hyperledger, offering robust security with potential vulnerabilities. Effective key management is crucial for RSA and AES encryption in a blockchain environment, with weaknesses in key generation, storage, or distribution potentially compromising security. Blockchain security vulnerabilities, such as smart contract vulnerabilities, consensus algorithm flaws, and network attacks, can impact EHR confidentiality and integrity. Hyperledger Fabric smart contract vulnerabilities, like reentrancy attacks, integer overflows, or logic errors, can lead to unauthorized access or security breaches.

Privacy concerns may arise from storing sensitive medical data on blockchain, even when encrypted, due to metadata and transaction details potentially revealing sensitive information.

Studies in [32] [33] [34] [35] [36] [37]used only ECC encryption for EHRs in cloud and blockchain environments, offering strong security but with implementation vulnerabilities and limitations. Weak curve parameters can lead to private key recovery or signature forgery if insecure or poorly chosen elliptic curves are used. Weak random number generation can result in predictable or insecure keys, making encryption easier to break. Side-channel attacks can reveal sensitive information about the private key through unintended leakage during cryptographic operations. Fault injection attacks can provide attackers with information about the private key or plaintext data by inducing errors during execution. Implementation bugs, such as coding errors or inadequate testing, can lead to exploitable vulnerabilities. Secure key management is essential, with weaknesses in key storage, handling, or sharing potentially undermining ECC implementation security. Blockchain technology's security vulnerabilities can impact EHR confidentiality and integrity, requiring a multi-layered security approach.

Researchers in [38] used only Blowfish encryption in cloud and blockchain environments , may lack comprehensive security due to implementation vulnerabilities and limitations. Secure key management is vital for Blowfish encryption, with weaknesses in key generation, storage, or distribution potentially compromising confidentiality. Cryptanalysis advancements could expose Blowfish algorithm vulnerabilities, requiring organizations to stay updated and adapt encryption schemes. Brute-force attacks' effectiveness may increase with computational power, but longer key lengths can help mitigate this risk. Side-channel attacks can reveal sensitive information through unintended leakage during cryptographic operations, posing a risk to Blowfish implementations. Implementation bugs, such as coding errors or inadequate testing, can lead to exploitable vulnerabilities.

The task of managing electronic health records (EHRs) across multiple medical platforms is a challenge for current systems. Blockchain technology offers potential with its secure sharing capabilities, but the impracticality of storing entire records in the blockchain due to size and cost remains a significant obstacle. Although cloud computing provides ample storage and scalability, it may not always ensure security. To address these challenges, this work proposes a model that combines blockchain technology and cloud computing for secure and private EHR sharing. This proposed model addresses the security and privacy concerns of cloud systems by using blockchain technology. This proposed model uses a two-layered encryption approach, employing two distinct(AES and Blowfish)algorithms for heightened security. The encrypted records are then stored in a cloud computing environment, ensuring secure data transmission and maintaining patient privacy. This proposed model offers a secure and efficient solution for EHR sharing, addressing the shortcomings of existing systems. By combining blockchain technology and cloud computing, this work achieves high levels of security, privacy, and seamless data sharing in a cloud-enabled EHR system.

3. Methodology

Figure 1: showing the research methodology.

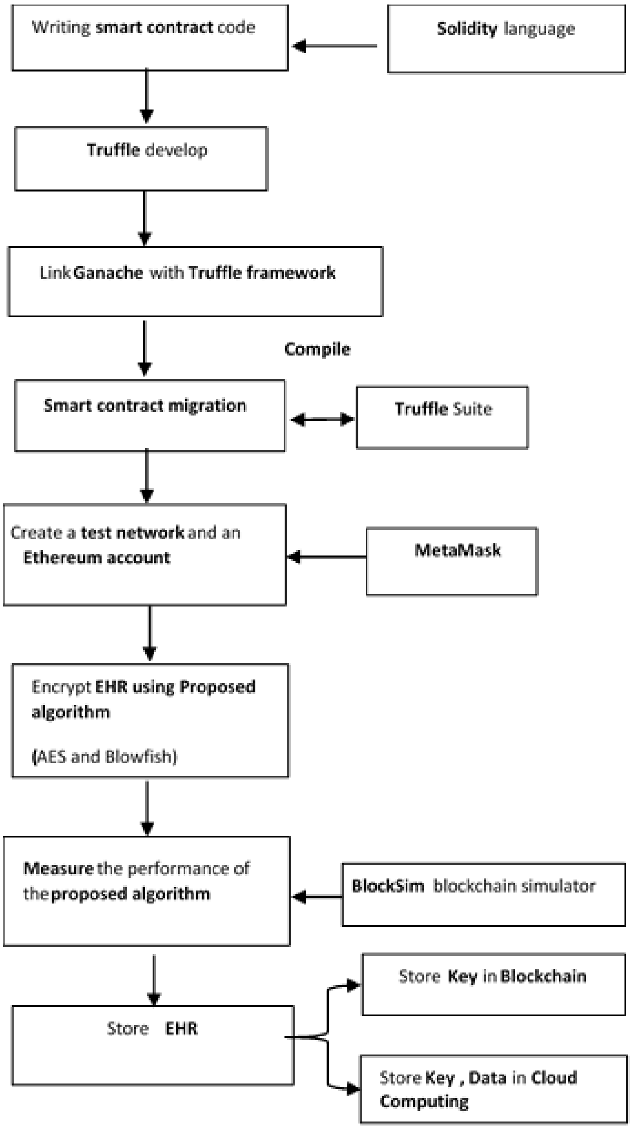

Writing smart contract code
Solidity language
Truffle develop
Link Ganache with Truffle framework
Compile
Smart contract migration
Truffle Suite
Create a test network and an Ethereum account
MetaMask
Encrypt EHR using Proposed algorithm
(AES and Blowfish)
Measure the performance of the proposed algorithm
BlockSim blockchain simulator
Store EHR
Store Key in Blockchain
Store Key , Data in Cloud Computing

Fig 1: Research methodology workflow chart

4. The SC2M-EHR-B proposed model

The SC2M-EHR-B model for implementing cloud computing in hospitals provides security of confidential patient data, through the use of blockchain technology that ensures strong security of the patient's medical record.

The patient data (patient’s medical record) is transferred using medical data collection devices, and then the collected data is transferred to the blockchain technology located within the cloud computing of the hospital attended by the patient, where the blockchain records the medical record information, updates and analyzes it with the creation of an index for each Health record, then encrypt the patient’s health record using an encryption hybrid algorithm proposed consists of two algorithms (AES and blowfish), and due to the problem of limited storage in the blockchain, the blockchain maintains the index of the patient’s health record information, while the encrypted information of the patient’s medical record is saved in the private cloud computing of the hospital attended by the patient.

Patients can allow their data to be shared, added, or downloaded to a center or hospital using the index in the blockchain. The proposed model consists of a simple and inexpensive public cloud with a large storage capacity as needed, and this cloud needs little management, as medical records information for hospitals that do not have private clouds are stored and managed in this cloud. Also, the patient’s health records are stored for medical departments that not found in any hospital. In the proposed heterogeneous model, the public cloud is linked to several private blockchain owned by private hospitals, medical care centers, and public hospitals that are linked to each other in a decentralized manner.

In the hospital blockchain attended by the patient, confidential patient data is processed, updated, and encrypted, and backup copies are made to prevent this data from being lost and sent to the public cloud for storage, and the patient data is only processed after obtaining permission from that patient to give the authorized persons in the hospital Access to and control of his medical data.

The hospital or medical center sends a request to other hospitals to search for the patient’s medical record using a special index of this record , to share the record after taking the patient’s permission, and if there is an update of the data in private blockchain, a new block is created and stored in the public cloud.

This research created smart contracts using the Solidity programming language and the Ethereum platform. And deployed and ran the code for the smart contract on the Ethereum blockchain after it was compiled. Figure 2 shows the workflow diagram of the proposed model.

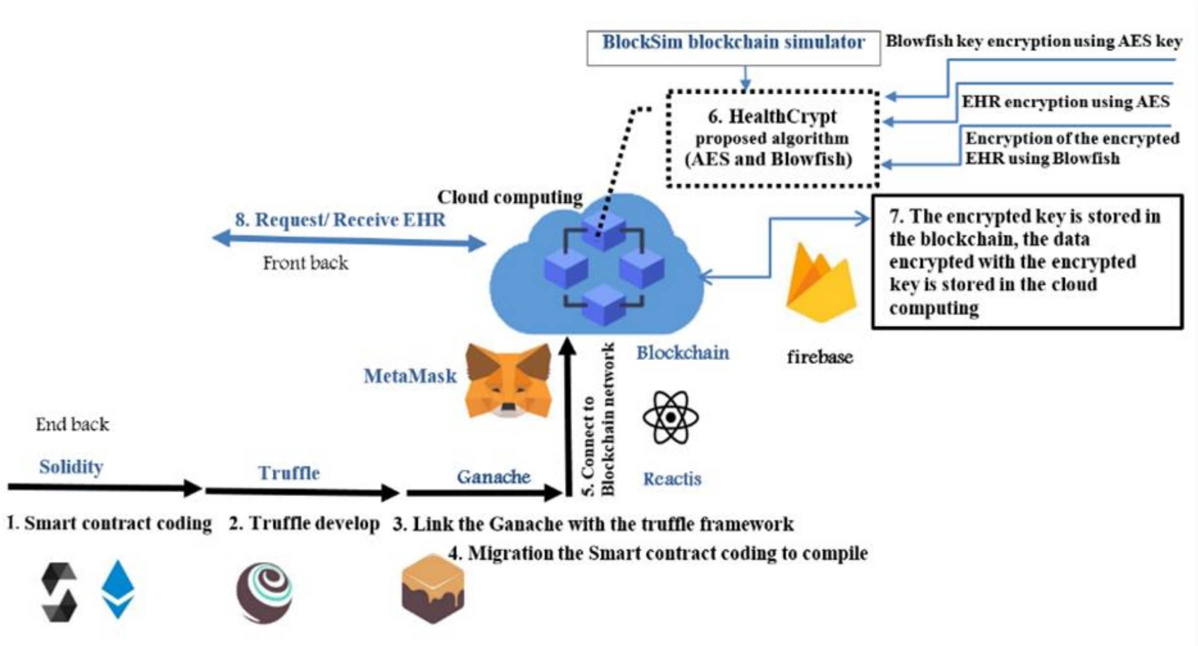
The SC2M-EHR-B proposed model uses four Ethereum-based smart nodes to manage EHR sharing between hospitals and patients, encrypt it using encryption proposed hybrid algorithm, and then store it for future use.

Before communicating with the smart contract, the beneficiaries (doctor, technician, laboratory, patient, and administrator) are given a unique blockchain address, which will serve as an identifier and distinguish users from each other.

Furthermore, in order to reuse this address and connect to it using other apps, browsers, or wallets, they are given a private key using MetaMask.

The address given to the patient (for example, x038536...a9d96C682) is unique and can only be used by the patient. The proposed model creates a free local network using the Ganache program and MetaMask, and to program the Ethereum-based smart contract, this study use the Solidity 0.5.0 language. In this work compiled the smart contract using Truffle Suite and migrated it for development on the local blockchain, and further evaluation and testing were carried out by Ganache.

The communication between the front end and the blockchain is controlled by web3.js, which is an Ethereum JavaScript API. Restricting access to unauthorized users is vital in smart contracts. For the purpose of managing access control and smart contract security, OpenZeppelin , a security tool of Solidity, was used.



BlockSim blockchain simulator
Blowfish key encryption using AES key
EHR encryption using AES
Encryption of the encrypted EHR using Blowfish
6. HealthCrypt proposed algorithm (AES and Blowfish)
Cloud computing
8. Request/ Receive EHR
Front back
7. The encrypted key is stored in the blockchain, the data encrypted with the encrypted key is stored in the cloud computing
Blockchain
firebase
MetaMask
5. Connect to Blockchain network
Reactis
End back
Solidity
Truffle
Ganache
1. Smart contract coding
2. Truffle develop
3. Link the Ganache with the truffle framework
4. Migration the Smart contract coding to compile

Fig 2 : Process flow diagram for of the proposed model

5. HealthCrypt proposed algorithm

The HealthCrypt algorithm proposed in this research consists of two algorithms, AES and Blowfish, to encrypt the electronic health record. This encryption method provides a high level of security by combining the strengths of the AES and Blowfish algorithms,

Encryption process

Table 1 show the steps of HealthCrypt proposed algorithm

Table 1 : Pseudo of HealthCrypt proposed algorithm

Step1 : The secret key (K) for the AES encryption algorithm is generated using a secure random number generator .

Step2 : The secret key (K) for the Blowfish encryption algorithm is generated using a secure random number generator and the Blowfish key is then encrypted using the AES key .

Step3 :The message (M) to be encrypted is divided into blocks (each of size n bytes), forming a plaintext (P).

Step 4:The AES encryption algorithm is applied to encrypt the plaintext blocks.

Step 5:The Blowfish encryption algorithm is applied to encrypt the ciphertext blocks produced by the AES algorithm.

Step 6:The encrypted blocks (C1, C2, ..., Cn) are concatenated to form the ciphertext (C).

Step 7:The ciphertext (C) is sent to the receiver.

Decryption process (Upon receiving the ciphertext (C), the receiver carries out the reverse process)

Table 2: Pseudo of HealthCrypt proposed algorithm

Step1 : Decrypt Blowfish key using AES key.

Step2 : The ciphertext (C) is divided into blocks (C1, C2, ..., Cn).

Step 3: The Blowfish decryption algorithm is applied to decrypt the ciphertext blocks.

Step 4: The AES decryption algorithm is applied to decrypt the plaintext blocks produced by the Blowfish algorithm.

Step 5: The decrypted plaintext blocks (P1, P2, ..., Pn) are concatenated to form the original message (M).

6. Measure the performance of HealthCrypt proposed algorithm

To measure the performance of the proposed algorithm in terms of encryption time , decryption time, And cost of communication ,we used the BlockSim blockchain simulator.

Installation and Requirements

To run the BlockSim: Blockchain Simulator, we installed Python 3.12. Additionally, we installed the following packages:

- pandas , numpy, scikit-learn and xlsxwriter.

Once we have Python and these packages installed, we run the simulator by triggering the main class **Main.py** from the command line: **python3 Main.py**.

we use a laptop with a 2.80GHz Intel(R) Core(TM) i7-7600U CPU with16 GB RAM running on Windows 10.

7. Running the simulator

Before we run the simulator, we can access the configuration file **InputsConfig.py** to choose the model of interest (Base Model 0, Bitcoin Model 1 and **Ethereum Model 2**) and to set up the related parameters. We chose in this work **Model 2,** then defines **input configurations** for an Ethereum model. The parameters are categorized into three sections: Block Parameters, Transaction Parameters, and Simulation Parameters, see table 3 .

Table 3 : Parameters used in the simulation

	NO	Parameter	Description	Value
Block Parameters	1	Binterval	The average time (in seconds) for creating a block in the blockchain. This parameter can be used to simulate the block creation time and measure the performance of the encryption algorithms in terms of block creation time.	0.5
	2	Bsize	The block size in MB. This parameter can be used to simulate the block size and measure the performance of the encryption algorithms for different block sizes.	0.0001285
	3	Blimit	is the block gas limit	8000000
Transaction Parameters	1	hasTrans	is a boolean variable to enable or disable transactions in the simulator	True
	3	Tn	The rate of the number of transactions to be created per second. This parameter can be used to simulate the load on the system and measure the performance of the encryption algorithms under different loads.	20
	5	Tsize	The average transaction size in MB. This parameter can be used to simulate the size of the electronic medical records and measure the performance of the encryption algorithms for different sizes of records.	0.0001285
Simulation Parameters	1	simTime	The simulation length (in seconds). This parameter can be used to set the duration of the simulation and measure the performance of the encryption algorithms over a specific period of time.	500 s
	2	Runs	The number of simulation runs. This parameter can be used to run multiple simulations and measure the average performance of the encryption algorithms.	2

8. Simulation Resulted

In this paper, the data set was a file containing a patient report.

When we measured the performance of the proposed algorithm in the BlockSim blockchain simulator to encrypt and decrypt patient data and calculate the communication cost to know the data transfer rate per second from the blockchain to cloud computing, the results were as follows:

Table 4 : Simulation results of the HealthCrypt proposed algorithm

Parameters	HealthCrypt proposed algorithm
Encryption time(s)	0.050 s
Decryption time(s)	0.001 s
Communication cost	296

Parameters	RSA+AES	ECC+RSA	HealthCrypt proposed algorithm
Encryption time(s)	0.091 s	0.078 s	0.050 s
Decryption time(s)	0.004	0.003 s	0.001 s
Communication cost	614	384	296

9. Discussion

In this research, a hybrid algorithm was used that combines the strengths of the two algorithms (AES and Blowfish) and thus will

provide high security. Unlike previous studies in [25] [26] [38 ,32] [33] [34] [35] [36] [37] [28] [29] that used an one algorithm, which makes it vulnerable to attacks and hacks because it is not secure enough.

In this research uses a hybrid algorithm for encryption using blockchain technology in a cloud computing environment, which enhances security and performance, Unlike study in [30] that used hybrid algorithm in a cloud computing environment, but they did not use blockchain technology to provide stronger security in addition to the hybrid encryption algorithm. This contradicts with this research.

This research also used the Ethereum platform, and this contradicts the study in [31] that used hybrid cryptography in a cloud and blockchain environment, but on the Hyperledger platform, as this platform is a better choice for institutional use cases, but the Ethereum platform is the better choice because it focuses more on decentralized applications and blockchain networks public.

In this work, we measured the performance of the proposed hybrid algorithm and then compared its performance with the hybrid algorithm in the study [31] and the hybrid algorithm in the study in [39] in the blockchain simulator and on the same patient report file, and we reached the results recorded in the following table: **Table 5: A comparison between HealthCrypt proposed algorithm and algorithms proposed by previous studies**

9.1. Comparison of Encryption and Decryption Time

The results of the previous table 5 showed that the hybrid algorithm for this research took less time to encrypt the patient's data and less time to decrypt the data than the algorithms proposed in previous studies. This shows that the hybrid algorithm for this work has better performance in terms of data encryption speed. In addition, decrypt it, see figure 3,figure 4.

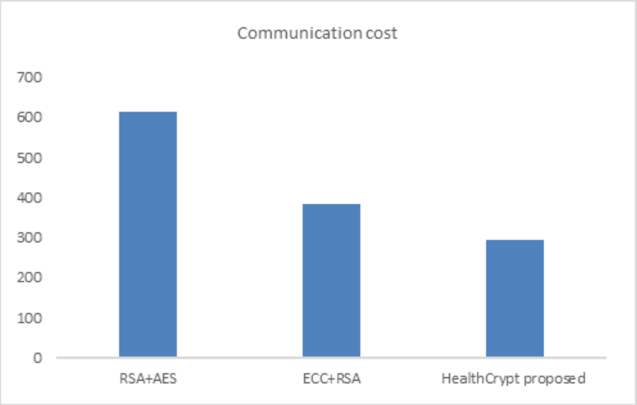


Fig 3 : Compare Communication cost

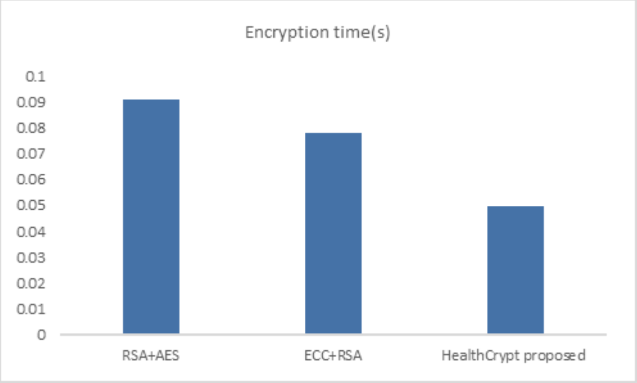


Fig 2 : Compare encryption time

9.2. Comparison communication cost

The results also indicate that the communication cost of the hybrid algorithm for this work is lower compared to previous studies, which means a lower data transfer rate per second, which may lead to faster transmission times, less bandwidth usage, and potentially reduced opportunities for interception or tampering ,see figure 5.

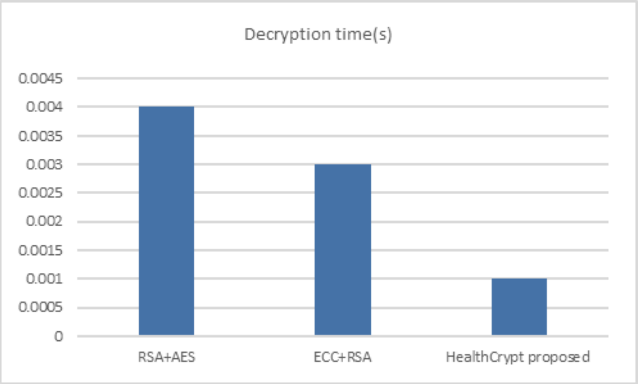


Fig 5 : Compare Decryption time(s)

Conclusion and Future Work

This paper has demonstrated the critical need for improved security and privacy protection in traditional and cloud-based electronic health systems. The study has addressed the security threats faced by EHRs stored in cloud systems, including data privacy, integrity, and confidence, by introducing SC2M-EHR-B proposed model , a new secure cloud computing model for electronic health records using blockchain technology.

This paper introduces SC2M-EHR-B proposed model , a secure cloud computing model for electronic health records (EHRs) using

blockchain technology. The SC2M-EHR-B model combines blockchain to secure and share medical records, enhancing security, and provide a patient control over their medical data, more over the model make use of the cloud computing to store medical records.

This paper also proposed a hybrid algorithm consisting of two(AES And Blowfish) algorithms to encrypt the electronic health record using blockchain. The performance of the hybrid algorithm was measured using the BlockSIM blockchain simulator, and the results showed better performance compared to previous studies. The results successfully demonstrates the effectiveness of the proposed model in and enhancing security , ensuring secure storage and sharing of medical records, at a lower communication cost .

The importance of this research lies in providing high-quality medical services, increasing patient confidence and satisfaction, and improving patients' ability to monitor their medical records.

As Future Work , a critical area for future work includes investigating the scalability and optimization of the SC2M-EHR-B model to handle large amounts of electronic health record (EHR) data as well as image data such as x-rays and other information from a variety of healthcare providers. The goal is to ensure that the system can efficiently manage and process comprehensive data sets.and real-world deployment evaluation testing the SC2M-EHR-B model in real-world healthcare settings is essential to evaluate its practical applicability and gather valuable feedback from stakeholders. Through partnerships with healthcare institutions, pilot programs will be launched to evaluate the system’s performance, ease of use, and impact on workflow.

These real-world deployments will provide important insights into the model's effectiveness and areas for improvement, ensuring that it meets the needs and expectations of healthcare providers and patients alike. A comprehensive cost-benefit analysis is critical to evaluate the economic feasibility of deploying the SC2M-EHR-B model on a large scale.

Recommendations

1. Provide comprehensive training to healthcare professionals and patients on using the SC2M-EHR-B system to maximize its benefits and ensure proper handling of EHRs.
2. Ensure that the SC2M-EHR-B model complies with relevant regulations and ethical standards, such as GDPR and HIPAA, to protect patient rights and data privacy.

By addressing future work areas and following the recommendations, the SC2M-EHR-B model can be further enhanced to provide a more secure, efficient, and user-friendly solution for managing electronic health records in cloud-based environments.

References

[1] J. Liu, X. Li, L. Ye, H. Zhang, X. Du, and M. Guizani, "BPDS: A blockchain based privacy-preserving data sharing for electronic medical records," in *2018 IEEE Global Communications Conference (GLOBECOM)*, 2018, pp. 1-6.

[2] S. Amofa, E. B. Sifah, O.-B. Kwame, S. Abla, Q. Xia, J. C. Gee, *et al.*, "A blockchain-based architecture framework for secure sharing of personal health data," in *2018 IEEE 20th International Conference on e-Health Networking, Applications and Services (Healthcom)*, 2018, pp. 1-6.

[3] N. Jothi and W. Husain, "Data mining in healthcare–a review," *Procedia computer science,* vol. 72, pp. 306-313, 2015.

[4] Y. Zhang, M. Chen, D. Huang, D. Wu, and Y. Li, "iDoctor: Personalized and professionalized medical recommendations based on hybrid matrix

factorization," *Future Generation Computer Systems*, vol. 66, pp. 30-35, 2017.

[5] X. Yue, H. Wang, D. Jin, M. Li, and W. Jiang, "Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control," *Journal of medical systems*, vol. 40, pp. 1-8, 2016.

[6] X. Liang, J. Zhao, S. Shetty, J. Liu, and D. Li, "Integrating blockchain for data sharing and collaboration in mobile healthcare applications," in *2017 IEEE 28th annual international symposium on personal, indoor, and mobile radio communications (PIMRC)*, 2017, pp. 1-5.

[7] A. Al Omar, M. S. Rahman, A. Basu, and S. Kiyomoto, "Medibchain: A blockchain based privacy preserving platform for healthcare data," in *International conference on security, privacy and anonymity in computation, communication and storage*, 2017, pp. 534-543.

[8] [8] A. F. Hussein, N. ArunKumar, G. Ramirez-Gonzalez, E. Abdulhay, J. M. R. Tavares, and V. H. C. de Albuquerque, "A medical records managing and securing blockchain based system supported by a genetic algorithm and discrete wavelet transform," *Cognitive Systems Research*, vol. 52, pp. 1-11, 2018.

[9] L. Zhu, Y. Wu, K. Gai, and K.-K. R. Choo, "Controllable and trustworthy blockchain-based cloud data management," *Future Generation Computer Systems*, vol. 91, pp. 527-535, 2019.

[10] Y. Sharma and B. Balamurugan, "A survey on privacy preserving methods of electronic medical record using blockchain," *Journal of Mechanics of Continua and Mathematical Sciences*, vol. 15, pp. 32-47, 2020.

[11] V. Mantzana, M. Themistocleous, Z. Irani, and V. Morabito, "Identifying healthcare actors involved in the adoption of information systems," *European Journal of Information Systems*, vol. 16, pp. 91-102, 2007.

[12] [12] P. K. Bollineni and K. Neupane, "Implications for adopting cloud computing in e-Health," ed, 2011.

[13] O.-S. Lupşe, M. M. Vida, and L. Stoicu-Tivadar, "Cloud computing and interoperability in healthcare information systems," in *INTELLI: The First International Conference on Intelligent Systems and Applications*, 2012.

[14] P. Mell and T. Grance, "The NIST definition of cloud computing," 2011.

[15] B. Pardamean and R. R. Rumanda, "Integrated model of cloud-based E-medical record for health care organizations," in *10th WSEAS international conference on e-activities*, 2011, pp. 157-162.

[16] A. S. Babrahem and M. M. Monowar, "Preserving confidentiality and privacy of the patient's EHR using the OrBAC and AES in cloud environment," *International Journal of Computers and Applications*, vol. 43, pp. 50-61, 2021.

[17] M. A. Zardari, L. T. Jung, and N. Zakaria, "K-NN classifier for data confidentiality in cloud computing," in *2014 International Conference on Computer and Information Sciences (ICCOINS)*, 2014, pp. 1-6.

[18] S. Tanwar, K. Parekh, and R. Evans, "Blockchain-based electronic healthcare record system for healthcare 4.0 applications," *Journal of Information Security and Applications*, vol. 50, p. 102407, 2020.

[19] G. C. Kessler, "An Overview of Cryptography (Updated Version 24 January 2019)," 2019.

[20] M. A. Engelhardt, "Hitching healthcare to the chain: An introduction to blockchain technology in the healthcare sector," *Technology Innovation Management Review*, vol. 7, 2017.

[21] I. Al Ridhawi, M. Aloqaily, Y. Kotb, Y. Al Ridhawi, and Y. Jararweh, "A collaborative mobile edge computing and user solution for service composition in 5G systems," *Transactions on Emerging Telecommunications Technologies*, vol. 29, p. e3446, 2018.

[22] T. Mikula and R. H. Jacobsen, "Identity and access management with blockchain in electronic healthcare records," in *2018 21st Euromicro conference on digital system design (DSD)*, 2018, pp. 699-706.

[23] A. G. M. Alzahrani, A. Alenezi, A. Mershed, H. Atlam, F. Mousa, and G. Wills, "A framework for data sharing between healthcare providers using blockchain," 2020.

[24] P. J. Taylor, T. Dargahi, A. Dehghantanha, R. M. Parizi, and K.-K. R. Choo, "A systematic literature review of blockchain cyber security," *Digital Communications and Networks*, vol. 6, pp. 147-156, 2020.

[25] D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne, "Blockchain for secure EHRs sharing of mobile cloud based e-health systems," *IEEE access*, vol. 7, pp. 66792-66806, 2019.

[26] A. Mubarakali, "Healthcare services monitoring in cloud using secure and robust healthcare-based BLOCKCHAIN (SRHB) approach," *Mobile Networks and Applications*, vol. 25, pp. 1330-1337, 2020.

[27] J. Tang, C. Huang, H. Liu, and N. Al-Nabhan, "Cloud Storage Strategy of Blockchain Based on Genetic Prediction Dynamic Files," *Electronics,* vol. 9, p. 398, 2020.

[28] P. Wei, D. Wang, Y. Zhao, S. K. S. Tyagi, and N. Kumar, "Blockchain data-based cloud data integrity protection mechanism," *Future Generation Computer Systems,* vol. 102, pp. 902-911, 2020.

[29] G. Verma, N. Pathak, and N. Sharma, "A Secure Framework for Health Record Management Using Blockchain in Cloud Environment," in *Journal of Physics: Conference Series*, 2021, p. 012019.

[30] N. Saravanan and A. Umamakeswari, "Lattice based access control for protecting user data in cloud environments with hybrid security," *Computers & Security,* vol. 100, p. 102074, 2021.

[31] B. Wang and Z. Li, "Healthchain: A privacy protection system for medical data based on blockchain," *Future Internet,* vol. 13, p. 247, 2021.

[32] T. Benil and J. Jasper, "Cloud based security on outsourcing using blockchain in E-health systems," *Computer Networks,* vol. 178, p. 107344, 2020.

[33] A. Al Omar, M. Z. A. Bhuiyan, A. Basu, S. Kiyomoto, and M. S. Rahman, "Privacy-friendly platform for healthcare data in cloud based on blockchain environment," *Future generation computer systems,* vol. 95, pp. 511-521, 2019.

[34] D. K. Murala, S. K. Panda, and S. K. Sahoo, "Securing electronic health record system in cloud environment using blockchain technology," in *Recent advances in blockchain technology: real-world applications*, ed: Springer, 2023, pp. 89-116.

[35] A. Kumari, V. Kumar, M. Y. Abbasi, S. Kumari, P. Chaudhary, and C.-M. Chen, "Csef: cloud-based secure and efficient framework for smart medical system using ecc," *IEEE Access,* vol. 8, pp. 107838-107852, 2020.

[36] M. Kim, S. Yu, J. Lee, Y. Park, and Y. Park, "Design of secure protocol for cloud-assisted electronic health record system using blockchain," *Sensors,* vol. 20, p. 2913, 2020.

[37] M. Mayuranathan, M. Murugan, and V. Dhanakoti, "Enhanced security in cloud applications using emerging blockchain security algorithm," *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, pp. 6933-6945, 2021.

[38] A. Gupta, S. Namasudra, and P. Kumar, "A secure VM Live migration technique in a cloud computing environment using blowfish and blockchain technology," 2024.

[39] F. Sammy and S. Vigila, "An Efficient Blockchain Based Data Access with Modified Hierarchical Attribute Access Structure with CP-ABE Using ECC Scheme for Patient Health Record," *Security and Communication Networks,* vol. 2022, 2022.