SCIENTIFIC CULTURE
www.sci-cult.com

SCIENTIFIC CULTURE, Vol. 12, No. 4, (2026), pp. 21-35
Open Access. Online & Print

DOI: 10.5281/zenodo. 12426103

ENHANCING SECURITY IN ELECTRONIC HEALTH RECORDS USING GENETIC ALGORITHM-DRIVEN BLOCKCHAIN ENCRYPTION

Ankita Srivastava[1]*, Shish Ahmad[2]

[1,2]Department of CSE, Integral University, Lucknow.

Received: 01/12/2025
Accepted: 02/01/2026

Corresponding author: Ankita Srivastava (ankita@iul.ac.in)

ABSTRACT

The safety of Electronic Health Records (EHRs) has risen to the forefront of healthcare providers' minds as they embrace the digital age. Security and privacy of EHRs have arisen as major problems in the quickly developing field of healthcare digitization. Innovative and strong solutions are required to overcome these obstacles. This study aims to present a fresh method for bolstering EHR security by employing Genetic Algorithm-Driven Blockchain Encryption (GADBE). The suggested method creates a dynamic and secure encryption strategy for EHRs by fusing the immutability and decentralized aspects of blockchain technology with the adaptive and optimization features of genetic algorithms. Extensive simulations and comparative analyses show that the GADBE approach is effective in addressing the critical challenges related to EHR security in modern healthcare systems, allowing for a high level of confidentiality, integrity, and access to electronic health records.

KEYWORDS: Electronic Health Records (EHRs), Security, Privacy, Blockchain Encryption, Genetic Algorithm, Healthcare Digitization, Integrity, Confidentiality.

1. INTRODUCTION

The formation of the healthcare sector was prompted by growing expenditure on chronic diseases, including cancer, diabetes, and hypertension, in both general and specialist medicine [1]. Electronic health records, or EHRs, are a digital representation of a patient's paper medical chart maintained by a healthcare provider throughout treatment [2]. These records contain information such as the patient's demographics, current symptoms, past medical history, current medications, vital signs, immunization records, laboratory results, and X-ray images. Because of the massive paper trail created by healthcare facilities and organizations' reliance on paper health records, several of these institutions are considering switching to electronic health records [3]. EHRs are superior to paper records in several ways, including cost savings, higher levels of patient satisfaction with their care, greater uptake of the best available medical research, and easier access to medical history. Complete data, resilience to failure, high availability, and security policy consistency are all necessary features of an effective electronic health record system [4]. For developing nations like India, which is experiencing rapid economic growth, the EHR System is an innovative new tool for medical records management. The EHR in a national health system connects all the hospitals using Electronic medical records (EMRs) from various networks. With the help of EHR, doctors and hospitals can easily communicate and organize patient information. Healthcare providers are high on hackers' hit lists because they store so much sensitive patient information [5].

EHRs are crucial because they allow doctors and other medical staff to view patient records at any time, from any location. It is recommended that a cloud-based strategy be incorporated by healthcare institutions into the adoption of EHR at all levels of the healthcare system so that patient data can be accessed in real-time and without restriction. Using a cloud-based electronic health record system facilitates communication between medical staff at various facilities regarding individual patients. The cloud benefits the healthcare ecosystem by facilitating communication between healthcare facilities and supporting institutions like laboratories, pharmacies, medical billing services, etc [6]. A cloud-enabled architecture, including capabilities for exchanging patient data without restriction across many geographical locations, is built based on an analysis of the current healthcare system in India, as seen in Figure 1.

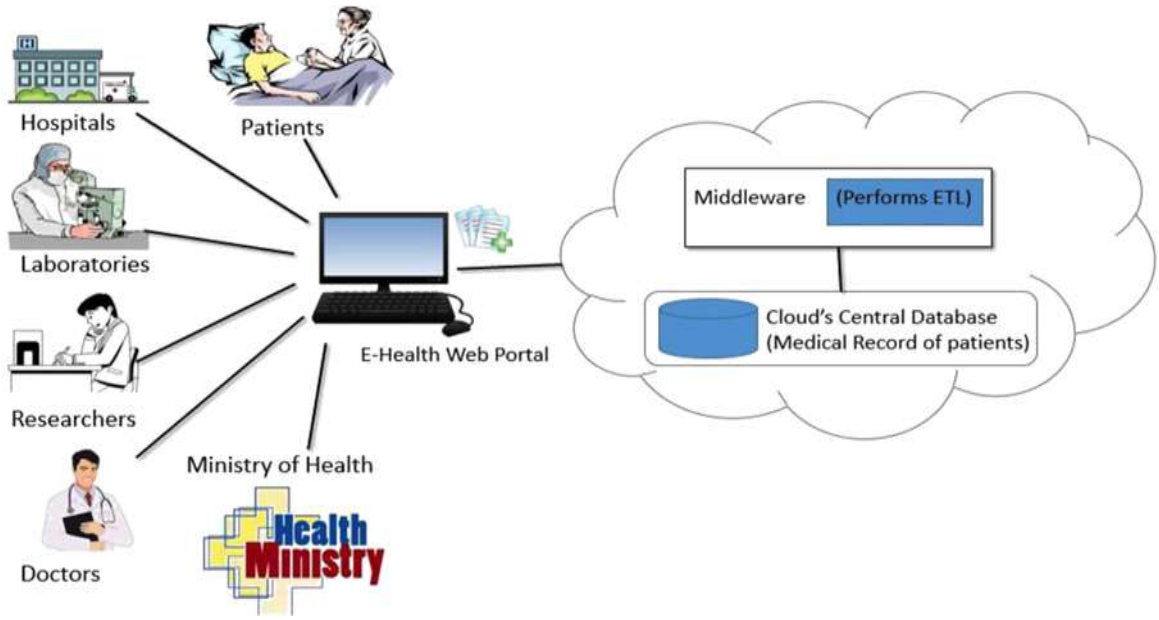

Figure 1: Architecture of Cloud-Based EHR System [7]

1.1. Security Framework in Electronic Health Records

The EHR system shown in Figure 2 [8] safeguards EHR data during its creation, storage, and maintenance phases. Developers of healthcare applications might benefit from its ability to guide them through a well-defined security procedure that helps them assess risks and devise solutions. The confidentiality, integrity, and security of the electronic health record system are guaranteed by the inclusion of security standards in the framework, such as administrative, physical, and technical safeguards [9].

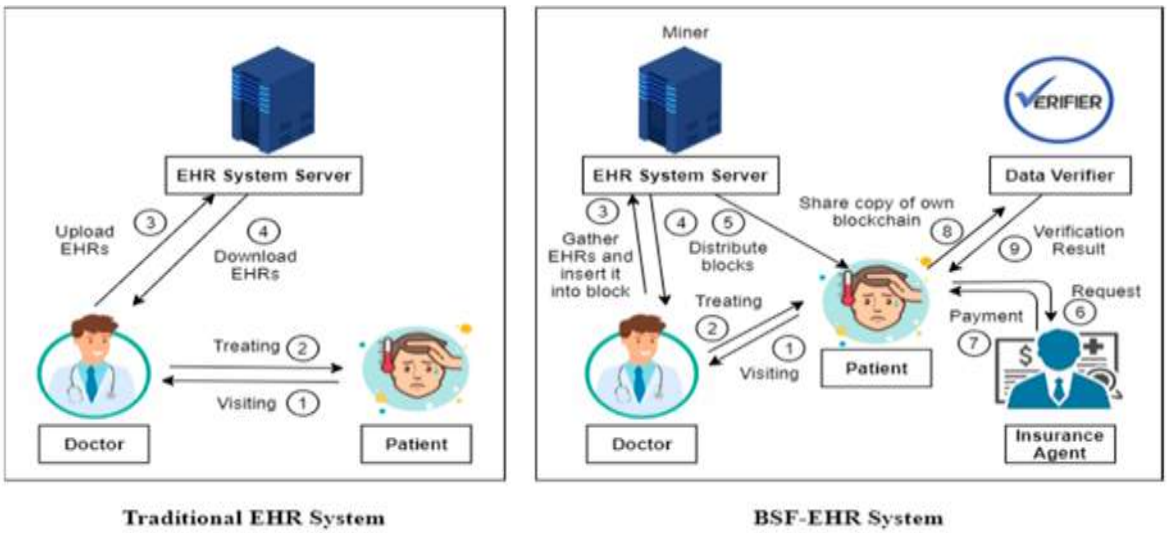

Figure 2: Block Chain Security Framework of EHR [8]

Since their inception, blockchains have been a fascinating topic for academic study, and many other sectors have begun to experience the benefits. Blockchain's security, privacy, confidentiality, and decentralization are all major selling points in the healthcare industry as well. However, EHR systems have issues with storage, management, and the security of patient data [10]. The adoption of blockchain technology to revamp EHR systems offers hope for resolving these problems. Data can be handled, communicated, saved, and displayed in a form that can be read by specialized software on the blockchain. In its initial form, a blockchain block would have a header, a timestamp, transaction data, and a reference to the prior Block [11]. The possible infrastructure for EHR blockchain adoption in the healthcare industry [12]. Blockchain is a decentralized database system that was born out of the world of digital currencies [13].

To ensure the safety of its network nodes, blockchain technology relies on cryptographic operations.

The hashes saved to the blocks are encrypted using the SHA-256 technique. These hashes, known as Secure Hashing Algorithm (SHA) hashes, protect the authenticity of data on the blockchain and, thus, its security. Strong one-way functions, known as cryptographic hashes, generate an unrecoverable checksum of digital data. Because of the cryptographic safeguards built into the blockchain, it is a viable alternative for use in applications where user privacy is paramount [14].

1.2. Challenges Faced by Blockchain Technology in HER

- Scalability and Storage Capacity: Two major issues arise when information is stored on the blockchain: privacy and scalability. The patient's medical history, records, lab results, X-ray reports, MRI reports, and many other reports would all be saved on the blockchain, and this massive amount of data would have a significant impact on the blockchain's storage capacity [15].
- Lack of Social Skills: Few individuals understand how blockchain technology operates. The development and refinement of this technology are ongoing processes. However, it will take some time for hospitals and other healthcare institutions to fully transition to blockchain technology from established EHR systems [16].
- Lack of Universally Defined Standards: Since this technology is continuously developing and changing rapidly, there is currently no accepted norm for it. The healthcare industry will need additional time and effort to fully deploy this technology due to the need for approved standards from the international bodies responsible for monitoring the standardization of all technologies [17].
- Infrastructure and Adoption: To facilitate blockchain's widespread use in healthcare, a need to build a solid infrastructure and work together across disciplines. Blockchain adoption could be slowed by the healthcare industry's historical reluctance to embrace new technologies [18].
- Technical Complexity: Implementing and maintaining a blockchain system calls for expert technical knowledge. Healthcare practitioners and administrators may lack the expertise essential to manage and debug blockchain systems successfully [19].

1.3. Security in Electronic Health Records Using Genetic Algorithm (GA)

In the broadest sense, EHRs are clinical information systems that gather, archive, and present electronic data in a longitudinal format during the provision of health care [20]. The majority of EHR usage at the user level is still concentrated on the billing process despite the widespread adoption of EHRs in hospitals and ambulatory care facilities. The primary purpose of most EHRs in the United States is billing, followed by clinical workflow and, increasingly, research [21]. The confidentiality and integrity of patient information make protecting EHRs a top priority in the healthcare industry. Due to the ever-changing nature of healthcare data and the ever-evolving nature of cyber threats, traditional encryption methods may not be able to keep up. This research suggests using GAs to increase EHR security and thereby address these issues. The goal of this study is to create a comprehensive solution for managing EHRs that uses GAs to optimize the trade-off between security and computing performance, considering evolving security needs. The study's novel methodology aids in the improvement of EHR security and further ensures the confidentiality of patient's medical records in today's increasingly digital healthcare system. Medical applications require efficient, safe, and adaptable access to healthcare resources. This makes it possible for devices with very dissimilar hardware and software features to communicate with one another in a way that is completely invisible to the user [22]. The diagnostic processes in healthcare revolve around medical pictures. They've given doctors a non-invasive way to see patients and assess their diagnosis and treatment progress by looking at cross-sections of organs, tissues, bone, and other features [23]. With the advancements in ICT, it is now common practice to do tele-diagnostics, -surgeries, and -consultations via the Internet. It is now crucial to protect sensitive patient information in medical photographs by ensuring their privacy, authenticity, and integrity [24].

There are many problems in this field. One of them is the technology known as cloud computing offers service assistance for the storing and analyzing of large amounts of data. The cloud is being used to store an increasing amount of data and apps, which enables access and exchange in real time. During the same period, a multitude of data protection and cloud data leaking vulnerabilities have been exposed. There are generally three significant trust hazards associated with using cloud computing platforms:

- Loss of control- Users that save their information, code, and processes in the cloud would no longer have control over such items once they have uploaded them to distant servers.
- Lack of transparency- Users of cloud computing has concerns about the manipulation of their privacy since they are unaware of the fundamental working mechanics of the service. This makes cloud computing seem to them like a black box.
- Lack of clear security assurance- Even though most cloud service providers publish their Service Level Agreements (SLAs), in which they seek to demonstrate a certain level of adherence to service dependability, security, and privacy, the definitions included in SLAs are usually ambiguous and general.

Hence, in this research, a novel model is designed for storing and managing healthcare data on cloud computing using blockchain technology and an optimized Genetic Algorithm (GA). The results that are obtained are quite promising. The following are the objectives of the research:

- Evaluate the effectiveness of encryption techniques in securing electronic medical data by comparing encryption methods based on strength, efficiency, and resistance to potential attacks.
- Enhance the security and integrity of medical data stored in a blockchain model through the implementation of advanced cryptographic algorithms.
- Investigate the scalability and performance of the proposed system for handling electronic medical data to assess its ability to manage increasing data access requests and storage requirements.

Assess the privacy and access control mechanisms of the proposed system, analyzing the effectiveness of authentication processes and access control measures to restrict access to authorized parties only.

2. RELATED WORK

This section presents a review of literature related to the topic of "Enhancing Security in Electronic Health Records using Genetic Algorithm-Driven Blockchain Encryption".

Hajian et al. (2023) [25] aimed to add to the existing body of knowledge by investigating the potential of blockchain to impact patients'

engagement with EHR systems. In addition, the endogeneity issues were tackled by employing a two-stage least-squares regression approach in this study. Both statistical and mathematical methods were used to arrive at these conclusions. The findings demonstrate how blockchain-based information systems might give patients more agency by giving them a sense of ownership over their medical records.

Chelladurai et al. (2022) [26] stated that the goal of developing smart contracts on the blockchain is to meet the regulated needs of patients, doctors, and healthcare providers. The suggested solution intends to construct a smart e-health system by exchanging health information over a blockchain network. The suggested system's results reveal that blockchain technology boosts throughput and speed, reduces latency in the network, and requires fewer resources.

Pang et al. (2022) [27] offered both attribute-based and multi-keyword encryption schemes for EHRs. To stop the Byzantine nodes from inserting themselves into the consortium blockchain, authors have created a Practical Byzantine Fault Tolerance consensus method (sc-PBFT) that can verify the status of each node. The experimental evidence demonstrates the superior handling capacity and decreased consensus delay of the proposed sc-PBFT method.

Kaur et al. (2021) [28] provided a framework for utilizing the Internet of Things (IoT) in e-health that is both secure and energy-efficient. The experimental results show that the proposed method is superior to the current best practices in picture encryption. For this reason, the suggested framework can be utilized to safeguard data transfer in environmentally friendly IoT networks by encrypting and decrypting images at a much faster rate.

Xiao et al. (2021) [29] introduce this study to improve model prediction accuracy. The authors propose mapping aspects of procedures, medications, and diagnoses from EHRs to Purified Protein Derivative (PPD) tensors and then training a convolutional neural network on those features. It is considered how these medical aspects interact with one another. Based on testing results, it appears to be able to greatly improve the efficiency of traditional machine learning-based models.

Parah et al. (2020) [30] stated a method of concealing EHRs in medical photos that is both computationally efficient and safe is described for use in an IoT-driven healthcare system. The system is predicated on modular arithmetic and the Pixel Repetition Method (PRM). Based on the results of the experiments, the suggested system can provide a secure and large embedding capacity while preserving reasonable imperceptibility.

Enaizan et al. (2020) [31] suggested an evaluation methodology for individual, security, and privacy factors that affect EMR adoption and use. The suggested paradigm is grounded in a multicriteria viewpoint developed with input from Malaysian healthcare experts. Findings from this study can aid makers of electronic medical record software by revealing areas of improvement.

Guo (2020) [32] provides a hybrid architecture that utilizes both blockchain and edge nodes to improve EHR administration. Specifically, the author deploys a multi-authority attribute-based encryption (ABE) strategy to protect EHR data at the edge node and an attribute-based multi-signature (ABMS) scheme to verify user signatures without disclosing private information. The results demonstrated that the signature and verification times are constant at roughly 32 ms and 243 ms, respectively, regardless of the attribute length.

Sun et al. (2020) [33] study reported that they developed a system for secure storing and effective distributing of electronic medical records in an IPFS storage environment using an attribute-based encryption system based on the ciphertext policy and blockchain technology. The selective security proof for the choice keyword attacks demonstrates that the technique is secure. The system is efficient and practical, as demonstrated by performance studies and simulated tests using real data sets.

Tith (2020) [34] creates a method for EHRs to readily share patient information without the need for a centralized monitoring system. Use a consortium blockchain built on Hyperledger Fabric to create a distributed system that incorporates preexisting. The EHR address book is stored on a shared ledger amongst peer nodes. The outcomes proved the system's viability, showing how doctors can access patient records and ensure they have their patients' permission to do so. Medical history from other facilities can be transferred to a patient without any fuss. For auditing purposes, the ledger stores the access log in a transparent and immutable format.

Nguyen et al. (2019) [35] presented a new framework for exchanging EHRs that utilizes blockchain technology and the distributed interplanetary file system (IPFS) in a mobile cloud environment. Build a reliable access control mechanism based on smart contracts to enable the safe exchange of EHRs between patients and their

respective healthcare providers. The empirical findings confirm that the idea offers a viable method for secure data transfers in mobile clouds, protecting personally identifiable health information from prying eyes. Lightweight access control design, low network latency, and high security and privacy levels are only some of how the current data-sharing models are shown to be outperformed by the system assessment and security analysis.

Chen et al. (2019) [36] suggested A searchable encryption system for electronic health records (EHRs) based on the blockchain. For a data user to search for EHRs, an index is built using complicated logic expressions and stored on the blockchain. The data owners retain complete control over who has access to their EHR data, as only the index is transferred to the blockchain to permit propagation. Evaluations of the proposed scheme's performance and security have indicated its viability and efficacy. The confidentiality of patient's health information and other personal details stored in EHRs is at risk if data leaks occur.

De Oliveira et al. (2019) [37] presented a blockchain-based method for securing EMR in healthcare applications with a focus on individual patients' sovereignty over their own data access. The plan encrypts EMRs in the blockchain, and the patient gives the decryption key only to reliable medical personnel. In a distributed peer-to-peer network, blockchain enables untrusted nodes to connect correctly and verifiably without the need for a trusted third party. Through simulations, researchers explore the scalability of the method. Since the quantity of the stored chain grows linearly with the total number of nodes within the network, the results suggest that it scales well. The results also show that, despite a rise in the total number of nodes, the time required to add a new EMR to the blockchain is surprisingly constant.

Ying et al. (2018) [38] stated that the study is based on the proposal on CP-ABE to preserve the EHR system. The authors developed an algorithm that conceals the complete access policy and then recovers the concealed characteristics via the access matrix. The system was able to preserve policies and restore attributes with minimal overhead, as demonstrated by the evaluation results.

Ramani et al. (2018) [39] provide a method for patients and healthcare providers to share data using easily and safely blockchain technology. The proposed method is secure enough to safeguard patients' personal information as well. The security research demonstrates that the method not only protects the system from common assaults but also prevents those attempts from succeeding. In addition, the suggested system's viability has been tested using an Ethereum-based implementation.

3. RESEARCH METHODOLOGY

The concept of designed architecture is examined in the context of research methodology. Initially, the electronic medical records are transformed into cipher text using GA. Then, the cipher text was chunked and stored in the Block and formed a blockchain model. Whenever a doctor or a patient sends a request to access the data, the authentication process is performed in which the public key of the doctor/ patient is verified, and if the identity is successfully verified, then the encrypted text is read and decrypted using the private key, and finally, the machine learning model is applied for the classification of the data, and then performance evaluation is performed for evaluating the performance of the designed architecture.

3.1. Techniques Used

In this section, various techniques are discussed which are used in the designing of the proposed architecture.

3.1.1. Blockchain

Understanding a blockchain is like understanding state machines. In this design, a service oversees maintaining a certain state while clients perform operations to modify that state and provide results. A blockchain might mimic a "trusted" computing service by using a decentralized protocol maintained by nodes linked across the Internet. Each node has a vested interest in the output of the service, which it either generates or represents [40].

All the nodes want to keep the service running, but they don't have complete confidence in one another to do so. A permissionless blockchain, such as the one that underpins the Bitcoin cryptocurrency, allows anybody to run a node and join the network by providing proof of work and spending computing resources. A public blockchain is open to the public. Moreover, permissioned blockchains can employ their authentication and protocol, and they frequently function as a consortium with established identities. Blockchains that function under the public paradigm is unable to wield this control [41]. Figure 3 shows the workings of the blockchain.

Using a GADBE system, blockchain technology can be used to improve the security of EHRs. The following scenarios call for this strategy: Immutable Tamper Resistant, Data Privacy, and Genetic Algorithm-Driven Encryption.

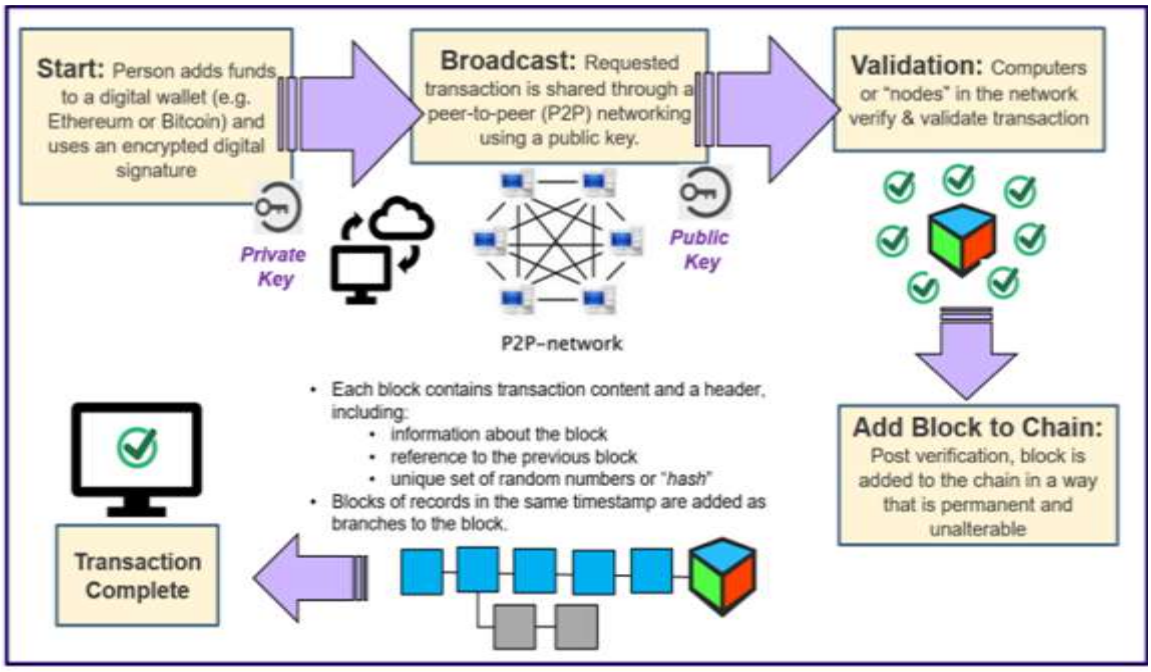

Figure 3: Working on Blockchain [42]

The following scenarios call for this strategy:

- Immutable Tamper Resistant: There can be no changes made to blockchain data. The impossibility of tampering with or erasing data stored on a blockchain protects the accuracy of patient medical records. This is especially important in healthcare, where the repercussions of tampering with patient records could be devastating.
- Data Privacy: In terms of data privacy and security, blockchain can be configured to meet a variety of needs. By using encryption and permission-based systems, authors may restrict access to health records and ensure that only authorized individuals or organizations have access to private patient information.
- Genetic Algorithm-Driven Encryption: Encryption methods can be optimized with genetic algorithms for specific criteria like data safety and computing efficiency. As a result, it can be assured that the system employs a secure encryption method appropriate for medical records.

Blockchain technology is based on a digital ledger or record of transactions that is maintained by itself rather than by any one person or group. This decentralized database maintains track of a growing list of data blocks that are all cryptographically linked. Depending on the contest regulations, each of these pieces might be considered a distinct submission [43].

3.1.2. Hyperledger

Hyperledger Fabric is a blockchain platform designed for enterprises. It is a private network that only those with access to it may use. A user-defined smart contract might be run on its modular structure, which includes pluggable consensus mechanisms. There are also full security and authentication solutions available. Their basis is built on open-source software and industry-recognized standards. To promote blockchain technology, which has the potential to transform worldwide corporate operations, an open system architecture for distributed ledgers that can be utilized across sectors is being sought after and deployed [44].

The use of Hyperledger technology to increase the safety of Electronic Health Records (EHR) using Genetic Algorithm-Driven Blockchain Encryption provides several benefits and solves certain problems plaguing the healthcare sector:

i. Decentralization: Hyperledger offers a distributed and decentralized framework. This is critical in the healthcare industry since it removes a potential vulnerability and safeguards sensitive information. Because every node in a network has a copy of the full blockchain, there is redundancy and resistance to attacks.
ii. Interoperability: Hyperledger facilitates the sharing of data between various medical networks. This is crucial for EHR since it facilitates the safe transfer of information between various healthcare organizations without jeopardizing the accuracy of the data.
iii. Data Privacy and Security: Hyperledger is a widely used open-source blockchain platform with a stellar reputation for safety. Hyperledger's use in EHR systems helps guarantee that sensitive patient information is kept safely out of

the wrong hands. The blockchain's immutability guarantees that information cannot be altered after it has been recorded, offering a robust safeguard against manipulation.

The Linux Foundation's goal with the Hyperledger platform is to create a network in which commercial and corporate members collaborate on the development of blockchain infrastructure for use in global, real-time applications [45]. Features of Hyperledger are shown in Figure 4.

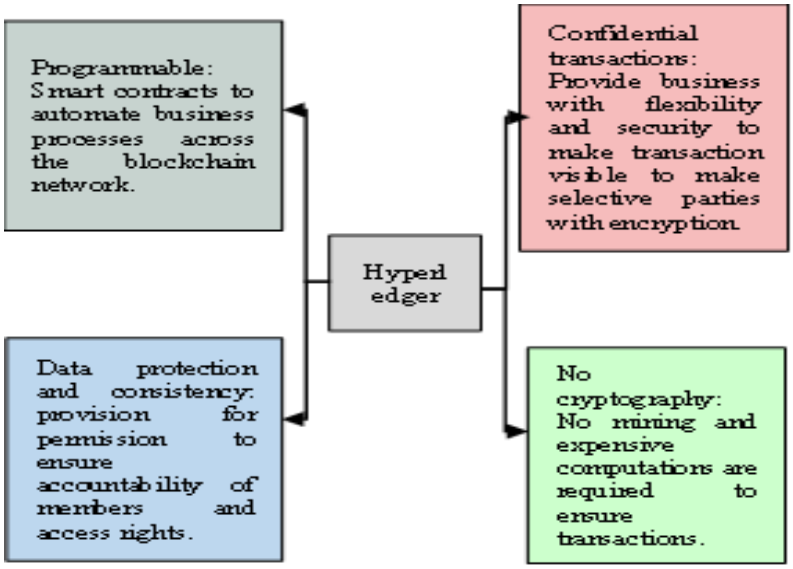

Figure 4: Hyperledger-based Enterprise Solutions [45]

For a transaction to be processed on a platform that employs hyperledgers, the nodes must be able to communicate with one another securely and update their ledgers independently [46]. No information other than the amount transferred is available to a third party during a trade.

3.1.3. Genetic Algorithm (GA)

The term "block encryption" refers to the method by which equal-sized chunks of the input text are encrypted using a random selection mechanism. The length of the blocks is determined by the chosen length of the secret key, which in turn is determined by the selection of the secret key. Before beginning the encryption process, the client is given the option of selecting a key length size. This option controls how encryption keys are generated and how blocks are encrypted. In the absence of a user-specified key length size, a value determined by the parameters is used [47].

The usage of a GA in combination with blockchain encryption to increase the safety of EHRs is a prime example of the potent combination of these two technologies. The use of GAs to improve EHR security using blockchain encryption involves several important considerations. Using the principles of natural selection as a model, GAs can optimize many encryption parameters, including key length, encryption algorithms, and settings, to strike a fine balance between security and performance [48]. By using GAs for key generation and administration, a new dynamic paradigm is introduced in which encryption keys evolve, making them more secure and resistant to attacks such as brute force. The overall safety of EHRs is improved by this method.

Furthermore, GAs can improve blockchain transaction security by improving the transaction validation process, creating efficient consensus algorithms, and maintaining the blockchain's integrity and reliability to prevent tampering. Network intrusion detection systems built using GAs can learn and adapt to spot unusual activity on a network, protecting sensitive EHR data from prying eyes. In addition to improving the blockchain network's security, scalability, and efficiency, GAs can also be used to optimize consensus mechanisms, block validation algorithms, and network protocols, which further strengthens the network's ability to protect EHR data.

As soon as the key length is established, the plaintext is transformed into binary and split into two halves, the right and left sides. Then, the local information-based method is used to produce the Encryption Key. Finally, the binary representation of the text is ciphered using the encryption key and GA operators. The ciphertext is created by recombining all the encrypted blocks. The steps in this procedure are as follows [49]:

Start

1. Input text
2. Optimal Key Size for Encryption.
3. Limiting the size of the Block to the length of the Encryption Key.
4. Change Text to Binary.

- Letters in plaintext are translated into their corresponding ASCII codes.
- Conversion into binary values of corresponding ASCII values utilizing the division remainder method.

5. Separate the binary code into two halves.
6. Create a key for encryption.
7. With the Encryption key created in Step 6, combine the Right half generated in Step 5.
8. Use Genetic Algorithm operators on the combined result from the previous stage.
9. Combine this with the left side, which is made in Step 5.
10. Ciphertext is the result.

End

Cryptographic hash functions are the source of the SHA definition. The suggested technique employs the robust SHA-384 in conjunction with the 384-bit block cipher algorithm, in which the intermediary hash value is encrypted utilizing a message block with a key obtained using the GA [50]. The hash function takes in the Block, and the keys, and the most recent hash value is tied to the one before it in a chain [51].

3.2. Proposed Methodology

Figure 5 shows the designed architecture of the proposed model.

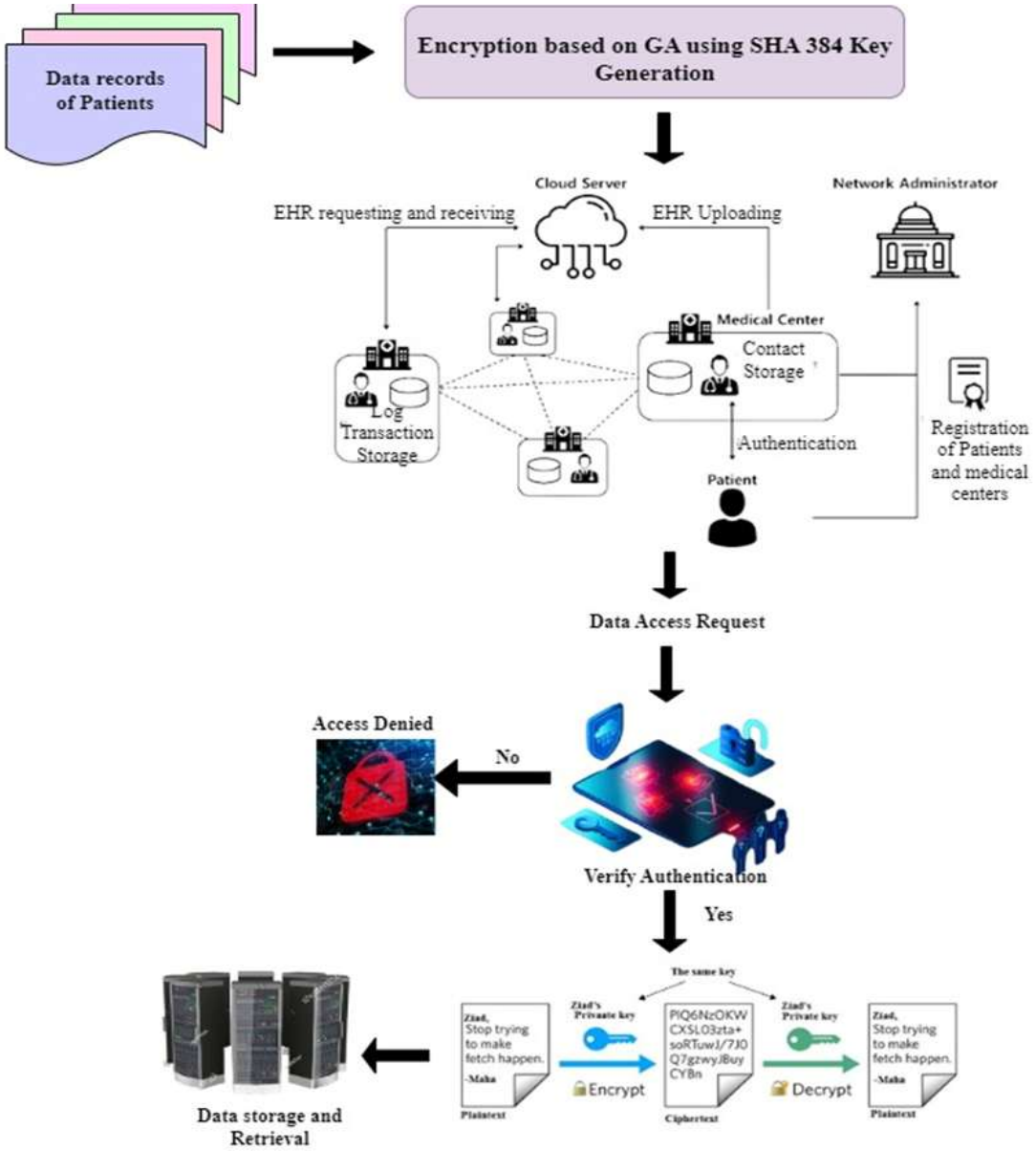

Figure 5: Designed architecture of the proposed framework

3.3. Proposed Algorithm

Start

Input:

Step 1: Data encryption for patients' electronic health records

- Assume D represents a patient's electronic medical records.
- Let it denote by E(D) the encrypted version of D, generated using a secure encryption technique.
- Put E(D) in a secured place.

Step 2: Apply the Genetic Algorithm and SHA-384 for EHR data encryption.

Genetic Algorithm Loop:

- Generate the initial population using `generate_population`.
- Iterate through a specified number of generations (`num_generations`).
- In each generation, evaluate the fitness of everyone using the fitness function.
- Select the fittest individuals (F1, F2……. Fn) for reproduction using the selection function.
- Create new child individuals (N1, N2……. Nn) through crossover and mutation.
- Replace the old population with the new population.
- Repeat the process for the specified number of generations.
- Return Fittest Individual (F):
- After all, generations are processed
- Select the fittest individual (F) from the final population based on the fitness score calculated by the fitness function.

Pass the Fittest Individual (F) to SHA-384:

- Convert the fittest individual to a string representation using `str(token)`.
- Encode the string as bytes using the UTF-8 encoding (`encode('utf-8') `).
- Compute the SHA-384 hash of the bytes using the `sha384` function from the hashlib module.
- Get the hexadecimal representation of the hash using `hexdigest () ` as the key.

Step 3: Implement the Blockchain EHR system.

- Key encryption Elliptic Curve Integrated Encryption Scheme using the recipient's public key.
- Create a new block and include the encrypted key and any other necessary information.
- Include the verified Block in the Blockchain ledger.

Step 4: Data access request, verification, and authorization

- Consider the request to be the user's request to access the data. Allow the user to be the logged-in user.
- Go on to the subsequent stage.

Output:

Step 5: Verification of Authentic Person by Various Factors of Authentication

- If any of the authentication Factors fail, terminate the algorithm.

Step 6: Assuming the user is legitimate, decrypt the record.

- Find the user's encrypted medical file and read it.

Step 7: Information can be stored and retrieved.

- Give the user a safe place to save and handle decrypted Data.
- Allow users with varying degrees of access to search for and get the appropriate medical records.

End

4. RESULT AND DISCUSSION

To evaluate the effectiveness of the EHRs sharing model with the anticipated access restriction, the author provides two use cases: one with allowed access and one without. The framework's purpose is to prevent unauthorized users from accessing the cloud-stored EHRs while facilitating quick and easy retrieval by authorized users (such as medical staff).

4.1. Signup Page

The intuitive program makes it possible for anyone, even doctors who wish to access their patients' cloud-based electronic health information, to create an Ethereum account and register with their information to interact with the blockchain (see Figure 6).

Figure 6: Signup Page

4.2. EHRs access results of an authorized user

Once the cloud EHR administrator approves his request, he will launch a transaction to gain access to the EHRs by providing the patient's address, which will include the AreaID and PatientID, as shown in Figure 7.

Figure 7: Detail Entry

The results of data access would subsequently be made available on the EHR system's interface (Figure 7), which would be regularly updated. The doctor is then able to examine the patient with all their medical history at their fingertips and provide the best care possible. The cloud miner will now append the EHR access method to the blockchain, making it visible to all parties involved in the network.

4.3. Transaction record of authorized EHR access (see Figure 8


```
{
  "PID": "706",
  "Pregnancies": "1",
  "Glucose": "1",
  "BloodPressure": "1",
  "SkinThickness": "1",
  "Insulin": "1",
  "BMI": "1",
  "DiabetesPedigreeFunction": "1",
  "Age": "1",
  "Outcome": "1",
  "prev_block": {
    "hash": "5e9f4e9a6bd76aae57b432804495590f",
    "filename": "40"
  }
}
```


Figure 8: Transaction record of authorized EHR access

4.4. EHRs access results of an unauthorized user

To establish if an unauthorized user has gained access, the smart contract will consult the access protocol's built-in policy list. Unauthorized requests of this nature are immediately blocked, and the offending records are deleted from the EHRs database; the requester is then notified via a warning notice (see Figure 9).

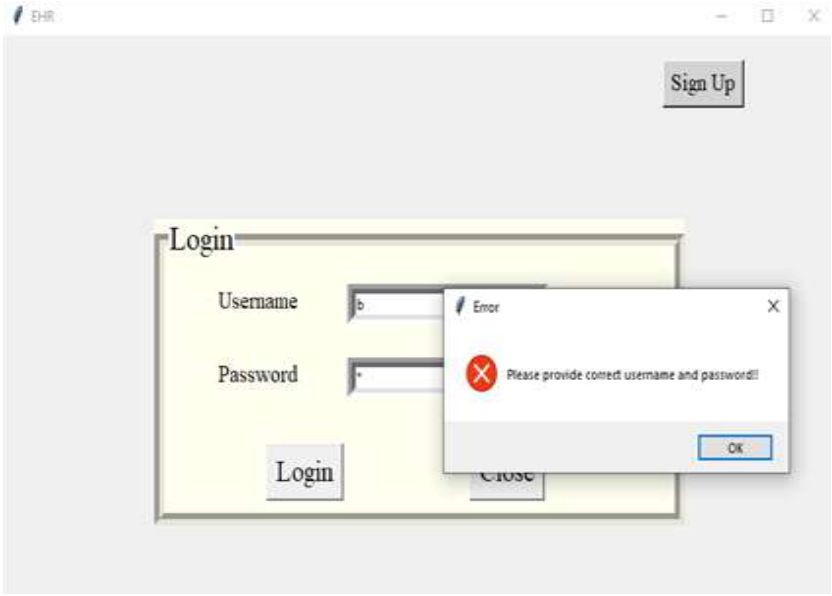

Figure 9: Unwanted access

4.5. Transaction record of unauthorized EHR access (see Figure 10) user

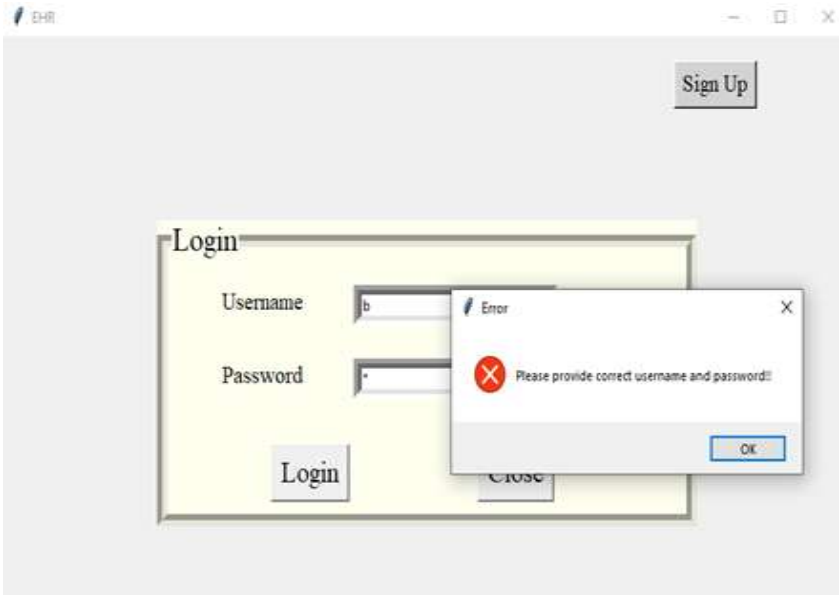

Figure 10: Transaction record of unauthorized EHR access

4.6. Comparison Analysis

Table I demonstrates the model's viability in real-world usability settings; here describes and evaluates the proposed EHRs sharing system using several performance measures.

Table 1: The model's viability in real-world.

Features	Ying et al., [50]	Ramani et al., [51]	HER Sharing System
Flexibility	N	N	Y
Availability	N	N	Y
Decentralized Access	N	Y	Y
Identity Management	Y	N	Y
User Authentication	Y	Y	Y
Integrity	Y	Y	Y
Data privacy	Y	Y	Y

5. CONCLUSION

In conclusion, there is significant potential in using a Genetic Algorithm-Driven Blockchain Encryption system to increase the safety of EHR. The results demonstrated the efficiency of the proposed strategy in maintaining confidentiality, trustworthiness, and simplicity of access to EHR data, which was emphasized in the introduction. Future steps in this investigation include perfecting the genetic algorithm for optimizing encryption processes, delving into other cryptographic methods, and designing a friendly interface so that this solution can be easily integrated into healthcare infrastructure. In addition to improving EHR security, expanding the framework to include cutting-edge technologies like the Internet of Things (IoT) and artificial intelligence-based analytics creates the basis for a more complete and effective healthcare ecosystem.

REFERENCES

Faisal, M., Sadia, H., Ahmed, T., & Javed, N. (2022). Blockchain technology for healthcare record management. In *Pervasive healthcare: A compendium of critical factors for success* (pp. 255–286).

Keshta, I., & Odeh, A. (2021). Security and privacy of electronic health records: Concerns and challenges. *Egyptian Informatics Journal, 22*(2), 177–183.

Carey, D. J., Fetterolf, S. N., Davis, F. D., Faucett, W. A., Kirchner, H. L., Mirshahi, U., Murray, M. F., Smelser, D. T., Gerhard, G. S., & Ledbetter, D. H. (2016). The Geisinger MyCode community health initiative: An electronic health record–linked biobank for precision medicine research. *Genetics in Medicine, 18*(9), 906–913.

Allard, T., Anciaux, N., Bouganim, L., Guo, Y., Le Folgoc, L., Nguyen, B., Pucheral, P., Ray, I., Ray, I., & Yin, S. (2010). Secure personal data servers: A vision paper. *The VLDB Journal, 3*(1–2), 25–35.

Ganiga, R., Pai, R. M., & Sinha, R. K. (2020). Security framework for cloud-based electronic health record (EHR) system. *International Journal of Electrical and Computer Engineering, 10*(1), 455.

Sindhu, C. S., & Hegde, N. P. (2017). A novel integrated framework to ensure better data quality in big data analytics over cloud environment. *International Journal of Electrical & Computer Engineering, 7*(5).

Sarwar, M. A., Bashir, T., Shahzad, O., & Abbas, A. (2019). Cloud-based architecture to implement electronic health record (EHR) system in Pakistan. *IT Professional, 21*(3), 49–54.

Abunadi, I., & Kumar, R. L. (2021). BSF-EHR: Blockchain security framework for electronic health records of patients. *Sensors, 21*(8), 2865.

Azeez, N. A., & Van der Vyver, C. (2019). Security and privacy issues in e-health cloud-based system: A comprehensive content analysis. *Egyptian Informatics Journal, 20*(2), 97–108.

Shi, S., He, D., Li, L., Kumar, N., Khan, M. K., & Choo, K.-K. R. (2020). Applications of blockchain in ensuring the security and privacy of electronic health record systems: A survey. *Computers & Security, 97*, 101966.

Anwar, M. R., Apriani, D., & Adianita, I. R. (2021). Hash algorithm in verification of certificate data integrity and security. *Aptisi Transactions on Technopreneurship, 3*(2), 181–188.

Shahnaz, A., Qamar, U., & Khalid, A. (2019). Using blockchain for electronic health records. *IEEE Access, 7*, 147782–147795.

Credit, M., & Fischer, M. (2019). Blockchain and more—Algorithm driven food traceability. *Food Control, 105*, 45–51.

Gordon, W. J., & Catalini, C. (2018). Blockchain technology for healthcare: Facilitating the transition to patient-driven interoperability. *Computational and Structural Biotechnology Journal, 16*, 224–230.

Pirtle, C., & Ehrenfeld, J. (2018). Blockchain for healthcare: The next generation of medical records? *Journal of Medical Systems, 42*(9), 172.

Kumar, N. M., & Mallick, P. K. (2018). Blockchain technology for security issues and challenges in IoT. *Procedia Computer Science, 132*, 1815–1823.

Siyal, A. A., Junejo, A. Z., Zawish, M., Ahmed, K., Khalil, A., & Soursou, G. (2019). Applications of blockchain technology in medicine and healthcare: Challenges and future perspectives. *Cryptography, 3*(1), 3.

Eberhardt, J., & Tai, S. (2017). On or off the blockchain? Insights on off-chaining computation and data. In *Service-oriented and cloud computing* (pp. 3–15). Springer.

Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). An overview of blockchain technology: Architecture, consensus, and future trends. In *2017 IEEE International Congress on Big Data* (pp. 557–564). IEEE.

Cowie, M. R., Blomster, J. I., Curtis, L. H., Duclaux, S., Ford, I., Fritz, F., Goldman, S., et al. (2017). Electronic health records to facilitate clinical research. *Clinical Research in Cardiology, 106*, 1–9.

Kim, E., Rubinstein, S. M., Nead, K. T., Wojcieszynski, A. P., Gabriel, P. E., & Warner, J. L. (2019). The evolving use of electronic health records (EHR) for research. *Seminars in Radiation Oncology, 29*(4), 354–361.

Castiglione, A., Pizzolante, R., De Santis, A., Carpentieri, B., Castiglione, A., & Palmieri, F. (2015). Cloud-based adaptive compression and secure management services for 3D healthcare data. *Future Generation Computer Systems, 43*, 120–134.

Cao, F., Huang, H. K., & Zhou, X. Q. (2003). Medical image security in a HIPAA mandated PACS environment. *Computerized Medical Imaging and Graphics, 27*(2–3), 185–196.

Al-Husainy, M. A. F. (2012). A novel encryption method for image security. *International Journal of Security and Its Applications, 6*(1), 1–8.

Hajian, A., Prybutok, V. R., & Chang, H.-C. (2023). An empirical study for blockchain-based information sharing systems in electronic health records: A mediation perspective. *Computers in Human Behavior, 138*, 107471.

Chelladurai, U., & Pandian, S. (2022). A novel blockchain-based electronic health record automation system for healthcare. *Journal of Ambient Intelligence and Humanized Computing*, 1–11.

Pang, Z., Yao, Y., Li, Q., Zhang, X., & Zhang, J. (2022). Electronic health records sharing model based on blockchain with checkable state PBFT consensus algorithm. *IEEE Access, 10*, 87803–87815.

Kaur, M., Singh, D., Kumar, V., Gupta, B. B., & Abd El-Latif, A. A. (2021). Secure and energy efficient-based e-health care framework for green internet of things. *IEEE Transactions on Green Communications and Networking, 5*(3), 1223–1231.

Xiao, X., Wei, G., Zhou, L., Pan, Y., Jing, H., Zhao, E., & Yuan, Y. (2021). Treatment initiation prediction by EHR mapped PPD tensor based convolutional neural networks boosting algorithm. *Journal of Biomedical Informatics, 120*, 103840.

Parah, S. A., Sheikh, J. A., Akhoon, J. A., & Loan, N. A. (2020). Electronic health record hiding in images for smart city applications. *Future Generation Computer Systems, 108*, 935–949.

Enaizan, O., Zaidan, A. A., Alwi, N. H. M., Zaidan, B. B., Alsalem, M. A., Albahri, O. S., & Albahri, A. S. (2020). Electronic medical record systems. *Health and Technology, 10*, 795–822.

Guo, H., Li, W., Meamari, E., Shen, C.-C., & Nejad, M. (2020). Attribute-based multi-signature and encryption for EHR management. In *2020 IEEE International Conference on Blockchain and Cryptocurrency* (pp. 1–5). IEEE.

Sun, J., Yao, X., Wang, S., & Wu, Y. (2020). Blockchain-based secure storage and access scheme for electronic medical records in IPFS. *IEEE Access, 8*, 59389–59401.

Tith, D., Lee, J.-S., Suzuki, H., Wijesundara, W. M. A. B., Taira, N., Obi, T., & Ohyama, N. (2020). Application of blockchain to maintaining patient records in electronic health record. *Healthcare Informatics Research, 26*(1), 3–12.

Nguyen, D. C., Pathirana, P. N., Ding, M., & Seneviratne, A. (2019). Blockchain for secure EHRs sharing of mobile cloud-based e-health systems. *IEEE Access, 7*, 66792–66806.

Chen, L., Lee, W.-K., Chang, C.-C., Choo, K.-K. R., & Zhang, N. (2019). Blockchain-based searchable encryption for electronic health record sharing. *Future Generation Computer Systems, 95*, 420–429.

De Oliveira, M. T., Reis, L. H. A., Carrano, R. C., Seixas, F. L., Saade, D. C. M., Albuquerque, C. V., Fernandes, N. C., Olabarriaga, S. D., Medeiros, D. S. V., & Mattos, D. M. F. (2019). Towards a blockchain-based secure electronic medical record. In *IEEE International Conference on Communications* (pp. 1–6). IEEE.

Ying, Z., Wei, L., Li, Q., Liu, X., & Cui, J. (2018). A lightweight policy preserving EHR sharing scheme in the cloud. *IEEE Access, 6*, 53698–53708.

Ramani, V., Kumar, T., Bracken, A., Liyanage, M., & Ylianttila, M. (2018). Secure and efficient data accessibility in blockchain-based healthcare systems. In *IEEE GLOBECOM* (pp. 206–212). IEEE.

Swanson, T. (2015). *Consensus-as-a-service: A brief report on the emergence of permissioned, distributed ledger systems*.

Jones, K. L. (2019). Blockchain: Building consensus and trust across the space sector. In *35th Space Symposium* (pp. 1–19).

Chen, Y., Xie, H., Lv, K., Wei, S., & Hu, C. (2019). DEPLEST: A blockchain-based privacy-preserving distributed database. *Information Sciences, 501*, 100–117.

Cachin, C. (2016). Architecture of the Hyperledger blockchain fabric. In *Workshop on Distributed Cryptocurrencies and Consensus Ledgers* (pp. 1–4).

Aggarwal, S., & Kumar, N. (2021). Hyperledger. In *Advances in Computers* (Vol. 121, pp. 323–343). Elsevier.

Arshad, M. J., Umair, M., Munawar, S., Naveed, N., & Naeem, H. (2020). Improving cloud data encryption using customized genetic algorithm. *International Journal of Intelligent Systems and Applications, 12*(6), 46–55.

Pham, V.-T.-N., Nguyen, Q.-C., Nguyen, V.-T.-T., Ho, T.-P., & Nguyen, Q.-V. (2023). Blockchain solution for electronic health records using Hyperledger Fabric. In *Conference on Information Technology and Its*

Applications (pp. 380–390). Springer.

Myint, S. M., Myint, M. M., & Cho, A. A. (2019). A study of SHA algorithm in cryptography. *International Journal of Trend in Scientific Research and Development, 3*, 1453–1454.

Pan, Y., Yang, Y., & Li, W. (2021). A deep learning trained by genetic algorithm to improve the efficiency of path planning. *IEEE Access, 9*, 7994–8005.

Denis, R., & Madhubala, P. (2021). Hybrid data encryption model integrating multi-objective adaptive genetic algorithm. *Multimedia Tools and Applications, 80*, 21165–21202.

Karatsiolis, S., & Schizas, C. N. (2012). Region based support vector machine algorithm for medical diagnosis. In *IEEE International Conference on Bioinformatics & Bioengineering* (pp. 139–144). IEEE.

Sathyadevan, S., & Nair, R. R. (2015). Comparative analysis of decision tree algorithms. In *Computational intelligence in data mining* (pp. 549–562). Springer.