[1]Ankita Srivastava
[2] Shish Ahmad

Performance Evaluation of Genetic Algorithm-Driven Blockchain Encryption for EHR Management and Validation

Journal of Electrical Systems

Abstract: - In the realm of electronic health record (EHR) management, ensuring robust security and validation mechanisms is paramount due to the sensitive nature of healthcare data. This research focuses on the performance evaluation of a genetic algorithm-driven blockchain encryption approach for enhancing EHR security and validation. The proposed method leverages genetic algorithms to optimize encryption parameters within a blockchain framework, aiming to safeguard patient privacy and prevent unauthorized access. By integrating advanced cryptographic techniques like Elliptic Curve Cryptography (ECC) and Keyed-Hash Message Authentication Code (HMAC)-based authentication, along with machine learning for data classification. The evaluation of the approach holds significant promise in advancing secure EHR management practices, addressing critical challenges in data privacy and integrity within healthcare environments. Finally, as a result, this study presents a comparative analysis of cryptographic systems genetic algorithm-driven blockchain encryption (GADBE)+ECC and GADBE+ Advanced Encryption Standard (AES), focusing on the scaling of encryption and decryption times relative to key sizes and data volumes. Results show that both systems exhibit increasing times with larger key sizes and data sizes. ECC consistently demonstrates superior speed over AES, with decryption times ranging from 0.4 to 3.5 seconds for key sizes from 128 to 512 bits, indicating potential performance advantages of ECC in cryptographic applications.

Keywords: Genetic Algorithm, Blockchain, electronic health records (EHRs) Management, Encryption, Security, Health care.

I. INTRODUCTION

In the modern era, effectively managing and securing electronic health records (EHRs) presents substantial challenges due to the sensitive nature of healthcare data [1][2]. As healthcare organizations transition towards digital systems for managing patient information, the importance of implementing strong encryption measures cannot be overstated [3-5]. Robust encryption techniques are essential to protect patient privacy and to mitigate the risk of unauthorized access or data breaches [6][7]. Ensuring the confidentiality of EHRs is crucial not only for maintaining patient trust but also for complying with stringent healthcare regulations designed to safeguard sensitive medical information [8][9].

The increasing adoption of electronic platforms in healthcare underscores the urgent need for advanced encryption methods tailored specifically for EHR management [10][11]. Healthcare data is highly valuable and susceptible to cyber threats, making encryption a fundamental component of secure information management practices [12][13]. By addressing the unique security challenges associated with EHRs through effective encryption strategies, healthcare organizations could enhance data protection, minimize risks, and uphold the integrity of patient records in an increasingly digital healthcare landscape [14-16]. For handling all these challenges Genetic Algorithms and blockchain technologies can enhance EHR management and validation by providing a secure, decentralized, and immutable platform. Through blockchain, EHR data can be encrypted, stored, and shared securely among authorized parties, ensuring data integrity and privacy. Smart contracts can automate validation processes, improving efficiency and transparency in healthcare data management. Figure 1 illustrates the robustness of the blockchain-enabled system for managing Electronic Health Records (EHR).

[1] *Corresponding author: Department of Computer Science & Engineering, Integral University, ankita@iul.ac.in
[2] Department of Computer Science & Engineering, Integral University, shish@iul.ac.in

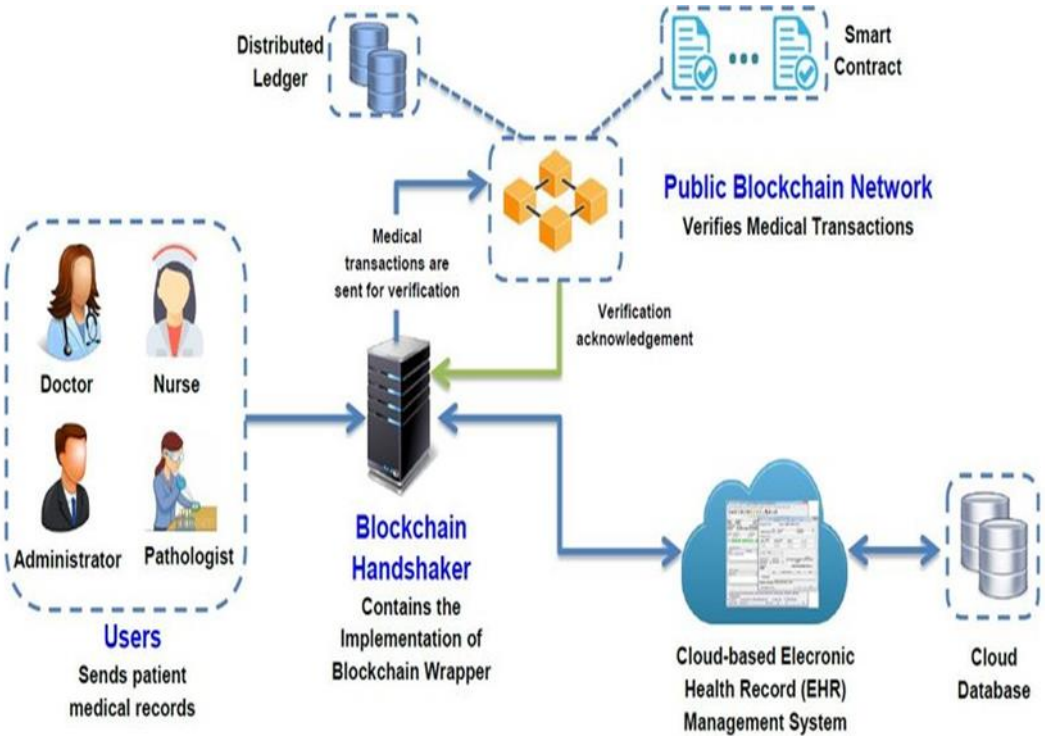

Figure 1: Design and structure of blockchain-enabled systems for managing electronic health records [17]

A. Genetic Algorithms and Blockchain Encryption

Genetic algorithms (GAs) are a subset of evolutionary algorithms inspired by natural selection processes [18][19]. These algorithms utilize principles such as selection, crossover, and mutation to evolve towards optimal solutions for complex problems [20][21]. In the context of blockchain encryption for EHR management, genetic algorithms could be applied to optimize cryptographic techniques and enhance security measures [22][23]. Figure 2 shows the workflow of the genetic algorithm.

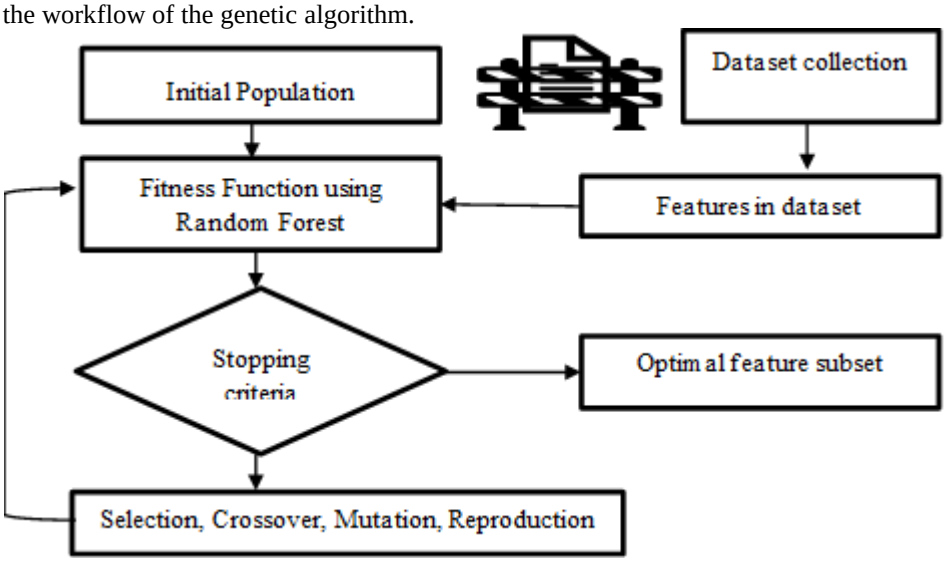

Figure 2: Workflow of genetic algorithm [24].

Blockchain technology, initially developed as the underlying framework for cryptocurrencies like Bitcoin, has gained attention across various industries due to its decentralized and immutable nature [25][26]. In healthcare, blockchain offers a promising solution for securely storing and managing EHRs by creating a tamper-resistant ledger of transactions [27-29]. However, one of the primary challenges associated with blockchain in this context is ensuring robust encryption methods to protect sensitive patient data from unauthorized access and breaches [30][31]. Figure 3 shows the use of blockchain algorithms in the field of healthcare.

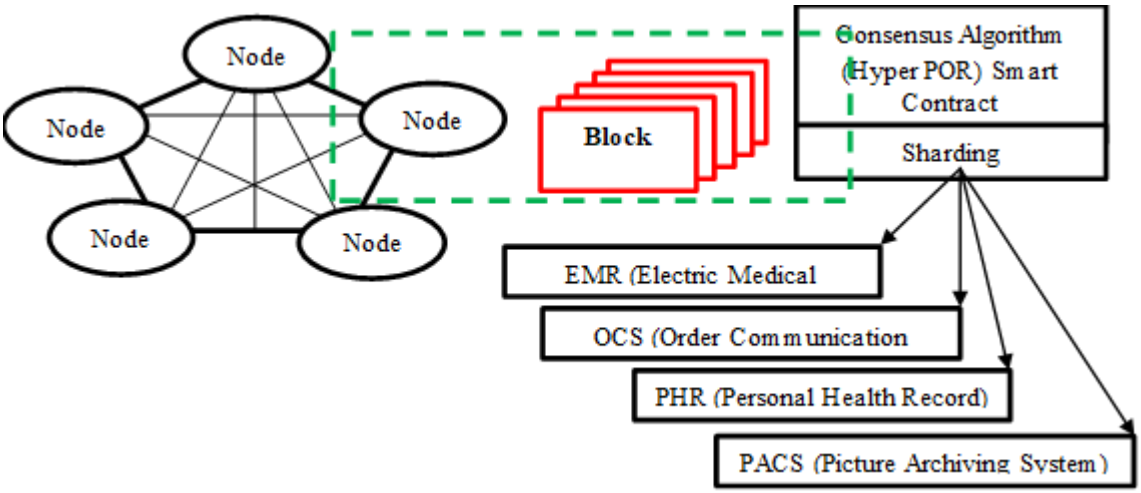

Figure 3: Blockchain algorithm for healthcare [32].

B. Encryption Security in Cryptography

Encryption plays a pivotal role in ensuring the confidentiality and integrity of EHRs. However, traditional encryption methods may not be sufficiently robust to address evolving cybersecurity threats [33][34]. The healthcare sector is particularly vulnerable to data breaches, highlighting the critical need for advanced encryption techniques that could withstand sophisticated attacks and ensure data privacy [35][36].

Developing advanced encryption techniques tailored for EHR management is essential to address the unique security requirements of healthcare data [37]. Unlike other forms of data, EHRs contain extremely sensitive information, including medical history, diagnoses, and treatment plans [38]. Any compromise in data security could have severe implications for patient safety and confidentiality [39]. Therefore, implementing effective encryption strategies is crucial for maintaining trust and compliance with privacy regulations. This research's main aim is to evaluate the performance of genetic algorithm-driven blockchain encryption for EHR management. By harnessing the power of genetic algorithms, this study seeks to enhance the security and efficiency of EHR systems while ensuring compliance with healthcare data protection standards [40].

The relevance of this research extends beyond the realm of theoretical cryptography to practical applications in healthcare data management and information security. Healthcare organizations are increasingly adopting digital solutions for EHR management, emphasizing the urgent need for robust encryption technologies that could mitigate risks associated with data breaches and unauthorized access.

The potential impact of this research lies in its ability to contribute to the development of innovative encryption solutions tailored for healthcare environments. By evaluating the performance of genetic algorithm-driven blockchain encryption, this study aims to provide insights into enhancing data privacy, integrity, and accessibility within EHR systems. The findings of this research could inform best practices for secure and efficient healthcare data management, benefiting patients, healthcare providers, and regulatory authorities alike.

The intersection of genetic algorithms, blockchain technology, and encryption holds immense promise for revolutionizing EHR management. This research endeavours to assess the efficacy and feasibility of genetic algorithm-driven blockchain encryption in enhancing data security and integrity within healthcare systems, paving the way for safer and more resilient healthcare data management practices. The contributions of the research are as follows:

- The research contributes to establishing interoperability standards for blockchain-based EHR systems enhanced by genetic algorithms. This would ensure seamless integration with existing healthcare IT infrastructures and facilitate data exchange among different healthcare providers securely.
- The research contributions involve developing comprehensive evaluation frameworks to assess the performance of genetic algorithm-driven blockchain encryption in real-world EHR scenarios. This includes metrics for security, efficiency, scalability, and compliance with healthcare data regulations.
- The research contributes by demonstrating improved security and privacy of electronic health records (EHRs) using genetic algorithm-driven blockchain encryption. This includes developing advanced encryption methods that are resistant to attacks and unauthorized access.

II. Related Work

This section presents a summary of previous research on evaluating the performance of genetic algorithm-driven blockchain encryption for managing and validating electronic health records (EHRs).

Fatima and Siddiqi (2024) [41] analyzed a variety of machine-learning methods for making reliable illness and side effect predictions. Various Machine Learning (ML) techniques were used to analyze the dataset. In terms of

accuracy (89.32%), precision (84.04%), sensitivity (86.63%), and specificity (82.45%), the experimental findings showed that the created Deep Belief Network (DBN) method is quite effective.

Garima Verma (2024) [42] implemented a new blockchain system to safeguard cloud-based health information, which helps with authentication and provides records with integrity. The research employed an enhanced Blowfish model, integrating blockchain with optimal encryption while ensuring authentication characteristics. The suggested approach outperformed the other predefined models based on key generation time by 91.48%.

Ragab et al. (2024) [43] introduced a method for analyzing electronic health records (EHRs) that was both blockchain-driven and privacy-preserving. This method is called BPEHR-SCADL, and it uses a deep learning model in conjunction with a sine-cosine approach (SCA). The BPEHR-SCADL method mainly developed an AFSA using an encryption methodology to ensure the safe transmission of electronic health records (EHRs). The results showed that the BPEHR-SCADL method was superior to other contemporary techniques, with a maximum accuracy of 98.65%.

Jakhar et al. (2024) [44] developed a blockchain-based access control system to safeguard healthcare data from unauthorized access while maintaining data accessibility, integrity, and privacy using consensus-driven decentralized data management built on top of peer-to-peer distributed computing platforms. This blockchain-based system resulted in a framework that showed great promise in terms of accuracy, dependability, security, regulatory compliance, and adaptability.

Miriam et al. (2023) [45] introduced the LGE-HES algorithm, which stands for Lionized Golden Eagle-centered Homomorphic Elapid Security, to safeguard blockchain applications in healthcare networks. By executing a hash function, the blockchain algorithm maintains the confidentiality of the medical picture. At least one malicious message was successfully discovered in 94.9% of cases.

Miyachi and Mackey (2021) [46] recommended a privacy-preserving architecture called hOCBS, which is a modular combination of off-chain with on-chain blockchain systems. It was tested on three distinct reference models to show how blockchain technology may improve healthcare data management. Off-chain blockchain System (OCBS) distributed governance would be a great match for the multi-party, rather complicated, and regulatory-mandated current health information systems.

Ismail et al. (2020) [47] introduced BlockHR, a healthcare record management system that is patient-centric and uses blockchain technology to provide efficient and cost-effective medical treatment. Patients may input their social data, such as their sleeping patterns, physical activity, and present location, while healthcare professionals can input their medical record data into the blockchain network. Therefore, the BlockHR management system handled the present client/server's security, privacy, data fragmentation, and vulnerability concerns.

Fatima and Ahmad (2020) [48] improved the security of encryption keys in a remote cloud setting and suggested a threshold secret-sharing technique that uses a Newton division difference interpolating polynomial (TSSNIP). When it came to key splitting along with key reconstruction, the suggested approach employed an interpolating polynomial that is Newton divided by difference. The findings showed that the suggested approach for secret sharing with reconstruction takes much less time on average than all other secret sharing methods.

Cao et al. (2019) [49] developed a cloud-based eHealth solution dubbed Tamper-Proofing EHR (TP-HER) to safeguard electronic health records (EHRs) against unauthorized access and change while also guaranteeing their confidentiality. Results from experiments show that TP-EHR can outsource EHRs into the cloud in under a second for a doctor with access to a computer, in contrast to the usual three minutes it takes to complete a transaction in Ethereum.

III. RESAERCH METHODOLOGY

This section is structured into four subsections. The first subsection discusses the dataset utilized for training and testing the model. The second subsection details the proposed GADBE (Genetic Algorithm-Driven Blockchain Encryption) model, which integrates genetic algorithms (GA), AES (Advanced Encryption Standard), and blockchain technology in an ensemble approach. The third subsection presents the architecture of the proposed system, outlining the components and their interactions within the GADBE model. Finally, the fourth subsection describes the proposed algorithm, illustrating the flow of the architecture and how the various components work together in the encryption and management of electronic health records (EHRs).

A. Dataset

Kaggle hosts MIMIC-III, a popular healthcare dataset. "Medical Information Mart to Feed Intensive Care III" is what it stands for. Electronic medical records of more than forty thousand patients in critical care are de-identified and included in the MIMIC-III dataset. Information on the patient's demographics, vital signs, test

results, drugs, treatments, and more is all part of it. MIMIC-IIIc is the acronym for "merged" and "aggregated," and it describes the dataset that is the result of merging many subsets. Data scientists and researchers often use MIMIC-IIIc to investigate and create models and applications for healthcare [50]. The MIMIC-III dataset includes:

- Patient demographics (age, gender, ethnicity, admission/discharge dates)
- Clinical data (vital signs, lab measurements, medications, procedures, diagnoses)
- Notes and reports (progress notes, discharge summaries, radiology reports, nursing documentation)
- Procedures and interventions (surgeries, intubation, ventilation, dialysis, medication administration)
- Severity scores (SAPS, SOFA, MPM) to assess illness severity and predict outcomes.
- ICU-specific data (admission/discharge times, length of stay, ICU care team details)
- Data linkage for comprehensive analyses across different aspects of patient care

B. Proposed Genetic Algorithm Driven Blockchain Encryption (GADBE) Model

The GADBE model is designed to evaluate the performance of genetic algorithm-driven blockchain encryption in electronic health record (EHR) management and validation. The model involves several key steps: first, employing HMAC-based authentication for patient and doctor verification; then generating EHR data followed by encrypting it using Elliptic Curve Cryptography (ECC) and uploading the encrypted and optimized data onto a blockchain platform. Genetic algorithms (GA) are then utilized to optimize encryption parameters, ensuring secure data transmission.

- **GA**

Genetic algorithms (GAs) are a type of evolutionary algorithm inspired by natural selection processes [51]. In the context of optimizing encryption parameters for the performance evaluation of genetic algorithm-driven blockchain encryption for EHR management and validation, GAs could be utilized to find the most effective set of encryption parameters (such as key lengths, cryptographic algorithms, or encryption methods) that maximize security and efficiency while minimizing computational overhead. GAs work by representing potential solutions as individuals within a population, applying selection, crossover, and mutation operations to evolve towards optimal solutions over successive generations. By using GAs in this context, the encryption parameters could be dynamically adjusted and optimized based on predefined fitness criteria, leading to enhanced security and performance of the blockchain-based EHR management system [52].

- **ECC**

Elliptic Curve Cryptography (ECC) is a type of public-key cryptography that utilizes elliptic curves over finite fields to secure data through encryption [53]. ECC offers strong security with shorter key lengths compared to other encryption methods like RSA, making it suitable for resource-constrained environments such as electronic health record (EHR) systems. In the context of the performance evaluation of genetic algorithm-driven blockchain encryption for EHR management and validation, ECC is used to encrypt EHR data securely before uploading it onto the blockchain. The integration of ECC within this framework ensures that sensitive healthcare information remains confidential and protected against unauthorized access. The performance of this encryption approach, alongside genetic algorithms optimizing encryption parameters within blockchain systems, is evaluated to assess its effectiveness in enhancing data security and integrity in healthcare settings [54].

- **Blockchain**

Blockchain is a decentralized digital ledger technology that stores records of transactions across a network of computers, ensuring transparency, security, and immutability of data [55]. Encrypting and optimizing electronic health record (EHR) data for blockchain upload and performance evaluation often entails employing cryptographic methods such as Elliptic Curve Cryptography (ECC) for data encryption before blockchain network integration. This encrypted data is then optimized using genetic algorithms (GA), which adjust encryption parameters to enhance security and efficiency in data storage and validation within the blockchain. The combination of blockchain technology, encryption methods, and genetic algorithms aims to provide a secure and scalable solution for managing and validating sensitive healthcare data [56].

C. Proposed Architecture

This section presents a block diagram in Figure 4 illustrating the proposed architecture. Key verification processes ensure data integrity and authenticity. When another medical centre requests EHR data, the model facilitates the retrieval, decryption, and uploading of EHR data into the local database. Subsequently, data collection occurs, followed by applying machine learning (ML) classification techniques using Logistic Regression (LR) and Random Forest (RF). Finally, the model undergoes performance evaluation to assess its effectiveness in securely managing and validating EHRs.

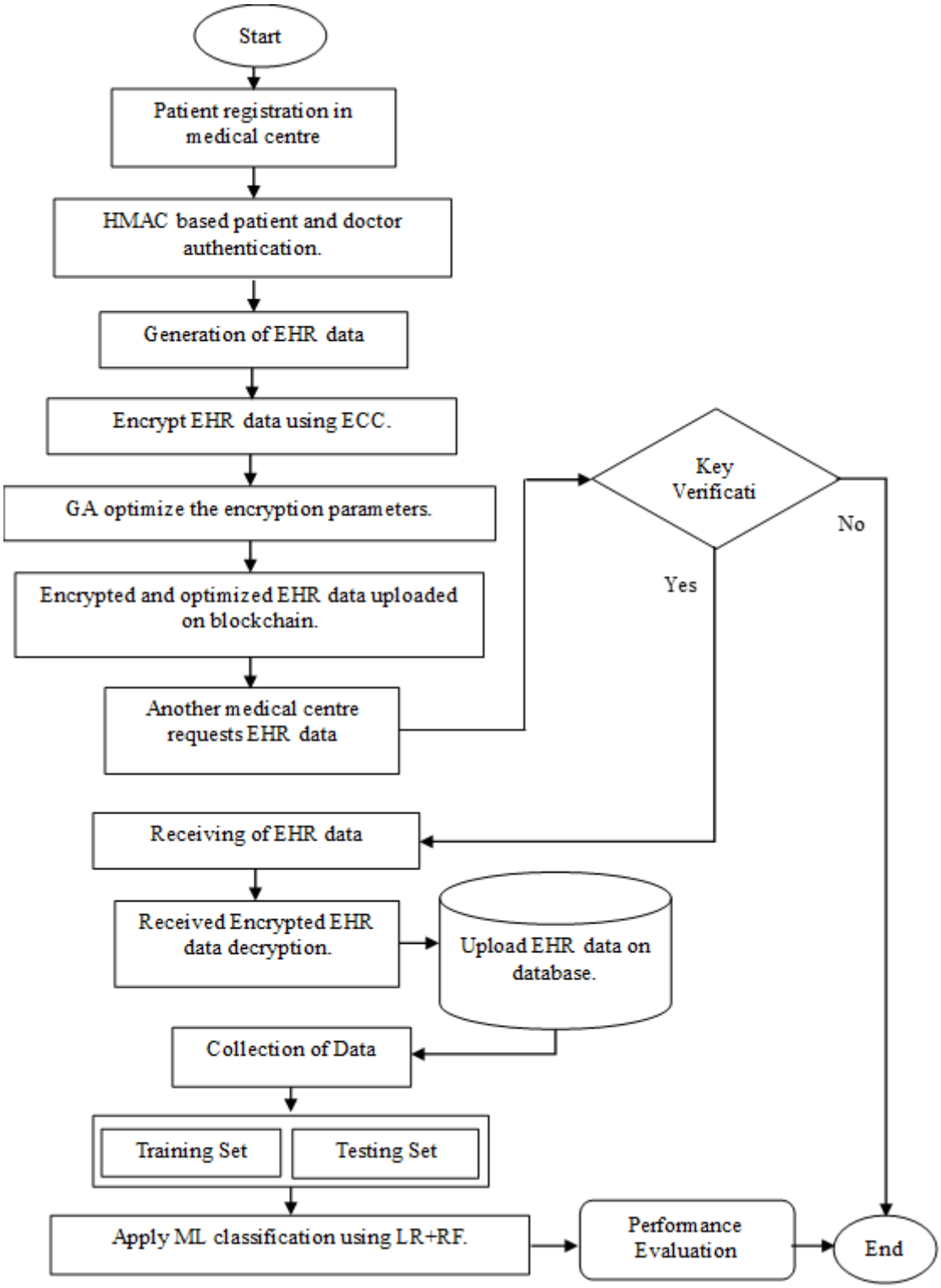

Figure 4: Proposed Architecture

Step 1: Start
Step 2: Patient Registration
At the beginning of the process, patients register at a medical centre to generate an Electronic Health Record (EHR).
Step 3: Patient-Doctor Authentication
Authentication between patients and doctors is secured using the Hash-based Message Authentication Code (HMAC).
Step 4: EHR Record Generation
EHR data is generated and prepared for further processing.
Step 5: EHR Data Encryption
The EHR data is encrypted using Elliptic Curve Cryptography (ECC), generating a public key and a private key.
Step 6: Genetic Algorithm Optimization

A genetic algorithm optimizes the encryption parameters to enhance security and efficiency before the data is stored on the blockchain.

Step 7: Data Upload to Blockchain

Encrypted and optimized EHR data is uploaded to the blockchain for secure, immutable storage.

Step 8: EHR Data Request and Verification

Another medical centre requests EHR data from the blockchain.

- A key verification condition is applied to authenticate the requesting medical centre.
- If the key is verified, data is sent; otherwise, the process ends.

Step 9: Decryption

The encrypted EHR data is decrypted using the private key generated during the encryption process.

Step 10: Database Upload

EHR data is uploaded to a database for persistent storage and later retrieval.

Step 11: Data Collection

The EHR data is collected from the database and split into two parts, namely train data and test data.

Step 12: Classification

Machine learning classifiers, namely Random Forest (RF) and Logistic Regression (LR), are applied for the classification of the EHR data.

Step 13: Performance Evaluation

The performance of the classifiers is evaluated at this stage.

Step 14: The Process Ends

IV. Results and Discussion

This section provides a brief description of the result gained from the proposed methodology using the MIMIC-III dataset.

A. Key Size vs Encryption/Decryption Time

The increase in encryption and decryption time with larger key sizes is a notable pattern, primarily due to the heightened computational demands associated with larger keys. This effect is particularly evident in public key cryptosystems such as ECC, where larger keys necessitate more intricate mathematical operations, especially in tasks like point multiplication. Interestingly, when considering the GADBE+AES combination, slightly higher computation times are observed at larger key sizes compared to AES alone. Given that AES is a symmetric key algorithm typically not prone to significant time increases with key size, this difference likely stems from the overhead introduced by GADBE. This disparity may indicate less optimization in the GADBE component when paired with AES, or it could be influenced by specific parameters within the AES implementation (such as key expansion) that impact performance as key sizes increase.

The plotted data in Figure 5 demonstrates the scaling of encryption and decryption times relative to key sizes for GADBE+ECC and GADBE+AES systems. Encryption times for both systems increase as key sizes grow: GADBE+ECC rises from 1.5 seconds at 128 bits to 3.8 seconds at 512 bits, while GADBE+AES increases from 1.7 seconds to 4.0 seconds over the same range. Similarly, decryption times also lengthen with larger key sizes: GADBE+ECC decrypts in 1.2 seconds at 128 bits and 3.5 seconds at 512 bits, whereas GADBE+AES takes 1.3 seconds at 128 bits and 3.7 seconds at 512 bits. Notably, AES exhibits marginally longer times at higher key sizes compared to ECC, suggesting that ECC could provide more efficient performance in terms of speed as key sizes increase.

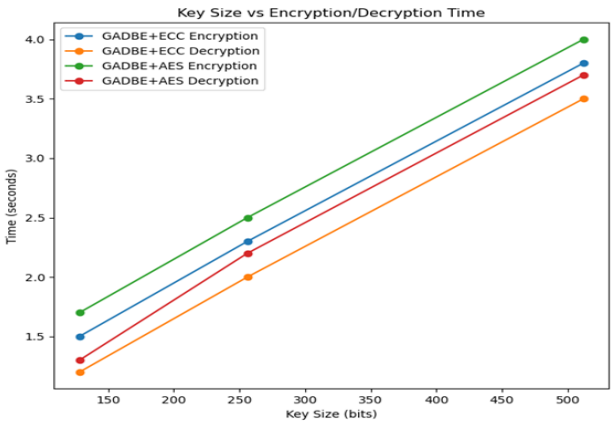

Figure 5: Key Size vs Encryption/Decryption Time

B. Data Size vs Encryption/Decryption Time

The variation observed between these encryption systems involves a linear increase in processing time with data size expansion. As both systems handle more data bits, the time required per bit increases proportionally. Notably, there remains a consistent performance gap between ECC and AES, with ECC generally exhibiting greater computational intensity than AES. However, ECC demonstrates better efficiency when handling larger data blocks, showing less incremental time increase per block compared to AES. This finding could indicate that ECC is more adept at managing larger data blocks efficiently within the context of GADBE, potentially due to improved integration or reduced computational overhead per block.

The plotted data in Figure 6 illustrates how encryption and decryption times scale with increasing data size for two cryptographic systems: GADBE with ECC and GADBE with AES. For encryption, both systems show a rise in time from 1.0 seconds (ECC) and 1.1 seconds (AES) at 100 MB to 2.5 seconds (ECC) and 2.8 seconds (AES) at 300 MB. Similarly, decryption times increase from 0.8 seconds (ECC) and 0.9 seconds (AES) at 100 MB to 2.2 seconds (ECC) and 2.5 seconds (AES) at 300 MB. This pattern mirrors that of key sizes, indicating a linear relationship between processing time and data volume. The slightly slower performance of AES compared to ECC suggests a potential pattern towards higher computational overhead with AES encryption.

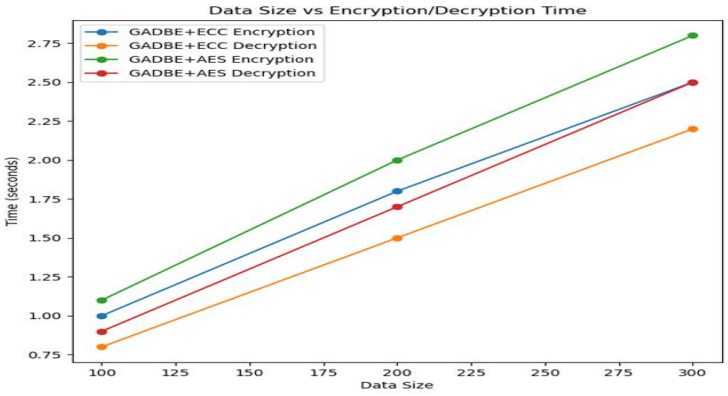

Figure 6: Data Size vs Encryption/Decryption Time

C. Compressed Key Size vs Encryption/Decryption Time

The relationship between key size and encryption/decryption time remains consistent with uncompressed keys despite compression of the keys, indicating that compression primarily reduces storage or transmission overhead rather than computational complexity. Despite key compression, elliptic curve cryptography (ECC) retains a performance advantage over other methods, likely due to its inherent efficiency in computational demands compared to other algorithms processing equivalent key sizes, regardless of whether the keys are compressed or uncompressed.

The encryption and decryption times for GADBE combined with ECC and AES exhibit notable increases when transitioning from smaller to larger key sizes. Specifically, the encryption time for GADBE+ECC rises from 0.5 to 1.5 seconds, while for GADBE+AES, it increases from 0.6 to 1.8 seconds. Decryption times rise from 0.4 to 1.3 seconds with GADBE+ECC and from 0.5 to 1.6 seconds with GADBE+AES. Despite employing compressed key sizes, figure 7 illustrates that ECC consistently outperforms AES, likely due to ECC's lower computational demands.

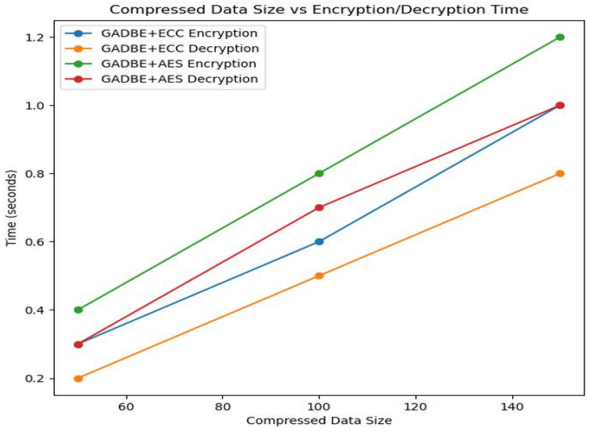

Figure 7: Compressed Key Size vs Encryption/Decryption Time

D. Compressed Data Size vs Encryption/Decryption Time

The observed variations highlight the efficiency gains of data compression before encryption. Smaller increases in processing time for compressed data compared to uncompressed data indicate the significant time savings achieved by reducing the amount of data that needs to be encrypted and decrypted. This underscores the advantage of applying compression before encryption to streamline processing. Additionally, the slight outperformance of ECC over AES suggests that ECC's inherent efficiency in compression extends not only to data but also to key compression, demonstrating a consistent performance advantage in scenarios involving compressed data environments. Therefore, employing ECC for both key and data compression could be beneficial for optimizing processing efficiency in encrypted systems.

In Figure 8, the plotted graph illustrates the encryption and decryption times for two encryption methods, GADBE+ECC and GADBE+AES, across varying data sizes. For encryption, GADBE+ECC exhibits a time range of 0.3 seconds at 50 MB up to 1.0 seconds at 150 MB, while GADBE+AES ranges from 0.4 seconds at 50 MB to 1.2 seconds at 150 MB. In terms of decryption, GADBE+ECC ranges from 0.2 seconds at 50 MB to 0.8 seconds at 150 MB, and GADBE+AES from 0.3 seconds at 50 MB to 1.0 seconds at 150 MB. The data highlights that even with compressed data sizes, ECC maintains a slightly better time efficiency compared to AES, which is consistent with previous observations.

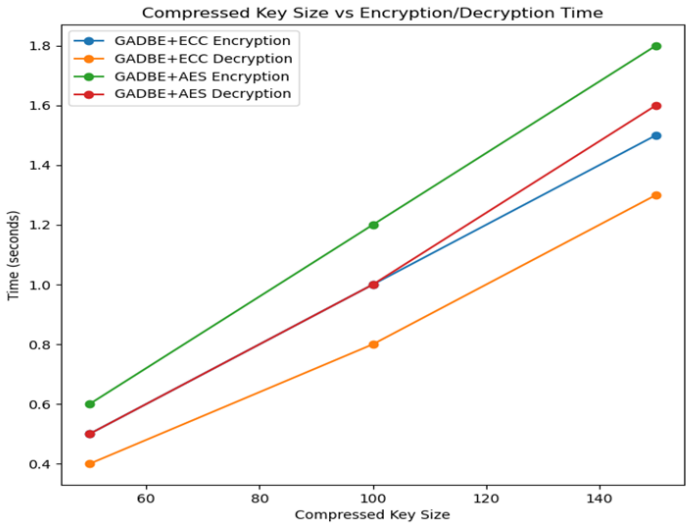

Figure 8: Compressed Data Size vs Encryption/Decryption Time

E. Compression Ratio Comparison

The variations in compression ratios, including AES achieving higher ratios and differences across key sizes, can be attributed to various factors within the GADBE system. The integration of AES might facilitate a more streamlined data handling process, potentially leading to more compact representations or the optimization of compression algorithm parameters. Furthermore, the variable compression ratios across different key sizes could stem from the differing efficiencies of each cryptographic algorithm within the system, as they manage redundancy and data structures differently depending on the length of the encryption key.

The bar plot in Figure 9 illustrates the comparison of compression ratios achieved by two methods: GADBE+ECC and GADBE+AES. The compression ratios for GADBE+ECC fall within the range of 2.0 to 2.5, while those for GADBE+AES range from 2.1 to 2.7. Notably, despite GADBE+AES exhibiting slightly slower processing times consistently, it achieves a generally higher compression ratio than GADBE+ECC. This finding suggests a discernible trade-off between time efficiency and data reduction effectiveness across these methods, emphasizing the need to balance processing speed with compression performance depending on specific application requirements.

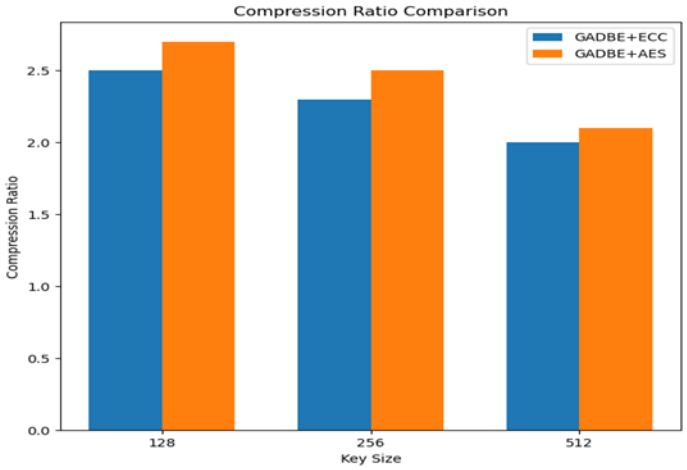

Figure 9: Compression Ratio Comparison

F. Comparison of Random Number Generators

Table 1 compares several random number generators according to the distribution of bits they produce statistically. The proposed method has been tested along with Linear Congruential and Blum Blum Shub generators. The number of '0' и '1' bits created by each generator, together with the resultant difference, is listed in the table. It is worth mentioning that the Blum Blum Shub generator always shows more '0' bits than '1' bits, regardless of the bit length (32, 64, 128, 256, 512). The results produced by the Linear Congruential approach are more evenly distributed bits, whilst those of the Proposed approach display intermediate qualities. The variations that have been seen indicate that these algorithms generate bits in different ways, which might mean that their usefulness varies depending on the needs of the application, whether it's for cryptographic security, randomness, or bias. A visual depiction of comparative table 1 is shown in Figure 10.

Table 1: Comparison between random number generators

S.No	No. of Bits	Random Generator	No. of '0'	No. of '1'	Difference
		Blum Blum Shub	17	15	2
		Linear Congruential	13	19	6
1	32	Proposed Method	17	15	2
		Blum Blum Shub	34	30	4
		Linear Congruential	32	32	0
2	64	Proposed Method	31	33	2
		Blum Blum Shub	70	58	12
		Linear Congruential	62	65	3
3	128	Proposed Method	63	64	1
		Blum Blum Shub	144	112	32
		Linear Congruential	131	128	3
4	256	Proposed Method	120	136	16
		Blum Blum Shub	276	236	40
		Linear Congruential	260	252	8
5	512	Proposed Method	259	254	5

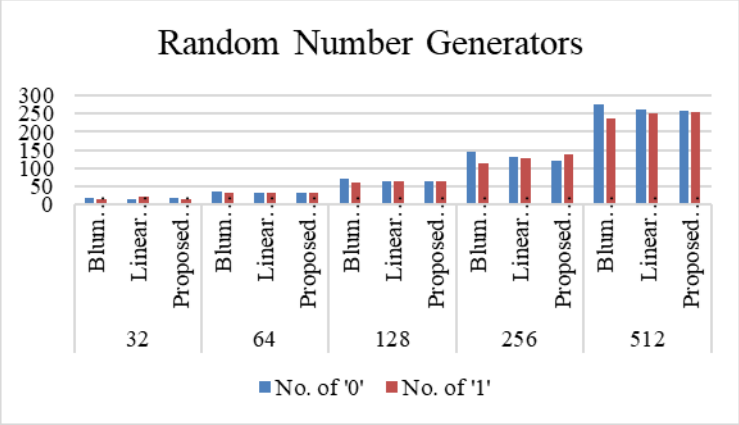

Figure 10: graphical representation of random number generators

G. Avalanche Effect in Encryption Algorithms

In encryption algorithms, the avalanche effect is a desired attribute that causes a substantial change in the output (ciphertext) from a little change in the input data (plaintext). Because it guarantees that even little changes to the input result in an entirely different encrypted output, this feature is critical for strong security. Figure 11, which is a graph format derived from Table 2, shows the avalanche percentages for several encryption techniques that display this pattern. A stronger avalanche effect is indicated by higher percentages, such as 66.4% for the Proposed Method, 53.5% for the Hybrid Encryption Framework, and 49.3% for Blowfish. This indicates that these algorithms are great at spreading input changes throughout the output space, making the system more secure and resistant to cryptanalysis. This quality is critical for determining how effective encryption methods are in preventing unauthorized access to critical information.

Table 2: Avalance effect

Avalance Effect	
Encryption Algorithms	**Avalanche percentage**
AES	48.2
Triple DES	32.5
Rivest Cipher	46.2
Blowfish	49.3
Hybrid Encryption Framework	53.5
Proposed Method	66.4

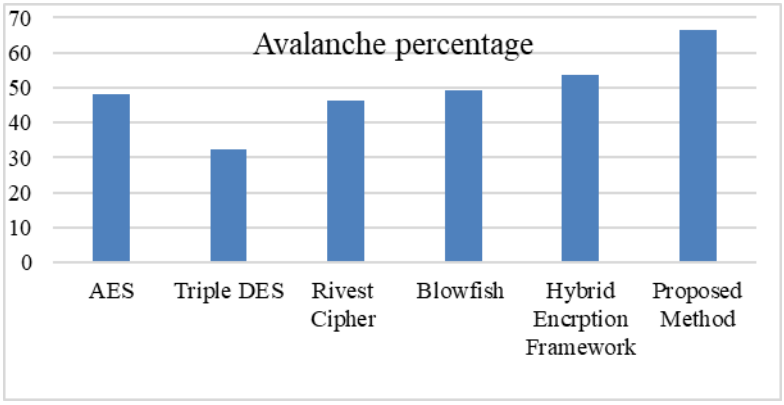

Figure 11: Avalance effect graphical representation

V. CONCLUSION

The performance evaluation of genetic algorithm-driven blockchain encryption for electronic health record (EHR) management and validation presents a critical exploration of leveraging advanced technologies to enhance data security and integrity in healthcare systems. This research assessed the effectiveness of integrating genetic

algorithms with blockchain encryption to optimize EHR management, ensuring robust data protection and validation. By combining genetic algorithms for encryption parameter optimization and blockchain technology for secure data storage and verification, this research underscores the potential of innovative approaches to address the evolving challenges of healthcare data security in the digital age. This study contributes valuable insights into the practical application of innovative technologies like genetic algorithms and blockchain in safeguarding sensitive patient information and ensuring the reliability of electronic health record systems. Finally, the resulting comparative analysis of cryptographic systems GADBE+ECC and GADBE+AES reveals notable patterns. Encryption and decryption times scale with key sizes and data volumes: GADBE+ECC and GADBE+AES show increasing times with larger key sizes and data sizes. ECC consistently outperforms AES in speed across these metrics, with ECC decryption times ranging from 0.4 to 3.5 seconds at 128 to 512 bits, while AES times were generally longer.

REFERENCES

[1] Keshta, Ismail, and Ammar Odeh. "Security and privacy of electronic health records: Concerns and challenges." Egyptian Informatics Journal 22, no. 2 (2021): 177-183.

[2] Shah, Shahid Munir, and Rizwan Ahmed Khan. "Secondary use of electronic health record: Opportunities and challenges." IEEE Access 8 (2020): 136947-136965.

[3] Mbunge, Elliot, Benhildah Muchemwa, and John Batani. "Sensors and Healthcare 5.0: the transformative shift in virtual care through emerging digital health technologies." Global Health Journal 5, no. 4 (2021): 169-177.

[4] Abdel-Rahman, Mohamed. "Advanced cybersecurity measures in IT service operations and their crucial role in safeguarding enterprise data in a connected world." Eigenpub Review of Science and Technology 7, no. 1 (2023): 138-158.

[5] Akindote, Odunayo Josephine, Abimbola Oluwatoyin Adegbite, Adedolapo Omotosho, Anthony Anyanwu, and Chinedu Paschal Maduka. "Evaluating the effectiveness of its project management in healthcare digitalization: a review." International Medical Science Research Journal 4, no. 1 (2024): 37-50.

[6] Sharma, Priynka, Jasvir Bir, and Surya Prakash. "Navigating Privacy and Security Challenges in Electronic Medical Record (EMR) Systems: Strategies for Safeguarding Patient Data in Developing Countries–A Case Study of the Pacific." In International Conference on Medical Imaging and Computer-Aided Diagnosis, pp. 375-386. Singapore: Springer Nature Singapore, 2023.

[7] Afolabi, Lekan. "Leveraging Advanced Information Systems for Enhanced Data Management and."

[8] Bani Issa, W., I. Al Akour, A. Ibrahim, A. Almarzouqi, S. Abbas, F. Hisham, and J. Griffiths. "Privacy, confidentiality, security and patient safety concerns about electronic health records." International Nursing Review 67, no. 2 (2020): 218-230.

[9] Thapa, Chandra, and Seyit Camtepe. "Precision health data: Requirements, challenges and existing techniques for data security and privacy." Computers in biology and medicine 129 (2021): 104130.

[10] Akhter Md Hasib, Kazi Tamzid, Ixion Chowdhury, Saadman Sakib, Mohammad Monirujjaman Khan, Nawal Alsufyani, Abdulmajeed Alsufyani, and Sami Bourouis. "Electronic health record monitoring system and data security using blockchain technology." Security and Communication Networks 2022 (2022): 1-15.

[11] Liu, Xiangyu, Riya Shah, Ananya Shandilya, Manan Shah, and Aum Pandya. "A systematic study on integrating blockchain in healthcare for electronic health record management and tacking medical supplies." Journal of Cleaner Production (2024): 141371.

[12] Ganiga, Raghavendra, Radhika M. Pai, and Rajesh Kumar Sinha. "Security framework for cloud-based electronic health record (EHR) system." International Journal of Electrical and Computer Engineering 10, no. 1 (2020): 455.

[13] Chenthara, Shekha, Khandakar Ahmed, Hua Wang, and Frank Whittaker. "Security and privacy-preserving challenges of e-health solutions in cloud computing." IEEE Access 7 (2019): 74361-74382.

[14] Fatima, Shahin, and Shish Ahmad. "An exhaustive review on security issues in cloud computing." KSII Transactions on Internet and Information Systems (TIIS) 13, no. 6 (2019): 3219-3237.

[15] Basil, Nduma N., Solomon Ambe, Chukwuyem Ekhator, Ekokobe Fonkem, Basil N. Nduma, and Chukwuyem Ekhator. "Health records database and inherent security concerns: A review of the literature." Cureus 14, no. 10 (2022).

[16] Huang, Chunya, Ross Koppel, John D. McGreevey III, Catherine K. Craven, and Richard Schreiber. "Transitions from one electronic health record to another: challenges, pitfalls, and recommendations." Applied Clinical Informatics 11, no. 05 (2020): 742-754.

[17] Rahman, Mohammad Saidur, Ibrahim Khalil, Pathum Chamikara Mahawaga Arachchige, Abdelaziz Bouras, and Xun Yi. "A novel architecture for tamper-proof electronic health record management system using blockchain wrapper." In Proceedings of the 2019 ACM international symposium on blockchain and secure critical infrastructure, pp. 97-105. 2019.

[18] Alam, Tanweer, Shamimul Qamar, Amit Dixit, and Mohamed Benaida. "Genetic algorithm: Reviews, implementations, and applications." arXiv preprint arXiv:2007.12673 (2020).

[19] Alhijawi, Bushra, and Arafat Awajan. "Genetic algorithms: Theory, genetic operators, solutions, and applications." Evolutionary Intelligence (2023): 1-12.

[20] Zainuddin, Farah Ayiesya, Md Fahmi Abd Samad, and Durian Tunggal. "A review of crossover methods and problem representation of genetic algorithm in recent engineering applications." International Journal of Advanced Science and Technology 29, no. 6s (2020): 759-769.

[21] Malik, Ashima. "A study of genetic algorithm and crossover techniques." International Journal of Computer Science and Mobile Computing 8, no. 3 (2019): 335-344.

[22] Mahajan, Hemant, and K. T. V. Reddy. "Secure gene profile data processing using lightweight cryptography and blockchain." Cluster Computing (2023): 1-19.

[23] Marichamy, V. Santhana, and V. Natarajan. "Blockchain-based securing medical records in big data analytics." Data & Knowledge Engineering 144 (2023): 102122.

[24] Iwendi, Celestine, Joseph Henry Anajemba, Cresantus Biamba, and Desire Ngabo. "Security of things intrusion detection system for smart healthcare." Electronics 10, no. 12 (2021): 1375.

[25] Alsuqaih, Hanan Naser, Walaa Hamdan, Haythem Elmessiry, and Hussein Abulkasim. "An efficient privacy-preserving control mechanism based on blockchain for E-health applications." Alexandria Engineering Journal 73 (2023): 159-172.

[26] Haddad, Alaa, Mohamed Hadi Habaebi, Md Rafiqul Islam, Nurul Fadzlin Hasbullah, and Suriza Ahmad Zabidi. "Systematic review on ai-blockchain based e-healthcare records management systems." IEEE Access 10 (2022): 94583-94615.

[27] Usman, Muhammad, and Usman Qamar. "Secure electronic medical records storage and sharing using blockchain technology." Procedia Computer Science 174 (2020): 321-327.

[28] Hang, Lei, Eunchang Choi, and Do-Hyeun Kim. "A novel EMR integrity management based on a medical blockchain platform in hospital." Electronics 8, no. 4 (2019): 467.

[29] Faisal, Mohammad, Halima Sadia, Tasneem Ahmed, and Nashra Javed. "Blockchain Technology for Healthcare Record Management." Pervasive Healthcare: A Compendium of Critical Factors for Success (2022): 255-286.

[30] Reegu, Faheem, Salwani Mohd Daud, and Shadab Alam. "Interoperability challenges in healthcare blockchain system-a systematic review." Annals of the Romanian Society for Cell Biology (2021): 15487-15499.

[31] Durneva, Polina, Karlene Cousins, and Min Chen. "The current state of research, challenges, and future research directions of blockchain technology in patient care: Systematic review." Journal of Medical Internet Research 22, no. 7 (2020): e18619.

[32] Kim, Seong-Kyu, and Jun-Ho Huh. "Artificial neural network blockchain techniques for healthcare system: Focusing on the personal health records." Electronics 9, no. 5 (2020): 763.

[33] Mahapatra, Bandana, Rajalakshmi Krishnamurthi, and Anand Nayyar. "Healthcare models and algorithms for privacy and security in healthcare records." Security and privacy of electronic healthcare records: Concepts, paradigms and solutions (2019): 183.

[34] Oh, Se-Ra, Young-Duk Seo, Euijong Lee, and Young-Gab Kim. "A comprehensive survey on security and privacy for electronic health data." International Journal of Environmental Research and Public Health 18, no. 18 (2021): 9668.

[35] Javaid, Mohd, Abid Haleem, Ravi Pratap Singh, and Rajiv Suman. "Towards insight cybersecurity for healthcare domains: A comprehensive review of recent practices and patterns." Cyber Security and Applications (2023): 100016.

[36] Yaqoob, Tahreem, Haider Abbas, and Mohammed Atiquzzaman. "Security vulnerabilities, attacks, countermeasures, and regulations of networked medical devices—A review." IEEE Communications Surveys & Tutorials 21, no. 4 (2019): 3723-3768.

[37] Yeng, Prosper, M. Ali Fauzi, Bian Yang, John-Bosco Diekuu, Peter Nimbe, Filip Holik, Pankaj Khatiwada, Akbar Fahmi, and Luyi Sun. "SecHealth: Enhancing EHR Security in digital health transformation." In Proceedings of the 8th International Conference on Sustainable Information Engineering and Technology, pp. 538-544. 2023.

[38] Holmes, John H., James Beinlich, Mary R. Boland, Kathryn H. Bowles, Yong Chen, Tessa S. Cook, George Demiris et al. "Why is the electronic health record so challenging for research and clinical care?" Methods of information in medicine 60, no. 01/02 (2021): 032-048.

[39] Habibzadeh, Hadi, Brian H. Nussbaum, Fazel Anjomshoa, Burak Kantarci, and Tolga Soyata. "A survey on cybersecurity, data privacy, and policy issues in cyber-physical system deployments in smart cities." Sustainable Cities and Society 50 (2019): 101660.

[40] Tariq, Monis, and Mohd Suaib. "A Review on Intrusion Detection in Cloud Computing." International Journal of Engineering and Management Research 13, no. 2 (2023): 207-215.

[41] Fatima, Nudrat, and Sifatullah Siddiqi. "Acute Myocardial Infarction: Prediction and Patient Assessment through Different ML Techniques." International Journal of Intelligent Systems and Applications in Engineering 12, no. 13s (2024): 106-121.

[42] Verma, Garima. "Blockchain-based privacy preservation framework for healthcare data in the cloud environment." Journal of Experimental & Theoretical Artificial Intelligence 36, no. 1 (2024): 147-160.

[43] Ragab, Mahmoud, Adel A. Bahaddad, Diaa Hamed, Ahmed Alkhayyat, Deepak Gupta, and Romany F. Mansour. "Blockchain-Driven Privacy Preserving Electronic Health Records Analysis Using Sine Cosine Algorithm with Deep Learning Model." HUMAN-CENTRIC COMPUTING AND INFORMATION SCIENCES 14 (2024).

[44] Jakhar, Amit Kumar, Mrityunjay Singh, Rohit Sharma, Wattana Viriyasitavat, Gaurav Dhiman, and Shubham Goel. "A blockchain-based privacy-preserving and access-control framework for electronic health records management." Multimedia Tools and Applications (2024): 1-35.

[45] Miriam, Hephzibah, D. Doreen, Deepak Dahiya, and C. R. Rene Robin. "Secured Cyber Security Algorithm for Healthcare System Using Blockchain Technology." Intelligent Automation & Soft Computing 35, no. 2 (2023).

[46] Miyachi, Ken, and Tim K. Mackey. "hOCBS: A privacy-preserving blockchain framework for healthcare data leveraging an on-chain and off-chain system design." Information processing & management 58, no. 3 (2021): 102535.

[47] Ismail, Leila, Huned Materwala, and Moien AB Khan. "Performance evaluation of a patient-centric blockchain-based healthcare records management framework." In Proceedings of the 2nd International Electronics Communication Conference, pp. 39-50. 2020.

[48] Fatima, Shahin, and Shish Ahmad. "Secure and effective key management using secret sharing schemes in cloud computing." International Journal of e-Collaboration (IJeC) 16, no. 1 (2020): 1-15.

[49] Cao, Sheng, Gexiang Zhang, Pengfei Liu, Xiaosong Zhang, and Ferrante Neri. "Cloud-assisted secure eHealth systems for tamper-proofing EHR via blockchain." Information Sciences 485 (2019): 427-440.

[50] https://www.kaggle.com/datasets/drscarlat/mimic3c

[51] Rundo, Leonardo, Carmelo Militello, Salvatore Vitabile, Giorgio Russo, Evis Sala, and Maria Carla Gilardi. "A survey on nature-inspired medical image analysis: a step further in biomedical data integration." Fundamenta Informaticae 171, no. 1-4 (2020): 345-365.

[52] Zong, Nansu, Victoria Ngo, Daniel J. Stone, Andrew Wen, Yiqing Zhao, Yue Yu, Sijia Liu, Ming Huang, Chen Wang, and Guoqian Jiang. "Leveraging genetic reports and electronic health records for the prediction of primary cancers: algorithm development and validation study." JMIR Medical Informatics 9, no. 5 (2021): e23586.

[53] Ullah, Shamsher, Jiangbin Zheng, Nizamud Din, Muhammad Tanveer Hussain, Farhan Ullah, and Mahwish Yousaf. "Elliptic Curve Cryptography; Applications, challenges, recent advances, and future patterns: A comprehensive survey." Computer Science Review 47 (2023): 100530.

[54] Arora, Vansh. "A Framework for Cloud-Based EHR Security Using Hybrid Cryptographic Methods of AES and ECC." (2023).

[55] Uddin, Mueen, M. S. Memon, Irfana Memon, Imtiaz Ali, Jamshed Memon, Maha Abdelhaq, and Raed Alsaqour. "Hyperledger fabric blockchain: Secure and efficient solution for electronic health records." Computers, Materials & Continua 68, no. 2 (2021): 2377-2397.

Sharma, Yogesh, and Balamurugan Balamurugan. "Preserving the privacy of electronic health records using blockchain." Procedia Computer Science 173 (2020): 171-180.