AFCP Data Security Model for EHR Data Using Blockchain

D. Selvaraj[1], J. Jeno Jasmine[2], R. Ramani[3], D. Dhinakaran[4,*], G. Prabaharan[4]

[1]Department of Electronics and Communication Engineering, Panimalar Engineering College, Chennai, India
[2]Department of Computer Science and Engineering, R.M.K. Engineering College, Chennai, India
[3]Department of Computer Science and Engineering, P.S.R Engineering College, Sivakasi, India
[4]Department of Computer Science and Engineering, Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Chennai, India
Emails: mails2selvaraj@yahoo.com; jenojasmine@gmail.com; rramani.ananth@gmail.com; drdhinakarand@veltech.edu.in; drprabaharang@veltech.edu.in

Abstract

The problem of data security in EHR is deeply concerning, as well as the methods used in session, feature, service, rule, and access restriction models. However, they fail to achieve higher security performance, which degrades the trust of data owners. To handle this issue, an efficient Adaptive Feature Centric Polynomial (AFCP) data security model is described here. The proposed method can be adapted to enforce security on any kind of data. The AFCP scheme classifies the features of EHR data under different categories based on their importance in being identified from the data taxonomy. By maintaining different categories of data encryption schemes and keys, the model selects a specific key for a unique feature with the use of the polynomial function. The method is designed to choose a dynamic polynomial function in the form of m(x) n, where the values of m and n are selected in a dynamic way. The method generates a blockchain according to the feature values and adapts the cipher text generated by applying a polynomial function to data encryption. The same has been reversed to produce the original EHR data by reversing the operation. The method enforces the Healthy Trust Access Restriction scheme in restricting malicious access. By adapting the AFCP model, the security performance is improved by up to 98%, and access restriction performance is improved by up to 97%. The proposed method increases the access restriction performance in the ratio of 19%, 16%, and 11% to HCA-ECC, EHRCHAIN, and PCH methods. Similarly, security performance is increased by 17% 13%, and 11% to HCA-ECC, EHRCHAIN, and PCH methods.

Keywords: Data Security; Polynomial Encryption; AFCP Model; Data Encryption; Blockchain; Access Restriction

1. Introduction

Modern organizations maintain a variety of data from various sources in their databases. The data maintained would belong to different owners and contain a number of sensitive and private pieces of information. By maintaining diverse and sensitive data, they took responsibility [1]. The medical organization would provide services to the users of the environment towards various goals. For example, the medical practitioner would access the data maintained by the medical organization for various purposes like diagnosing, treating patients, and so on. To perform such a task, the medical practitioner needs to access the medical data through the various services provided. Various users of the environment [2] would access the services provided by any service provider. However, the users can be categorized in terms of their profile and not all of them would be given access to all the features. The EHR data contains different information about various persons, including personal, medical, and diagnosis results [3]. In any medical organization, users can be classified based on their role and should be restricted from accessing the EHR (Electronic Health Record). Similarly, access restriction and data encryption schemes are used to enforce secure access and data security on any kind of data. To increase data security and

DOI: https://doi.org/10.54216/JCIM.150103
Received: January 26, 2024 Revised: April 23, 2024 Accepted: July 14, 2024

privacy preservation, a few methods use data encryption and some of them use access restriction schemes [4]. In terms of data encryption, different schemes are used in producing cipher text, where the selection of encryption scheme is performed based on service, feature, role, profile, and so on. In cases of access restriction, it has been performed based on feature, service, role, profile, behavior, history, and so on. In both ways, the methods are suffering to achieve higher security performance.

To handle all the issues discussed above, an efficient adaptive feature-centric Centric Polynomial Data Security Model (AFCP) is sketched here. It is concerned with restricting malicious access to EHR data in two ways. One by restricting malicious access by allowing the user to trust. To measure the trust of the user, the method applies the Healthy Trust Access Restriction algorithm. According to the result of the HTAR algorithm, the method allows or denies access to data. Second, malicious access is restricted by adapting blockchain techniques. The blockchain is the most recent popular technique in securing sensitive data at sharing. It has been used in several situations like banking applications, defines data, and so on. Unlike other techniques, the blockchain is the methodology that stands for the data owner by splitting the data into blocks and adapting hash codes in each block to support decoding the data. The blocks of the chain have two parts like data part and the hash code part. The legitimate user can be able to decode the original data only when he is able to decode the hash code. The hash code has been used to represent both the encryption scheme and the key being used to produce the cipher text. By maintaining different schemes and keys to produce cipher text, the method would be able to choose a dynamic scheme and key where the hash code is produced in a meaningful way that can be understood by the legitimate user. Even though the efficacy of the method is foolproof. The generation or selection of scheme and key must be performed in a non-tempering way. The detailed working of the proposed model is discussed in the next section.

Contribution:

This article contributes the following aspects towards security enhancement:

- Describes Adaptive Feature Centric Polynomial (AFCP) model, which uses healthy trust access restriction scheme in restricting malicious access on electronic health record data.
- Uses category-based data encryption scheme where the data features are categorized according to the importance.
- Polynomial function is used for the selection of scheme and key to be used for data encryption and decryption.
- Selection of polynomial function is performed in dynamic way.
- Blockchain has been used for secure transmission of electronic health record data.

This article presents the detailed introduction about data security and use of block chain in Section 1. Section 2, presents the detailed literature about the problem and methods. Section 3, presents the detailed working of the proposed model and section 4, presents the detailed analysis of results and discussion. Section 5, presents the conclusion and summary of the article.

2. Related Work

The data security problem in EHR data has been approached by different techniques in the literature. Among them, a few techniques that are more effective are discussed in this section. A detailed analysis of enforcing privacy preservation in EHR data is performed in [5], which discusses the effect of blockchain technique in preserving private data in EHR records. A shared EHR model is presented in [6], which clubs blockchain with an interplanetary file system in the cloud. The method uses a contract-based access control scheme to share data between patients and providers. A deep analysis is performed over the adaptation of blockchain with EHR data in [7], which analysed various scientific articles and the methods discussed. An identity-based signature scheme is presented in [8], which restricts collusion attacks by using blockchain techniques to restrict the malicious user with multiple authorities. To share data among different healthcare organizations, a two-step authentication model named HCA-ECC is presented [9], which uses elliptic curve cryptography (ECC) to maintain session keys to communicate with others and uses ECC to perform encryption with blockchain on healthcare records.

A blockchain-based EHR model named (EHRChain) is presented in [10], which uses homomorphic encryption with blockchain to secure the data. A node state checkable Practical Byzantine Fault Tolerance consensus algorithm (sc-PBFT) is presented in [11], which applies attribute-based encryption to safeguard EHR data. A rule-based approach is presented in [12], to support security on EHR data, which uses granular access rules to improve data security with blockchain technique. A patient-centric healthcare framework (PCH) is presented in [13], which uses blockchain with tiered architecture to enforce data security. Similarly, a secure data-sharing model for patient data is presented in [14], which uses blockchain to improve security and uses session keys in access restriction. A

DOI: https://doi.org/10.54216/JCIM.150103
Received: January 26, 2024 Revised: April 23, 2024 Accepted: July 14, 2024

blockchain-assisted verifiable outsourced attribute-based encryption scheme (BVOABSC) is presented in [15], which applies an attribute-based encryption and verification scheme for improved security. A multi-attribute-based encryption and key aggregation scheme (M-ABS-KA) is presented in [16], which collects public keys and generates signatures to be used in a group to improve data security.

A block chain model is presented in [17], which restricts the access of data records by segmenting the data records into different lists. A secure platform is designed in [18] to handle the EHR records in the most secure and transparent way using blockchain. The model has combined different cryptographic tools to enforce data security. A solidity-based smart contract system is presented in [19], which combines blockchain with the solid ecosystem to improve data security on EHR data. A FL-based EHR model (FL-EHR) is presented in [20], which adapts layered architecture with blockchain to secure electronic health records. In [21], proposes a distributed database consensus protocol designed to improve the performance of EHR insertion operations, a particularly critical issue in medical imaging cases due to the data volume. It explores the personal and non-transferable nature of EHR and the proposed methodology reduces the data contention through data isolation, improving the overall retrieval performance and detection of misbehaving parties. A systematic study on the security and privacy requirements of EHR data is presented in [22], which considers various security measures and interoperable chances for the data. A blockchain with a smart contract system is presented in [23], which has been developed using Ganache. The model is designed to store EHR data according to the blockchain and smart contracts. A block chain-based EHR data-monitoring scheme is presented in [24], which limits the access of third parties. The method uses smart contracts and peer-to-peer encrypted technology, which restrict the hacker from gaining access to the data. The model has been enforced with a web model and enforces various profiles maintained at the local server to enforce higher data security. A systematic review on adapting blockchain technology in secure electronic health records is presented in [25]. A blockchain-based EHR data security model is presented in [26], which controls information access using different cryptographic techniques and uses decentralization of data towards effective restriction. From the literature survey, we identified several issues with the methods of securing EHR data. Most approaches use blockchain, but they do not focus on data encryption performance, which leads to data leakage. The data encryption schemes used are not dynamic; they are not dedicated to attribute level and are time consuming. In addition, the methods suffer from poor performance in data security, access restriction, and time complexity.

3. AFCP Data Security Model with Block Chain

The proposed AFCP data security model using blockchain works according to the earlier traces of service access. The model receives the user's request and identifies the service and features requested. Further, using the access trace available, the method performs Health Trust Access Restriction (HTAR), which identifies the trust of the user in restricting malicious access. Further, the method accesses the data requested and generates block chain with the Polynomial Blockchain Scheme, which generates the chain according to the features and encrypts the data to be added to the blockchain. The encryption scheme is selected from the list in a dynamic way and used to encrypt data. The generated blockchain has been given to the receiver, who can revise the process to obtain original data. The working model is sketched in Figure 1, which has a number of functional components, and each of them is discussed in detail in this section.

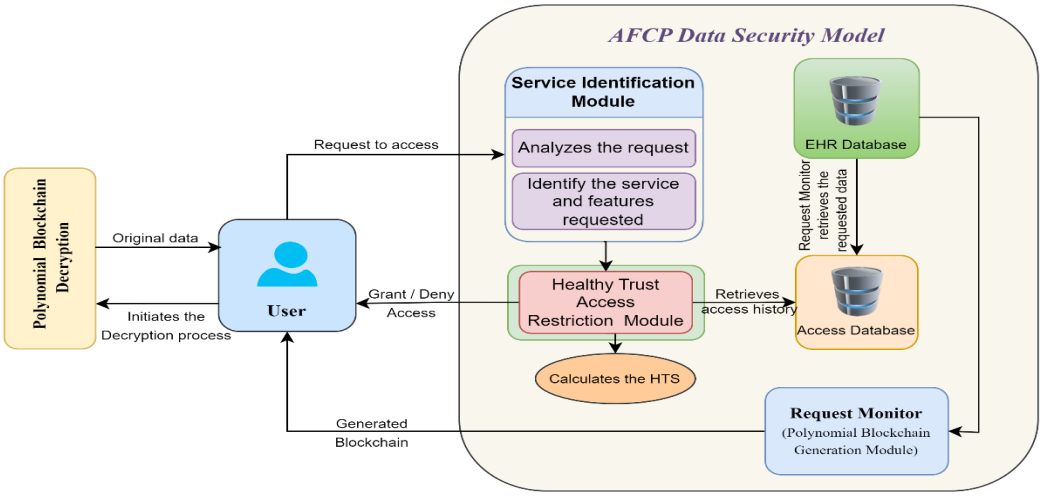

Figure 1. Architecture of AFCP Model

DOI: https://doi.org/10.54216/JCIM.150103
Received: January 26, 2024 Revised: April 23, 2024 Accepted: July 14, 2024

A. Request Monitor

The request monitor has received the request being generated by any client. From the request received, the method identifies the service and features requested. Further, the method identifies the user ID and verifies the trust of the user with the use of the Healthy Trust Access Restriction algorithm. If the trust value returned by the HTAR algorithm is higher than the specific threshold, then the user has been allowed to access the service. Otherwise, the user has been declined to access the service. Further, the method accesses the service and gets the service data. The resultant data has been used to generate polynomial blockchain and polynomial blockchain decryption schemes. Finally, result has been given to the user.

Algorithm for Request Monitor:

Start
Read user request *R*
Retrieve service access history *SAH*
Extract feature taxonomy *FT*
Loop continuously
Identify user *U* from *UserID* in *R*
Determine requested service *Sr* from *ServiceID* in *R*
Compute Healthy Trust Score *HTS* using HTAR *(U, Sr, SAH)*
If *HTS* exceeds threshold *Th*
Access service data *SD* for *Sr*
Encrypt *SD* using Polynomial Blockchain Encryption, producing blockchain *B*
Transmit B to user U
Decrypt B to obtain Cipher Text CT
Otherwise, deny access request
End loop
Stop

The request monitor always monitors the incoming request and estimates the trust of the user to restrict malicious request. Further, the method generates the block chain using polynomial algorithm and produces result to the user. The receiver in turn would obtain the original data according to the same reverse operation.

B. Healthy Trust Access Restriction (HTAR)

The trustworthiness of the user in accessing different features of the environment or features of the electronic health record is measured at this stage. To measure the Healthy Trust Score (HTS), the method considers the previous access traces. From the historical access traces of features, the method computes the service level healthy score (SLHS), and feature level healthy score (FLHS). Using both the values of SLHS and FLHS, the model measures the HTS value. Accordingly, user trust is measured.

Algorithm: Healthy Trust Access Restriction (HTAR)

Start
Read Service Access History (SAH), Service (S), and User (U)
Identify user traces *UTr* from SAH where the User matches U and the Service matches S
Compute Service Level Healthy Score (SLHS) based on the completion status in *UTr*
Compute Feature Level Healthy Score (FLHS) based on features from the service taxonomy (ST)
Calculate Healthy Trust Score (HTS) by combining SLHS and FLHS
Stop

The healthy trust access restriction algorithm computes service level and feature level healthy score for the user given based on previous access history. Around the values measured, the HTS score is measured and access restriction is enforced accordingly.

C. Polynomial Blockchain Encryption

The service data obtained by accessing the service has been encrypted and encoded in blockchain generated. To perform this, the number of features is identified using service taxonomy. According to the number of features,

DOI: https://doi.org/10.54216/JCIM.150103
Received: January 26, 2024 Revised: April 23, 2024 Accepted: July 14, 2024

the method generates a blockchain with the size of features accessed by the service. The method uses a single block for each feature accessed by the service. The service data has been split according to the feature value and for each feature value; the method generates a block and adds to the chain [27]. The feature value belonging to the block has been encrypted with the key and scheme being selected. To perform the scheme selection and key, the method uses the polynomial function. For example, if the polynomial function is m(x) n, then the method generates two different random values. The first random number denotes the value of m, whereas the second random value denotes the value of n. By applying the value of both m and n in the polynomial function, the method selects the scheme and key for the specific feature to perform data encryption. Similarly, for each feature, the same procedure is performed to encrypt the data part. Further, the method generates the hash code and adds to the hash code part of each block concerned. The generated blockchain has been shared with the receiver, who performs the reverse operation to obtain the original data.

Algorithm: Polynomial Blockchain Encryption

Start
Read Service Data Sd, Scheme set *ss*, and Key set *Kset*
Count the number of features in *Sd* and set as Feature Count *Fc*
Initialize blockchain *B* with *Fc* blocks
For each feature *F* in *Sd*
Generate random values mmm (1 to 10) and *n* (1 to 3)
Calculate index *I* using the polynomial function $m(x)^n$
Select scheme *s* from *ss* and key *k* from *Kset* based on *I*
Encrypt *Sd(F)* using *s* and *k* to obtain cipher text *T*
Assign *T* to the data field of block *B(F)*
Create hash code *H* using mmm and *n*
Add *H* to the hash code field of block *B(F)*
End
Stop

The above polynomial block chain algorithm generates the block chain with k number of blocks equal to the number of features in the service data. Each has been encrypted with specific key and scheme identified according to the polynomial functions submitted with the random numbers generated.

D. Polynomial blockchain decryption

The user requests that the service be provided with the blockchain generated at the encryption stage. The receiver identifies the number of blocks, and from each block; the method identifies the hash code [28]. From the hash code, the method extracts the two integer's m and n. The values of m and n are applied over the polynomial function where the value of x is proactively given to the user. Based on the value obtained by the polynomial equation, the method identifies the index of both scheme and key. Using this scheme and key, the method performs decryption on each block to obtain the original data.

Algorithm: Polynomial Blockchain Decryption

Start
Read Blockchain *B*, Scheme set *Ss*, Key set *Kset*, and Service Data *Sd*
Initialize Original Text *OT* as an empty string
For each block *b* in *B*
Extract hash code *H* from *b*
Split *H* into string set *Sset* using delimiter "#"
Convert *Sset(0)* to integer *M*
Convert *Sset(1)* to integer *N*
Calculate index *I* using the polynomial function $m(x)^n$
Decrypt *b.data* using scheme *Ss(I)* and key *Kset(I)* to obtain original text *T*
Append *T* to *OT*

End
Stop

DOI: https://doi.org/10.54216/JCIM.150103
Received: January 26, 2024 Revised: April 23, 2024 Accepted: July 14, 2024

The polynomial blockchain decryption algorithm decodes the hash code to apply on the polynomial equation, which yields the index of scheme and key to be used. Further, the method decrypts the encoded text in each block to obtain the original value. Obtained original results are given as result to the user.

4. Results and Discussion

The proposed Adaptive Feature Centric Polynomial Data Security Model (AFCP) with blockchain has been implemented and evaluated for its performance under various circumstances. The outcomes are analyzed across several factors, which are detailed below. The experimental setup, as outlined in Table 1, utilized the Microsoft Azure platform to leverage its extensive cloud infrastructure. The implementation included 100 distinct services, each with unique security requirements, encompassing 30 different features within the Electronic Health Records (EHR) data. The user base for this experiment consisted of 500 individuals, providing a comprehensive scenario to test the model's adaptability and scalability. The analysis results observed are presented in this section, focusing on the following key metrics: Access Restriction Performance, Security Performance, Data Security performance, Encryption / Decryption Performance, Analysis on Time Complexity, Analysis on Throughput Performance, and Network Overhead in Bytes Analysis on Time Complexity.

Table 1: Experimental Details

FACTOR	VALUE
Tool Used	Microsoft Azure
Number of Services	100
Throughput	500 TPS
Number of Features	30
Block Size	1 MB
Dataset Size	10 GB
Number of Users	500

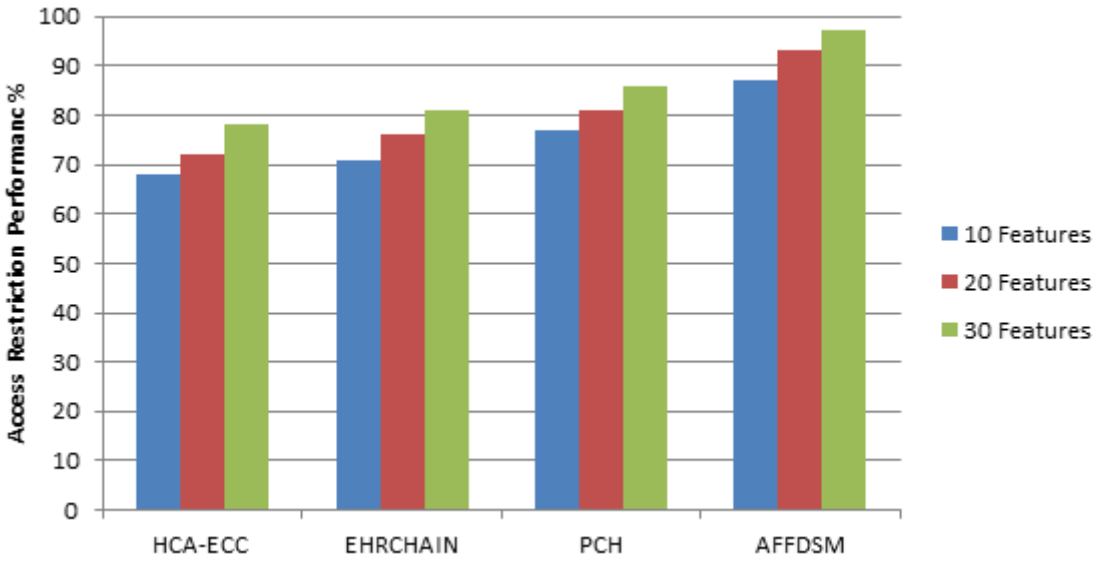

Figure 2. Access Restriction Performance Comparison

A. Access Restriction Performance

Access restriction performance measures the efficacy of a method in identifying malformed access and efficiently detecting illegal access attempts. The performance of various methods in restricting malicious access, with the proposed AFCP model demonstrating superior results compared to existing methods. The performance results in Fig. 2 illustrate the significant improvements achieved by the AFCP model. To further elucidate these results, two specific scenarios are considered: In a small-scale implementation involving 10 features, the AFCP model achieves an access restriction performance of 87%, compared to 68%, 71%, and 77% for HCA-ECC, EHRCHAIN, and

DOI: https://doi.org/10.54216/JCIM.150103
Received: January 26, 2024 Revised: April 23, 2024 Accepted: July 14, 2024

PCH, respectively. This indicates that even with a limited number of features, AFCP provides robust protection against unauthorized access. The higher performance can be attributed to the model's adaptive feature-centric approach, which tailors' security measures to the specific importance of each feature. In a more extensive implementation involving 30 features, the AFCP model's access restriction performance increases to 97%. This is significantly higher than the 78% achieved by HCA-ECC, 81% by EHRCHAIN, and 86% by PCH. The improvement in performance in this scenario highlights the scalability of the AFCP model. As the number of features increases, the model's ability to dynamically select and apply polynomial functions enhances its effectiveness in securing EHR data. The superior access restriction performance of the AFCP model across different scales of implementation underscores its efficacy in protecting against unauthorized access and ensuring data security in diverse scenarios.

B. Data Security performance

The effectiveness of various methods in security enforcement is measured and presented in Fig 3. The proposed AFCP model demonstrates superior security performance compared to existing methods. The performance results highlight the significant security improvements achieved by the AFCP model. Two specific scenarios are considered to further illustrate these results: In a small-scale implementation with 10 features, the AFCP model achieves a security performance of 86%, compared to 72%, 73%, and 79% for HCA-ECC, EHRCHAIN, and PCH, respectively. This demonstrates the model's capability to provide robust security even with a limited number of features. The dynamic selection of polynomial functions and adaptive feature-centric approach ensure that each feature is adequately protected, resulting in enhanced overall security. In a large-scale implementation involving 30 features, the AFCP model's security performance reaches 98%. This is significantly higher than the 81% achieved by HCA-ECC, 85% by EHRCHAIN, and 87% by PCH. The substantial increase in performance in this scenario highlights the scalability and efficiency of the AFCP model. As the number of features increases, the model's ability to dynamically select and apply appropriate polynomial functions ensures that all features are securely encrypted, thus maximizing the security of the EHR data. The superior security performance of the AFCP model across different scales of implementation underscores its effectiveness in enforcing data security and protecting sensitive information in diverse scenarios.

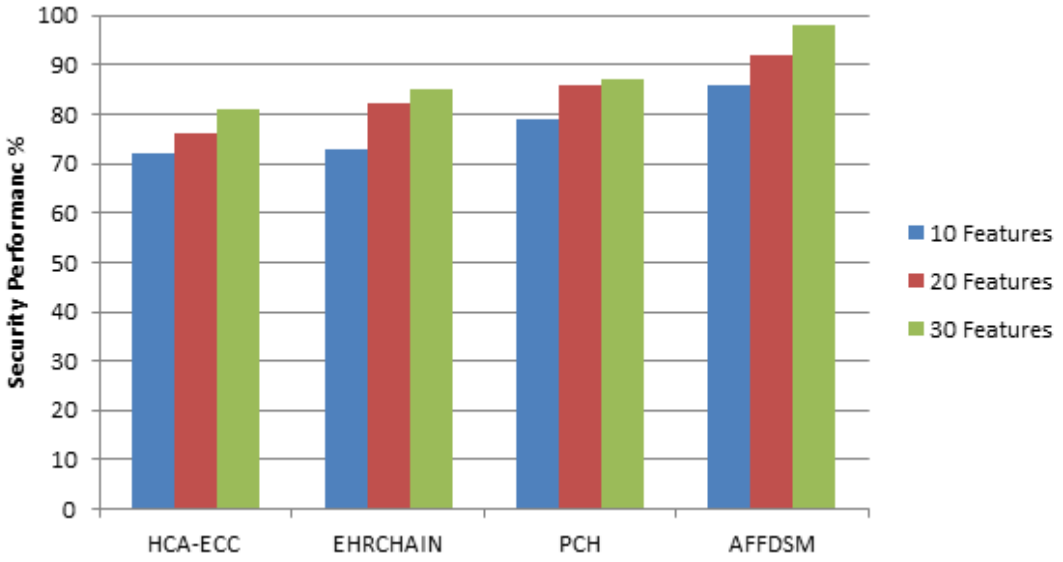

Figure 3. Security Performance Comparison

C. Encryption / Decryption Performance

The efficacy of various methods in performing encryption and decryption is measured and presented in Fig. 4. The proposed AFCP scheme demonstrates higher performance compared to existing methods. The performance results illustrate the significant improvements in encryption and decryption achieved by the AFCP scheme. Two specific scenarios are considered to further elucidate these results: In a small-scale implementation with 10 features, the AFCP scheme achieves an encryption/decryption performance of 85%, compared to 65%, 72%, and 75% for HCA-

DOI: https://doi.org/10.54216/JCIM.150103
Received: January 26, 2024 Revised: April 23, 2024 Accepted: July 14, 2024

ECC, EHRCHAIN, and PCH, respectively. This indicates that even with a limited number of features, the AFCP scheme provides efficient and robust encryption and decryption processes. The dynamic polynomial function selection and adaptive feature-centric approach ensure that each feature is securely encrypted and decrypted, resulting in enhanced overall performance. In a large-scale implementation involving 30 features, the AFCP scheme's encryption/decryption performance reaches 96%. This is significantly higher than the 78% achieved by HCA-ECC, 83% by EHRCHAIN, and 87% by PCH. The substantial increase in performance in this scenario highlights the scalability and efficiency of the AFCP scheme. As the number of features increases, the model's ability to dynamically select and apply appropriate polynomial functions ensures that all features are efficiently encrypted and decrypted, thus maximizing the overall performance. The superior encryption/decryption performance of the AFCP scheme across different scales of implementation underscores its effectiveness in providing secure and efficient data encryption and decryption processes in diverse scenarios.

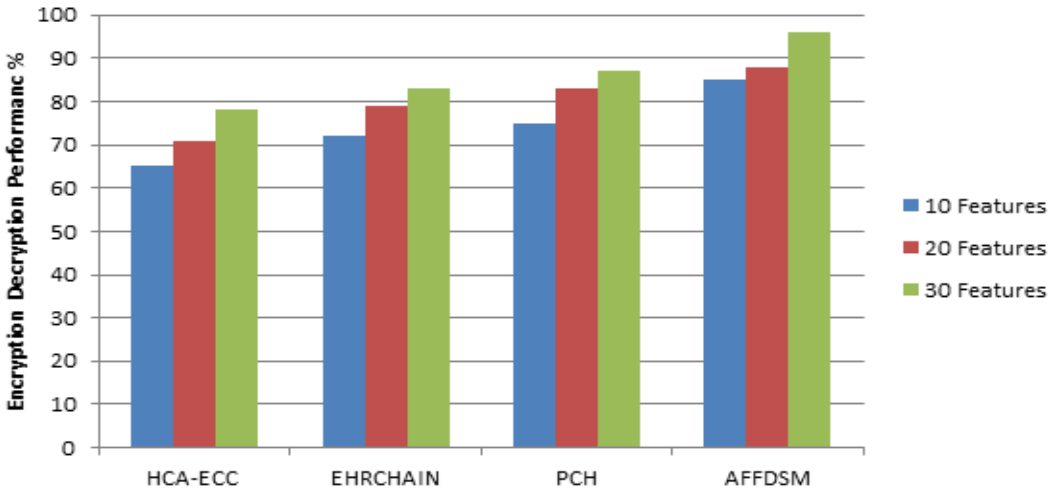

Figure 4. Encryption / Decryption Performance Comparison

D. Time Complexity

The time complexity of various approaches is measured in seconds and presented in Fig. 5. The proposed AFCP model demonstrates significantly lower time complexity compared to existing methods. The performance results highlight the substantial reduction in time complexity achieved by the AFCP model. Two specific scenarios are considered to further elucidate these results: In a small-scale implementation with 10 features, the AFCP model achieves a time complexity of 35 seconds, compared to 78 seconds for HCA-ECC, 75 seconds for EHRCHAIN, and 68 seconds for PCH. This significant reduction in time complexity indicates that the AFCP model provides faster encryption and decryption processes, even with a limited number of features.

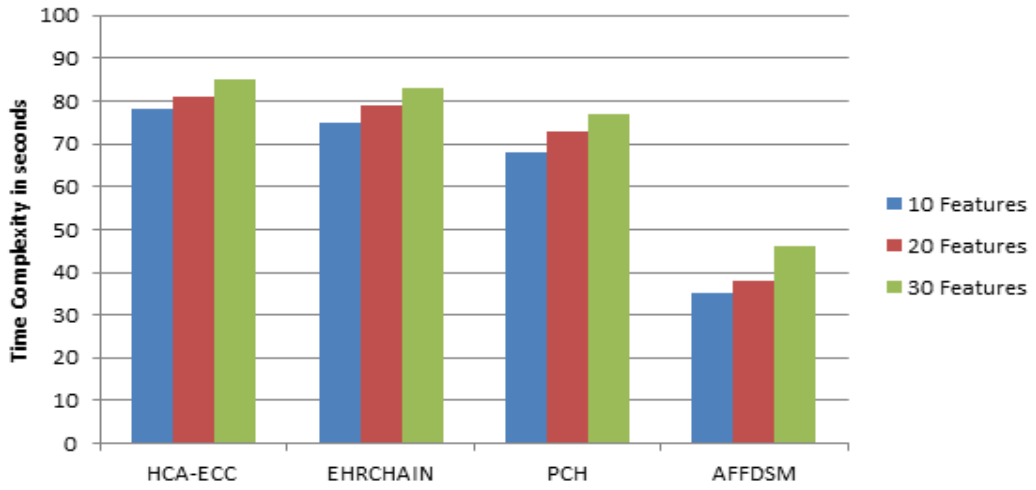

Figure 5. Time Complexity Comparison

DOI: https://doi.org/10.54216/JCIM.150103
Received: January 26, 2024 Revised: April 23, 2024 Accepted: July 14, 2024

The dynamic polynomial function selection and adaptive feature-centric approach contribute to the model's efficiency, resulting in reduced processing times. In a large-scale implementation involving 30 features, the AFCP model's time complexity increases to 46 seconds, which is still considerably lower than the 85 seconds for HCA-ECC, 83 seconds for EHRCHAIN, and 77 seconds for PCH. The substantial reduction in time complexity in this scenario highlights the scalability and efficiency of the AFCP model. As the number of features increases, the model's ability to dynamically select and apply appropriate polynomial functions ensures that all features are processed quickly and efficiently, thus minimizing overall time complexity. The superior performance of the AFCP model in terms of time complexity across different scales of implementation underscores its effectiveness in providing fast and efficient data encryption and decryption processes in diverse scenarios.

E. Throughput Performance

The throughput performance of various approaches is measured and presented in Fig.6. The proposed AFCP model demonstrates significantly higher throughput performance compared to existing methods. The performance results illustrate the significant improvements in throughput achieved by the AFCP model. Two specific scenarios are considered to further elucidate these results: In a small-scale implementation with 10 features, the AFCP model achieves a throughput performance of 87%, compared to 74%, 78%, and 81% for HCA-ECC, EHRCHAIN, and PCH, respectively. This indicates that even with a limited number of features, the AFCP model provides higher throughput, ensuring efficient processing and data transfer rates. The dynamic polynomial function selection and adaptive feature-centric approach contribute to the model's enhanced performance. In a large-scale implementation involving 30 features, the AFCP model's throughput performance reaches 96%. This is significantly higher than the 82% achieved by HCA-ECC, 86% by EHRCHAIN, and 89% by PCH. The substantial increase in throughput in this scenario highlights the scalability and efficiency of the AFCP model. As the number of features increases, the model's ability to dynamically select and apply appropriate polynomial functions ensures that all features are processed efficiently, thus maximizing throughput.

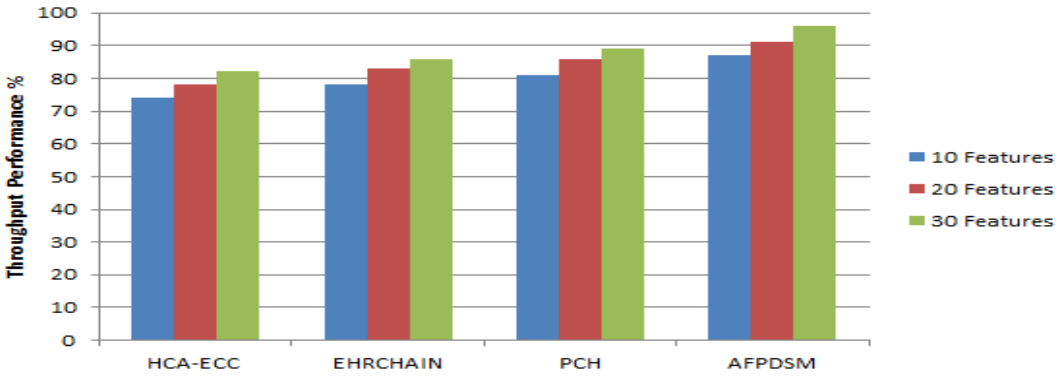

Figure 6. Throughput Performance Comparison

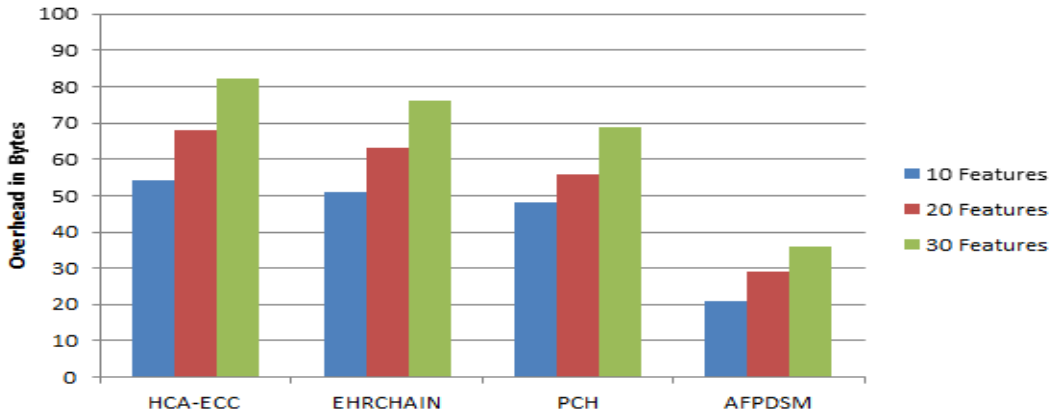

Figure 7. Network Overhead Comparison

DOI: https://doi.org/10.54216/JCIM.150103
Received: January 26, 2024 Revised: April 23, 2024 Accepted: July 14, 2024

F. Network Overhead

The network overhead introduced by various approaches is measured in bytes and presented in Fig. 7. The proposed AFCP approach demonstrates significantly lower network overhead compared to existing methods. The performance results in Table 7 highlight the substantial reduction in network overhead achieved by the AFCP approach. Two specific scenarios are considered to further elucidate these results: In a small-scale implementation with 10 features, the AFCP approach achieves a network overhead of 21 bytes, compared to 54 bytes for HCA-ECC, 51 bytes for EHRCHAIN, and 48 bytes for PCH. This significant reduction in network overhead indicates that the AFCP approach provides data that are more efficient transmission with minimal additional load on the network. The dynamic polynomial function selection and adaptive feature-centric approach contribute to the reduced overhead. In a large-scale implementation involving 30 features, the AFCP approach's network overhead increases to 36 bytes, which is still considerably lower than the 82 bytes for HCA-ECC, 76 bytes for EHRCHAIN, and 69 bytes for PCH. The substantial reduction in network overhead in this scenario highlights the scalability and efficiency of the AFCP approach. As the number of features increases, the model's ability to dynamically select and apply appropriate polynomial functions ensures efficient data transmission with minimal network load.

5. Conclusion

This article presented an Adaptive Feature Centric Polynomial (AFCP) Model with blockchain for securing EHR data. The model processes service requests by identifying the requested service and the data to be accessed, applying the Health Trust Access Restriction scheme, which computes feature-level and service-level healthy scores to determine a healthy trust score. Based on this score, the method restricts malformed access. Additionally, the model generates data for the user and creates a blockchain using a polynomial blockchain scheme that applies dynamic data encryption to the data blocks. The encrypted data, encapsulated within the generated blockchain, is then sent to the receiver, who can reverse the process to retrieve the original data. The proposed method significantly enhances data security and access restriction performance. Key performance highlights include achieving up to 98% security performance, surpassing HCA-ECC by 17%, EHRCHAIN by 13%, and PCH by 11%; achieving up to 97% access restriction performance, with improvements of 19% over HCA-ECC, 16% over EHRCHAIN, and 11% over PCH; demonstrating superior encryption/decryption performance, reaching 96% with 30 features; significantly reducing time complexity to 46 seconds for 30 features; achieving up to 96% throughput performance for 30 features; and reducing network overhead to 36 bytes for 30 features. Overall, the AFCP model offers a robust and efficient approach to securing EHR data, ensuring both high security and efficient access restriction.

Future research can build on the AFCP Model by exploring several promising directions. One potential avenue is the integration of advanced machine learning algorithms to enhance the adaptive capabilities of the model, allowing it to better predict and respond to emerging security threats. Additionally, expanding the model to support a broader range of data types and applications beyond EHR can increase its versatility and applicability in various domains. Another critical area for exploration is the optimization of the polynomial blockchain scheme to further reduce computational overhead and improve scalability, particularly in large-scale implementations. Investigating the integration of quantum-resistant cryptographic techniques could also provide enhanced security against future quantum computing threats. Finally, conducting comprehensive real-world testing and validation in diverse environments will be essential to ensure the robustness and reliability of the AFCP model in practical applications.

Funding: This research received no external funding.

Conflicts of Interest: The authors declare no conflict of interest.

References

[1] Venugopal, L.K.; Rajaganapathi, R.; Birjepatil, A.; Raja, S.E.; Subramaniam, G., “A Novel Information Security Framework for Securing Big Data in Healthcare Environment Using Blockchain,” Eng. Proc. 2023, Vol 59, Issue No. 1, Pp 107.

[2] D. Dhinakaran, L. Srinivasan, S.M. Udhaya Sankar, and D. Selvaraj, “Quantum-based privacy-preserving techniques for secure and trustworthy internet of medical things an extensive analysis,” Quantum Information and Computation, Vol. 24, No. 3&4, pp. 0227–0266, 2024.

[3] R. Jayasri, D. Jayakumar, S. Joshila Roselin and M. O. Ramkumar, "Plan of Block-chain Enabled Confirmed Key Management Protocol for Internet of Medical Things Development," 2022 3rd

DOI: https://doi.org/10.54216/JCIM.150103
Received: January 26, 2024 Revised: April 23, 2024 Accepted: July 14, 2024

International Conference on Electronics and Sustainable Communication Systems (ICESC), Coimbatore, India, 2022, pp. 668-673.

[4] Dhinakaran, D, Selvaraj, D, Dharini, N, Raja, S. E, and Priya, C. S. L. (2023). Towards a Novel Privacy-Preserving Distributed Multiparty Data Outsourcing Scheme for Cloud Computing with Quantum Key Distribution. International Journal of Intelligent Systems and Applications in Engineering, 12(2), 286–300.

[5] R. G. Sonkamble, S. P. Phansalkar, V. M. Potdar and A. M. Bongale, "Survey of Interoperability in Electronic Health Records Management and Proposed Blockchain Based Framework: MyBlockEHR," in IEEE Access, vol. 9, pp. 158367-158401, 2021.

[6] D. C. Nguyen, P. N. Pathirana, M. Ding and A. Seneviratne, "Blockchain for Secure EHRs Sharing of Mobile Cloud Based E-Health Systems," in IEEE Access, vol. 7, pp. 66792-66806, 2019.

[7] A. A. Mamun, S. Azam and C. Gritti, "Blockchain-Based Electronic Health Records Management: A Comprehensive Review and Future Research Direction," in IEEE Access, vol. 10, pp. 5768-5789, 2022.

[8] F. Tang, S. Ma, Y. Xiang and C. Lin, "An Efficient Authentication Scheme for Blockchain-Based Electronic Health Records," in IEEE Access, vol. 7, pp. 41678-41689, 2019.

[9] H. Ghayvat et al., "CP-BDHCA: Blockchain-Based Confidentiality-Privacy Preserving Big Data Scheme for Healthcare Clouds and Applications," in IEEE Journal of Biomedical and Health Informatics, vol. 26, no. 5, pp. 1937-1948, May 2022.

[10] F. Li, K. Liu, L. Zhang, S. Huang and Q. Wu, "EHRChain: A Blockchain-Based EHR System Using Attribute-Based and Homomorphic Cryptosystem," in IEEE Transactions on Services Computing, vol. 15, no. 5, pp. 2755-2765, 1 Sept.-Oct. 2022.

[11] Z. Pang, Y. Yao, Q. Li, X. Zhang and J. Zhang, "Electronic Health Records Sharing Model Based on Blockchain With Checkable State PBFT Consensus Algorithm," in IEEE Access, vol. 10, pp. 87803-87815, 2022.

[12] A. Shahnaz, U. Qamar and A. Khalid, "Using Blockchain for Electronic Health Records," in IEEE Access, vol. 7, pp. 147782-147795, 2019.

[13] A. N. Gohar, S. A. Abdelmawgoud and M. S. Farhan, "A Patient-Centric Healthcare Framework Reference Architecture for Better Semantic Interoperability Based on Blockchain, Cloud, and IoT," in IEEE Access, vol. 10, pp. 92137-92157, 2022.

[14] Jena Catherine Bel D, Esther C, Zionna Sen G B,Tamizhmalar D, Dhinakaran D, Anish T. P,"Trustworthy Cloud Storage Data Protection based on Blockchain Technology," 2022 International Conference on Edge Computing and Applications (ICECAA), 2022, pp. 538-543.

[15] X. Yang, T. Li, W. Xi, A. Chen and C. Wang, "A Blockchain-Assisted Verifiable Outsourced Attribute-Based Signcryption Scheme for EHRs Sharing in the Cloud," in IEEE Access, vol. 8, pp. 170713-170731, 2020.

[16] R. Guo, K. Li, X. Li, Y. Zhang and X. Li, "Compact Multiple Attribute-Based Signatures With Key Aggregation and Its Application," in IEEE Systems Journal, vol. 16, no. 2, pp. 3025-3035, June 2022.

[17] Dinesh Kumar K; B. Prabhu Shankar; Dhinakaran D; Shanthi H J; G. Vennila; P. Senthil, "Multiple Precision Arithmetic with Blowfish Crypto Method for Medical Data Storage Using Blockchain Technology," 2023 International Conference on Innovative Computing, Intelligent Communication and Smart Electrical Systems (ICSES), Chennai, India, pp. 1-6, 2023.

[18] A. A. Omar et al., "A Transparent and Privacy-Preserving Healthcare Platform With Novel Smart Contract for Smart Cities," in IEEE Access, vol. 9, pp. 90738-90749, 2021.

[19] H. Ghayvat, M. Sharma, P. Gope and P. K. Sharma, "SHARIF: Solid Pod-Based Secured Healthcare Information Storage and Exchange Solution in Internet of Things," in IEEE Transactions on Industrial Informatics, vol. 18, no. 8, pp. 5609-5618, Aug. 2022.

[20] V. A. Patel et al., "Adoption of Federated Learning for Healthcare Informatics: Emerging Applications and Future Directions," in IEEE Access, vol. 10, pp. 90792-90826, 2022.

[21] M. Pedrosa, R. Lebre and C. Costa, "A Performant Protocol for Distributed Health Records Databases," in IEEE Access, vol. 9, pp. 125930-125940, 2021.

[22] Tertulino, R., Antunes, N. & Morais, H. Privacy in electronic health records: a systematic mapping study. J Public Health (Berl.) Vol. 32, pp. 435–454, 2023.

[23] K. Y. Kumar, N. J. Kumar, D. Dhinakaran, S. M. Udhaya Sankar, U. J. Kumar and V. Yuvaraj, "Optimized Retrieval of Data from Cloud using Hybridization of Bellstra Algorithm," 2023 World Conference on Communication & Computing (WCONF), RAIPUR, India, pp. 1-6, 2023.

[24] Kazi Tamzid Akhter Md Hasib, 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 Networking for Healthcare

DOI: https://doi.org/10.54216/JCIM.150103
Received: January 26, 2024 Revised: April 23, 2024 Accepted: July 14, 2024

Information Exchange and Storage in the Big Data Ecosystem, Electronic Health Record Monitoring System and Data Security Using Blockchain Technology, vol. 2022, No. 2366632,2022.

[25] D. Selvaraj, S. M. Udhaya Sankar, D. Dhinakaran, T. P. Anish, "Outsourced Analysis of Encrypted Graphs in the Cloud with Privacy Protection," SSRG International Journal of Electrical and Electronics Engineering, vol. 10, no. 1, pp. 53-62, 2023.

[26] Yogesh Sharma, B. Balamurugan, Preserving the Privacy of Electronic Health Records using Blockchain, Procedia Computer Science, Volume 173, 2020, Pages 171-180, ISSN 1877-0509.

[27] N. Jagadish Kumar, D. Dhinakaran, A. Naresh Kumar, A. V. Kalpana, "Swarm Intelligence with a Chaotic Leader and a Salp algorithm: HDFS optimization for reduced latency and enhanced availability," e8127, Vol.36, Issue 17, pp. 1-26, 2024. Doi:10.1002/cpe.8127.

[28] Venugopal, L.K.; Rajaganapathi, R.; Birjepatil, A.; Raja, S.E.; Subramaniam, G. A Novel Information Security Framework for Securing Big Data in Healthcare Environment Using Blockchain. Eng. Proc. 2023, Vol 59, Issue No. 1, Pp 107. https://doi.org/10.3390/engproc2023059107

DOI: https://doi.org/10.54216/JCIM.150103
Received: January 26, 2024 Revised: April 23, 2024 Accepted: July 14, 2024