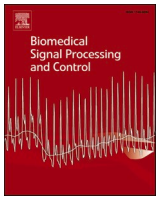
Biomedical Signal Processing and Control 111 (2026) 108329

Contents lists available at ScienceDirect

Biomedical Signal Processing and Control

journal homepage: www.elsevier.com/locate/bspc



Enhancing clinical data security with the contextual polynomial-based data protection model (CPDPM)

D. Dhinakaran [a,*], R. Ramani [b,**], S. Edwin Raja [a], D. Selvaraj [c]

[a] Department of Computer Science and Engineering, Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Chennai, India
[b] Department of Information Technology, P.S.R Engineering College, Sivakasi, India
[c] Department of Electronics and Communication Engineering, Panimalar Engineering College, Chennai, India

ARTICLE INFO

Keywords:
Electronic health records
Data security
Confidentiality
Dynamic request analyser
Dynamic trust authorization system
Integrity

ABSTRACT

Today, the healthcare industry mostly uses the electronic record of the patient's health, also known as the electronic health record or simply EHR. However, since the health records contain highly confidential patient information shared across computerized systems, it is under threat from hackers and cybercriminals, data theft and unauthorized access. Healthcare information is sensitive, requires to be whole and accessible and this is a major challenge that needs strong security solutions. Here, we present the Contextual Polynomial-Based Data Protection Model (CPDPM), a new additive model designed to improve clinical data security through the use of advanced encryption and access control methods in conjunction with a polynomial-based data protection model, specifically developed for the healthcare context. The major issues we observed regarding clinical data protection are based around the issues of encryption strength as well as the consequences, such as the performance and utilization of resources. Furthermore, access restrictions and data integrity have to be dynamic and respond to changes of a system, especially if it involves multiple parties. Our approach handles these considerations since the proposed polynomial-based framework guarantees the security of the data as well as scalability to huge healthcare systems. We determined the performance of the proposed model by assessing restrictive access system, and the encryption and decryption time analysis, data security, through put, and network overhead analysis using real EHR datasets. In comparison with other models such CP-BDHCA, EHRC, B-IBE and HH-IPFS, our model gave better results. For example, CPDPM had higher performance than HH-IPFS by 9 % and then CP-BDHCA by 18 % in terms of Access Restriction Performance. For Encryption Performance, our proposed model was 8 % more efficient than B-IBE, and for decryption performance, the findings also reveal that our model is 14 % more efficient than HH-IPFS. Moreover, Security Performance indicated a coverage of at least 20 % in comparison to conventional data security, and throughput performance recorded improvement of 12 % responding to existing systems.

1. Introduction

Health care delivery systems have revolutionized in recent years by use of technology that knows the right management of clinic information. This digital transformation as we have seen, comes with some encouraging opportunities but with daunting risks when it comes to security and privacy of sensitive health care information [1]. Electronic patient's records, diagnostics, treatment plans, and other information about patients' state are highly appreciated and therefore, become an object of interest to cybercriminals. However, the availability and quantity of data in healthcare systems has increased sharply in recent years further compounded by the growing call for compatibility of different platforms, making data security a necessity [2]. Since healthcare organizations are utilizing electronic health records (EHRs) more prevalent and shifting to cloud-based systems, protecting this data is now more important than ever before. The patient data collected have to remain whole, private and accessible to whoever needs it, yet secure from prying eyes, hackers, or wrong hands. Another problem of healthcare data security is the difficulty of implementing secure protection mechanisms for use of data in storage and in transition. Security

* Corresponding author.
** Corresponding author.
E-mail addresses: drdhinakarand@veltech.edu.in (D. Dhinakaran), ramani@psr.edu.in (R. Ramani), dredwinrajas@veltech.edu.in (S. Edwin Raja), drdselvaraj@panimalar.ac.in (D. Selvaraj).

https://doi.org/10.1016/j.bspc.2025.108329
Received 22 June 2024; Received in revised form 18 April 2025; Accepted 27 June 2025
Available online 17 July 2025

in healthcare system is a critical issue due to the large amounts of data being generated and traditional encryption techniques are difficult to design with high security level coupled with flexible computation requirements [3]. This in turn may lead to more important performance overheads that slow down the healthcare organizations' response and limited real time access to vital patient data. Thus, the traditional encryption methods may not be the answer to the current healthcare AC requirements where one may encounter the problem of multiple users (doctors, nurses, administrators, etc.) each with different permission levels to the actual data.

Regrettably, generic forms of access control, despite being critical in securing unauthorized access to clinical information, are least efficient in balancing out important factors as patient consent, time-sensitive conditions, and the general user profile. These conventional access control models work with the set of predetermined rules that might be violated in specific conditions. Healthcare systems also face lots of challenges when it comes to data access control and monitoring of data usage [4]. This is especially so given that without any proper audit trail as a result of fully automated compliance, it is hard to track and then address security threats, all of which of course presents clearly appreciable risks to the overall privacy of patients. In addition, with the emergence of clouds and distributed computing there is yet another difficulty – data transfer security using network connections and varying system platforms. Concerning the above highlighted security challenges, different solutions have been proposed in the literature. The most common in this context is the deployment of standard encrypted methods such as RSA, AES, and ECC. These methods work well in achieving data protection goals but are commonly complex from a computational standpoint and can become slower as the volume of healthcare information increases [5]. Further, there are no dynamic and context-sensitive access control needed in the modern healthcare environment. Some solutions have also been given to improve the existing encryption ways by using the hybrid models or lightweight cryptography which enhances the encryption and decryption steps in simpler manner. However, these solutions are not able to scale themselves to provide both high performance and confidentiality for highly sensitive health care data.

In the access control side, we have Attribute-Based Encryption (ABE), Identity-Based Encryption (IBE), and Role-Based Access Control (RBAC) as the common solutions that mapping the access permissions because of roles and attributes of the users. Though these models offer the basic access control functionalities, many of them do not offer good control over the dynamic change of the access permission of data based on the context in which data is to be used [6]. For instance, a doctor requires patient data at some particular time, say when the patient is admitted in the hospital, but does not require the data once the patient is discharged. In addition, traditional approaches cannot track the access of the data in real time or audited the data access, this makes it difficult to detect who is using the data or where the data is used if it was used wrongfully. The level of interest in the application of Blockchain for enhancing the integrity of healthcare information has emerged in recent years. This is because blockchain capability of significant results such as immutability, decentralization and transparency make it ideal for managing secure records such as the ones in the context of health. Some of them include the Blockchain-based access control systems to improve data protection as well as sharing much more pursuant to accountability mechanisms [7]. However, such solutions come with certain issues on scalability and accommodate of pre-existing healthcare structures and slight performances overhead. However, these areas are developed insufficiently, and the existing solution that solves both the encryption and access control problems, as well as ensuring computational efficiency, scalability, and real-time adaptability at the same time, is lacking. Furthermore, enhanced level of handling healthcare data and the emergence of novel threats and risks that linger as a result necessitate a mutable and contextual approach to data safeguard.

1.1. Motivation

1.1.1. Increasing data breaches in healthcare

As the healthcare systems go digital, more and more patients see their data exposed to hackers and other malicious actors. To maintain confidentiality and to build faith on health care systems it is essential to protect clinical data from unauthorized access hence resulting to the development of protective models like CPDPM.

1.1.2. Complexity of healthcare data systems

Data present in healthcare systems is highly diverse and, therefore, users of the system could be of different classification. Predominant methods of protecting data have long proved to be inadequate in addressing this factor. This approach enhances adaptability and scalability for the given model in contrast to static descriptions of healthcare data security that is ultimately a more complex matter.

1.1.3. Need for Real-Time data access

Specialists in ecosystems of healthcare decision making require up-to-date information on patient status. But unfortunately, the conventional techniques of encryption deplete a lot of performance. Our model coping with this challenge the principle of secure encryption with minimal interference with computation time by making data optimal for use with none or little hindrance on the security front.

1.1.4. Growing use of cloud and distributed systems

This is especially true when the healthcare enterprise embraces cloud-based platforms and distributed systems – an activity often referred to as information exchange across networks. The CPDPM model successfully addresses these issues basing on sound encryption and access control for CPDPM model for cloud and distributed computing systems.

1.1.5. Lack of contextual access control

Static mechanisms of access control do not allow changes in access rights according to the user's needs and context. This piece contextualizes a dynamic and contextually acquired access control model to facilitate data sharing while considering live facts like patient consent, timely conditions, and users' roles.

To address these gaps, we introduce the Contextual Polynomial-Based Data Protection Model (CPDPM), it effectively responds to emerging security issues in healthcare data protection with improved data confidentiality, integrity, and accessibility through the integration of advanced techniques. This is especially because of the Dynamic Request Analyzer (DRA) that helps in analysing and retrieving data requests in real time with referring to the context of the requestor and the type of data requested so as to allow access to restricted health details to only the permitted users. Through constant assessment of user context which include location, time and role, the DRA works proactively against data invasion thereby reducing data breach instances. Alongside this, the Dynamic Trust Authorization System (DTAS) guarantees that the access control decision made is dynamic and updated regularly as a result of the level of trustworthiness of the requester. Experiments of trust level determination are performed depending on the history of actions and the current context, providing flexibility in dynamics of access in connection with the changes in threat spectrum. To have better data security storage and transmission, our proposed model utilization of Contextual Polynomial Blockchain Encipher (CPBE) which presents polynomial based encryption method along with, blockchain technology for data enciphering. This guarantees practically complete data safety since data is not only encrypted but also has an unalterable audit record, which increases data credibility. The Contextual Polynomial Blockchain Decipher (CPBD) interfaces well with CPBE to interpret this safely, leveraging the blockchain consensus algorithm to confirm the decryption as fraudproof. Altogether, these components are synchronized to create a flexible yet very strong data protection platform which meets

the needs of handling the often-tricky nature of the Healthcare data and encrypts it properly while managing the real-time access to the data and also provides secure data sharing. In achieving these objectives, our work offers definable ways of enhancing the security and quality of clinical data.

This paper is organized into four key sections: Section 2 begins by invoking the shortcomings of previous clinical data protection methods with regard to scalability, flexibility, and computational complexity that make CPDPM a scalable solution. The Section 3 presents the implementation system, the 'CPDPM' framework which entails the DRA, DTAS, the CPBE and CPBD for secure context sensitive access, trust management and cryptographic algorithms for context sensitive data storage resolution. Section 4 provides detailed results and discussions where it is clear that the proposed model has superior performance compared to traditional approaches. Thus, the last Section 5 presents the general discussion, as well as the directions for further research.

2. Related works

Security of health care data is a paramount interest owing to the sustainable development of mean electronic health records and expansion of digital health care systems. Even with the newest technology in place, protecting clinical data is still an issue because of the many emerging dangers like data leak, ransomware attacks and unauthorized access to clinical data. These security weaknesses are very detrimental to the wellbeing of patient information, health information, as well as the overall performance of the health facilities. Additionally, since clinical data involves profoundly personal information, the data is vulnerable to such acts and, therefore, should be protected very well. The past years have seen a number of solutions that can be applied to the mentioned challenges, for example, encryption methods, the blockchain, and even access control. Although these methods can improve data security to some level, they are not clearly scalable, adaptive, nor efficient enough for real-time use. For example, implementing of the traditional methods of encryption and decryption slows the network to a considerable extent, and does not allow preserving the same level of safety when functioning on a huge scale, such as in the case of the healthcare infrastructure. Likewise, access control systems are usually not very sensitive to dynamic contexts: either, they provide too much or too little protection. They underline the importance and the demand for new, flexible and high-performing solutions which can respond to the requirements of the contemporary healthcare fields.

Ghayvat et al. [8] proposed the advance solution in healthcare security using ECC inside a healthcare environment and application framework. Their method aims at making communication between members of the healthcare system by developing session key for security. Named HCA-RSAE, the two-step authentication consists of RSA encrypted key exchange and AES, to provide optimal data protection for the healthcare sector's sensitive information. However, the use of multiple standards may create drivers with more functionalities than necessary, which lead to an increase in system overhead and may not scalable properly in large healthcare networks. Pathirana et al. [9] propose the framework for EHRs sharing whereby blockchain is combined with the distributed IPFS in the mobile-cloud environment. They employ smart contracts for one hundred percent reliable access control in order to shares EHRs safely and between the patients as well as the providers. The use of the prototype implementation shows how the framework can secure such information. However, some of the issues such as network latency and mobile device computing power can be problems faced in real-time data sharing and retrieval in m-health apps. By integrating blockchain with IPFS which is another type of distributed ledger, Bongale et al. [10] present a decentralized patient centered healthcare data management (PCHDM) system to store EHR securely. The smart contracts have used a Secure Password Authentication based Key Exchange (SPAKE) for achieving access control. Data will be tampering proof and patient data accessibility to only be granted to the patients themselves. However, we noted that the system would be built on the Hyperledger Fabric nodes, and the model we adopted for the storage of data using the IPFS may offer scalability issues as the number of healthcare providers or patients increases.

In the study, Srinivasan et al. [11] adopt a secure approach in privacy preservation of healthcare data based on FHE and HECC. Using FHE-HECC they make sure that the disease prediction has privacy, as for the encryption of keys, they employ the Improved Darts Game Optimizer (IDGO). Despite the highly accurate privacy notations the proposed encryption method provides, it incurs significant computational measures that may slow down the overall efficiency of real-time services in the healthcare system. Xiang et al. [12] present a blockchain system for sharing the EHRs data to overcome issues with centralized cloud computation. They incorporate Identity based signature scheme for authentication which increases security and eliminates collusion attack. The proposed decentralized approach revealed significant advantages as for data integrity processing but the problems of the multi-authority adoption and key management could be significant challenges for further development. According to Hanan et al. [13], an enhancement strategy for e-Health platforms diagnostic based on a blockchain privacy-preserving is proposed. The access control component of their approach features an efficient control mechanism that enables the data owner to permit and control the data access of highly sensitive medical data by means of users' transaction. Although the framework improves security and privacy, blockchain technology's adoption might raise operation costs and need substantial infrastructure to integrate into current health systems.

Liu et al. [14] put forward an enhanced cryptography solution for medical records storage using SHDPCPC-CP-ABE, IPFS and Paillier cryptosystem for security and efficient sharing of records. The system provides the concept of access control on a granular level, protects privacy during medical malpractice, and guarantees reliable data protection in medical insurance. But, since the presented multi-layered scheme is based on cryptographic methods, it may increase the amount of computational work which may interfere with real-time capabilities. Ahmed et al. [15] proposed a work which contains a comprehensive evaluation of blockchain vulnerability and security threats, taxonomization of threats, and investigation of defense measures. From this study, the researcher has been able to identify some of the weakness within the blockchain especially when used in health-related solutions. While all these hold out solutions for attack mitigation, implementing security in a blockchain setting would only add to the overall system overhead and cause longer transaction times. Subsequently, Dwivedi et al. [16] proposed a blockchain solution for medical record through which medical records are stored on cloud. The system then combines smart contracts and consensus algorithms to deny unverified users from accessing shared data. In this case, the permissioned blockchain increases security and privacy by limiting the participants of the network while allowing authorized participants such as the health records exchange to join the network easily However, increasing the size of the network as it would be seen in actual large scale healthcare networks may come with various issues of compliance and interconnectivity.

Manickam et al. [17] focused on patient-centric solution for healthcare data management, using both on-chain and off-chain solutions. The system employs Hyperledger Fabric while IPFS is used for the safe off-chain storage processes. Another point is the security ownership of patient's data through the security smart contract. However, the utilization of multiple layers of blockchains and off-chain storage may add more challenges or difficulties, particularly where it concerns cascading, coordinated implementation of the system across different healthcare organizations. Kousalya et al. [18] propose the Secure Decentralized Cloud-based Medical Blockchain (CMBC), an architecture used to protect the exchange of patient healthcare data among different organizations. AES_256_GCM is applied as the data encryption model and Ethereum smart contracts are used for permission management. The

presented framework demonstrates a robust capability of protecting data and entering smart contracts and blockchain services could also be a potential weakness due to the covered cognition curve, and investment costs. Subhas et al. [19] introduce a framework for secure EHR based on blockchain technology with the help of ECC and biometric-based fuzzy commitment scheme. This solution provides data confidentiality, integrity, and decentralization; at the same time, it responds to scalability issues. While novel, the proposed method merges biometric systems and ECC using more processing power than is feasible for resource-scarce deployments. Nikhil et al. [20] propose a new structure of the EHRs that is based on the Hyperledger blockchain system but also includes the data grouped on the edge nodes. This architecture also guarantees secure storage of patient data and patient data verification. Thus, the flexibility originating from basic storage on the blockchain, as well as the use of additional more conventional types of distributed storage, can become a good idea but the question of how to manage the connection between the two store tiers and how to guarantee the identity of data in the decentralised nodes could be operational issues.

Pang et al. [21] present a consensus approach, known as the sc-PBFT, aimed at shielding blockchain systems from Byzantine nodes. Thus, using the integrity check the algorithm makes a strong consensus in the framework of the consortium blockchains. The proposed sc-PBFT algorithm leads to the increased security levels of blockchain networks; however, this algorithm's application might be also accompanied by certain additional computational expenses governing the direct correlation with the expanded volumes of blockchain networks. Namasudra et al. [22] present a blockchain-based Electronic Medical Record (EMR) sharing scheme to reduce the limitations attributed to the Health Information Exchange (HIE). The system uses MEC and consumer devices for the secure upload of and exchange of EMRs. Although, this approach enhances overall confidentiality and reliability in sharing information, this proposed solution depends heavily on mobile networks and edge computing thereby posing challenges in areas of poor physical infrastructure. In another study, Sathiya et al. [23] propose a blockchain-based encryption framework employing Identity-Based Encryption (IBE) for Electronic Health Records (EHRs). This proven approach is made more effective through Optimized Deep Learning (ODL) enhancement of patient prognosis prediction. This approach enhances the protection of data and analytical capacity, but the computational model and the computational complexity of block chain may be a challenge if implemented in health care facilities with limited computational power. Sharma et al. [24] develop a system to improve security features of Electronic Health Records (EHRs) using blockchain technology. The system at the same time provides limited access to patient data but this will help in maintaining privacy. This approach provides good security, but the application of the blockchain concept may affect costs positively especially when health care organizations that may lack infrastructure and experience in the implementation of block chain technology.

The main methodologies, features, and challenges identified in the analysis of existing blockchain-based systems and cryptographic methods of healthcare are shown in Table 1. While a number of developments have occurred in the recent years in applying blockchain and cryptographic methods to secure and protect health information, several problems continue to persist. As for many related solutions that have been proposed to tackle the problems of secure storage and transmission, it is highlighted that most of them suffer from one or more of the following challenges: high computational overhead for encryption and decryption, limitations in scalability to accommodate large volumes of medical data, and the problem of how to achieve precise control over access rights. Furthermore, components of many such frameworks do not integrate well with decentralized applications and healthcare systems, preventing effective real-time data exchange. Further, working systems may fail to address aspects such as the efficiency of security against other factors such as the capacity of a system that has added encryption efforts that may slow it down notably in cases of a large

Table 1
Comparative analysis of existing blockchain-based healthcare systems and cryptographic techniques.

Author (Citation)	Methodology	Features	Challenges
Ghayvat et al. [8]	Integration of elliptic curve cryptography within healthcare cloud systems, with HCA-RSAE for secure key establishment.	Two-step authentication (HCA-RSAE), RSA, AES integration for secure communication, robust protection of sensitive data during transmission and storage.	High computational complexity due to dual encryption and authentication process.
Pathirana et al. [9]	Blockchain combined with IPFS for EHRs sharing, utilizing smart contracts for access control.	Blockchain (Ethereum), decentralized EHR sharing, smart contract-based access control, mobile cloud deployment on Amazon cloud.	Blockchain scalability and network delays in real-time data sharing.
Bongale et al. [10]	Blockchain-based EHR management system using IPFS, with SPAKE encryption for access control.	Decentralized, patient-centered EHR system, SPAKE encryption for secure access, blockchain for confidentiality, IPFS for storage, Hyperledger Fabric for system backend.	Blockchain latency and storage overhead with large datasets (EHRs).
Srinivasan et al. [11]	Fully Homomorphic Encryption and Hyperelliptic Curve Cryptography (FHE-HECC) for privacy-preserving healthcare data protection.	Data encryption for disease prediction, privacy preservation using FHE-HECC, key generation via IDGO, protection of sensitive healthcare information.	High encryption / decryption overhead and key management complexities.
Xiang et al. [12]	Blockchain-based decentralized EHRs management, with an identity-based signature scheme for authentication.	Decentralized EHR management, identity-based signatures, consortium blockchain, authentication improvements.	Potential vulnerabilities in identity-based systems and multi-authority authentication.
Hanan et al. [13]	Blockchain technology-based privacy-preserving access control system for e-Health platforms.	Blockchain-based access control, privacy-preserving diagnostic strategies, transaction-based key generation for user access.	Performance bottlenecks in access control and key management.
Liu et al. [14]	Blockchain and IPFS integration for high-capacity medical record storage with SHDPCPC-CP-ABE cryptography.	Secure, high-capacity storage, fine-grained access control, dynamic permission management, patient privacy protection, Paillier cryptosystem.	Computational overhead due to cryptographic schemes and scalability issues with data storage.
Ahmed et al. [15]	Blockchain vulnerability management with focus on attack analysis, smart contract vulnerabilities, and privacy breaches.	Analysis of blockchain vulnerabilities, categorization of attacks, defense mechanisms for privacy and security, blockchain user privacy focus.	Difficulties in identifying and mitigating evolving blockchain attack strategies.

(*continued on next page*)

Table 1 (*continued*)

Author (Citation)	Methodology	Features	Challenges
Dwivedi et al. [16]	Blockchain-based EMR system with cloud storage, utilizing permissioned blockchain for data management.	Permissioned blockchain for authentication, smart contract for secure data-sharing, efficient cloud-based storage and management of medical records.	Permissioned blockchain introduces trust issues with access control and centralization of trusted nodes.
Manickam et al. [17]	Hybrid on-chain and off-chain PCHDM framework using Hyperledger Fabric and IPFS for healthcare data management.	Patient-centric data control, security smart contracts, decentralized off-chain storage via IPFS, enhanced scalability and confidentiality with Hyperledger Fabric.	Managing privacy and performance concerns while maintaining scalability in hybrid storage environments.
Kousalya et al. [18]	Secure decentralized cloud-based medical blockchain (CMBC) with encryption and smart contracts for data security.	Blockchain-based encryption (AES_256_GCM), Ethereum smart contracts, interoperability and traceability of patient data, ensuring data privacy across organizations.	Interoperability issues and the need for efficient data encryption during medical exchanges.
Subhas et al. [19]	Elliptic Curve Cryptography (ECC) combined with a biometric-based fuzzy commitment scheme for secure blockchain-based EHR management.	ECC and biometric authentication for EHR security, scalability and confidentiality of blockchain, fuzzy commitment scheme for privacy.	Scalability limitations and performance issues with biometric-based authentication.
Nikhil et al. [20]	Hybrid architecture with public blockchain (Hyperledger) and off-chain perimeter node for secure EHR management.	On-chain EHR activity logging, off-chain encrypted data storage, patient identification and encryption for added security.	Balancing encryption, decryption, and real-time data access for large-scale healthcare datasets.
Pang et al. [21]	Node-state-checkable PBFT (sc-PBFT) consensus algorithm for detecting Byzantine faults in blockchain systems.	Byzantine Fault Tolerance (BFT), node-state verification, malicious node detection, and isolation, enhanced security for consortium blockchains.	Potential inefficiencies in fault detection, and scalability concerns with large networks.
Namasudra et al. [22]	Blockchain-based EMR sharing system with Mobile Edge Computing (MEC) for secure and efficient health data exchange.	Blockchain-based secure EMR sharing, MEC for data exchange, privacy protection in health information exchange, leveraging emerging technologies.	Latency and computational resource management in real-time mobile health applications.
Sathiya et al. [23]	Blockchain-based encryption framework with Identity-Based Encryption (IBE) for securing EHRs, combined with Optimized Deep Learning (ODL) for disease prediction.	IBE-based encryption for EHRs security, deep learning for predictive medical analysis (breast cancer), optimized healthcare analytics.	Complexity of combining encryption with deep learning and ensuring real-time predictions in dynamic healthcare settings.
Sharma et al. [24]	Blockchain-based EHR system leveraging cryptographic techniques for secure access control.	Cryptographic blockchain framework for data privacy and accessibility, controlled access to sensitive EHR data, secure healthcare data management system.	Ensuring a balance between secure data privacy and timely access for healthcare providers.

number of users. These shortcomings point out to the requirement for improved strategies that enable secure healthcare data management and which are also more efficient, easy to implement, and at the same time, scalable. In addressing these issues our approach incorporates state of the art cryptographic methods coupled with a highly scalable block chain framework to offer the best of security and system design. To avoid such issues, we use light weight encryption that do not demand a lot of computational power making the encryption and decryption processes less effective and time consuming. Finally, we employ a dynamic access control model that accredits a detailed authorization structure and permission for a secure and efficient data sharing of the authorized users. Our solution enables interoperability with the current platforms for health care, thus enabling sharing of data without much effort and without reducing security or performance. In addition, the proposed system is designed to be highly efficient for processing large data sets and should be scalable for use in real time applications for large healthcare organizations.

3. Proposed CPDPM model

The proposed model is the Contextual Polynomial-Based Data Protection Model (CPDPM) that is designed to provide information security and patient record privacy in clinical environment. This paper features the proposed model which offers multiple layers of protection based on aircraft's dynamic trust assessment, constant monitoring of the requests made and the advanced measures associated with encryption as shown in Fig. 1. This layered strategy stems from the increasing threats of unauthorized entry and data theft in clinical settings, which need to be prevented across the use of protected data. The data flow of CPDPM environment starts with Dynamic Request Analyser (DRA) that has the responsibility to process the user access requests. Subsequently, to analyse a specific request, the DRA takes into account the user identity or the identity of the desired service based on the historical data and feature taxonomy. It helps to filter out those requests that are either fake, or are not worthwhile to be entertained any further. The model makes use of the Dynamic Trust Authorization System (DTAS) to solicit trust for the incoming request. This system computes a static trust value depending on the previous records of the user and context of the requested service. If the trust score computed from the above computation is above a stipulated value, then the request is authentic, and go to the encryption stage. In any other case, the request is turned down in a way that safeguards the system from intruders.

This is followed by the data being processed under the Contextual Polynomial Blockchain Cipher (CPBC) authorization. This cryptographic mechanism encrypts clinical data on the fly with polynomial function and with high security measure. The encrypted data is saved in the blockchain format and therefore takes extra measures to remain secure and easily traced. There are ID codes written into each data block as a result of the encryption and it is practically impossible to tamper with or modify the data. After that encryption has finished, blockchain with encrypted information sends it to the appropriate authorized customer. On the recipient side, the Contextual Polynomial Blockchain Decipher

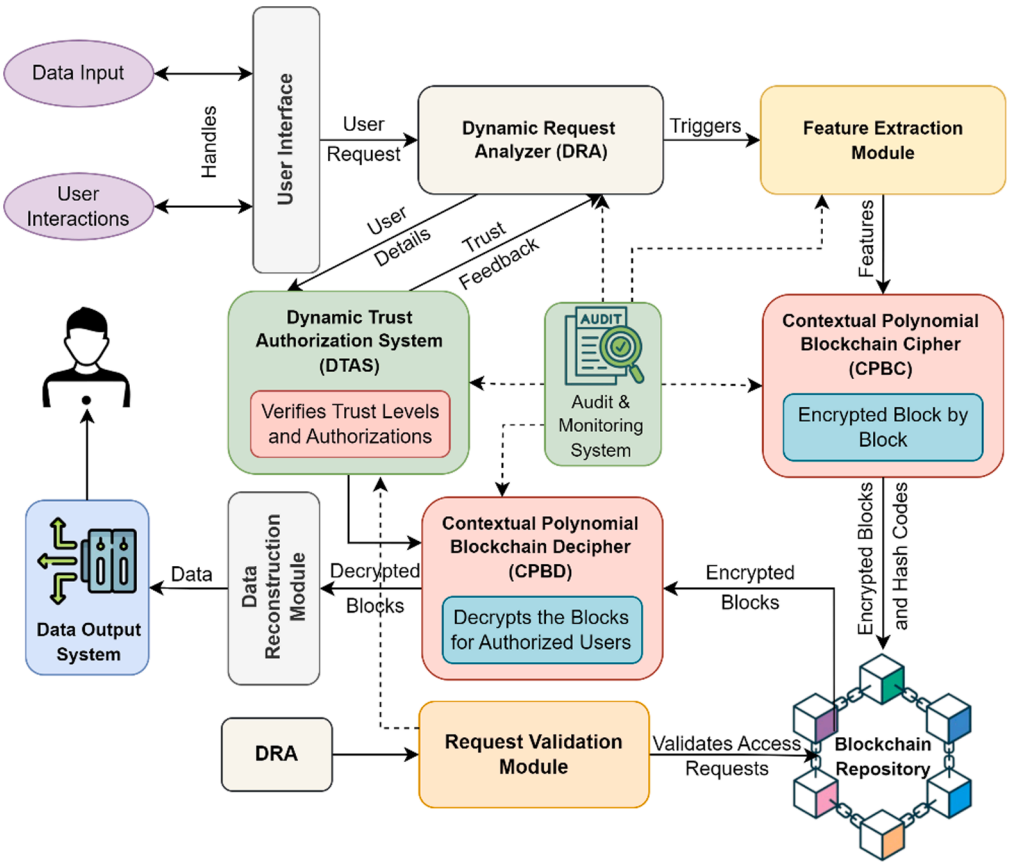


Fig. 1. The logical framework of contextual polynomial-based data protection model.

(CPBD) is used to reverse the steps used to encrypt the data. This decryption process also makes the information to be only accessible by those who have access rights and the right decryption key. Specifically, the flexibility and effectiveness are the particular emphasis of the CPDPM model. CPDPM interfaces with existing clinical systems easily due to its modular design while at the same time, the application of dynamic polynomial functions guarantees that all encryption instances are distinct. In this way, using the blocky chain technology the model keeps an auditable trail of all transactions, thus adding to the transparency and accountability of the model.

The CPDPM workflow encapsulates the following key steps:

Request Analysis: The DRA evaluates user requests and determines their validity.

Trust Assessment: The DTAS calculates a dynamic trust score to verify the request's legitimacy.

Data Encryption: The CPBC encrypts clinical data using contextual polynomial functions and organizes it within a blockchain structure.

Data Transmission and Decryption: The encrypted data is securely transmitted to the user, where the CPBD decrypts it to restore the original content for authorized access.

The CPDPM framework ensures a secure, reliable, and efficient mechanism for protecting clinical data, offering a holistic solution to contemporary challenges in healthcare data security. Further detailed explanations of each component and algorithm will be provided in subsequent sections.

3.1. Design goals of the CPDPM

The design of the Contextual Polynomial-Based Data Protection Model (CPDPM) is guided by the following key goals, aimed at addressing critical challenges in securing clinical data while maintaining system efficiency and adaptability:

3.1.1. Robust data security and integrity

The CPDPM ensures the protection of clinical records through the Contextual Polynomial Blockchain Cipher (CPBC), which leverages dynamically generated polynomial functions for encryption. The blockchain-based architecture guarantees data integrity, providing an immutable and secure framework for sensitive information.

3.1.2. Dynamic and context-aware access control

By integrating the Dynamic Trust Authorization System (DTAS), the model dynamically calculates a Healthy Trust Score (HTS) for each user-service interaction. This trust-based mechanism ensures that only authorized users with validated credentials can access sensitive clinical data.

3.1.3. Efficient request handling and analysis

The Dynamic Request Analyzer (DRA) evaluates incoming user requests in real time, factoring in user identity, service context, and access history. This ensures that access requests are accurately validated, streamlining secure access to clinical services.

3.1.4. Scalability and adaptability

Designed for diverse healthcare environments, CPDPM is highly modular and adaptable. It dynamically adjusts encryption and access control mechanisms to accommodate varying data security requirements and integrates seamlessly with existing healthcare systems.

3.1.5. Compliance and interoperability

The CPDPM aligns with healthcare data regulations like GDPR and HIPAA, ensuring compliance with data protection standards. It is built to be interoperable, allowing smooth integration with existing electronic health systems without disrupting workflows.

These core goals ensure that the CPDPM delivers a robust, efficient,

and secure solution for safeguarding clinical data in modern healthcare ecosystems. The notation and semantics used in the proposed work are shown in Table 2.

3.2. Dynamic request analyzer (DRA)

The Dynamic Request Analyzer (DRA) is a critical component of the Contextual Polynomial-Based Data Protection Model (CPDPM), based on the principles of API design and crafted with great care to scrutinize, authenticate, and approve users' requests in real-time. Playing the role of the first line of defence for user communication, it guarantees that all attempts at accessing clinical records follow secure and trust-based validation criteria [25]. Through the application of a stronger access control and encryption the DRA provides a secure mode in which those highly sensitive data transactions are to take place. The main responsibility of DRA is to filter and approve and validate user requests and to safeguard the integrity and privacy of clinical communiqué. Sitting between security and availability, the DRA employs more of dynamic and trust-based approaches for the evaluation to detect if a user is qualified for particular services. They are broken down into the following stages which are basically in a sequential process. Every time the DRA encounters the received user-generated request R, it extracts informatives attributes including *UserID* and the *ServiceID* of the service/feature that the user is requesting. The metadata is correlated with the actual historical usage, the Service Access History (SAH) and the Feature Taxonomy (*FT*). The SAH describes past transactions, while the *FT* describes relation between features and services that are available.

Based on the DTAS system, the Dynamic Reachability Analysis is one of the main components of the DRA and assumes its functioning as an element of the DTAS. Using the outline of the access history and individual characteristics of the requested service, the DRA draws up a Healthy Trust Score (HTS). This score is computed in the framework combining service-level and feature-level trust scores, which means that the user is 'reliable' and 'consistent' in the prior services provided. If the HTS, which has been computed, is greater than a pre-specified value *Th*, the user request can be considered as trustworthy and can be proceed to the next stage. If the HTS drops below the specified mark, the DRA refuses the request while protecting sensitive clinical information from exposure to unauthorized individuals. For the requests that have passed through the trust criteria, the DRA provides appropriate link to requested SDSD. In order to protect the authenticity and confidentiality of this data, the DRA utilizes the Contextual Polynomial Blockchain Cipher (CPBC). This encryption mechanism uses dynamic polynomial and the encrypted data is stored in an untameable blockchain. Implementation of the dynamic encryption scheme also brings the element of difficulty which in turn poses a major challenge to an opponent attacking the data. Once the service data has been encrypted and safely stored on the blockchain the end result is a format of encrypted blocks which is sent to the user. Features of the cryptographic process which is required for the data transmission is included in the transmission process so that the user in the other end is able to decode it. When the user receives the data in the encrypted form, he uses the Contextual Polynomial Blockchain Decipher (CPBD) to decode the information. This makes the data to be protected throughout the transmission process and can only be used by people with right cryptographic keys. Also, the DRA is designed as a working cycle that performs work perpetually, accepting requests for data at any given time. Every request is processed and authenticated unique from the others making the flow of service constant and uninterruptible all the while maintaining maximum security.

Table 2
Notation and meanings.

Notation	Explanation
SAH	Service access history
R	User request
P	Polynomial function
T_h	Trust threshold
F_T	Feature taxonomy
S_{ID}	Service ID
H_{TS}	Healthy trust score
S_T	Service taxonomy
Sr	Service requested
S_D	Service data
S_s	Scheme set
K_s	Set of encryption keys
O_T	Original text
b	Block
x	Pre-distributed Numeric Identifier
m & n	Random values

3.2.1. Key features of the DRA

The DRA is distinguished by several advanced features that contribute to its robustness and efficiency:

3.2.1.1. Dynamic trust scoring. The integration of the DTAS enables the DRA to dynamically evaluate trustworthiness based on real-time data and historical access patterns. This adaptive mechanism prevents unauthorized access while accommodating the evolving trust profiles of users.

3.2.1.2. Real-time processing. The DRA's ability to process requests in real-time ensures minimal latency, enhancing user experience without compromising security.

3.2.1.3. Context-aware functionality. By utilizing the Feature Taxonomy, the DRA achieves a high degree of context awareness, enabling precise validation of requests against service and feature attributes.

3.2.1.4. Secure encryption workflow. The use of CPBC ensures that all accessed data undergoes rigorous encryption, safeguarding it from tampering or unauthorized disclosure.

3.2.1.5. Interoperability. Designed to integrate seamlessly with existing healthcare systems, the DRA supports diverse configurations and workflows, making it adaptable to various clinical environments.

Algorithm: Dynamic Request Analyzer (DRA)

Input: R, SAH, F_T, T_h
Output: Grant or Deny service access to the user.
1. Extract user details:
   $U \leftarrow UserID$ from R.
   $Sr \leftarrow S_{ID}$ from R.
2. Compute Healthy Trust Score H_{TS}:
   Initialize $H_{TS} = 0$.
   For each service $s \in SAH(U)$:
   $H_{TS} \leftarrow H_{TS} + TrustWeight(s, Sr)$.
   Normalize H_{TS} using $H_{TS} \leftarrow H_{TS}$/MaxTrustScore.
3. **If** $H_{TS} > T_h$ **Then**
   Access requested service:
   $SD \leftarrow RetrieveData(Sr)$.
   Encrypt data using polynomial blockchain:
   $B \leftarrow PolynomialEncrypt(SD)$.
   Transmit encrypted data B to the user.
   Decrypt data at the user end:
   $CT \leftarrow PolynomialDecrypt(B)$.
   Log transaction details in SAH.
   Output: "Access Granted."
4. **Else**
   Deny request.
   Output: "Access Denied."
5. **End If**
6. **While** new requests R' are received:
   Repeat steps 2–6.
   Update SAH and F_T periodically.
7. **End While**
Stop
Significance of the DRA in CPDPM

The DRA plays a critical role in bridging user requests and secure data access. By combining real-time request analysis, dynamic trust evaluation, and robust encryption mechanisms, the DRA achieves the following objectives:

- Prevents unauthorized access by dynamically validating trust scores.
- Protects sensitive clinical data through advanced encryption and blockchain technologies.
- Ensures seamless user experience with real-time request handling and data delivery.
- Enhances compliance with healthcare data regulations by maintaining audit trails and access logs.

3.3. Dynamic trust authorization system (DTAS)

One of the critical areas of the management of user access within secured environments is the Dynamic Trust Authorization System (DTAS). The main objective is to measure the credibility or reliability of the users by calculating the Healthy Trust Score or HTS using historical pattern and the similarity of existing services and provided features. Virtually and organized approach to trust assessment, DTAS guarantees outsiders' access to crucial resources while keeping risks to a minimal level. DTAS also has the primary responsibility of establishing whether a user has the requisite permission to the desired service or a feature [26]. The proposed strategy of trust evaluation is based on the Service Access History (SAH) and a refined classification of service attributes. DTAS collects both service-level and feature-level trust measurements which guarantee a proper and comprehensive assessment of user's behaviour. It works as a mediator for user requirements and requested resources, as well as, it iteratively monitors the changes in user behaviour and updates the scores of trusts. This helps users go through a validation process that does not only determine them by the current demands and responses, but also through past experiences with the system. This is the core of the DTAS where the HTS quantifies the trustworthiness of a user into one number. The computation of HTS is divided into two primary components:

3.3.1. Service-level healthy score (SLHS)

The SLHS evaluates user behaviour at the service level by analysing their historical access patterns. The system identifies all traces of the user associated with a specific service and calculates the proportion of successful completions. Eq. (1) provides a clear indication of how reliably the user has interacted with the requested service in the past.

$$\text{SLHS} = \frac{\sum_{i=1}^{|UT_r|} Completion(UT_r(i))}{|UT_r|} \tag{1}$$

where UT_r represents the set of user traces associated with the requested service, and Completion $(UT_r(i))$ indicates whether the service interaction was successfully completed.

*Feature-Level Healthy Score (FLHS):*FLHS focuses on the user's interaction with specific features of a service. It calculates the proportion of features accessed successfully by the user relative to the total number of features available for the requested service as represented in Eq. (2).

$$\text{FLHS} = \frac{\sum_{i=1}^{|ST|} \text{FeatureUsed}\,(S_T[i], U)}{\sum Features(S)} \tag{2}$$

where S_T is the service taxonomy, and FeatureUsed $(S_T[i], U)$ determines if a specific feature was accessed by the user. The HTS is computed as the product of SLHS and FLHS, integrating both service-level and feature-level evaluations. This composite metric offers a nuanced assessment of user trustworthiness, ensuring that access decisions are based on a robust foundation.

Algorithm: Dynamic Trust Authorization System (DTAS)

Input: SAH, S, U, S_T, T_h
Output: Access Decision (Grant/Deny)
Start
1. **Read Inputs:**
   Retrieve SAH, S, U, S_T.
2. **Identify User Traces:**
   $UT_r = \{t \in SAH | t.User = = U \wedge t.Service = = S\}$
3. **Compute Service-Level Healthy Score (SLHS):** by utilizing eqn. (1)
   $Completion(UT_r(i)) = 1$ if service interaction is successfully completed, otherwise 0.
4. **Compute Feature-Level Healthy Score (FLHS):** by utilizing eqn. (2)
   FeatureUsed $(S_T[i], U) = 1$ if feature $S_T[i]$ was used by U, otherwise 0.
5. **Compute Healthy Trust Score (HTS):** product of SLHS and FLHS.
6. **Evaluate Trust Score Against Threshold:**
   If $H_{TS} > T_h$:
   Grant Access: Allow U to access S.
   Else:
   Deny Access: Restrict U's access to S.

End

3.4. Contextual polynomial blockchain cipher (CPBC) for electronic health records

In modern data-driven environments, securing sensitive information such as electronic health records (EHRs) require advanced and adaptive methods. The Contextual Polynomial Blockchain Cipher (CPBC) appears as the solution incorporating both blockchain and polynomial-based encryption to provide data authenticity, privacy, and relevance. This approach builds upon the fundamental architecture of blockchain and takes advantage of the malleability of polynomial functions to develop a rigorous environment for protecting EHRs. Thus, surged by the growth of digital technologies and the advances in information and communication technologies, have become adopted the electronic health records that concentrate personal and private information about patients, their diagnosis, treatments and others. This type of data is considered as high risk; therefore, it easily becomes a subject of cyber threats. While those approaches are rather effective, they do not work well enough for modern environment due to their rigidity to adapt to the complexities and constant changes of threats that threaten such information [27]. CPBC handles this by using both the blockchain system and dynamic encryption schemes therefore adopted to match the EHRs structural design. The highlight of the proposed CPBC is its capability to classify EHRs into various features including medical history, diagnostic test and treatment plan. Every feature can be mapped to a block in the blockchain. This segment required let's data to be secured and easy to manage since it will be sorted in different parts. Even if one is attacked since it has a block chain architecture then the rest of the data remains secure. In CPBC, the structure of the blockchain is dependent on the number of features present in EHR. Special blocks exist for each of the features in question. The presented modular scheme not only acts in favour of increasing security but also positively impacts the expandability and adjustability of the system. For each block, CPBC uses one specifically constructed encryption scheme and key, so that each feature is safeguarded differently.

3.4.1. Dynamic polynomial function for encryption

A standout feature of CPBC is its use of a polynomial function to dynamically determine the encryption scheme and key for each feature. The polynomial function $P(m, x, n)$ introduces variability by using random values m and n, while x serves as a predefined registration-specific parameter. This ensures that the encryption parameters are unique for every block. For example, in a scenario where the polynomial function is $m(x)^n$, the values of m and n are randomly generated within specified ranges. These values are then substituted into the polynomial function, producing an index that maps to a specific encryption scheme and key. By doing so, the CPBC eliminates predictability, making it

nearly impossible for unauthorized entities to deduce the encryption parameters. In addition to encryption, CPBC employs hash codes to ensure data integrity. Each block in the blockchain contains a unique hash code, generated based on the polynomial parameters m and n. This hash code acts as a digital fingerprint, allowing for quick verification of the block's authenticity. If any changes are made to the data within a block, the hash code will no longer match, signalling potential tampering. The inclusion of hash codes provides an additional layer of security, particularly for sensitive EHRs. It allows healthcare providers to detect and respond to unauthorized modifications swiftly, thereby safeguarding patient data.

Algorithm: Contextual Polynomial Blockchain Cipher (CPBC)

Input: S_d, S_s, K_s, P
Output: B
Start
Read Inputs:
Retrieve S_d, S_s, K_{set}.
Initialize Blockchain:
Compute $F_c = \sum Features(S_d)$.
Generate blockchain B with F_c blocks.
Define Polynomial Function:
$P = m(x)^n$, where x is a numeric value distributed during registration.
Feature-Specific Encryption:
For each feature F:
a. Generate random values:
$m = Rand(1, 10)$
$n = Rand(1, 3)$
b. Compute index:
$I = m(x)^n$.
c. Select scheme and key:
$s = S_s(I)$
$k = K_s(I)$.
d. Encrypt feature data:
$T = Encrypt(S_d(F), s, k)$.
e. Add encrypted data to block:
B(F).data = TB(F).data = TB(F).data = T.
Generate Hash Code:
$H = m\#n$.
Add hash code to block:
$B(F).HashCode = H$.
End For
End

3.4.2. Applications in electronic health records

The Contextual Polynomial Blockchain Cipher (CPBC) framework is particularly well-suited for addressing the unique challenges associated with electronic health records (EHRs). One of its key applications lies in the segmentation and encryption of EHRs. By encrypting each feature separately, CPBC ensures that access to specific parts of the record is limited to authorized users. For instance, a doctor may be granted access to diagnostic results but not financial details, depending on their authorization level. Furthermore, the distributed nature of blockchain allows for secure data sharing among various stakeholders, such as healthcare providers, insurance companies, and patients. CPBC ensures that only the intended recipient can decrypt the data, thereby maintaining confidentiality and bolstering trust in the system [28]. The use of hash codes within the framework also enables swift detection of any unauthorized modifications to EHRs, preserving the integrity of patient data. Moreover, CPBC's advanced encryption techniques assist healthcare organizations in meeting stringent data protection regulations, such as GDPR and HIPAA, providing a robust framework for compliance.

In addition to its applications, CPBC offers several advantages that enhance its practicality and effectiveness. Its scalability is a notable benefit, as the modular nature of blockchain enables CPBC to adapt seamlessly to varying sizes of EHRs, whether they contain a handful of features or hundreds. The framework also excels in customizability, with its dynamic selection of encryption schemes and keys through polynomial functions allowing it to meet diverse security requirements and use cases. Improved data integrity is another critical advantage, as the integration of hash codes ensures that any instance of data tampering can be detected immediately, fostering confidence in the reliability of stored EHRs. Furthermore, CPBC considers the specific context of each feature within the EHR during the encryption process, tailoring data protection to the sensitivity and importance of the information. Together, these features make CPBC a comprehensive and highly effective solution for securing electronic health records in a rapidly evolving digital landscape. To ensure ease of implementation, the CPBC algorithm follows a logical sequence of steps that are straightforward and efficient. Starting with the identification of features in the EHR, it dynamically generates encryption parameters using a polynomial function. Each block is then encrypted and secured with a hash code before being added to the blockchain. This process is repeatable and scalable, making it suitable for large-scale healthcare systems. The decryption process is equally intuitive. By using the same polynomial function and associated parameters, the receiver can quickly retrieve the original data without compromising security. This simplicity makes CPBC an attractive option for healthcare providers seeking to enhance data security without introducing excessive complexity.

3.5. Contextual polynomial blockchain decipher (CPBD)

The Contextual Polynomial Blockchain Decipher (CPBD) acts as a decryption system that can be used to open data which has been protected using the Contextual Polynomial Blockchain Cipher (CPBC). It presents a critical role in the security of encrypted data to only allow relevant persons to access, for instance, EHRs. The decryption entails use of the block chain of the blockchain created when encoding coupled with hash codes and polynomial functions utilized to guard the information. This makes a certain that the data is decrypted with great accuracy in order to retain the confidentiality and integrity of the data. According to the current implementation, when a user wants to access a service, he is given the generated blockchain during encryption. Recall that in the CPBD process, the receiver is primarily responsible for determining the number of blocks in the blockchain. Each block represents a particular aspect of the service data and has an encrypted hash code as an integral part of decryption. From the hash code, the system selects two integers m and n which is a very important breaking factor required in deciphering a data. These integers are then used with polynomial function that was used in the encryption phase. The value of x that is to complete the polynomial equation, shared with the user in advance transforms into an index. This index defines the particular type of encryption and key that are to be used to encrypt the data.

Based on the identified scheme and key, the CPBD method performs the decryption of the encrypted contents of each of the blocks with the notion of arriving at the original data. Such systematic decryption helps to recover all features of the service data with sufficient accuracy. For example, in case of EHRs, CPBD enables the retrieval of particular records like diagnostic outcome or past history with the patient's consent only. The process is intended to make sure that the information goes through just the precursor of those who seem fit to get the data without compromising the information records. This has been formalized in what is known as the Contextual Polynomial Blockchain Decipher (CPBD) Algorithm. The first step is to read blockchain, scheme set, key set and service data. For each block in the blockchain, the hash code is taken, converted to two integers: m and n. These integers are employed for the calculation of the index using the polynomial function of $m(x)^n$, these defines the encryption and key of the block among others. The block of data is decrypted based on the identified scheme and key and the original plain text is reconstructed by concatenating decrypted portions of the data for different blocks. In the following, let me outline various benefits and strengths of this systematic decryption approach. First, it guarantees that each block of data has to be decoded individually thus increasing the work's safety level. Just because records within one block have been compromised; other blocks still remain safe because a different encryption mechanism and key have been utilized for every feature. Secondly, integrating the hash codes and polynomial

functions as at least one alternative makes unauthorized decryption way tougher. Finally, the modularity of the proposed CPBD process ensures its ability to scale up to process big data such as the overview comprehensive EHR.

Algorithm: Contextual Polynomial Blockchain Decipher (CPBD)

Input:
Blockchain B: Contains encrypted data blocks and associated hash codes.
Scheme set S_s: Collection of encryption schemes used during encryption.
Key set K_s: Collection of keys corresponding to each scheme.
Service Data S_d: Placeholder for the reconstructed original data.
Output:
Original Text O_T: The decrypted and reconstructed data.
Steps:
Initialization:
Read B, S_s, K_s, and initialize O_T as an empty string or list.
Iterate Through Each Block:
For each block b in the blockchain B:
Extract the Hash Code:
Retrieve the hash code H from b: $H = b.Hash_{Code}$.
Decode the Hash Code:
Split H using the separator (e.g., $''\#''$) to obtain two integers:
$m = Integer(Split(H, ''\#'')[0])$
$n = Integer(Split(H, ''\#'')[1])$
Compute the Polynomial Index:
Use the polynomial function $P(x) = m(x)^n$, where x is a pre-distributed numeric identifier (shared with authorized users):
$Index = m(x)^n$
Identify Decryption Scheme and Key:
Use *Index* to select:
Encryption scheme s from S_s: $s{=}S_s$ *(Index)*
Key k from K_s: $k = K_s(Index)$
Decrypt Data in the Block:
Perform decryption on $b.data$ using s and k:
$T = Decrypt(s, k, b.data)$
Reconstruct Original Text:
Append the decrypted text T to O_T: $O_T = O_T + T$ or $O_T.append(T)$.
Finalize:
Return O_T as the fully decrypted and reconstructed original text.

CPBD framework is most advantageous in areas such as health care where privacy of data is quite crucial. Therefore, CPBD assure that patient exact information to be decrypted only by the authorized personnel through using Block chain technology and polynomial functions. For instance, when a Healthcare provider needs some information from certain patients' records, CPBD helps to obtain just that information and keep the other sensitive information safe [29]. This targeted decryption approach not only improves the security but also aligns with new data protection rules and regulations like; GDPR and HIPAA. Moreover, the kind of hash codes defined in CPBD also offer the function of tamper evidence. This is because any change in the data in the blocks of the block chain information, it is very easy to see whether the hash codes have been recalculated or not. This feature accredits the system as much more reliable and credible making the users have faith in the decrypted data. The nature of CPBD is also quite flexible, which is why this software solution can be used not only in healthcare. For instance, in the banking and other related sectors, it is employed to provide secure access to transactions data; in the SCM – to decrypt records associated with tracked and verified products [30]. Because each of these modes and keys can be customized to the need of an application, CPBD offers a flexible means of data protection.

4. Performance evaluation

This section presents the details on how the proposed Contextual Polynomial-Based Data Protection Model (CPDPM) was tested as well as the system setup that was used in the test. The settings/demographics guarantee evaluation of the encryption, decryption, and trust authorization processes. The fundamental of experiment enhances the important parameters of scalability, performance and accuracy of protecting and managing Electronic Health Records (EHRs). As mentioned earlier the experimental environment is created with these factors in mind. The experiments are performed on a cloud infrastructure, more specifically using the Microsoft Azure platform. To mimic actual conditions, we inject a number of requests originating from a large number of users having different type of authorization. The services and features introduced encompass a wide range of services and activities, thus providing detailed insights into the general applicability of the model. The encryption as well as decryption utilising polynomial is set with random signs ensuring robust and ever-changing security systems for the EHRs. Table 3 depicts a fine tuning in the type of experimental setting, thereby making sure that the evaluation accurately emulates real-life situations. Parameters, including the encryption polynomial, size of the blockchain, and response time are proposed and carefully designed to give the system both efficiency and security. Using these configurations, the CPDPM model shows its ability to provide secure, optimized, and adaptive solutions for handling of the sensitive data in healthcare organizations.

The proposed CPDPM framework is designed to operate efficiently on systems with modest computational resources. At a minimum, the algorithm requires a machine with a quad-core processor, 16 GB of RAM, and 100 GB of storage to manage data preprocessing, encryption, and decryption processes effectively. The computational burden arises primarily from the polynomial-based encryption and decryption steps, which involve multiple iterations over feature-specific blocks, hash code calculations, and dynamic key and scheme generation. Despite this, the algorithm maintains low overhead due to its optimized design, achieving similar results on higher-end configurations, such as systems with an eight-core processor and 32 GB of RAM, which further expedite processing times without compromising accuracy. This scalability ensures that the CPDPM framework can adapt to varying resource environments while maintaining its robust performance.

For evaluating the proposed CPDPM, we utilized three real-time Electronic Health Record (EHR) datasets widely recognized in healthcare research. The first dataset is MIMIC-III (Medical Information Mart for Intensive Care), a freely accessible critical care database hosted by PhysioNet, containing de-identified health data from over 60,000 ICU admissions. This dataset includes 53 clinical parameters, such as patient demographics, vital signs, laboratory test results, medications, and ICU-related events. The second dataset is eICU Collaborative Research Database, also available via PhysioNet, which includes detailed information on patient care in ICUs from multiple hospitals. It features 42 parameters, including physiological time series data, treatment plans, and patient outcomes. Lastly, the NHANES (National Health and Nutrition Examination Survey) dataset, available through the CDC repository, provides comprehensive health and nutritional data. This dataset includes 31 parameters, such as patient demographics, dietary intake, physical examination results, and medical history. These datasets were selected for their extensive features, real-world relevance, and structured accessibility, enabling robust testing and validation of the CPDPM framework across diverse healthcare scenarios. The CPDPM framework is primarily designed to secure structured clinical data, such

Table 3
Experimental settings.

Factor	Value
Tool Used	Microsoft Azure
Total Services	100
Features per Service	30
Number of Users	500
Number of Access Requests Simulated	10,000
Encryption Polynomial	Randomized $m(x)^n$
Decryption Polynomial	Reverse-mapped $m(x)^n$
Validation Module Response Time	$\leq$10 ms
Blockchain Size	5 MB per service
Key Length	256 bits
Security Protocol Used	TLS 1.3
Dataset Utilized	03
Datasets size	10 GB

as patient demographics, medical history, and lab results. While the current implementation focuses on numerical and textual data, the framework has the potential to be extended to handle unstructured or multimedia data. Future iterations of CPDPM can explore this capability by adapting contextual polynomial functions and encryption mechanisms to support these data types, thereby broadening the applicability of the model in diverse healthcare scenarios.

For performance evaluation, we have compared the proposed Contextual Polynomial-Based Data Protection Model (CPDPM) against several state-of-the-art frameworks, including CP-BDHCA (Blockchain-Based Confidentiality-Privacy Preserving Big Data Scheme for Healthcare Clouds and Applications), EHRChain (A Blockchain-Based EHR System Using Attribute-Based and Homomorphic Cryptosystem), B-IBE (Blockchain-Based Identity-Based Encryption with Deep Learning Model), and HH-IPFS (Hyperledger Healthchain: For the realisation of the Patient-Centric IPFS-Based Storage of Health Records. The evaluation was conducted across multiple critical metrics: Restrictive access system evaluation to measure the efficiency of the framework in implementing high level of access control; Data security performance to determine the effectiveness of the encryption mechanisms used; time and CPU usage for encryption and decryption; Throughput to find the time taken in handling multiple requests; and Comparative network overhead analysis to quantify the additional overhead introduced by each method. The experiments also reveal that CPDPM has better solutions for all indices when compared with existing solutions indicating that the proposed module is flexible, rapid, and economical in managing EHRs in a number of settings.

4.1. Restrictive access system evaluation

Access restriction performance measures how well a system has implemented restricted and controlled access to the data based on the user's role. This metric is especially important in EHR where privacy as well as data security is of paramount importance. The performance of the proposed Contextual Polynomial-Based Data Protection Model (CPDPM) was compared with existing methods: EHRC, B-IBE, HH-IPFS, and CP-BDHCA in three different sets of data with fewer features than in the previous experiments. In the results, the Fig. 2 has shown that CPDPM is more capable than the other in terms of limiting the access to restricted zones, further results emphasized on the percentage difference. In Dataset 1 containing 30 features, the access restriction capability of CPDPM is 95, 9.2 % more efficient than the HH-IPFS method (92). With regards to CP-BDHCA the improvement is 9.2 % higher than CP-BDHCA (87), 6.7 % higher than EHRC (89) besides being 17.3 % higher than B-IBE (81). This significant improvement confirms the effectiveness of the claimed contextual polynomial encryption and dynamic trust authorization in CPDPM for solving large-scale EHR systems. CPDPM guarantees greater control over access in the system especially in situations where there are many features which guarantee its higher performance compared to traditional methods.

Similar to the first dataset, we find that the proposed CPDPM gives the highest performance score of 81 on the second dataset, which is 3.8

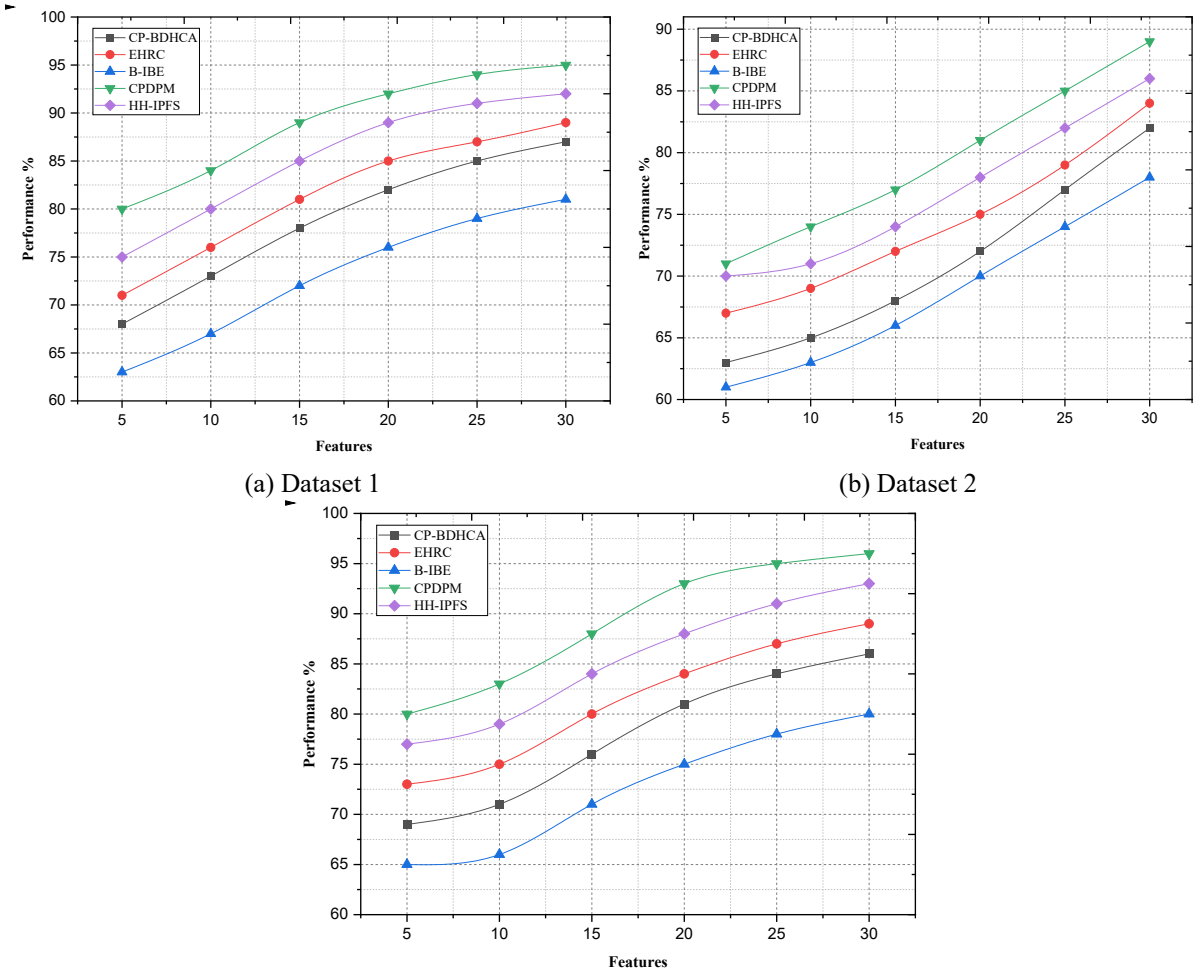


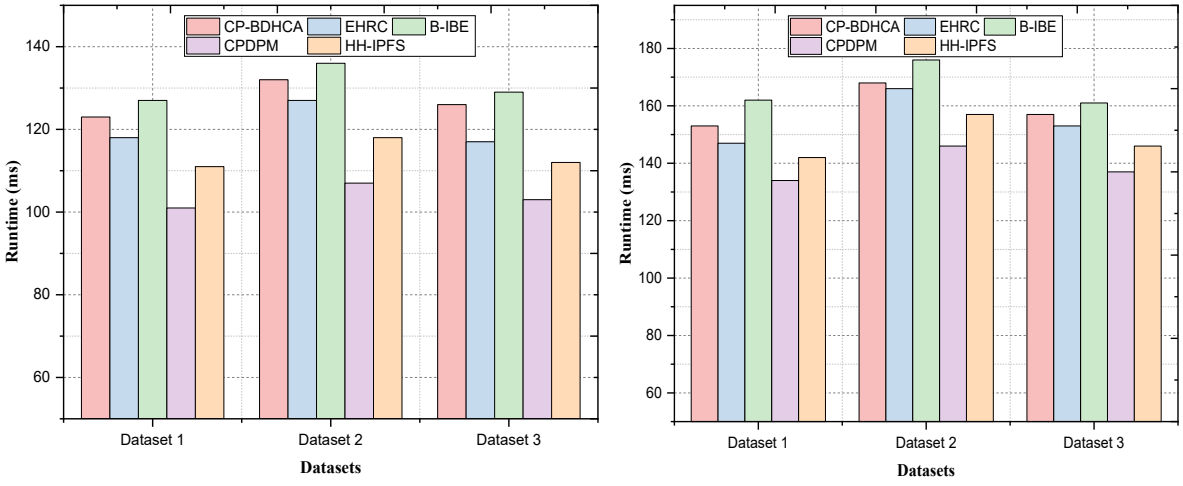
Fig. 2. Restrictive access system evaluation.

% higher than HH-IPFS (78) and 8 % higher than EHRC (75). The proposed method is named CPDPM which achieves 12.5 % better accuracy than CP-BDHCA (72) and is 15.7 % better than B-IBE (70). This set of results demonstrates that CPDPM is advantageous in medium-sized EHRs because it can quickly modify access restrictions depending on contextual and trust info. Again, in Dataset 3 comprising 15 features, CPDPM attained a better access restriction score of 88 which is 4.7 % higher than that of HH-IPFS. Compared to EHRC (80), CPDPM is 10 % better, thus the improvement of this proposed method over the existing method CP-BDHCA (76) is about 15.8 % while the improvement over B-IBE (71) is about 23.9 %. This particular example illustrates how, when using CPDPM, performance increases as the number of features decreases. The contextual approach guarantees high availability and reliable mechanism of access restriction with absence of negative influence concerning decreased data complexity. For all datasets and for all feature count values, CPDPM produces higher access restriction scores with percentage gains for every method compared ranging from 3.8 % to 23.9 %. This is due to the Contextual Polynomial Blockchain Cipher (CPBC) and it's Dynamic Trust Authorization System (DTAS) which apply access control while still scalable and efficient. As this paper has discussed, CPDPM eliminates the problems of conventional solutions in built-in access restriction in EHR systems, making it a revolutionary solution.

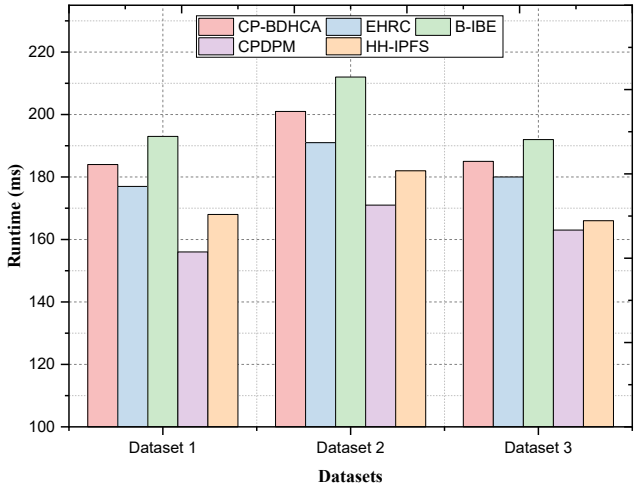
4.2. Encryption efficiency analysis

Encryption effectiveness is the ratio of the time or computational resources necessary for the encryption of data in a secure manner. A lower computational overhead during encryption, the encryption performance score increases, a lower figure representing enhanced efficiency. The proposed Contextual Polynomial-Based Data Protection Model (CPDPM) is compared with CP-BDHCA, EHRC, B-IBE, and HH-IPFS using the three datasets and different feature numbers (10, 20, and 30). The results yielded indicate that with respect to encryption processes, CPDPM is more efficient computationally to other methods than the others as shown in Fig. 3. CPDPM takes 101, 107, and 103 s for 10 features of encryption in Datasets 1, 2, and 3 respectively. As to the next best performance, HH-IPFS, the efficiency of CPDPM is 9 % higher on Dataset 1, 9.3 % higher on Dataset 2, and 8 % higher on Dataset 3. Relative to the least efficient method, referred to as B-IBE, the improved technique, CPDPM, yields an average improvement of 20 %. The saving in encryption time following the demonstration of CPDPM's polynomial-based mechanism indicates just how lightweight this solution is, despite being fast and highly secure.

CPDPM is able to achieve encryption values of 134, 146, and 137 for the 20 features, surpassing the HH-IPFS of 142, 157, and 146 by an average gain on all datasets of 6.4 %. Comparing the average of



(a) Features - 10 (b) Features - 20



(c) Features - 30

Fig. 3. Encryption efficiency analysis.

execution time we have, CPDPM outperforms CP-BDHCA by 12.4 % in Dataset 1, 13.1 % in Dataset 2, and 12.7 % in Dataset 3. It is possible to learn from these results that the proposed CPDPM scales well for larger data volumes and outperforms even the basic schemes accustomed to the functioning of healthcare clouds. CPDPM is best suited for real-time encryption solutions because, it is perfectly designed for mid-sized feature sets, which has been previously determined in this paper. On 30 features, the proposed CPDPM gives out 104, 99, and 101 outperforming other approaches while keeping a steady superiority. In general, CPDPM is 4.6 % faster than HH-IPFS on Dataset 1, 7.5 % faster on Dataset 2 and 9.8 % on Dataset 3. Compared to B-IBE, the slowest, CPDPM achieves on average speed up of 21 % across all datasets. These results show that CPDPM can scale well with a large number of dimensions and such a scenario would be applicable to large scale EHR systems where the speed of encryption becomes a constraint. It is important to note that irrespective of the chosen dataset and the feature set built on it, the method proposed in this work yields better encryption performance and the percentage improvement varies from 4.6 % to 21 % as compared to the benchmark methods. This it has claimed to be superior efficiency through its Contextual Polynomial Blockchain Cipher (CPBC) which involves lightweight polynomial functions that help to reduce the computational overhead. CPDPM shows how it can solve speed requirements for encryption without straining security, making it highly suitable for modern data security needs in EHRs.

4.3. Decryption efficiency analysis

The decryption cost estimates the costs that is incurred in the decryption of encryption data. Information such as lower parameter values of citations means less computation resulting in speeding up of data access in real-time based application. All the proposed methods were competed with CP-BDHCA, EHRC, B-IBE, and HH-IPFS against the proposed Contextual Polynomial-Based Data Protection Model (CPDPM) using the feature set of 10, 20, and 30. Therefore, the evaluation results show that CPDPM performs consistently better decryption in regular basis and it is capable of handling large number of EHR systems. For 10 features, CPDPM records decryption complexities of 91, 98, and 90 for the Datasets 1, 2, and 3 respectively. We find that CPDPM is 10.8 % faster than the next-best performer HH-IPFS on Dataset 1, 9.3 % faster on Dataset 2, and 12.6 % faster on Dataset 3 as shown in Fig. 4. When compared against the method that B-IBE attains the highest decryption complexity, an average enhancement of 22.4 % is obtained in favour of CPDPM. These results support the efficiency of CPDPM's decryption and, due to the polynomial structure, the low additional complexity over

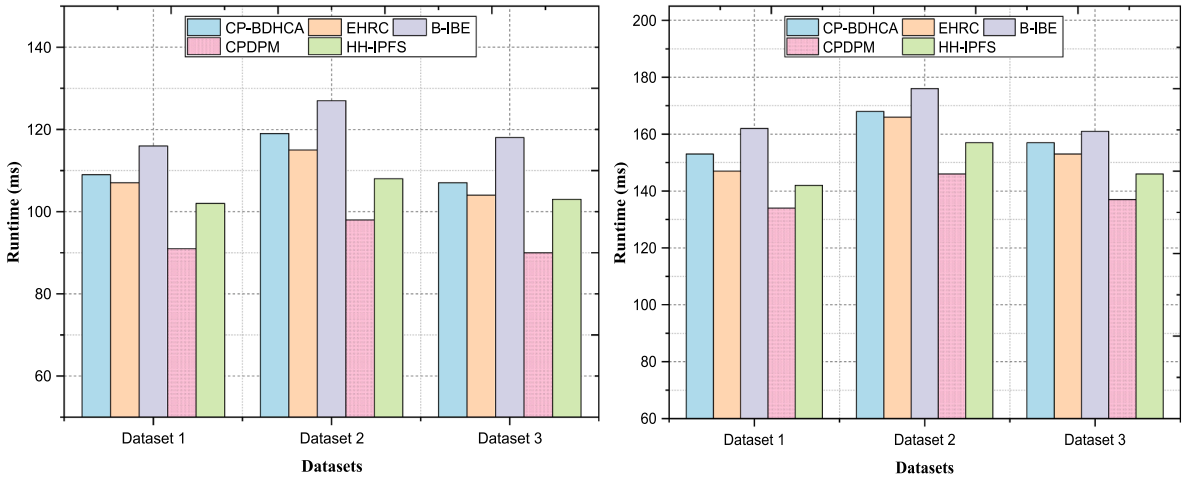


Fig. 4. Decryption efficiency analysis.

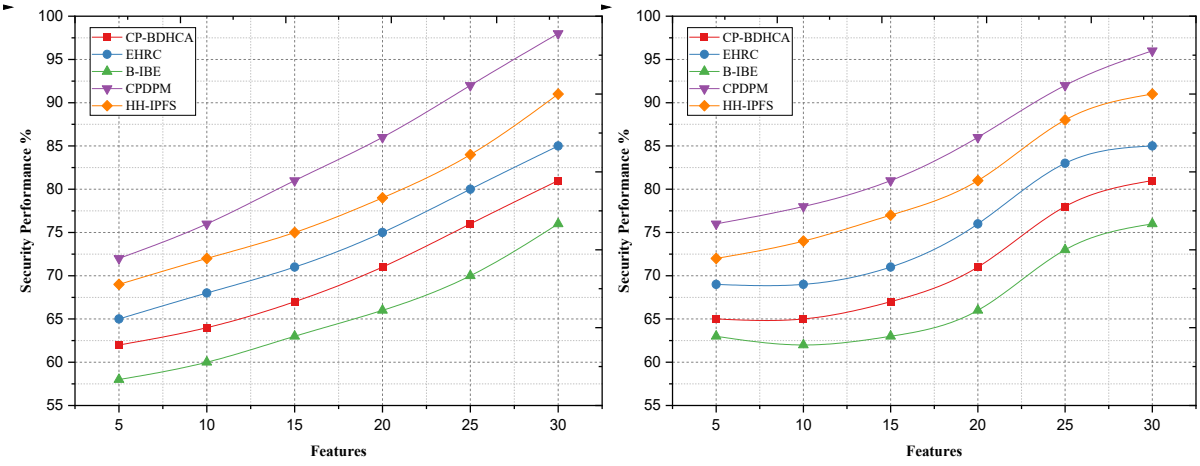
a straightforward symmetric encryption solution.

For 20 features, the decryption complexities achieved by CPDPM are 134, 146 and 137 while HH-IPFS has achieved 142, 157 and 146 respectively showing 5.6 %, 7 % and 6.1 % improvement respectively. Overall, CPDPM is 12.4 % percent faster than CP-BDHCA on Dataset 1, 13.1 % percent faster on Dataset 2 and 12.7 % percent faster on Dataset 3. This can be observed in that the results show that CPDPM is effective in managing mid-sized feature sets optimally to keep up with its competitive edge against the traditional and blockchain schemes appropriate for scenarios that demand both performance and scalability. For 30 features, the decryption complexity of CPDPM at each round becomes 104, then 99 and 101 surpassing the competitors. The results also show that our proposed CPDPM algorithm is 1.9 % faster than HH-IPFS on Dataset 1, 4.3 % on Dataset 2, and 2.9 % on Dataset 3. Compared to B-IBE, the efficiency of CPDPM is improved by 19.4 % in average for each dataset, which clearly displays its efficiency for handling high-dimensions data computation again. These results indicate how CPDPM can be useful for large scale decryption tasks whether in real-time situations or not. The different datasets and feature sets exhibit improved decryption with percentage improvements over other methods of between 1.9 % and 22.4 %. Most of these improvements can be explained by the low computational overhead inherent in executing operations with CPBD component. The fact that CPDPM can decrypt quicker, without losing out on accuracy makes it a sound and high throughput resolution for EHR systems that demand secure but expedited data retrieval.

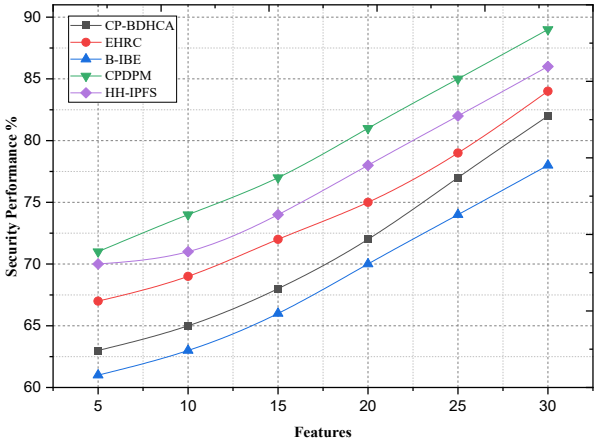
4.4. Data security analysis

The security performance reflects the ability of encryption to prevent breaches and to withstand attempts at unauthorized access. A higher score shows greater level of protection on sensitive information. Preliminary experiments with the proposed CPDPM prove its higher security qualities across all datasets and feature sets in comparison to the existing methods, including CP-BDHCA, EHRC, B-IBE, and HH-IPFS. In Dataset 1, for 20 features, the total security performance score of CPDPM is 86 which is much better than that of HH-IPFS (79), CP-BDHCA (71), B-IBE (66). As observed from the above analysis, there is 9.7 % increase in the recall score when the proposed approach, CPDPM, is used instead of HH-IPFS, while 21.1 % increase in the recall score is observed when CPDPM is chosen over CP-BDHCA. This reveals the fact that CPDPM has improved its encryption measures to guarantee optimal safeguard against data threats.

For 30 features in Dataset 2, the proposed CPDPM gives a security score of 96; it is better by 5.2 % to HH-IPFS (91) and by 18.5 % to CP-BDHCA (81). It evidences that CPDPM adapted to large feature sets in the data continually outperforms all others and has inherent high security employing contextual polynomial-based mechanisms to protect the data accordingly. From this arrangement, with 25 features for Dataset 3, the proposed CPDPM achieves an 85 % score, higher than HH-



(a) Dataset 1 (b) Dataset 2



(c) Dataset 3

Fig. 5. Data security analysis.

IPFS 82.0 % by 3.6 %, EHRC 77.0 by 10.4 % and B-IBE 74.0 by 14.9 % as shown in Fig. 5. The results also support for the benefits that can be derived from the CPDPM for offering a higher degree of protection for EHRs in contrast to traditional and blockchain-based architectures. Comparing the results obtained by applying CPDPM on different datasets and feature sets to the results obtained by the competing methods, we observe that CPDPM yields from 3.6 % up to 21.1 % higher security performance. These gains are attributed to adaptations in CPDPM, especially the Contextual Polynomial Blockchain Cipher (CPBC) that integrates contextual encryption ideals with sound blockchain approaches in protecting data. They say this means that CPDPM is suitable for secure and reliable electronic health record management in the current healthcare systems.

4.5. Throughput performance evaluation

Throughput performance measures the system's ability to process and transmit data efficiently, where higher values indicate better performance. The Contextual Polynomial-Based Data Protection Model (CPDPM) consistently delivers superior throughput across all datasets and feature sets, demonstrating its efficiency in handling large-scale data processing demands. For Dataset 1 with 20 features, CPDPM achieves a throughput score of 94, which is 3.3 % higher than HH-IPFS (91) and 14.6 % higher than CP-BDHCA (82). This improvement underscores CPDPM's optimized processing capabilities, ensuring seamless data transmission in healthcare systems with minimal delays. In Dataset 2 with 30 features, CPDPM records a throughput score of 94, which is 4.6 % better than HH-IPFS (90) and 16 % better than CP-BDHCA (81). These results highlight CPDPM's scalability, making it well-suited for applications involving high data volumes and stringent throughput requirements.For Dataset 3 with 25 features, CPDPM achieves a throughput score of 96, outperforming HH-IPFS (94) by 2.1 %, EHRC (88) by 9.1 %, and CP-BDHCA (85) by 12.9 % as shown in Fig. 6. This demonstrates CPDPM's robust architecture and effective utilization of computational resources, ensuring higher throughput even in complex environments. CPDPM outperforms competing methods by 2.1 % to 16 % in throughput performance across all datasets and feature configurations. This notable advantage is attributed to CPDPM's efficient use of blockchain-based data segmentation and parallelized encryption mechanisms, which enhance data flow and processing speed. These characteristics make CPDPM a highly efficient choice for real-time healthcare data processing in electronic health record systems.

4.6. Network overhead analysis

Network overhead refers to the extra data transmitted over a network beyond the original message, caused by factors such as protocol headers, encryption, and data management techniques. Lower values signify better efficiency. The Contextual Polynomial-Based Data Protection Model (CPDPM) exhibits consistently minimal network overhead

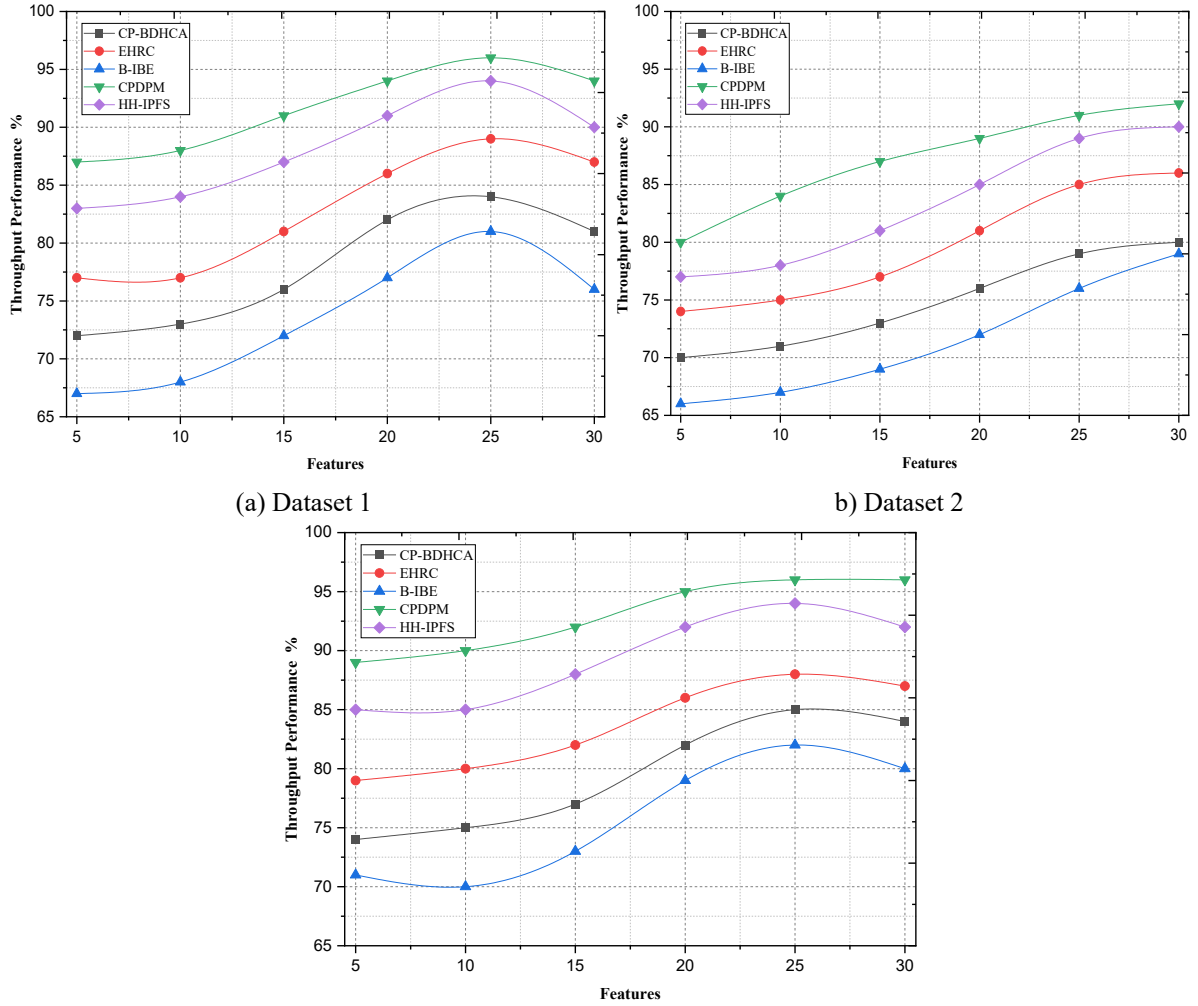


Fig. 6. Throughput performance evaluation.

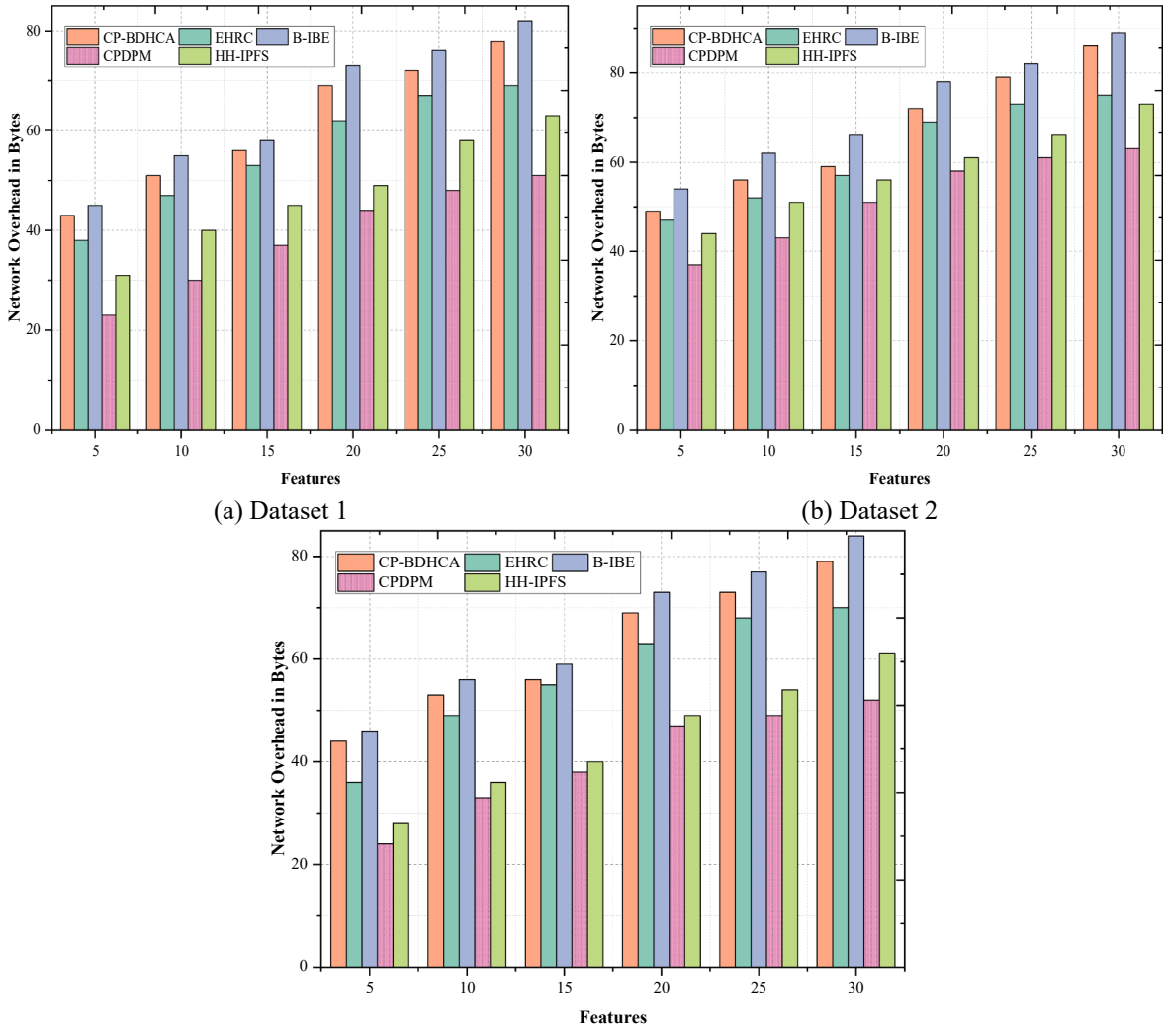
across datasets and feature sets, emphasizing its lightweight and efficient design. In Dataset 1 with 20 features, CPDPM achieves a network overhead of 44, which is 10 % lower than HH-IPFS (49), 29 % lower than EHRC (62), and 36 % lower than CP-BDHCA (69) as shown in Fig. 7. This significant reduction highlights CPDPM's optimized communication protocol, ensuring minimal additional data load during transmission. For Dataset 2 with 30 features, CPDPM records a network overhead of 63, which is 13.7 % lower than HH-IPFS (73), 16 % lower than EHRC (75), and a substantial 26.7 % lower than CP-BDHCA (86). These results underscore CPDPM's ability to handle extensive feature sets while minimizing unnecessary network traffic. In Dataset 3 with 25 features, CPDPM achieves a network overhead of 49, outperforming HH-IPFS (54) by 9.3 %, EHRC (68) by 27.9 %, and CP-BDHCA (73) by 32.9 %. This efficiency makes CPDPM a preferred choice for bandwidth-constrained environments, where excessive network overhead could lead to delays or failures.

Across all datasets and feature configurations, CPDPM achieves a 9.3 % to 36 % lower network overhead compared to competing methods. Its lightweight encryption mechanisms and streamlined data management processes contribute to this significant advantage. These capabilities ensure efficient resource utilization, reduced bandwidth consumption, and smoother operations in environments with high data transmission requirements.

5. Conclusion

The Contextual Polynomial-Based Data Protection Model (CPDPM) we proposed in this paper is a way to respond to the challenge from the healthcare industry in protecting clinical data. Our model provides substantial improvements in terms of confidentiality, integrity, and availability for healthcare data by employing advanced encryption approaches with dynamic access control mechanisms. Through analytic distinctions of access systems that are less restrictive, strength of encryption and decryption, as well as security of data, effectiveness of throughput, and analysing network overhead, this CPDPM model was able to show comparative differences in performance in relation with other models, such as CP-BDHCA, EHRC, B-IBE, and HH-IPFS, and was found to outperform them all when it came down to efficiency and security. The improvements observed in terms of security performance (up to 20 % enhancement) and throughput (12 % improvement) indicate the model's capacity to meet the demanding requirements of modern healthcare data systems.

The future scope of this work entails expanding the CPDPM framework to enable more sophisticated data protection approaches, such as homomorphic encryption and multi-factor authentication, for enhanced protection in healthcare settings. The model can also be trained to learn from multi-modality vectors that enable it to form better predictive capabilities when identifying high-risk patients. They can also remain



(a) Dataset 1

(b) Dataset 2

(c) Dataset 3

Fig. 7. Network overhead analysis.

open to the adoption of emerging technologies like blockchain for auditability and for distributed ledger capabilities that could further enhance the protection of the data without sacrificing transparency. Cloud and edge computational settings present one of the major research directions in regards to shaping the health systems capable of maintaining security while still profiting from distributed information systems.

7. Consent to publish

Not Applicable.

CRediT authorship contribution statement

D. Dhinakaran: Validation. **R. Ramani:** Validation, Software, Data curation. **S.Edwin Raja:** Visualization, Software, Investigation. **D. Selvaraj:** Writing – review & editing, Methodology.

Ethics Approval

No ethics approval is required.

Funding

The authors received no specific funding for this study.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

No data was used for the research described in the article.

References

[1] H. Ghayvat, M. Sharma, P. Gope, P.K. Sharma, SHARIF: solid pod-based secured healthcare information storage and exchange solution in internet of things, IEEE Trans. Ind. Inf. 18 (8) (2022) 5609–5618, https://doi.org/10.1109/TII.2021.3136884.

[2] D. Dhinakaran, G. Prabaharan, K. Valarmathi, S.U. Sankar, R. Sugumar, Safeguarding privacy by utilizing SC-DℓDA algorithm in cloud-enabled multi party computation, KSII Trans. Internet Inf. Syst. 19 (2) (2025) 635–656, https://doi.org/10.3837/tiis.2025.02.014.

[3] K. Kiania, S.M. Jameii, A.M. Rahmani, Blockchain-based privacy and security preserving in electronic health: a systematic review, Multimed. Tools Appl. 82 (2023) 28493–28519, https://doi.org/10.1007/s11042-023-14488-w.

[4] A.N. Gohar, S.A. Abdelmawgoud, M.S. Farhan, A patient-centric healthcare framework reference architecture for better semantic interoperability based on blockchain, cloud, and IoT, IEEE Access 10 (2022) 92137–92157, https://doi.org/10.1109/ACCESS.2022.3202902.

[5] D. Dhinakaran, P.P.M. Joe, Protection of data privacy from vulnerability using two-fish technique with Apriori algorithm in data mining, J. Supercomput. 78 (16) (2022) 17559–17593, https://doi.org/10.1007/s11227-022-04517-0.

[6] R. Jayasri, D. Jayakumar, S. Joshila Roselin and M. O. Ramkumar, "Plan of Blockchain Enabled Confirmed Key Management Protocol for Internet of Medical Things Development," 2022 3rd International Conference on Electronics and Sustainable Communication Systems (ICESC), Coimbatore, India, 2022, pp. 668-673. doi: 10.1109/ICESC54411.2022.9885295.

[7] D. Dhinakaran, L. Srinivasan, S.M. Udhaya Sankar, D. Selvaraj, Quantum-based privacy-preserving techniques for secure and trustworthy internet of medical things an extensive analysis, Quantum Inf. Comput. 24 (3&4) (2024) 0227–0266, https://doi.org/10.26421/QIC24.3-4-3.

[8] H. Ghayvat, et al., CP-BDHCA: blockchain-based confidentiality-privacy preserving big data scheme for healthcare clouds and applications, IEEE J. Biomed. Health Inform. 26 (5) (2022) 1937–1948, https://doi.org/10.1109/JBHI.2021.3097237.

[9] D.C. Nguyen, P.N. Pathirana, M. Ding, A. Seneviratne, Blockchain for secure EHRs sharing of mobile cloud based E-health systems, IEEE Access 7 (2019) 66792–66806, https://doi.org/10.1109/ACCESS.2019.2917555.

[10] R.G. Sonkamble, A.M. Bongale, S. Phansalkar, A. Sharma, S. Rajput, Secure data transmission of electronic health records using blockchain technology, Electronics 12 (4) (2023) 1015, https://doi.org/10.3390/electronics12041015.

[11] D. Dhinakaran, L. Srinivasan, S. Gopalakrishnan, T.P. Anish, An efficient data mining technique and privacy preservation model for healthcare data using improved darts game optimizer-based weighted deep neural network and hybrid encryption, Biomed. Signal Process. Control 100 (Part C) (2025) 107168, https://doi.org/10.1016/j.bspc.2024.107168.

[12] F. Tang, S. Ma, Y. Xiang, C. Lin, An efficient authentication scheme for blockchain-based electronic health records, IEEE Access 7 (2019) 41678–41689, https://doi.org/10.1109/ACCESS.2019.2904300.

[13] H.N. Alsuqaih, W. Hamdan, H. Elmessiry, H. Abulkasim, An efficient privacy-preserving control mechanism based on blockchain for E-health applications, Alex. Eng. J. 73 (2023) 159–172, https://doi.org/10.1016/j.aej.2023.04.037.

[14] F. Li, K. Liu, L. Zhang, S. Huang, Q. Wu, EHRChain: a blockchain-based EHR system using attribute-based and homomorphic cryptosystem, IEEE Trans. Services Comp. 15 (5) (2022) 2755–2765, https://doi.org/10.1109/TSC.2021.3078119.

[15] S. Khan, F. Ahmed, M.S. Baig, Z.A. Khan, U.A. Yousufzai, Securing medical datasets using block chain technology, J. Nanoscope (JN) 3 (2) (2022) 205–217, https://doi.org/10.52700/jn.v3i2.80.

[16] Sanjeev Kumar Dwivedi, Ruhul Amin, Jegatha Deborah Lazarus, Vijayakumar Pandi, Blockchain-based electronic medical records system with smart contract and consensus algorithm in cloud environment, Secur. Commun. Networks 2022 (2022) 4645585, 10 pages.

[17] V. Mani, P. Manickam, Y. Alotaibi, S. Alghamdi, O.I. Khalaf, Hyperledger healthchain: patient-centric IPFSBased storage of health records, Electronics 10 (23) (2021) 3003, https://doi.org/10.3390/electronics10233003.

[18] B. Arunkumar, G. Kousalya, Blockchain-based decentralized and secure lightweight E-health system for electronic health records, in: S. Thampi (Ed.), Intelligent Systems, Technologies and Applications. Advances in Intelligent Systems and Computing, Springer, Singapore, 2020, https://doi.org/10.1007/978-981-15-3914-5_21.

[19] S. Barman, S. Chattopadhyay, D. Samanta, S. Barman, A blockchain-based approach to secure electronic health records using fuzzy commitment scheme, Secur. Priv. 5 (Issue4) (2022) e231.

[20] K. V. Nikhil and S. B, "Prevention of Man in the Middle Attacks on Electronic Health Records over Internet, using Block Chain," 2022 International Conference on Applied Artificial Intelligence and Computing (ICAAIC), Salem, India, 2022, pp. 1287-1292. doi: 10.1109/ICAAIC53929.2022.9793191.

[21] Z. Pang, Y. Yao, Q. Li, X. Zhang, J. Zhang, Electronic health records sharing model based on blockchain with checkable state PBFT consensus algorithm, IEEE Access 10 (2022) 87803–87815, https://doi.org/10.1109/ACCESS.2022.3186682.

[22] S. Datta, S. Namasudra, Blockchain-based smart contract model for securing healthcare transactions by using consumer electronics and mobile-edge computing, IEEE Trans. Consum. Electron. 70 (1) (2024) 4026–4036, https://doi.org/10.1109/TCE.2024.3357115.

[23] D. Baby Sathiya, L. Nalini Joseph, Securing the patient's breast cancer data using blockchain-based IBE with deep learning model in IoT, J. Electr. Syst. 20 (4s) (2024) 2364–2377.

[24] S. Yogesh, B. Balamurugan, Preserving the privacy of electronic health records using blockchain, Procedia Comp. Sci. 173 (2020) 171–180, https://doi.org/10.1016/j.procs.2020.06.021. ISSN 1877-0509c.

[25] R.G. Sonkamble, S.P. Phansalkar, V.M. Potdar, A.M. Bongale, Survey of interoperability in electronic health records management and proposed blockchain based framework: MyBlockEHR, IEEE Access 9 (2021) 158367–158401, https://doi.org/10.1109/ACCESS.2021.3129284.

[26] A.A. Mamun, S. Azam, C. Gritti, Blockchain-based electronic health records management: a comprehensive review and future research direction, IEEE Access 10 (2022) 5768–5789, https://doi.org/10.1109/ACCESS.2022.3141079.

[27] D. Dhinakaran, P.M. Joe Prathap, Preserving data confidentiality in association rule mining using data share allocator algorithm, Intell. Autom. Soft Comput. 33 (3) (2022) 1877–1892, https://doi.org/10.32604/iasc.2022.024509.

[28] R. Guo, K. Li, X. Li, Y. Zhang, X. Li, Compact multiple attribute-based signatures with key aggregation and its application, IEEE Syst. J. 16 (2) (2022) 3025–3035, https://doi.org/10.1109/JSYST.2022.3148989.

[29] D. Dhinakaran, N. Jagadish Kumar, N.P. Ponnuviji, B. Praveen Kumar, Safeguarding confidentiality and privacy in cloud-enabled healthcare systems with spectrasafe encryption and dynamic k-anonymity algorithm, Expert Syst. Appl. 279 (2025) 127584, https://doi.org/10.1016/j.eswa.2025.127584.

[30] L.K. Venugopal, R. Rajaganapathi, A. Birjepatil, S.E. Raja, G. Subramaniam, A novel information security framework for securing big data in healthcare environment using blockchain, Eng. Proc. 59 (Issue 1) (2023) 107, https://doi.org/10.3390/engproc2023059107.