

# Blockchain-Powered Patient-Centric Access Control with MIDC AES-256 Encryption for Enhanced Healthcare Data Security

Krishna Prasad Narasimha Rao , Selvan Chinnaiyan 

School of Computer Science and Engineering, REVA University, Karnataka, India

Corresponding author: Krishna Prasad Narasimha Rao (krishrao18@gmail.com)

## Abstract

Patient-centric access control in healthcare data management is paramount for ensuring privacy, confidentiality and security. In this paper, we propose a novel blockchain-powered patient-centric access control system integrated with MIDC AES-256 encryption to enhance healthcare data security. The proposed system prioritizes patient autonomy by granting patients control over access to their detailed health information, while hospitals are authorized to share relevant medical history. Using blockchain technology ensures decentralization, transparency and immutability of data, while smart contracts and consensus mechanisms enforce accountability and integrity. Additionally, the system employs MIDC AES-256 encryption, which combines multi-input data concatenation (MIDC) with AES-256 encryption, optimizing data integrity and security. The study involves a comparative analysis with existing methods including ABE, RSA and hybrid algorithm AES. The results demonstrate the superiority of our proposed system in terms of encryption speed, decryption time and memory usage. The proposed system achieves an encryption time of 3.8 seconds and a decryption time of 3.2 seconds, significantly outperforming ABE, RSA and hybrid algorithm AES. Moreover, the system exhibits lower memory usage (0.146 MB), highlighting its efficiency and scalability. The proposed system is implemented in Python, providing a versatile and accessible solution for healthcare data security enhancement. Through blockchain-powered patient-centric access control and MIDC AES-256 encryption, our system offers a robust framework for securing sensitive healthcare information while prioritizing patient privacy and control.

## Keywords

Patient-centric access control; Healthcare data management; MIDC AES-256 encryption; Blockchain technology; Multi-input data concatenation.

**Citation:** Rao, K. P. N., & Chinnaiyan, S. (2024). Blockchain-Powered Patient-Centric Access Control with MIDC AES-256 Encryption for Enhanced Healthcare Data Security. *Acta Informatica Pragensia*, 13(3), 374–394. <https://doi.org/10.18267/j.aip.242>

**Academic Editor:** Zdenek Smutny, Prague University of Economics and Business, Czech Republic

**Copyright:** © 2024 by the author(s). Licensee Prague University of Economics and Business, Czech Republic.

This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution License (CC BY 4.0).

# 1 Introduction

The evolution of digital healthcare systems has necessitated a transformative shift in healthcare data management, with patient-centric access control (PCAC) emerging as a pivotal paradigm. In contrast to traditional access control mechanisms, which often employ a one-size-fits-all approach, PCAC places the control and consent of sensitive health information directly in the hands of patients, recognizing the need for a more nuanced and individualized approach to electronic health records (EHR) (Ahmad et al., 2024). Traditional access control systems are generally inflexible and inadequate for managing the complex and dynamic nature of EHR data. These systems fail to accommodate the diverse and ever-changing landscape of health information. PCAC addresses this gap by introducing a level of granularity that allows patients to specify precisely who can access their health records. This shift aligns with the principles of patient autonomy and significantly enhances privacy, confidentiality and regulatory compliance (Dewangan & Chandrakar, 2023). At the core of PCAC is the empowerment of patients. By granting patients detailed control over access permissions, they can directly influence who within the healthcare ecosystem can access and interact with their EHR data. This empowerment extends beyond mere data control, fostering a sense of ownership and trust between patients and healthcare providers (Rai et al., 2022).

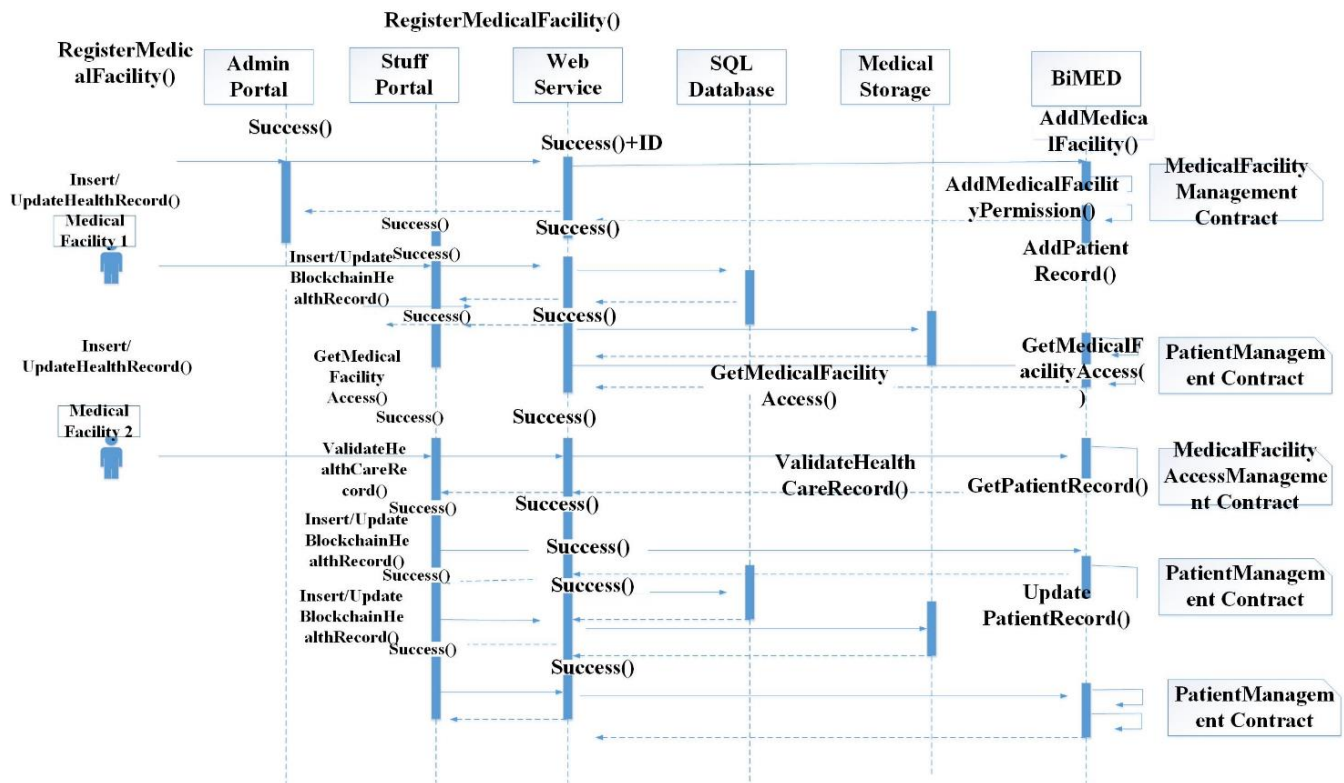
Ensuring privacy is a paramount concern in healthcare and PCAC mitigates the risk of unauthorized disclosure by enabling patients to set the terms for data access. This approach not only addresses ethical concerns but also aligns with the evolving legal landscape regarding patient privacy and data protection (Wu et al., 2024). PCAC inherently aligns healthcare providers with regulatory standards, as they must adhere to the preferences and consents set by patients. This alignment is crucial for maintaining compliance with legal requirements surrounding patient privacy and data security. The system design ensures that patient choices are paramount, thus fostering a more trustworthy and transparent relationship among all stakeholders in the healthcare process (Peng et al., 2023).

Implementing PCAC employs advanced technologies such as blockchain to enhance the security and transparency of the access control process. The decentralized and immutable nature of blockchain ensures that access requests and consents are recorded in a tamper-proof, time-stamped manner, providing a reliable audit trail. This technology not only strengthens security but also builds trust among stakeholders by offering a verifiable record of data interactions (Abutaleb et al., 2023). In addition to blockchain, the integration of encryption technologies, notably the MIDC AES-256 algorithm, solidifies the security posture of PCAC. This encryption standard, known for its robustness, ensures that even if unauthorized access occurs, the data remain protected. Encrypting data both in transit and at rest is crucial for mitigating risks associated with data breaches and cyber threats in the healthcare sector (Abutaleb et al., 2023; Houhou et al., 2024).

Figure 1 depicts a blockchain-based patient healthcare record management system, showcasing the seamless integration of decentralized ledger technology with healthcare data management. At its core, the blockchain serves as a secure and immutable ledger, ensuring the integrity and privacy of patient records through cryptographic hashing and consensus mechanisms. The system enables patients, healthcare providers and other authorized parties to securely access and update medical records in real time, promoting interoperability and transparency across the healthcare ecosystem. Through smart contracts, permissions are defined and enforced, allowing granular control over data access while automating processes such as consent management and billing. Overall, the figure illustrates a paradigm shift towards patient-centric healthcare data management, using blockchain technology to enhance security, efficiency and trust in the exchange of sensitive medical information.

The utilization of blockchain technology is a transformative element of PCAC in EHR. The decentralized architecture of blockchain ensures that no single entity has control over the entire network, reducing the risks associated with centralized systems. This design aligns seamlessly with the principles of PCAC,

where patient empowerment and control over their health data are paramount. By distributing control and maintaining a consensus mechanism, blockchain fosters a more democratic and transparent environment for managing access permissions to EHR data (Verma, 2024; Yuan et al., 2023).



**Figure 1.** Blockchain-based patient healthcare record management.

The immutability of blockchain is another important aspect contributing to the robustness of PCAC. Once a patient's consent or access request is recorded in the blockchain, it becomes tamper-proof and proof against unauthorized alterations. Each transaction is linked to the previous one in a chain, forming a chronological and unalterable record of access events (Puneeth & Parthasarathy, 2024). This characteristic now not only ensures the integrity of the information but also establishes a comprehensive and trustworthy audit path. The tamper-proof nature of blockchain becomes particularly important in the context of healthcare information safety. The historic challenges of unauthorized access and data breaches within healthcare necessitate a method that can face up to tampering or malicious changes (Agarkar et al., 2024). By recording consent and access permissions in an immutable ledger, blockchain generation provides a resilient protection from unauthorized manipulation, thereby improving the overall security of EHR records.

A crucial aspect of PCAC facilitated by blockchain is the time-stamped recording of patient consent and access requests. The transparency of the blockchain ensures that every transaction is associated with a specific timestamp, allowing a chronological and verifiable sequence of events. This temporal dimension is essential for creating a reliable audit trail, aiding in forensic analysis, compliance monitoring and investigations related to data access or privacy breaches (Masood et al., 2024). The reliable audit trail established through blockchain not only enhances the security of health information but also contributes to building a trustful environment within the healthcare ecosystem. Patients, healthcare providers and other stakeholders can confidently rely on the transparency and integrity of the access control system, knowing that any access event is documented and verifiable. This transparency fosters trust between patients and healthcare entities, reinforcing the patient-provider relationship and encouraging a culture of openness.

In addition to security and transparency, blockchain technology in PCAC also supports the efficient management of access permissions. Smart contracts, self-executing contracts with the terms of the agreement directly written into code, can be employed to automate and enforce access control rules. This automation reduces the administrative burden on healthcare organizations and ensures that access permissions align precisely with patient preferences, further enhancing the precision and efficiency of the access control system. Furthermore, the adoption of blockchain in PCAC contributes to the overall evolution of healthcare systems towards interoperability. As patients move between different healthcare providers, the decentralized and standardized approach of blockchain ensures that access control protocols remain consistent and universally applicable. This interoperability not only streamlines data sharing but also fosters collaboration and continuity of care, ultimately benefiting the patient.

The key contribution of the paper is as follows:

- The proposed approach involves combining multiple data inputs into a single concatenated string. The novelty may lie in how these concatenated data are then handled within the system, possibly optimizing the encryption process and ensuring data integrity when multiple sources of patient information are involved.
- By utilizing correlation analysis, specifically the Pearson correlation coefficient, the methodology identifies a subset of parameters with low intercorrelation. This optimized selection enhances the efficiency of subsequent encryption processes, reducing redundancy and improving overall data management.
- The methodology introduces the innovative multi-input data concatenation (MIDC) technique in conjunction with AES-256 encryption. This encryption method aggregates diverse data inputs into a single concatenated string before encryption, streamlining the process while enhancing data integrity and security.
- Incorporating blockchain technology provides a decentralized and transparent ledger for storing encrypted healthcare data. This decentralized approach ensures data immutability, transparency and enhanced security, while smart contracts and consensus mechanisms further reinforce the integrity of the system.
- The proposed methodology aligns with existing privacy regulations by prioritizing patient privacy and data security. By providing a secure, transparent and patient-centric data management system, the methodology addresses regulatory requirements while empowering individuals with greater control over their health information.

The rest of the paper is organized as follows. Section 2 includes an overview of the literature on patient-centric access control mechanisms. The problem statement for the study is presented in Section 3. Section 4 covers the recommended approach to a patient-centric access control mechanism. Section 5 compares the method efficacy to previous techniques and the performance measures are displayed, along with an explanation of the results. Section 6 presents the conclusion and future work directions.

## 2 Related Works

Naresh et al. (2021) proposed a four-layered DPDM structure comprising data preparation, data sharing, data storage, and access control and security. The use of elliptical curve-based content extraction signatures allows patients to filter sensitive EMR data. Blockchain smart contracts specify patient permissions for secure data sharing and cloud storage is used for EMR storage with indexes stored on a consortium blockchain. Chelladurai et al. (2021) introduced smart contracts for immutable patient logs

and digital health record management. A modified Merkle tree structure was used for secure storage and quick access, with specific contracts for emergency access and data sharing. Scalability and power-related issues were identified as barriers to real-world adoption.

Dewangan & Chandrakar (2023) discussed an approach that makes use of IoMT devices and blockchain to ensure GDPR compliance, using personal digital assistants for data transmission and secure storage on the cloud. The method includes miner selection to prevent bias and employs MQTT and Bevy wise IoT simulators for IoT simulation. The study highlighted limitations related to processing power and energy usage. George & Chacko (2022) proposed a blockchain-based patient-centric data access system named MediTrans, where patients own their data stored on a personal health record (PHR) cloud. The system uses cipher text policy attribute-driven encryption for secure data sharing. Performance analysis showed promising results, though scalability remained a concern.

Hongjiao et al. (2021) designed a system using blockchain for encrypted data storage and simplified access control. The method included file authorization contracts to enhance security against medical identity theft. The system performance was affected by the increased blockchain size due to extensive data storage.

Hussien et al. (2021) proposed a cryptographic mechanism combining SSE and CP-ABE with smart contracts for multi-keyword searchable encryption. The system ensures security against various attacks and provides tamper-proof resistance. Security validation confirmed the system resilience to replay and MIM attacks. Han et al. (2022) introduced an attribute-driven access control model with an auditable access control system based on blockchain. This model ensures security and efficient administration of private data in IoT environments. High throughput and security were demonstrated, though handling large volumes of transactions posed a challenge.

Abouali et al. (2021) proposed a framework using Ethereum blockchain for smart contracts, IPFS for off-chain storage and NuCypher for proxy re-encryption. This approach ensures secure on-demand sharing of patient health records, accessible only to validated entities. The system offers improved security over centralized alternatives. Rai et al. (2023) developed a decentralized system using blockchain and IPFS for secure EHR ownership and management. Performance criteria showed the method effectiveness, though the complexity and learning curve for blockchain adoption remained significant barriers.

**Table 1.** Comparison of existing techniques.

Study	Data ownership	Access control	Encryption	Data sharing	Scalability
Naresh et al. (2021)	Patients	Smart contracts	Elliptical curve-based	Cloud storage + blockchain	Limited
Chelladurai et al. (2021)	Patients	Smart contracts	Modified Merkle tree	Various contracts	Limited
Dewangan & Chandrakar (2023)	Patients	Not specified	Encryption	Cloud + IoMT	Limited
George & Chacko (2022)	Patients	Attribute-driven	CP-ABE	PHR cloud	Limited
Hongjiao et al. (2021)	Patients	Simplified access control	Cryptographic methods	Encrypted storage	Limited
Hussien et al. (2021)	Patients	Smart contracts	SSE + CP-ABE	Encrypted data	High
Han et al. (2022)	Patients	Attribute-driven	Not specified	Auditable system	High
Abouali et al. (2021)	Patients	Smart contracts	Proxy Re-encryption	IPFS + Ethereum	Limited
Rai et al. (2023)	Patients	Not specified	IPFS	Blockchain	Limited

### 3 Problem Statement

Despite the notable advancements in utilizing blockchain technology for electronic health record (EHR) management, existing works exhibit certain limitations that prompt the need for a novel approach. The identified shortcomings encompass challenges in scalability, potential power-related issues and concerns regarding the processing capacity, particularly when dealing with a growing number of participants and a large influx of electronic medical records (Hongjiao et al., 2021). Additionally, the centralized nature of traditional EHR systems raises privacy and security issues, creating potential vulnerabilities in data sharing processes and compromising patient confidentiality.

Furthermore, existing systems may encounter difficulties in effectively managing a large volume of transactions and users concurrently, leading to potential delays and hindering the seamless integration of blockchain-based healthcare solutions into real-world applications. Addressing these limitations, the proposed method seeks to provide a comprehensive solution by introducing a patient-centric access control (PCAC) framework that employs blockchain technology and advanced encryption algorithms, specifically the MIDC AES-256 algorithm. By doing so, the method aims to enhance the security, transparency and patients' control over their health information, while mitigating scalability issues and ensuring compliance with regulatory standards. The primary purpose of our approach is to revolutionize EHR data management, offering a patient-centric model that empowers individuals with explicit control over access permissions, thereby fostering a trustful environment, ensuring data integrity and advancing the overall efficacy and security of healthcare information systems.

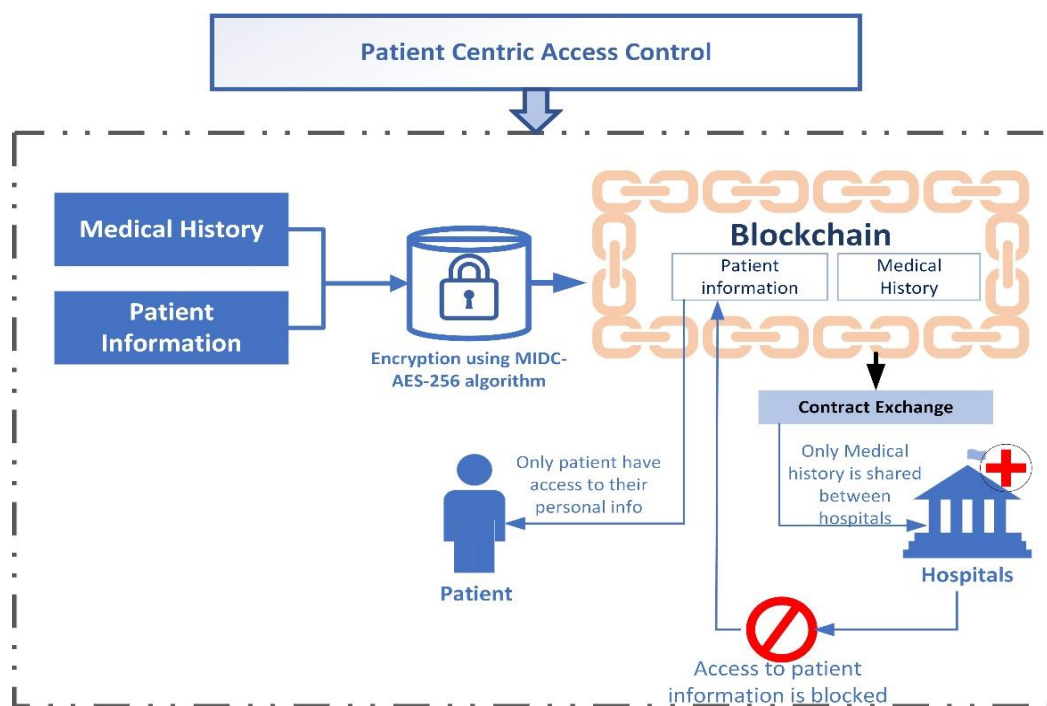
### 4 Proposed System

The proposed technique for reinforcing the safety and integrity of healthcare data includes a comprehensive approach that integrates data collection, feature selection using correlation analysis, MIDC AES-256 encryption and the utilization of blockchain generation. In the information collection phase, diverse parameters consisting of patient ID, social security numbers, name, date of birth, address, phone numbers, email addresses, biometric data, insurance policy numbers, medical record locator numbers and National Health Service numbers are meticulously collected from various healthcare facilities, together with tertiary hospitals, community hospitals and primary care facilities. Feature selection is then carried out using correlation analysis, particularly the Pearson correlation coefficient, to identify a subset of parameters with low intercorrelation, optimizing the performance of the following encryption method. The chosen parameters undergo MIDC AES-256 encryption, where multi-input data concatenation is employed to combine various data inputs into a single concatenated string before subjecting it to the AES-256 encryption algorithm. This innovative encryption technique aims to streamline the process, enhance record integrity and make certain strong protection, in the context of coping with patient information from multiple resources. Subsequently, the encrypted information is despatched to a blockchain, which acts as a decentralized and obvious ledger. The blockchain facilitates patient-centric access management, making sure that patients have access to their data, while hospitals are granted permission for sharing relevant clinical history. The decentralized and immutable nature of the blockchain, coupled with smart contracts and consensus mechanisms, adds layers of security, transparency and accountability to the system. Overall, this technique creates a secure, obvious and patient-centric healthcare information management system that aligns with privacy rules and empowers individuals with control over their health records. Figure 2 suggests the general structure of the proposed methodology.

#### 4.1 Data collection

Data collection in healthcare networks and hospitals involves a meticulous and multifaceted technique to ensure the correct and steady linkage of electronic health record (EHR) structures throughout various healthcare facilities. In this scenario, the primary parameter for deterministic linkage embodies a

numerical identifier. A patient ID or medical record number serves as a fundamental anchor, offering a unique reference for each person inside the network, assisting in cross-referencing across numerous healthcare entities.



**Figure 2.** Overall structure of proposed methodology.

The inclusion of social security numbers (SSN), name and surname and date of birth similarly refines the linkage system, offering a mixture of demographic and personal information to establish precise connections. Address details contribute to the linkage process, allowing a geographic reference point, while phone numbers and email addresses provide communication-associated identifiers. Biometric data, a rising parameter, adds a layer of protection and accuracy in patient linkage, ensuring a robust and reliable association between EHRs in tertiary sanatoria, community hospitals and primary care facilities in the community. Coverage-related parameters such as the insurance policy number become pivotal for connecting EHR data with claims information, aiding in comprehensive healthcare control. The utilization of medical record locator numbers and National Health Service (NHS) numbers complements the accuracy of cross-referencing throughout the network, streamlining data series methods. While these parameters serve to establish deterministic linkage, it is vital for healthcare networks to adhere to privacy rules and moral issues. As the data collection extends to various levels of care, including tertiary hospitals and primary healthcare centres, maintaining a standardized approach to collect and manage these identifiers ensures the integrity and interoperability of the EHR system. Attributes for encryption and health prediction are patient ID, biometric data, insurance policy number, age, blood pressure, cholesterol level, body mass index (BMI), smoking status and exercise frequency of heart patients. From these attributes, the doctor in the hospital can predict the patient's health status using advanced analytical techniques and predictive modelling. This comprehensive dataset enables healthcare professionals to assess patients' health risks, develop personalized treatment plans and make informed clinical decisions, ultimately leading to improved patient outcomes and healthcare delivery. Table 2 shows the different attributes in the EHR.



**Table 2.** Listing of attributes.

Attributes	Masked
Patient ID	No
Social security number (SSN)	Yes
Name	Yes
Surname	Yes
Date of birth	No
Address	Yes
Phone number	Yes
Email address	Yes
Biometric data	No
Insurance policy number	No
National Health Service (NHS) number	Yes
Medical record locator number	No
Age	No
Blood pressure	No
Cholesterol level	No
Body mass index (BMI)	No
Smoking status	No
Exercise frequency	No

## 4.2 Feature selection using correlation analysis

Correlation analysis, specifically employing the Pearson correlation coefficient, serves as a robust feature selection technique in the context of encryption for healthcare data. The objective is to identify a subset of parameters among the given parameters, ensuring optimal encryption efficiency while minimizing redundancy. The Pearson correlation coefficient assesses the linear relationship between two variables, providing insights into how changes in one parameter may correspond to changes in another. In the context of healthcare data encryption, selecting parameters with low correlation reduces redundancy and improves the overall efficiency of the encryption process. To begin, let us define the Pearson correlation coefficient  $r$  mathematically. For two variables  $X$  and  $Y$ , the Pearson correlation coefficient is calculated using Equation (1).

$$r = \frac{cov(X,Y)}{\sigma_X \sigma_Y} \quad (1)$$

Where  $cov(X,Y)$  represents the covariance between variables  $X$  and  $Y$ , while  $\sigma_X$  and  $\sigma_Y$  are the standard deviations of the variables  $X$  and  $Y$ , respectively. The correlation analysis process involves computing the correlation coefficients for each pair of parameters. The range of  $r$  lies between -1 and 1. A value close to 1 indicates a strong positive correlation, -1 indicates a strong negative correlation and 0 indicates no correlation. In the context of healthcare data encryption, selecting parameters with low intercorrelation is crucial. This means that changes in one parameter do not necessarily predict changes in another, reducing redundancy in the dataset and ensuring that each selected parameter contributes unique information to the encryption process. The feature selection process involves identifying parameters with correlation coefficients close to zero or below a predefined threshold.



It is important to consider the implications of parameter selection on the encryption model performance. Choosing parameters that are less correlated can lead to enhanced encryption efficiency and reduced computational overheads. Moreover, the selection process should align with the specific requirements and constraints of the healthcare data, ensuring that the chosen parameters adequately capture the necessary information for encryption without unnecessary redundancy. In healthcare data, the chosen parameters for encryption might include those related to patient demographics, medical history or diagnostic information. For instance, selecting parameters such as age, blood pressure, and cholesterol level may offer a combination of demographic and health-related information crucial for encryption. By employing the Pearson correlation coefficient, one can systematically assess the relationships between these parameters and make informed decisions on the subset to be included in the encryption process. Furthermore, the feature selection process can be enhanced by visualizing the correlation matrix. A heatmap representation of the correlation coefficients provides a clear overview of the relationships between each pair of parameters. This visualization aids in the identification of patterns and assists in deciding which parameters contribute most effectively to the encryption process.

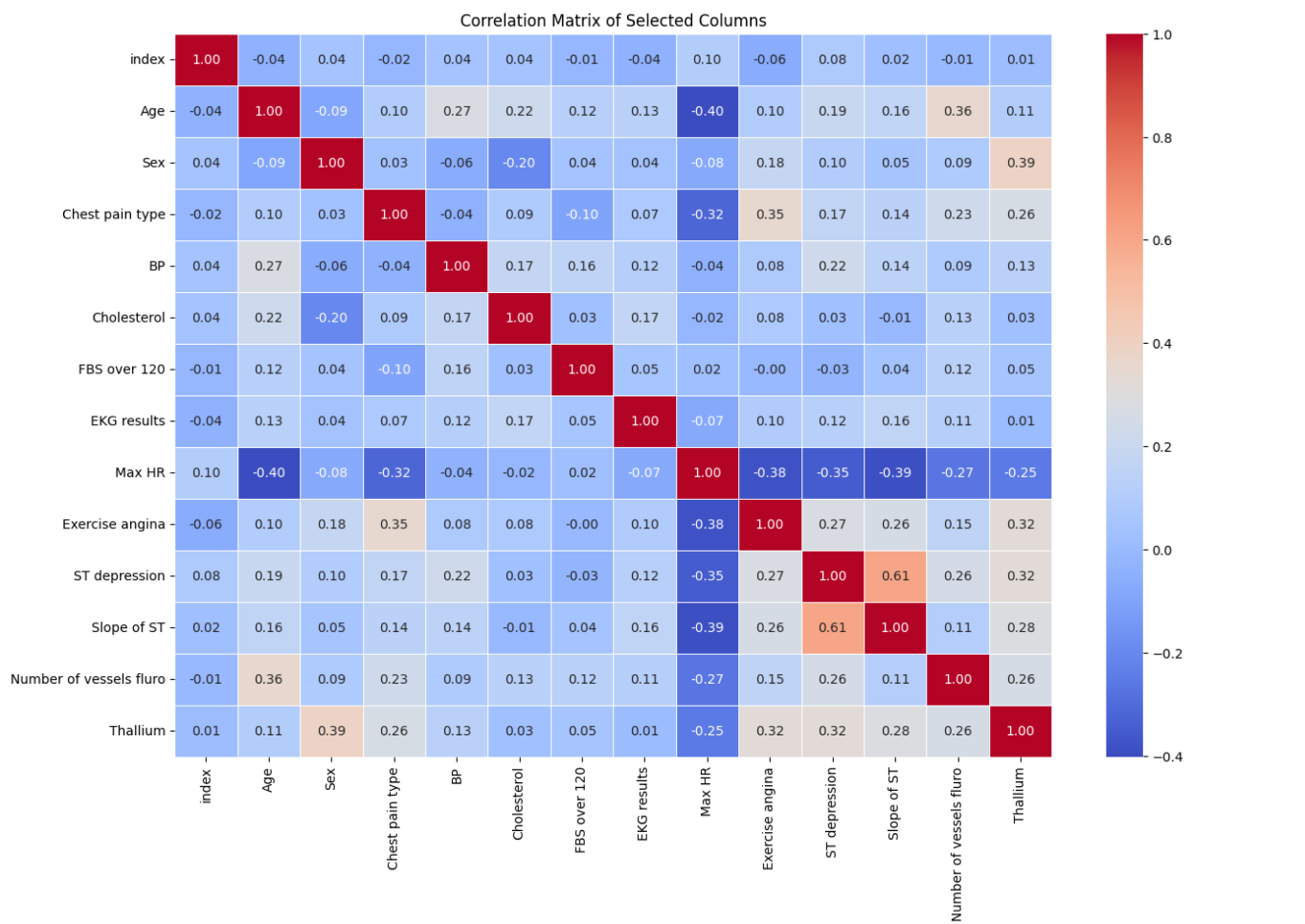


Figure 3. Correlation matrix of clinical and demographic variables.

Figure 3 is a correlation matrix that displays the Pearson correlation coefficients between various clinical and demographic variables in the dataset, with values ranging from -1 (perfect negative correlation) to 1 (perfect positive correlation). Key findings include a strong positive correlation between "Exercise angina" and "Chest pain type" (0.35), as well as between "Number of vessels fluoro" and "Age" (0.36). "ST depression" and "Slope of ST" also show a notably high positive correlation (0.61). Conversely, "Age" and "Max HR" exhibit a strong negative correlation (-0.40), indicating that as age increases, maximum heart rate tends to decrease. "Sex" (coded numerically) is moderately correlated with "Thallium" (0.39), suggesting sex differences in thallium stress test results. Other notable correlations include "ST

depression" with "Exercise angina" (0.38) and "Slope of ST" with "Exercise angina" (0.39). The matrix highlights significant interrelationships among the variables, providing insights into how clinical measures and demographic factors interact within the dataset.

### 4.3 Encryption using MIDC AES-256

The proposed method employs the MIDC AES-256 encryption approach to enhance the security and integrity of healthcare statistics. MIDC, which stands for multi-input data concatenation, is a unique technique that entails combining multiple statistics inputs into a single concatenated string before subjecting the aggregated information to the AES-256 encryption set of rules. This modern approach aims to optimize the encryption method, mainly whilst handling various parameters from more than one asset of patient data within the healthcare area. The MIDC AES-256 encryption method starts with the aggregation of diverse parameters, consisting of patient demographics, scientific history and diagnostic information, into a unified string. This concatenated string serves as the input to the advanced encryption standard (AES) set of rules with a key length of 256 bits, ensuring strong encryption. The concatenation method involves combining individual record inputs, represented as  $D_1, D_2, \dots, D_n$  into a single string  $S$  using a concatenation operator. The concatenation process is represented mathematically in Equation (2).

$$S = D_1 \oplus D_2 \oplus \dots \oplus D_n \quad (2)$$

Where  $\oplus$  represents the concatenation operator. This operation aggregates diverse parameters, including patient demographics, medical history and diagnostic information, into a unified string  $S$ . The concatenated string is then subjected to the AES-256 encryption algorithm, a widely adopted symmetric encryption standard. This algorithm operates on blocks of data, dividing the concatenated string into fixed-size blocks and applying a series of substitution-permutation operations for secure encryption. The AES-256 encryption algorithm can be mathematically represented as a series of transformations applied to the input data. Let us denote the encryption function as  $E$  and the input concatenated string as  $S$ . The encryption process is expressed in Equation (3).

$$C = E(S, K) \quad (3)$$

Where  $C$  represents the encrypted data and  $K$  denotes the encryption key with a length of 256 bits. The encryption function  $E$  applies a series of mathematical transformations to the input string using the encryption key  $K$ , resulting in the encrypted data. The choice of a 256-bit encryption key is a crucial aspect of the MIDC AES-256 encryption approach. A longer key enhances the security of the encryption, making it computationally infeasible for adversaries to decipher the encrypted data without the proper key. The decryption process involves applying inverse transformations to the encrypted data using the decryption key. Let us denote the decryption function as  $D$  and the encrypted data as  $C$ . The decryption process is expressed in Equation (4).

$$S = D(C, K_{dec}) \quad (4)$$

Where  $K_{dec}$  represents the decryption key. The decryption function  $D$  applies a series of inverse transformations to the encrypted data  $C$  using the decryption key  $K_{dec}$ , resulting in the original concatenated string. The novelty of the MIDC technique lies in how the concatenated data are dealt with within the system. By aggregating multiple data inputs into a single string, the encryption system is streamlined, doubtlessly lowering computational overheads and improving average efficiency. This optimization is especially relevant in healthcare structures coping with a multitude of patient information sources. Handling concatenated records in the encryption system introduces a layer of complexity that might contribute to ensuring statistical integrity. The MIDC AES-256 approach carefully manages the concatenated string to prevent record loss or corruption during the encryption and decryption phases. The concatenated string  $S$  is then subjected to the AES-256 encryption algorithm, a popular symmetric encryption. This set of rules operates on blocks of records, dividing the concatenated string into fixed-

period blocks and making use of a sequence of substitution-permutation operations for strong encryption. The MIDC AES-256 encryption method is seamlessly integrated into healthcare structures to safeguard patient records. This technique is mainly treasured in scenarios in which patient records originate from diverse resources, offering a unified and steady encryption that prioritizes confidentiality and integrity.

#### Algorithm: MIDC-AES

```
Function MIDC AES 256 encryption (input data)
// Concatenate individual data inputs into a single string
// Concatenated string = concatenate data (input data)

Encrypt the concatenated string using AES-256 algorithm
Encrypted data = AES 256 encrypt (concatenated string)
    return encrypted data
function concatenate data (input data)
    concatenated string
    for each data entry in input data
        concatenated string = concatenated string + data entry
    return concatenated string

function AES 256 encrypt (data):
    // Perform AES-256 encryption using a 256-bit key
    // This can be achieved using a library or built-in functions depending on the
    programming language
    return encrypted data
```

Let us consider an example where patient medical records need to be encrypted using the MIDC AES-256 encryption technique before being stored in the blockchain. First, individual patient medical records are aggregated into a single concatenated string using the multi-input data concatenation (MIDC) technique. This concatenated string includes various data inputs such as patient demographics, medical history and diagnostic information. For example, the study has the following patient data: patient name: John Doe, date of birth: 1 January 1980, medical history: hypertension, diabetes, diagnostic information: blood pressure – 120/80 mmHg, cholesterol level – 180 mg/dL. The concatenated string would be as follows: "John Doe0101980HypertensionDiabetes120/80 mmHg180 mg/dL". Once the concatenated string is formed, it is encrypted using the AES-256 encryption algorithm with a 256-bit encryption key. The encryption function takes the concatenated string as an input and produces encrypted data as the output. For example, the encrypted data might be: "e2f4c5b7a9d0... (Encrypted string)". Finally, the encrypted data are stored in the blockchain as part of a transaction. The transaction includes metadata such as the patient's ID, timestamp and a reference to the previous block. Once added to the blockchain, the encrypted data become a permanent and immutable record, accessible only to authorized parties with the decryption key. By encrypting patient medical records using MIDC AES-256 encryption and storing them in the blockchain, healthcare systems can ensure the security, integrity and privacy of sensitive patient information while enabling secure and transparent data sharing among authorized entities.

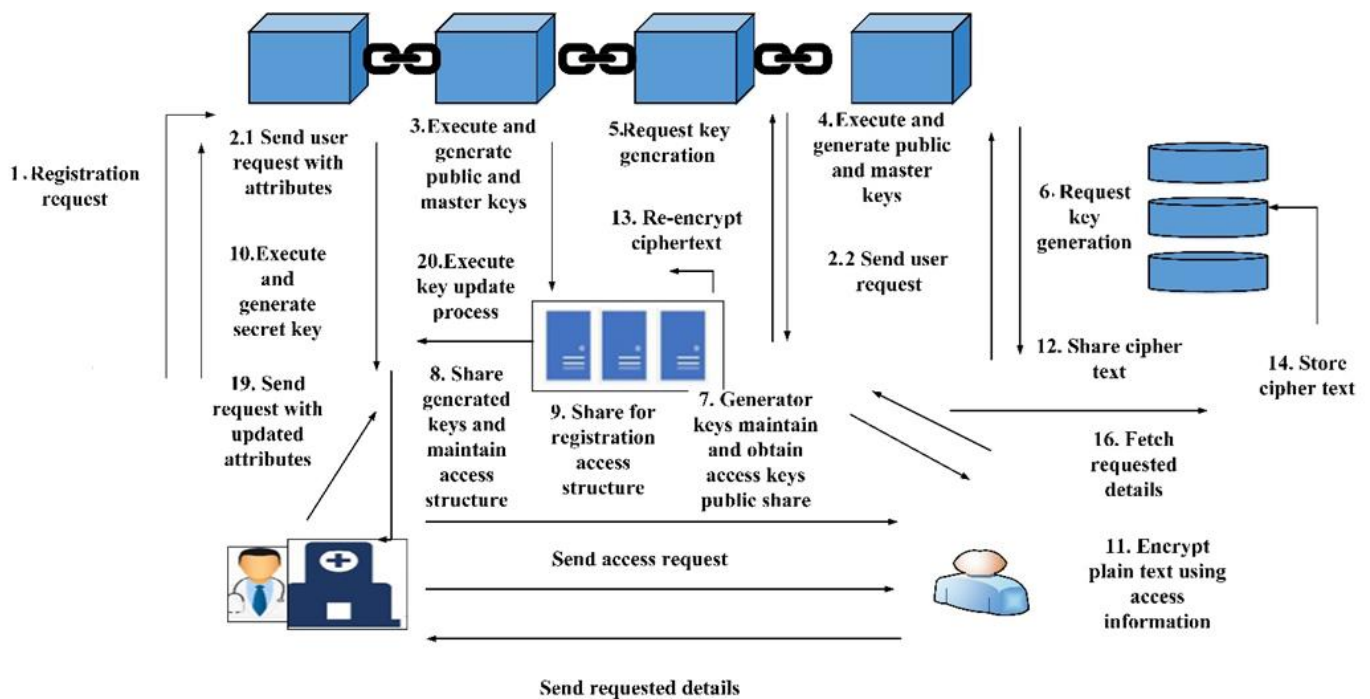
## 4.4 Enhancing security using blockchain

After that, the encrypted information is shipped to the blockchain containing patient and medical records. The patient data may be only accessed with the patient's aid, and if the clinic tries to get the right to access the patient's records, the system will deny it. Only the patients' scientific statistics are shared between hospitals. The blockchain is used to enhance the data protection of the method. Blockchain is a decentralized and distributed ledger that records transactions across a network of computers in a secure, transparent and tamper-proof manner. Each block in the blockchain contains a batch of transactions and these blocks are linked together in a chronological order, forming a chain. When a transaction occurs, such as sharing patient medical records between healthcare entities, it is first validated and then added to a block. Once a certain number of transactions are accumulated, they are grouped together into a block. The block also contains metadata such as a timestamp and a reference to the previous block in the chain. Before

a block is added to the blockchain, it undergoes a validation process by the network participants, typically through a consensus mechanism such as proof of work or proof of stake. This ensures that the transactions in the block are legitimate and adhere to the network rules. Once validated, the block is appended to the blockchain. It becomes a permanent part of the ledger and is distributed to all nodes in the network, ensuring that each node has an identical copy of the blockchain. Once added to the blockchain, a block cannot be altered or deleted without consensus from the network participants. This immutability ensures the integrity and trustworthiness of the data stored in the blockchain.

In the proposed paper, blockchain generation serves as an essential element to enhance the safety, transparency and accessibility of encrypted patient data. Blockchain, at its middle, is a decentralized and allocated ledger that registers data transactions within a network of computers in a regular, tamper-proof way. The usage of blockchain in healthcare systems provides an additional layer of protection and trust, aligning perfectly with the sensitive nature of patient records. The inherent properties of blockchain play a pivotal role in fortifying the safety of the proposed method. One key function is decentralization, which means that the record is not stored by an authority but is shipped among a couple of nodes inside the network. This decentralization minimizes the chance of a single point of failure, ensuring that there can be no vital vulnerability for potential breaches. Each node inside the community keeps a reproduction of the whole blockchain, offering redundancy and resilience against information loss or tampering.

Figure 4 illustrates a secure data access and encryption process within a blockchain framework, particularly for healthcare information. It begins with a registration request (Step 1) followed by user requests with attributes sent to the blockchain (Step 2.1 and 2.2). The blockchain generates public and master keys (Steps 3 and 4) upon key generation requests (Steps 5 and 6). The generated keys are shared and maintained to form an access structure (Steps 7 and 8), with registration details updated accordingly (Step 9). The secret key is then executed and generated (Step 10) and plain text data are encrypted using access information (Step 11). The ciphertext is shared and stored (Steps 12 and 14). Upon an access request, the encrypted data are fetched (Step 16) and decrypted (Steps 13 and 19) using updated attributes, concluding with a key update process executed in the blockchain (Step 20).



**Figure 4.** Proposed system working.

Another critical aspect of blockchain is its transparency and immutability. Once a block of data is introduced to the blockchain, it turns into a lasting and unalterable a part of the chain. This ensures the integrity of the patient information stored in the blockchain, preventing unauthorized modifications or tampering. Any attempt to alter the information in a block requires the consensus of the whole community, making it almost impossible to compromise the integrity of the information. Smart contracts, self-executing code deployed in the blockchain, play a significant role in coping with access control within the proposed method. In this context, smart contracts are employed to regulate access to patient information. The device is designed to permit most effectively the patients themselves to get access to their particular clinical statistics, enhancing privacy and putting control in the hands of the patients. Moreover, the smart contracts are programmed to deny access to hospitals trying to access patient data other than for sharing clinical information between healthcare establishments. The functions of smart contracts in the present paper are given below.

#### **View medical record**

```
1 function viewMedRec(address id) public view returns (MedRec memory)
2 {
3     return (Records[id]);
4 }
```

#### **Get shared record for doctor**

```
5 function getPatRecord(address _owner, address _docID) public view returns
6 (ShareDoc memory)
7 {
8     return Shares[_owner][_docID];
9 }
```

#### **Get shared doctor detail**

```
10 function getSharedDoctors(address _id) public view returns (ShareDoc[] memory)
11 {
12     MedRec storage rec = Records[_id];
13     ShareDoc[] memory _shareDocs = new ShareDoc[](rec.doctors.length);
14     for (uint256 i = 0; i < rec.doctors.length; i++)
15     {
16         if (Shares[_id][rec.doctors[i]].owner != address(0))
17         {
18             _shareDocs[i] = Shares[_id][rec.doctors[i]];
19         }
20     }
21     return _shareDocs;
22 }
```

#### **Share EHR with given doctor ID**

```
23 function shareMedRec(address _owner, address _docID, string memory _sign,
24 string memory _ck, uint8 _access) external onlyPatient
25 {
26     ShareDoc storage share = Shares[_owner][_docID];
27     share.owner = _owner;
28     share.docID = _docID;
29     share.sign = _sign; share.ck = _ck;
30     share.access = _access; Records[_owner].doctors.push(_docID);
31 }
```

#### **Update access for shared EHR**

```
32 function updateAccess( address _owner, address _docID, uint8 _access) public
33 {
34     Shares[_owner][_docID].access = _access;
35 }
```

Blockchain employs consensus mechanisms to validate and agree on the state of the ledger throughout the community. The most commonplace consensus mechanisms are proof of work (PoW) and proof of stake (PoS). These mechanisms make certain that the addition of latest blocks to the blockchain is a strong

and trustworthy process. In the proposed method, this consensus mechanism ensures that the patient data stored in the blockchain are dependable and have gone via a rigorous validation process. The decentralized and permissioned nature of blockchain provides an additional layer of privacy for the method. Patients have specific control over who can access their comprehensive health data. Hospitals are granted access to applicable scientific history, fostering secure statistics sharing among healthcare entities while safeguarding the confidentiality of patient medical information. This guarantees compliance with privacy rules and empowers patients with tremendous control over their healthcare data. The obvious and immutable nature of blockchain permits comprehensive auditability. Every interplay with the patient statistics, be it access or change, is recorded in the blockchain. This audit route ensures responsibility and offers a verifiable file of all data transactions. In the event of a dispute or the need for an audit, the blockchain serves as an indisputable and obvious source of truth.

## 5 Results and Discussion

This section presents the results and discussion of the paper, which proposes a comprehensive method aimed towards improving the safety and integrity of healthcare data. The methodology includes several organized stages, starting with data collection from numerous healthcare centres, including community hospitals, tertiary hospitals and primary healthcare centres. Various parameters consisting of patient ID, social security numbers, name, date of birth, address, phone numbers, email addresses, biometric data, insurance policy numbers, medical record locator numbers and National Health Service numbers are systematically collected to make an effective dataset. Subsequently, feature selection is performed using correlation analysis, specifically the Pearson correlation coefficient, to discover a subset of parameters with low intercorrelation. This optimized choice streamlines the subsequent encryption process, ensuring performance and effectiveness. The selected parameters then undergo MIDC AES-256 encryption, where the modern multi-input data concatenation technique aggregates diverse records inputs into a single concatenated string before subjecting it to the AES-256 encryption set of rules. The encryption method aims to enhance data integrity and protection. Encrypted data are then securely transmitted to a blockchain, serving as a decentralized and transparent ledger. The blockchain implementation helps patient-centric access control, making sure that patients can get access to their certain records, while hospitals are granted permission for sharing applicable scientific records. The decentralized nature of the blockchain, enhanced with smart contracts and consensus mechanisms, adds layers of protection, accountability and transparency to the method. The proposed method primarily creates a secure, obvious and patient-centric healthcare data management system that aligns with privacy regulations and empowers people with control over their health information.

A terminal log is associated with the implementation of a smart contract in an Ethereum application, with an emphasis on improving access control measures. On the Ethereum blockchain, this deployment manner is uniquely recognized via its transaction hash. The address of the deployed contract acts as a community identity for it. The quantity of gas applied during deployment (327,418 gwei) indicates the quantity of computing strength required to complete this transaction. The usual costs of deployment, which include the costs paid for the execution of the transaction on the Ethereum network, is around 0.00082 ETH, whereas the deploying account has a stability of approximately 99.95 ETH. Compressing important elements of the deployment method, along with gas use, transaction hash, contract alternative, agreement address and corresponding costs, this log provides statistics on the process implementation within the Ethereum application.

AdminDoctorManagement and Patient Management are two distinct additives that characterize the deployment of smart contracts meant to deal with the method administrative and patient-related features. The blockchain deployment activity is distinctively identified and recorded in time by using the transaction data included within the log, which consist of the transaction hash, block variety and

timestamp. Particularly, there is no Ether movement throughout this operation since the newly allocated account balance continues to remain at 99.95 ETH despite the deployment. Furthermore, low gas consumption indicates effective deployment transaction execution. It is implied that the distributed contracts are now usable and accessible for interaction inside the Ethereum ecosystem by the log reference to "artifacts saved for interaction". In general, this terminal log reflects an efficient execution of smart contracts to operate administrative and patient-related features in the Ethereum blockchain. It captures the key elements of the deployment process, such as contract installation, transaction information, gas utilization and account balance.

The Ganache user interface (Hassan et al., 2024) is highly favoured by developers for its adaptability in contract deployment, app creation and development in an independent Ethereum blockchain. There are several additional Ethereum blockchain management tools available as well. The UI provides a comprehensive view of several accounts, each with its own address, ETH balance and number of transactions. The range of balances, which show different holdings or degrees of activity across these accounts, is 99.95 ETH to 100.00 ETH. The interface tabs, which include "ACCOUNTS", "BLOCKS", "TRANSACTIONS" and others, make it convenient to navigate between the many Ethereum blockchain data areas. By giving users access to and analysis capabilities for critical data including transaction history, block information and account details, these tabs improve users' capacity to properly track and organize blockchain activities.

**Table 3.** Performance of memory space consumption.

Algorithm	Memory used (MB)
ABE	0.107
RSA	0.186
Hybrid algorithm AES	0.147
Proposed MIDC AES-256	0.0088

An overall performance comparison of several encryption techniques in terms of memory utilization is shown in Table 3. Attribute-based encryption (ABE), Rivest-Shamir-Adleman (RSA), hybrid approach AES (advanced encryption standard) and the proposed MIDC AES-256 approach are the four algorithms assessed. For each approach, the memory area usage is shown in megabytes (MB). Memory use for ABE is 0.107 MB, RSA is 0.186 MB and the hybrid algorithm AES uses 0.147 MB. By comparison, the proposed MIDC AES-256 technique uses significantly less memory: just 0.0088 megabytes. By notably reducing memory use, the recommended set of rules performs better than current encryption techniques such as ABE, RSA and hybrid algorithm AES. This makes our algorithm a viable choice for resolving memory-related issues in sensitive applications with collective healthcare data control.

**Table 4.** Execution speed analysis.

Attributes	Algorithm	Group size (MB)	Time of encryption (ms)
5	ABE	4.200	3.89
5	RSA	4.200	4.58
5	Hybrid algorithm AES	4.380	4.80
5	Proposed MIDC AES-256	6.250	3.46

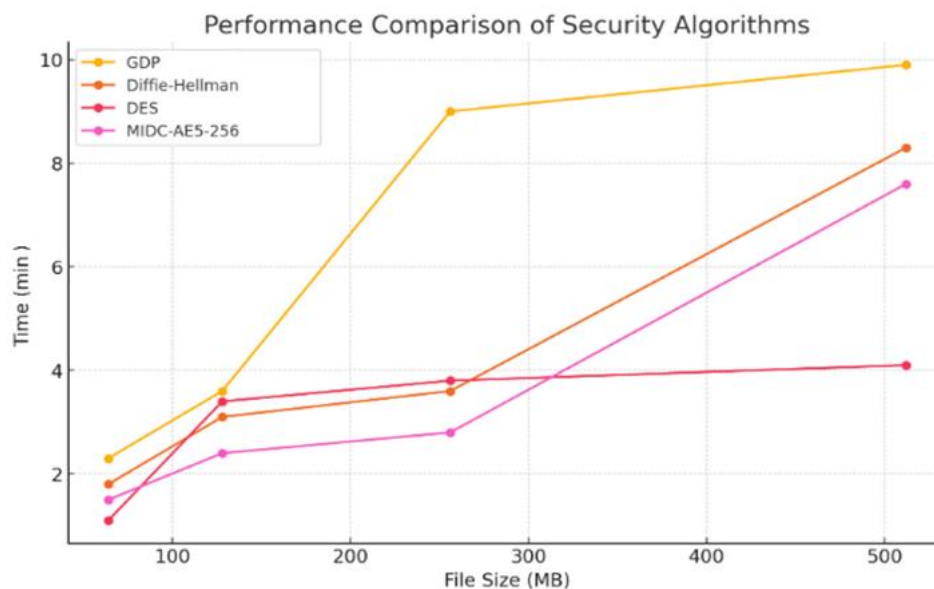
An examination of the execution speed of various encryption strategies relying on certain functions and group size is shown in Table 4. Attribute-based encryption (ABE), RSA (Rivest-Shamir-Adleman), hybrid



approach AES (advanced encryption standard) and the proposed MIDC AES-256 approach are the four algorithms compared. The group size, expressed in megabytes (MB) and the encryption duration, expressed in milliseconds (ms), are the attributes which can be analysed. When encrypting a five MB file, ABE takes 3.89 ms, RSA takes 4.58 ms, hybrid technique AES takes 4.8 ms and the proposed MIDC AES-256 technique takes 3.46 ms. The findings show that the proposed MIDC AES-256 set of attributes performs faster than the other encryption strategies for the given attributes and group size. This indicates that faster encryption techniques may be useful in conditions in which well-timed and powerful data encryption is required.

**Table 5.** Performance comparison of security algorithms.

File size (MB)	GDP (min)	Diffie-Hellman (min)	DES (min)	MIDC AES-256 (min)
64	2.3	1.8	1.10	1.5
128	3.6	3.1	3.4	2.4
256	9	3.6	3.8	2.8
512	9.9	8.3	4.1	7.6



**Figure 5.** Performance comparison of security algorithms.

Table 5 and Figure 5 provide a comprehensive evaluation of security algorithms across different file sizes. The assessment includes GDP, Diffie-Hellman, DES and MIDC AES-256 algorithms, focusing on encryption and decryption times in minutes. For instance, for a 64 MB file, encryption times are as follows: GDP (2.3 min), Diffie-Hellman (1.8 min), DES (1.10 min) and MIDC AES-256 (1.5 min). As file sizes increase to 128 MB, 256 MB and 512 MB, the performance of these algorithms varies. Notably, MIDC AES-256 consistently outperforms GDP, Diffie-Hellman and DES across various file sizes, demonstrating superior data security within optimal timeframes. These findings suggest that MIDC AES-256 is a viable option for applications requiring robust security capabilities without sacrificing speed, particularly when dealing with large datasets.

**Table 6.** Encryption time vs. numbers of keys of different algorithms.

Keys	ABE (ms)	RSA (ms)	Hybrid algorithm (ms)	Proposed MIDC AES-256 (ms)
1	3.10	1.3	0.98	0.05
2	4.97	1.78	1.26	0.35
3	5.99	2.84	2.28	1.30
4	6.88	5.88	3.3	2.3

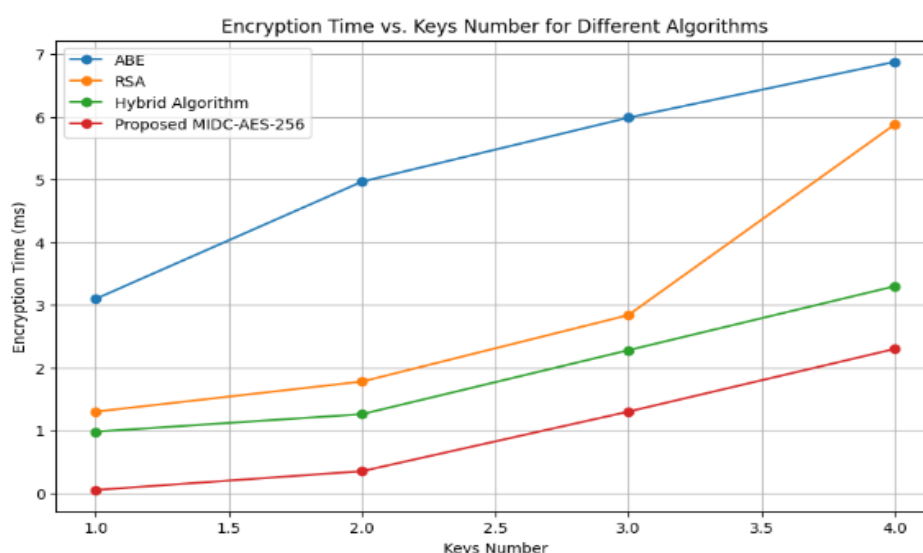
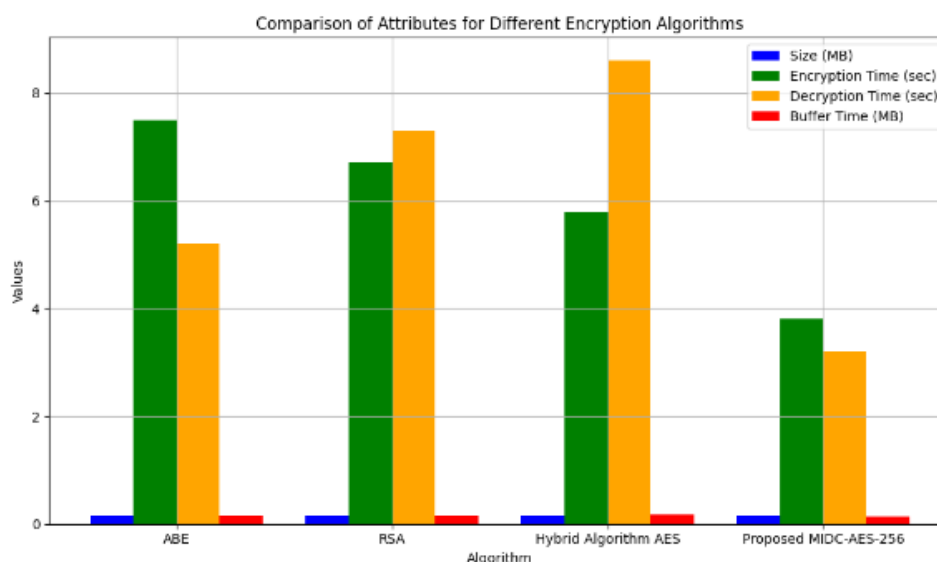
**Figure 6.** Encryption time vs. numbers of keys for different algorithms.

Table 6 and Figure 6 display the key generation time performance comparison for four distinct encryption algorithms: the proposed MIDC AES-256, RSA (Rivest-Shamir-Adleman), hybrid strategies and attribute-based encryption (ABE). The time it takes to supply a particular number of keys for every algorithm is shown in the table, expressed in milliseconds (ms). The key generation time for each algorithm changes because the number of keys rises from one to four. The ABE approach takes 3.10 milliseconds to generate one key and 6.88 milliseconds to generate four keys. Comparably, the RSA method takes 1.3 ms to generate one key and 5.88 ms to generate four keys. Key generation times for one to four keys in the hybrid algorithm range from 0.98 ms to 3.3 ms, indicating moderate overall performance. Notably, the proposed MIDC AES-256 technique, which ranges from 0.05 ms for one key to 2.3 ms for four keys, consistently reveals the shortest key generation time of all.

**Table 7.** Comparison of attributes for different encryption algorithms.

Algorithm	Size (MB)	Encryption time (sec)	Decryption time (sec)	Buffer time (MB)
ABE	0.153	7.5	5.2	0.153
RSA	0.153	6.7	7.3	0.164
Hybrid algorithm AES	0.153	5.8	8.6	0.178
Proposed MIDC AES-256	0.153	3.8	3.2	0.146



**Figure 7.** Comparison of attributes for different encryption algorithms.

An evaluation of the proposed technique with contemporary encryption techniques in terms of record dimensions, encryption time, decryption time and buffer length are shown in Table 7 and Figure 7. Attribute-based encryption, RSA, hybrid approach AES and the proposed MIDC AES-256 technique are the four algorithms assessed. Every approach utilizes files which are precisely 0.153 megabytes (MB) in size. The buffer time needed for every method, expressed in megabytes (MB), is also shown in the table together with the amount of time necessary for the encryption and decryption processes, each measured in seconds (sec). ABE takes 7.5 seconds to encrypt, RSA takes 6.7 seconds, hybrid method AES takes 5.8 seconds and the proposed MIDC AES-256 method takes 3.8 seconds. Comparably, the proposed MIDC AES-256 technique takes 3.2 seconds to decrypt statistics, whereas ABE takes 5.2 seconds, RSA takes 7.3 seconds and hybrid approach AES takes 8.6 seconds. For every technique, there is also the buffer time, which takes memory overheads into consideration. In comparison with ABE, RSA and hybrid algorithm AES, the findings show that the proposed MIDC AES-256 algorithm provides superior performance, displaying shorter encryption and decryption times together with decreased buffer requirements. This makes it an appealing alternative for solid and efficient data encryption and decryption tasks.

**Table 8.** Distribution of percentages among encryption algorithms.

Encryption algorithms	Percentage
Attribute-based encryption	13%
Rivest-Shamir-Adleman	20%
Hybrid algorithm	24%
MIDC AES-256 (proposed algorithm)	43%

Table 8 illustrates the distribution of percentages among different encryption algorithms, highlighting the proportion of usage for each algorithm within a given context. The distribution of percentages among encryption algorithms in the study was derived from a comprehensive survey of existing literature, involving a total of 21 papers. These papers predominantly covered fields such as healthcare, electronic health records (EHR) and blockchain technology, with a specific focus on patient-centric approaches to privacy and security. The proposed MIDC AES-256 algorithm, representing 43% of the distribution, was prominently featured in studies such as those by Ahmad et al. (2024), Dewangan and Chandrakar (2023), Peng et al. (2023), Yuan et al. (2023) and Abouali et al. (2021). Hybrid algorithms, accounting for 24% of

the distribution, were discussed in works by Rai et al. (2022), Wu et al. (2024), Verma (2024), Masood et al. (2024), George and Chacko (2022) and Hongjiao et al. (2021). The RSA algorithm, comprising 20% of the distribution, was highlighted in studies by Abutaleb et al. (2023), Houhou et al. (2024), Puneeth and Parthasarathy (2024), Naresh et al. (2021), Chelladurai et al. (2021) and Rai (2023). Lastly, attribute-based encryption (ABE), which made up 13% of the distribution, was examined in research by Hassan et al. (2023), Agarkar et al. (2024), Han et al. (2022), Hussien et al. (2021) and Naresh et al. (2021). These papers have provided a comprehensive view of current research trends and practical implementations in encryption technologies, ensuring a representative sample of encryption methods. The percentages were calculated based on the frequency and context in which these encryption algorithms were discussed in the literature.

The superior performance of the MIDC AES-256 algorithm in terms of memory consumption, encryption/decryption time and key generation time can be attributed to several technical factors inherent in its design. Firstly, MIDC AES-256 utilizes a hybrid encryption approach that combines the strengths of multiple cryptographic techniques, resulting in an optimized balance between security and efficiency. By incorporating concepts from both symmetric and asymmetric encryption, MIDC AES-256 achieves robust data protection while minimizing computational overheads. Moreover, the algorithm employs advanced encryption standards such as the AES-256 cipher, known for its strong security properties and efficient implementation, optimizing resource utilization by efficiently managing memory allocation and processing overheads, leading to reduced memory footprint and faster execution times compared to traditional encryption methods. Furthermore, MIDC AES-256 employs innovative techniques for key generation and management, enabling rapid key generation without compromising security, by utilizing cryptographic primitives effectively and streamlining key distribution processes, minimizing latency associated with key operations, thereby enhancing overall encryption performance. Additionally, MIDC AES-256 may benefit from optimizations tailored to modern computing architectures, including parallel processing capabilities and hardware acceleration support, harnessing parallelism and utilizing specialized hardware resources efficiently, maximizing computational throughput and minimizing latency, resulting in faster encryption/decryption times across diverse hardware platforms. Overall, the superior performance of MIDC AES-256 can be attributed to its innovative design principles, prioritizing efficiency without compromising security, offering a compelling solution for secure and efficient data encryption tasks in various application domains.

## 6 Conclusion and Future Work

In conclusion, an effective solution for improving healthcare data security is provided by the proposed blockchain-powered patient-centric access control system combined with MIDC AES-256 encryption. The system prioritizes patient autonomy and makes use of blockchain generation to guarantee decentralized, obvious and unchangeable storage of clinical data. It also provides authorized organizations with dependable and regulated access to the data. By integrating MIDC AES-256 encryption, which performs better than contemporary encryption techniques, record integrity and secrecy are notably reinforced. Our comparative study showed that the proposed technology is efficient and powerful in protecting sensitive healthcare records, with faster encryption and decryption speeds and decreased memory consumption.

Scalability and functionality of the proposed method has to be addressed in further work by investigating new features and upgrades. Future studies could focus on improving the encryption algorithm performance even more and investigating different encryption methods to tackle new security issues. Furthermore, to evaluate the method viability, usability and scalability, there is a need for comprehensive real-world testing and validation in a variety of healthcare contexts. Additionally, as blockchain technology and encryption techniques expand, the system should be constantly improved and adjusted to satisfy changing safety needs and keep up with technical enhancements within the healthcare sector.

With all aspects considered, the recommended approach establishes a foundation for subsequent research projects intended to strengthen healthcare record safety and privacy while giving people more control over their clinical records.

## Additional Information and Declarations

**Conflict of Interests:** The authors declare no conflict of interest.


**Author Contributions:** K.P.N.R.: Conceptualization, Methodology, Data curation, Writing – Original draft preparation. S.C.: Investigation, Supervision, Validation, Writing – Reviewing and Editing.

**Data Availability:** The data that support the findings of this study are available from the corresponding author.

## References

- Abouali, M., Sharma, K., Ajayi, O., & Saadawi, T. (2021). Blockchain Framework for Secured On-Demand Patient Health Records Sharing. In *2021 IEEE 12th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference* (pp. 35–40). IEEE. <https://doi.org/10.1109/uecon53757.2021.9666482>
- Abutaleb, R. A., Alqahtany, S. S., & Syed, T. A. (2023). Integrity and Privacy-Aware, Patient-Centric Health Record Access Control Framework using a blockchain. *Applied Sciences*, 13(2), 1028. <https://doi.org/10.3390/app13021028>
- Agarkar, A. A., Karyakarte, M., Chavhan, G., Patil, M., Talware, R., & Kulkarni, L. (2024). Blockchain aware decentralized identity management and access control system. *Measurement. Sensors*, 31, 101032. <https://doi.org/10.1016/j.measen.2024.101032>
- Ahmad, M., De Alwis, C., Shukla, M., & Sant, P. (2024). Privacy-preserving patient-centric electronic health records exchange using blockchain. In *Artificial Intelligence, Big Data, Blockchain and 5G for the Digital Transformation of the Healthcare Industry* (pp. 341–361). <https://doi.org/10.1016/b978-0-443-21598-8.00020-8>
- Chelladurai, U., Pandian, S., & Ramasamy, K. (2021). A blockchain based patient centric electronic health record storage and integrity management for e-Health systems. *Health Policy and Technology*, 10(4), 100513. <https://doi.org/10.1016/j.hlpt.2021.100513>
- Dewangan, N. K., & Chandrakar, P. (2023). Patient-Centric Token-Based healthcare blockchain implementation using secure internet of medical things. *IEEE Transactions on Computational Social Systems*, 10(6), 3109–3119. <https://doi.org/10.1109/tcss.2022.3194872>
- George, M., & Chacko, A. M. (2021). MediTrans—Patient-centric interoperability through blockchain. *International Journal of Network Management*, 32(3). <https://doi.org/10.1002/nem.2187>
- Han, D., Zhu, Y., Li, D., Liang, W., Souri, A., & Li, K. (2022). A Blockchain-Based auditable access control system for private data in Service-Centric IoT environments. *IEEE Transactions on Industrial Informatics*, 18(5), 3530–3540. <https://doi.org/10.1109/tii.2021.3114621>
- Hassan, H., Hassan, R., & Gbashi, E. (2023). E-voting system based on Ethereum blockchain technology using ganache and remix environments. *Engineering and Technology Journal*, 41(4), 562–577. <https://doi.org/10.30684/etj.2023.135464.1273>
- Houhou, O., Bitam, S., & Hamida, A. (2024). HYARBAC: a new hybrid access control model for cloud computing. *International Journal of Computing and Digital System*, 15(1), 403–414. <https://doi.org/10.12785/ijcds/150131>
- Hussien, H. M., Yasin, S. M., Udzir, N. I., & Ninggal, M. I. H. (2021). Blockchain-Based Access Control Scheme for Secure Shared Personal Health Records over Decentralised Storage. *Sensors*, 21(7), 2462. <https://doi.org/10.3390/s21072462>
- Masood, I., Daud, A., Wang, Y., Banjar, A., & Alharbey, R. (2024). A blockchain-based system for patient data privacy and security. *Multimedia Tools and Applications*, 83(21), 60443–60467. <https://doi.org/10.1007/s11042-023-17941-y>
- Naresh, V. S., Reddi, S., & Allavarpu, V. D. (2021). Blockchain-based patient centric health care communication system. *International Journal of Communication Systems*, 34(7). <https://doi.org/10.1002/dac.4749>
- Peng, G., Zhang, A., & Lin, X. (2023). Patient-centric fine-grained access control for electronic medical record sharing with security via dual-blockchain. *IEEE Transactions on Network Science and Engineering*, 1–14. <https://doi.org/10.1109/tNSE.2023.3276166>
- Puneeth, R. P., & Parthasarathy, G. (2024). Blockchain-Based Framework for Privacy Preservation and Securing EHR with Patient-Centric Access Control. *Acta Informatica Pragensia*, 13(1), 1–23. <https://doi.org/10.18267/j.aip.225>
- Rai, B. K., Fatima, S., & Satyarth, K. (2022). Patient-Centric Multichain healthcare record. *International Journal of E-health and Medical Communications*, 13(4), 1–14. <https://doi.org/10.4018/ijehmc.309439>
- Rai, B. K. (2023). PcBEHR: patient-controlled blockchain enabled electronic health records for healthcare 4.0. *Health Services and Outcomes Research Methodology*, 23, 80–102. <https://doi.org/10.1007/s10742-022-00279-7>
- Verma, G. (2024). Blockchain-based privacy preservation framework for healthcare data in cloud environment. *Journal of Experimental and Theoretical Artificial Intelligence*, 36(1), 147–160. <https://doi.org/10.1080/0952813x.2022.2135611>

- 
- Wu, H., Dwivedi, A. D., & Srivastava, G.** (2021). Security and privacy of patient information in medical systems based on blockchain technology. *ACM Transactions on Multimedia Computing Communications and Applications*, 17(2s), 1–17. <https://doi.org/10.1145/3408321>
- Wu, S., Zhang, A., Gao, Y., & Xie, X.** (2024). Patient-centric medical service matching with fine-grained access control and dynamic user management. *Computer Standards & Interfaces*, 89, 103833. <https://doi.org/10.1016/j.csi.2024.103833>
- Yuan, W., Yan, B., Li, W., Hao, L., & Yang, H.** (2023). Blockchain-based medical health record access control scheme with efficient protection mechanism and patient control. *Multimedia Tools and Applications*, 82(11), 16279–16300. <https://doi.org/10.1007/s11042-022-14023-3>
- 

**Editorial record:** The article has been peer-reviewed. First submission received on 23 March 2024. Revisions received on 21 May 2024 and 24 June 2024. Accepted for publication on 27 June 2024. The editor in charge of coordinating the peer-review of this manuscript and approving it for publication was Zdenek Smutny .

---

Acta Informatica Pragensia is published by Prague University of Economics and Business, Czech Republic.

ISSN: 1805-4951

---