

A Dynamically Zero Trust and Risk Aware Cryptographic Orchestration Framework of Secure Multi Cloud Electronic Health Records

D. Veerabhadra Rao¹, G. Appa Rao² and S. Anuradha²

¹Department of Artificial Intelligence and Data Science, GSCSE, GITAM University, Visakhapatnam, Andhra Pradesh, 530045, India

²Department of Computer Science and Systems Engineering GSCSE, GITAM University, Visakhapatnam, Andhra Pradesh, 530045, India

Article history

Received: 11-06-2026

Revised: 27-08-2026

Accepted: 16-09-2026

Corresponding Author:

D. Veerabhadra Rao
Department of Artificial
Intelligence and Data Science,
GSCSE, GITAM University,
Visakhapatnam, Andhra
Pradesh, 530045, India
Email: vdamiset@gitam.edu

Abstract: The adoption of multi-cloud infrastructures for Electronic Health Records (EHRs) improves scalability and accessibility but introduces security challenges such as fragmented trust management, high cryptographic overhead, and inefficient integrity verification. Existing frameworks rely on static authorization and uniform encryption mechanisms, which fail to dynamically evaluate behavioural risks associated with user access requests. Consequently, Distributed Trust Inconsistency, Cryptographic Scalability Saturation, and Distributed Integrity Verification challenges emerge in large-scale healthcare cloud environments. To address these limitations, this study proposes the Adaptive Intelligent Cryptographic Zero-Trust Multi-Cloud Electronic Health Records (AIC-ZTMC-EHR) framework, which integrates behavioural risk evaluation, adaptive encryption orchestration, and lightweight integrity verification. Initially, the Distributed Trust Inconsistency Problem is resolved through the Risk-Adaptive Behavioural Access Control-Extended (RABAC-E) technique, which evaluates behavioural patterns, device trust, access frequency, and location anomalies to generate a risk-based trust score for adaptive authorization. Subsequently, the Cryptographic Scalability Saturation Issue is mitigated through Tri-Partition Adaptive Encryption Orchestration (TAEO), employing AES-256, ChaCha20, and AES-128 encryption algorithms to generate encrypted EHR partitions. Furthermore, the Integrity-Confirmed Virtual Ledger Chain (ICVLC) enables lightweight SHA-256 hash-chain verification to provide tamper-resistant validation of distributed healthcare data. Experimental evaluation using the MIMIC-IV Electronic Health Records dataset within a simulated multi-cloud environment achieves 94.6% access control accuracy, 29 s encryption time, 235 ms integrity verification, 99% tamper detection, and 74 MB/s encryption throughput. The results indicate improved access security, enhanced cryptographic scalability, and efficient integrity validation for large-scale multi-cloud Electronic Health Record systems.

Keywords: Zero Trust Security, Electronic Health Records, Multi-Cloud Security, Risk-Aware Access Control, Adaptive Encryption, Data Integrity Verification

Introduction

The fast digitalization of healthcare systems has resulted in the use of large scale Electronic Health Records (EHRs) in storing, managing, and sharing patient

data among medical institutions (Sachdeva et al., 2024). The technologies of cloud computing have greatly enhanced the scalability, access and interoperability of healthcare data infrastructures. Over the last few years, there has been a growing tendency of healthcare providers

to move EHR storage and processing to multi-cloud environments to improve data availability, reliability, and computational flexibility (Sandhu et al., 2025; Kaur et al., 2025; Samonte et al., 2024). Multi-cloud systems enable healthcare organizations to spread patient records to several cloud service providers, thus decreasing the reliance on a single cloud service provider and enhancing system resilience (Chaturvedi et al., 2024). Nonetheless, these distributed characteristics of multi-cloud environments present serious security and privacy concerns, especially concerning the protection of extremely sensitive patient data against unauthorized access, data manipulation, and insider threats (Pendyala, 2025). Assurance of secure access control, scalable encryption schemes and trustworthy verification of data integrity has thus become a primary need in modern healthcare systems Tiwo et al. (2025).

Several security protocols are suggested to secure EHRs in cloud environments. Traditional healthcare data protection solutions are generally based on Role Based Access Control (RBAC), Attribute Based Access Control (ABAC) and cryptographic encryption methods to provide confidentiality and limit unauthorized access to data (Shojaei et al., 2024; Exceline and Nagarajan, 2024). Multiple cloud-based EHR systems have adopted multi-layered encryption schemes and multistage authentication frameworks to protect patient information. Also, architectures based on blockchains have been implemented to support tamper-evident verification of the integrity of medical data using distributed ledger mechanisms (Sangeetha et al., 2024). Although these mechanisms enhance the security of data confidentiality and integrity, many current systems are based on the principles of static authorization policies that allow access based on pre-established permissions instead of the dynamic assessment of the risk contextualized by each user request (Pandit and Chatterjee, 2025). Moreover, most encryption systems encrypt the entire datasets using similar cryptographic tools, and this generates significant computation redundancy when dealing with large datasets of medical data in the multi-cloud environment (Psarra et al., 2022).

Even with the current trends in healthcare cybersecurity, there are a few gaps that are undermining the present EHR protection models. Primarily, the policies of static access control do not continuously test behavioural patterns and contextual conditions throughout the user session, leading to the Distributed Trust Inconsistency Problem, where encrypted data is also safe, and access decisions are not dynamically re-evaluated during suspicious behaviour (Kumar et al., 2024; Mhiri et al., 2024; Faruk et al., 2023). Second, the growing amount of EHRs poses significant computational problems in the encryption and decryption processes, resulting in the Cryptographic Scalability Saturation

Problem in multi-cloud systems (Ullah et al., 2024). Traditional encryption methods are not linear with the size of datasets; therefore, their efficiency and processing latency are negatively affected as the size of the datasets increases (Yaseen et al., 2025). Third, whereas blockchain-based verification systems can improve integrity assurance, they are too computationally intensive and storage-intensive to be implemented effectively within the scale of a large healthcare cloud system (Swarnkar et al., 2024). Such constraints underscore the existence of a security architecture that can help to incorporate dynamic trust assessment, scalable cryptographic control and lightweight integrity checking into a distributed healthcare setting (Zhang et al., 2022).

To overcome these limitations, this study proposes the AIC-ZTMC-EHR framework for secure EHR management in distributed multi-cloud healthcare environments. Unlike existing healthcare security frameworks that independently employ Zero Trust authorization, cryptographic protection, or blockchain-based integrity verification, the proposed architecture unifies these mechanisms into a single adaptive security framework. It incorporates RABAC-E for continuous behavioural trust evaluation, TAEO for sensitivity-aware cryptographic scheduling using AES-256, ChaCha20, and AES-128, and ICVLC for lightweight SHA-256 hash-chain integrity verification. By integrating these complementary mechanisms, the framework simultaneously addresses the Distributed Trust Inconsistency Problem, Cryptographic Scalability Saturation Issue, and Distributed Integrity Verification Challenge, which are typically handled independently in existing Electronic Health Record security solutions. The major contributions of this work are summarized as follows:

- A behavioural risk-aware Zero Trust access control mechanism (RABAC-E) that continuously evaluates behavioural patterns, device trust, access frequency, and location anomalies to enable adaptive, context-aware authorization decisions
- A sensitivity-aware adaptive encryption orchestration strategy (TAEO) that partitions Electronic Health Records based on data sensitivity and dynamically applies AES-256, ChaCha20, and AES-128 to achieve an effective balance between security and computational efficiency
- A lightweight integrity verification mechanism (ICVLC) that employs SHA-256 hash chaining to provide tamper-resistant integrity verification while reducing the computational overhead associated with conventional blockchain consensus mechanisms
- A comprehensive experimental evaluation using the MIMIC-IV dataset in a simulated multi-cloud healthcare environment, demonstrating improvements in access control accuracy, encryption

efficiency, integrity verification performance, throughput, scalability, statistical reliability, and overall system performance

Literature Review

Mubarakali and Basha (2024) proposed to improve the security and privacy of EHRs in the cloud through a blockchain-based cryptographic framework. The SEHR-BC-CHG model used in the methodology consisted of cryptographic hash generation, Discrete Shearlet Transform encryption, and an optimization-based request verification mechanism. The results indicated a 16.38, 27.28, and 20.21% reduction in encryption time relative to existing SEHR-BC-MICEC, SEHR-BC-TRSA, and SEHR-BC-LFCA models, respectively, enhancing the security performance.

Soy and Balkrishna (2026) intended to enhance cybersecurity in healthcare through the implementation of a Zero Trust Architecture to secure sensitive patient information and related medical devices. The approach implied applying continuous authentication, device identification, and context-based access controls in the framework of Zero Trust. The results showed that the strategy enhanced the security of networks, minimized insider threats, and enhanced security of data vulnerability within healthcare systems.

Edo et al. (2024) intended to resolve the weaknesses of healthcare data and insider threats by adopting a Zero Trust Architecture. The approach entailed the use of context-based access control policies that involve the continued authentication and verification of users and devices. The results showed that the Zero Trust model was effective in minimizing the risk of data vulnerability and enhancing patient data security through the inhibition of unauthorized access and limiting lateral movement in healthcare systems.

Naidu et al. (2023) aimed to improve the security of E-Health Records with a multi-layer security architecture on a cloud platform. The approach included using a scalable multi-level architecture that can secure medical information against various cyber threats. The results showed that the framework enhanced security and flexibility of health systems in data protection, but there was complexity in implementation and frequent updates to counter emerging risks in cybersecurity.

Atlam and Yang (2025) intended to enhance the security of healthcare systems through the creation of a risk-conscious access control model that overcame the shortcomings of the conventional RBAC and ABAC methods. The approach combined RBAC with ABAC and Risk-Based Access Control by dynamically assessing the risk factors related to the context as part of the authorization. The results depicted enhanced accuracy, precision, and recall in the decision making of access control, which is effective in protecting sensitive healthcare information.

Chinnasamy and Deepalakshmi (2022) focused on improving the security of EHRs in cloud environments. The methodology used a hybrid cryptography scheme based on the Improved Key Generation Scheme of RSA and Blowfish encryption, and steganography based access control enabling safe sharing of keys and retrieval of data. The results showed that the data security was improved and the retrieval performance was more efficient than the current methods of hybrid encryption.

Critical Analysis of Existing Studies

While these studies reviewed have contributed significantly to the cloud-based security of healthcare systems, they tend to address individual security elements instead of offering a holistic solution for secure multi-cloud EHRs management. Mubarakali and Basha (2024) enhance confidentiality using blockchain-assisted cryptographic protection and decrease the encryption time; however, it adds computational overhead because of blockchain-based integrity verification and fails to conduct behavioural trust evaluation. Soy and Balkrishna (2026); Edo et al. (2024) improved security based on Zero Trust principles and continuous authentication to minimize insider threats and unauthorized access but did not include adaptive cryptographic management or efficient integrity checks. Atlam and Yang (2025) enhanced the authorization mechanisms with risk-aware access control, it does not address the scalability of encryption or distributed integrity verification. Chinnasamy and Deepalakshmi (2022) enhanced the level of confidentiality with hybrid cryptography, but such a consistent encryption approach to all EHRs could lead to higher computational demands for large healthcare datasets. Likewise, Naidu et al. (2023) suggested a scalable multi-layer cloud security architecture but mentioned implementation complexity and maintenance challenges. These studies contribute individually to healthcare security; however, each only covers a portion of the security requirements, leaving key security research challenges still to be resolved. A summary of their strengths, limitations, security characteristics and research gaps is provided in Table 1.

The comparative analysis identifies three major unresolved challenges in securing multi-cloud Electronic Health Record systems. First, the general lack of sensitivity-aware cryptographic orchestration in existing Zero Trust frameworks makes it difficult to provide computational efficiency in large-scale multi-cloud environments, while the focus is mainly on authentication and authorization. Second, many encryption-based approaches use the same encryption mechanism for all data, which implies unnecessary computational overhead and scaling problems. Third, blockchain-assisted integrity verification offers high tamper resistance, but also introduces verification latency, the synchronization overhead and storage complexity.

Table 1: Comparison of existing healthcare security frameworks and the proposed AIC-ZTMC-EHR framework

Study	Strength	Limitation	Behavioural Trust	Adaptive Encryption	Lightweight Integrity	Research Gap
Mubarakali and Basha (2024)	Strong cryptographic security	Blockchain verification overhead	×	Partial	No (Blockchain-based verification)	No adaptive trust evaluation
Soy and Balkrishna (2026)	Continuous Zero Trust authentication	No encryption orchestration	✓	×	×	No scalable encryption
Edo et al. (2024)	Effective insider threat mitigation	Limited integrity verification	✓	×	×	No adaptive cryptography
Naidu et al. (2023)	Scalable multi-layer cloud security	High implementation complexity	Partial	×	Partial	Scalability and maintenance issues
Atlam and Yang (2025)	Accurate risk-aware authorization	Focuses only on access control	✓	×	×	No encryption or integrity integration
Chinnasamy and Deepalakshmi (2022)	Strong hybrid encryption	Uniform encryption overhead	×	×	Partial	No behavioural trust evaluation
(Proposed AIC-ZTMC-EHR)	Integrated behavioural trust, adaptive encryption, and lightweight integrity verification	—	✓	✓	✓	Addresses the identified research gaps

Moreover, the mechanisms of behavioural trust evaluation, encryption and integrity verification are mostly developed as separate security mechanisms and not as an integrated adaptive architecture. These restrictions emphasize a unified framework which integrates continuous behavioural trust evaluation, sensitivity-aware encryption and light integrity verification. To address the identified research gaps, the proposed Adaptive Intelligent Cryptographic Zero-Trust Multi-Cloud Electronic Health Record (AIC-ZTMC-EHR) framework consists of RABAC-E, TAEO and ICVLC in a single Zero Trust framework. The framework incorporates continuous behavioural trust assessment, sensitivity-aware cryptographic orchestration, and lightweight hash chain based integrity checks, overcoming the challenges faced by current healthcare security systems and offering a secure, scalable, and computationally efficient solution for managing EHRs across multiple clouds.

Proposed AIC-ZTMC-EHR Framework

With the quick digitization of medical systems, EHRs can now be stored and managed in a distributed multi-cloud environment, which enhances accessibility, scalability, and interoperability of medical data. Migration to multi-cloud for healthcare data, however, poses various security issues, such as distributed trust management, dynamic insider threats, and larger cryptographic overhead for massive volumes of data. The traditional cloud EHR protection mechanisms are mostly

static access control policies and uniform encryption approaches, which do not continuously assess the behavioural risks linked to user access requests. Thus, the Distributed Trust Inconsistency Problem results, as authorization decisions are made only at the point of initial authentication and not continuously validated by behaviour. Moreover, the use of a single cryptographic scheme for encrypting large amounts of medical records poses computational inefficiencies and creates the Cryptographic Scalability Saturation Issue. Furthermore, enabling dependable tamper detection in a multi-cloud node scenario requires conventional blockchain mechanisms, which introduces a significant amount of verification latency and computation overhead, known as the Distributed Integrity Verification Challenge. The scientific novelty of the proposed AIC-ZTMC-EHR framework consists of the combination of three complementary security mechanisms in a single adaptive framework. Unlike the present healthcare security systems that independently enforce behavioural access control, encryption or integrity checks, the proposed framework continuously assesses behavioural trust using the RABAC-E mechanism, dynamically orchestrates cryptographic algorithms based on the EHR sensitivity using the TAEO, and verifies integrity as tamper-resistant using the ICVLC, which is lightweight. This integrated design simultaneously enhances access security, cryptographic scalability, and integrity assurance while reducing computational overhead in distributed multi-cloud Electronic Health Record systems.

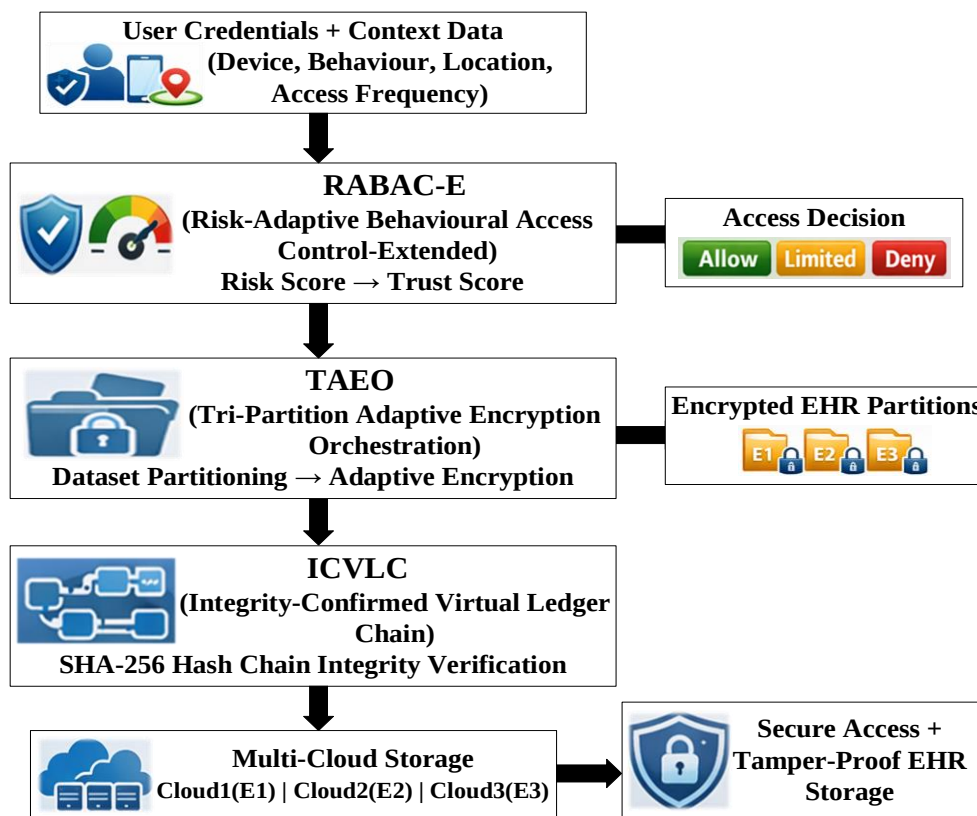


Fig. 1: AIC-ZTMC-EHR secure multi-cloud electronic health record architecture

Figure 1 depicts the design of the proposed Adaptive Intelligent Cryptographic Zero Trust Multi Cloud Electronic Health Records framework (AIC-ZTMC-EHR). A workflow begins when a healthcare user sends a request to get access to patient records with contextual attributes, such as device identity, frequency of access, and session behaviour. The RABAC-E module analyses these parameters to compute a dynamic trust score to continuously assess behavioural risks and therefore solve the Distributed Trust Inconsistency Problem by allowing adaptive, context-aware authorization. After validating the request, the EHR information is sent to the TAE0 component, where the information is divided according to sensitivity and encrypted with optimized tools like AES-256, ChaCha20, and AES-128 encryption, overcoming the Cryptographic Scalability Saturation Issue. Consequently, the ICVLC then computes chains of SHA-256 hash values to ensure tamper-evident validation of distributed cloud nodes to solve the Distributed Integrity Verification Challenge. The presented architecture is a combination of behavioural trust assessment, adaptive cryptographic orchestration, and distributed integrity verification into a single security model. The framework enhances the accuracy of access control, minimizes the encryption overhead on

sensitivity-wise partitioning, and facilitates efficient tamper detection without suffering the computational cost of the traditional blockchain implementation.

Risk Adaptive Behavioural Access Control-Extended (RABAC-E)

The RABAC-E module serves as the central decision-making part of the proposed framework by determining the trustworthiness of all user requests before access to EHRs is obtained. In contrast to traditional role-based access control systems that are based on fixed permissions only, this model dynamically analyses contextual behavioural indicators to establish the validity of an access attempt. Healthcare systems are highly sensitive settings whereby unauthorized access may result in gross privacy breaches; thus, access decisions made must include behavioural intelligence alongside normal authentication processes. RABAC-E model is a continuous analysis of the behavioural activity patterns, the legitimacy of the device used, frequency of access, as well as contextual attributes of each request to determine the degree of risk potential of the session. These indicators together lead to a computed behavioural risk score, which is simply the possibility of an abnormal or suspicious activity during a user session.

The behavioural risk score is mathematically expressed as:

$$R_s = w_1B + w_2D + w_3F \quad (1)$$

Where R_s represents the calculated behavioural risk score, B denotes behavioural activity patterns such as session duration, navigation behaviour, and request timing, D represents the trust level of the device used to initiate the request, and F indicates the frequency of record access within a given time interval. The parameters w_1 , w_2 and w_3 represent weighting coefficients assigned to each factor according to their influence on security risk. This equation allows the system to combine several behavioural indicators into one quantitative risk measure so that abnormal patterns can be found before sensitive records are read.

Because the risk values are not directly used to make authorization decisions, a calculated behavioural risk score is converted to a normalized trust score. This transformation makes the upper trust values represent more secure and trustworthy access conditions. The transformation can be defined as:

$$T_s = 1 - \frac{R_s}{R_{max}} \quad (2)$$

Where T_s is the trust score based on the risk value calculated and R_{max} is the maximum possible risk score in the evaluation range. The normalization process makes sure that the trust score is in a bounded range between one and zero. As the risk score rises because of suspicious behaviour, the trust score also declines, thus indicating less confidence in the validity of the request.

In the proposed framework, R_{max} is not a fixed constant but a dynamically computed upper bound of the behavioural risk score based on the current risk evaluation model. It is determined from the weighted combination of the maximum normalized values of all behavioural and contextual indicators considered during access evaluation. When only behavioural indicators are considered, the maximum risk score is computed using the weighted behavioural factors. When contextual location information is also included, the location anomaly component is incorporated into the maximum risk score computation. Accordingly:

$$R_{max} = w_1B_{max} + w_2D_{max} + w_3F_{max} + w_4L_{max} \quad (3)$$

Where B_{max} , D_{max} , F_{max} , and L_{max} denote the maximum normalized values of behavioural activity, device trust anomaly, access frequency, and location anomaly, respectively. Since the weighting coefficients satisfy the normalization constraint $w_1 + w_2 + w_3 + w_4 = 1$, the value of R_{max} is automatically updated

whenever the behavioural thresholds, weighting parameters, or organizational security policies are modified. This adaptive computation guarantees the trust-score normalization to be consistent with changing operational conditions in real healthcare environments, instead of using a static predefined maximum value.

In addition to the behavioural and device indicators, there are also contextual environmental factors, such as geographic location and network origin, contributing to the overall risk analysis. The extended risk computation model incorporates these aspects to increase the precision of the anomaly detection in the distributed healthcare environment. The extended behavioural risk formulation can thus be expressed as:

$$R_s = w_1B + w_2D + w_3F + w_4L \quad (4)$$

The weighting parameters are normalized such that:

$$w_1 + w_2 + w_3 + w_4 = 1 \quad (5)$$

This normalization is required to ensure that a sum of these behavioural indicators, device trust level, access frequency and location anomaly leads to a bounded and interpretable behavioural risk score. Here, L refers to the location anomaly score based on geographical access patterns, and w_4 the weighting parameter. This extension allows the framework to detect some unusual access patterns such as accessing an unexpected area of the system or an unusual network location that is a common indicator of a compromised credential or malicious activity.

After obtaining the trust score, the system performs adaptive authorization by comparing the trust score with pre-established threshold parameters that affect the level of authorization granted. The rule of the authorization decision is as follows:

$$A_d = \{Allow \ T_s \geq \theta_1 \ Limited \ \theta_2 \leq T_s < \theta_1 \ Deny \ T_s < \theta_2 \quad (6)$$

$$0 \leq \theta_2 < \theta_1 \leq 1 \quad (7)$$

The trust thresholds satisfy the constraint $0 \leq \theta_2 < \theta_1 \leq 1$, ensuring that authorization decisions remain consistent with the normalized trust score interval. Where A_d is the final access decision and θ_1 and θ_2 are predetermined trust threshold values used to categorize the authorization level. Once the calculated trust score passes the upper limit, a request is considered secure, and complete access to the requested EHR dataset is provided.

The system gives controlled or monitored access when the trust value falls within the two thresholds, restricting such sensitive operations as altering records or retrieving large data volumes. When the trust score falls below the lower threshold, the request is automatically rejected, and the event is logged as a possible security anomaly.

Algorithm 1: RABAC-E Adaptive Access Authorization

Input: User request $U = \{B, D, F, L\}$, weights w_1, w_2, w_3, w_4 , thresholds $\{\theta_1, \theta_2\}$
 Output: Access decision A_d and Trust score T_s
 Receive access request U from healthcare user
 Extract behavioural indicators B , device trust D , access frequency F , location anomaly L
 Normalize weighting parameters such that. $w_1 + w_2 + w_3 + w_4 = 1$
 Compute behavioural risk score
 $R_s = w_1B + w_2D + w_3F + w_4L$
 Compute the dynamic maximum risk value
 $R_{max} = w_1B_{max} + w_2D_{max} + w_3F_{max} + w_4L_{max}$
 using the current normalized behavioural indicators and security policy parameters
 Convert risk score into normalized trust score

$$T_s = 1 - \frac{R_s}{R_{max}}$$

 If $T_s \geq \theta_1$ then
 $A_d \leftarrow \text{Allow}$
 Else if $\theta_2 \leq T_s < \theta_1$ then
 $A_d \leftarrow \text{Limited Access}$
 Else $A_d \leftarrow \text{Deny}$
 End if
 Log authorization decision and session risk score
 Continue monitoring subsequent access requests and re-evaluate the trust score throughout the active session
 If $A_d \neq \text{Deny}$ then forward authorized request to TAE0 module
 Return A_d, T_s

Algorithm 1 evaluates the trustworthiness of a healthcare user's access request using behavioural and contextual indicators. Behaviour pattern, device trust, access frequency, and location anomaly are extracted and weighted to compute a behavioural risk score. The risk score is converted into a normalized trust score. Based on predefined trust thresholds, the system classifies the request as Allow, Limited Access, or Deny. Authorized requests are forwarded to the TAE0 encryption module for secure processing.

In accordance with Zero Trust principles, the proposed RABAC-E module continuously re-evaluates every subsequent access request throughout an active user session rather than relying solely on the initial authentication event. Behavioural activity, device trust, access frequency, and contextual location information are continuously monitored to update the trust score whenever additional Electronic Health Record resources are requested. If abnormal behavioural patterns, privilege escalation attempts, or unauthorized lateral movement across protected healthcare resources are detected, the trust score is immediately recalculated, and the authorization level is adaptively downgraded or revoked according to the predefined trust thresholds. This continuous verification mechanism minimizes insider threats, compromised sessions, and unauthorized movement within the distributed multi-cloud healthcare environment.

Through this adaptive evaluation mechanism, the RABAC-E module ensures that access control decisions continuously respond to behavioural and contextual indicators rather than relying solely on static permissions. Once the access request satisfies the required trust conditions, the authorized user request and associated EHR dataset are securely transferred to the TAE0 module, where encryption and secure data processing operations are performed before storage or retrieval within the distributed multi-cloud infrastructure.

Tri-Partition Adaptive Encryption Orchestration (TAE0)

Intelligent cryptographic control of EHRs datasets is conducted by the TAE0 module once the access request has been authenticated by the RABAC-E module. Healthcare information systems normally deal with heterogeneous data that encompasses various types of medical data of varying sensitivity levels. The confidentiality requirements of patient identification details, diagnostic reports, lab results, and administrative metadata are different. Encryption of the entire dataset with a single encryption scheme can thus provide both unnecessary compute costs and have an impact on system scalability in multi-cloud infrastructures. The TAE0 module addresses this issue by implementing a sensitivity-aware encryption orchestration strategy, which divides the EHR dataset into various logical segments and applies an appropriate encryption mechanism based on the security needs of a segment.

Let the whole EHR dataset be represented as D . The partitioning process divides the dataset into 3 logical subsets based on the sensitivity of data. This model of partitioning can be expressed as:

$$D = P_1 \cup P_2 \cup P_3 \quad (8)$$

$$P_1 \cap P_2 \cap P_3 = \emptyset \quad (9)$$

The partitions are mutually exclusive to make sure that every element of data can be attributed to a single sensitivity category. This condition can be expressed as $P_1 \cap P_2 \cap P_3 = \emptyset$, which ensures that the sensitive attributes are not duplicated across the various partitions and is used to avoid unnecessary encryption processes.

Where P_1 is highly sensitive patient information like personal identifiers, medical history, and insurance details, P_2 is clinical and diagnostic information like lab reports and physician observations, and P_3 is non-critical metadata, like appointment timestamps, indexing information, and logs. This tri-partition approach allows the framework to separate critical medical characteristics from less sensitive operational information, therefore allowing for better cryptographic management.

Although the initial tri-partitioning is performed according to predefined sensitivity policies, the proposed TAO module also supports dynamic re-classification of Electronic Health Record data whenever organizational security policies, legal requirements, regulatory compliance rules, or clinical workflows modify the sensitivity level of a data attribute. During such events, the affected records are automatically reassigned to the appropriate partition before encryption, and the corresponding encryption algorithm and cryptographic key are updated according to the revised sensitivity level. For example, metadata originally assigned to P_3 may be reclassified into P_1 or P_2 if subsequent legal or regulatory requirements identify it as sensitive information. This adaptive re-classification mechanism enables the framework to accommodate evolving healthcare regulations while maintaining secure, scalable, and sensitivity-aware cryptographic protection.

Based on the sensitivity classification of each partition, specific encryption algorithms are assigned to ensure an optimal balance between security strength and computational efficiency, as shown in Table 2.

Patient identity information is very sensitive, and it needs stronger cryptographic protection; operational metadata can employ lightweight encryption systems to minimize the computational overhead without affecting the overall system security.

The TAO module uses adaptive encryption scheduling, which selects the appropriate algorithms to use depending on the sensitivity of the data and the workload of the system. As the computational load grows, algorithms with fewer overheads are considered to ensure efficiency without compromising the high-security protection of very sensitive EHRs partitions.

Once the dataset is partitioned, each segment is subjected to an adaptive encryption process, which uses an appropriate encryption algorithm and key depending on the sensitivity level of the segment. The encryption of each partition can be defined as:

$$E_i = Enc(P_i, K_i) \quad (10)$$

Where E_i is the encrypted output of partition P_i , $Enc(\cdot)$ is the encryption method used on the data, and K_i is the cryptographic key used by the corresponding partition. Compartmentalization of security is enhanced using independent encryption keys such that compromise in one of these partitions does not automatically reveal the entire

data. This method enhances privacy and has module control over cryptographic functions.

In the proposed framework, the encryption keys K_1 , K_2 , and K_3 are independently generated to preserve cryptographic isolation among the three EHR partitions. Rather than being permanently stored within the three distributed cloud nodes, the encryption keys are securely maintained using a centralized or federated Key Management System (KMS) or Hardware Security Module (HSM), which performs secure key generation, storage, authenticated distribution, periodic key rotation, and key revocation. During encryption and decryption, only authorized services obtain temporary access to the required keys through secure authenticated channels, while the keys themselves remain outside the cloud storage infrastructure. Furthermore, periodic key rotation and lifecycle management ensure that compromised or expired keys are securely replaced without affecting the confidentiality or integrity of the remaining EHR partitions.

Besides basic encryption, the TAO model also presents the element of algorithm selection as a component of the orchestration mechanism. Selection of different encryption algorithms can be done dynamically based on sensitivity level and computational limitations. The algorithm assignment on each partition is represented as:

$$E_i = Enc_{A_i}(P_i, K_i) \quad (11)$$

Where A_i signifies the encryption algorithm chosen on partition P_i . Partitions like P_1 that are highly sensitive are then allocated a stronger cryptographic algorithm with larger key size to ensure maximum confidentiality protection, whereas partitions with operational or less critical information can be allocated a higher speed encryption algorithm with lower computational latency. This is an adaptive algorithm selection mechanism that allows the framework to balance between the security strength and efficiency of security processing in large-scale medical data.

The orchestration mechanism also examines the computational workload and sensitivity properties to identify the ideal encryption strategy to be used on each partition. This decision process can be modeled by an adaptive scheduling function that can be defined as follows:

$$A_i = f(S_i, C, L) \quad (12)$$

Table 2: Sensitivity-aware encryption assignment in TAO

Partition	Data Type	Encryption Algorithm
P1	Patient identifiers, medical history, insurance details	AES-256
P2	Clinical records, laboratory results, physician observations	ChaCha20
P3	Metadata, timestamps, indexing information, logs	AES-128

Where S_i is the sensitivity level of the partition P_i , C is the cost of computation using the encryption algorithm, and L is the current system workload or processing load. The scheduling function $f(\cdot)$ chooses the most suitable encryption algorithm to use in each partition at an optimal trade-off between the strength of security and processing efficiency. This adaptive scheduling feature avoids cryptographic bottlenecks, which are usually apparent with large healthcare datasets encrypted with uniform security policies.

Once the encryption processes are done, the resulting encrypted partitions are together represented as:

$$E = \{E_1, E_2, E_3\} \quad (13)$$

Where E_1, E_2 , and E_3 are the encrypted forms of partitions P_1, P_2 , and P_3 respectively. These encrypted partitions ensure privacy of patient data and support flexible storage and control over data across cloud environments spread across different locations. Parallel cryptographic processing by the partitioned encryption design is also enabled, enhancing its performance and scalability when considerable amounts of EHRs are being concurrently processed.

Algorithm 2: TAO Adaptive Encryption Orchestration

Input: EHR dataset D , sensitivity levels S_i , system workload L

Output: Encrypted partitions $E = \{E_1, E_2, E_3\}$

Receive authorized Electronic Health Record dataset D from RABAC-E module

Initialize empty partitions P_1, P_2, P_3

Check for updated organizational security policies, legal requirements, and regulatory compliance rules

If the sensitivity level of any record has changed, re-classify the affected record before partitioning

For each record $r \in D$ do

 If sensitivity level of r is High then

 Assign $r \rightarrow P_1$

 Else if sensitivity level of r is Medium then

 Assign $r \rightarrow P_2$

 Else

 Assign $r \rightarrow P_3$

End For

Determine encryption algorithm for each partition

 If partition = P_1 then

 Select algorithm $A_1 = AES - 256$

 Else if partition = P_2 then

 Select algorithm $A_2 = ChaCha20$

 Else if partition = P_3 then

 Select algorithm $A_3 = AES - 128$

Evaluate system workload L

 If workload is High, then

 Prioritize lower computational cost encryption for non-critical partitions

Generate independent encryption keys K_1, K_2 , and K_3

Securely store and manage the generated keys outside the cloud nodes using a KMS or HSM

Apply authenticated key distribution, periodic key rotation, and key revocation policies

Perform encryption for each partition

$$E_1 = Enc_{A_1}(P_1, K_1)$$

$$E_2 = Enc_{A_2}(P_2, K_2) E_3 = Enc_{A_3}(P_3, K_3)$$

Combine encrypted partitions

$$E = \{E_1, E_2, E_3\}$$

Forward encrypted dataset E to ICVLC integrity verification module

Return E

Algorithm 2 ensures the Electronic Health Record dataset is secured by dividing data according to the sensitivity level. All records are categorized as high, medium, or low sensitivity partitions. Each partition is assigned to appropriate encryption algorithms. AES-256 is used with the most sensitive data, ChaCha20 with clinical records, and AES-128 with metadata. Independent encryption keys are generated and securely managed using a KMS or HSM. Each partition is encrypted using its corresponding cryptographic key, while authenticated key distribution, periodic key rotation, and key revocation policies ensure secure key lifecycle management. The encrypted partitions are aggregated and sent to the ICVLC module to verify their integrity.

Once the encrypted partitions are generated, they are securely transferred to the Integrity Confirmed Virtual Ledger Chain (ICVLC) module. At this stage, cryptographic hash values are computed and linked through a verification chain to ensure that the encrypted data remains tamper-resistant during storage and transmission in distributed multi-cloud infrastructure. Through sensitivity-aware partitioning, adaptive algorithm selection, and workload-aware cryptographic scheduling, the TAO module effectively addresses the cryptographic scalability challenges associated with large scale Electronic Health Record systems while maintaining strong data confidentiality and operational efficiency.

Integrity Confirmed Virtual Ledger Chain (ICVLC)

The role of the Integrity Confirmed Virtual Ledger Chain (ICVLC) module is to assure the integrity and tamper-resistance of encrypted EHRs stored in distributed multi-cloud systems. The integrity of the patient records is as important to healthcare systems as confidentiality is because any disruption can result in wrong clinical decisions or even legal issues. The ICVLC module proposes a ledger-based verification structure, based on such principles as the chaining of hash values without the computational complexity of full blockchain implementation. The module uses a progressive cryptographic verification system to make sure that each encrypted data chunk can be verified both during the storage and retrieval processes.

Once the TAO module encrypts the data, every encrypted piece of data should be transformed into a distinct cryptographic fingerprint. This fingerprint is

created based on the SHA-256 hash cryptographic algorithm. The hashing operation is used to convert the encrypted partition into a fixed digest length, which is a unique representation of the content of the information. The hash generating algorithm is represented as:

$$H_i = Hash(E_i) \quad (14)$$

On this basis, the hashing function $Hash(\cdot)$ is employed using the SHA-256 cryptographic hash algorithm, which is highly resistant to collisions and pre-images and has a broad level of adoption across secure data integrity verification systems. Where H_i is the hash value of the encrypted partition E_i , and $Hash(\cdot)$ is the cryptographic hashing algorithm. The main objective of the equation is to generate a unique identifier of every encrypted chunk of data to ensure that any alteration made to the data in the storage automatically causes a different hash value to be generated. As cryptographic hash functions are developed to have a high collision resistance and pre-image resistance, a slight modification in the encrypted data results in a different hash value altogether.

After the collection of hash values of all encrypted partitions, the ICVLC module forms a chain of consecutive verifications, connecting each hash with the last ledger entry. Such a chaining arrangement makes sure that the integrity of the whole dataset is subject to the integrity of all the previous elements in the ledger. Mathematically, the chain formation is given as:

$$C_i = Hash(H_i \parallel C_{i-1}) \quad (15)$$

Where C_i is the current ledger block, H_i is the value of the hash of the current encrypted partition, and C_{i-1} is the predecessor block in the ledger chain. The symbol $\parallel$ implies concatenation of two values followed by hashing. This formula makes every ledger block hold the current hash of the partition and the past chain reference, which generates a successive chain of dependent verification records. When any encrypted partition is altered or changed, the corresponding hash value is altered, and this breaks the whole chain structure that, in turn, indicates a violation of data integrity.

When the hash chain is built, the encrypted partitions and the ledger entries are replicated on several cloud servers in the simulated multi-cloud infrastructure. This distribution approach improves availability, reliability and fault tolerance by eliminating one point of failure in the storage architecture. Encryption of partitions and their distribution to various clouds can be described as follows:

$$S = \{Cloud_1(E_1), Cloud_2(E_2), Cloud_3(E_3)\} \quad (16)$$

Where S is the distributed storage structure, $Cloud_1$, $Cloud_2$, and $Cloud_3$ are independent cloud storage nodes

that maintain various encrypted partitions. The framework enhances resistance to cloud outages, malicious tampering and localized data corruption by distributing encrypted fragments on various platforms.

The ICVLC module, during a data retrieval operation, also checks the data integrity by calculating the hash of the encrypted partition that is being accessed and comparing it to the store ledger value. This authentication procedure is mathematically expressed as:

$$V_i = \{1, Hash(E_i^*) = H_i, Hash(E_i^*) \neq H_i\} \quad (17)$$

Where V_i is the verification of the partition i , E_i^* is the retrieved encrypted partition, and H_i is the stored hash value in the ledger. A value of 1 would mean that the data has not been tampered with or corrupted, whereas a value of 0 would be a sign that there was tampering or corruption of the data. On detection of a mismatch, the system blocks access to the corrupted partition immediately and logs the security anomaly as an event in system logs.

Algorithm 3: Integrity Confirmed Virtual Ledger Chain

Input: Encrypted partitions $E = \{E_1, E_2, E_3\}$, previous ledger block C_{i-1}

Output: Verification result V_i and updated ledger chain C_i
Receive encrypted partitions $E = \{E_1, E_2, E_3\}$ from TAEO module

Initialize previous ledger block C_{i-1}

For each encrypted partition E_i in E do

Generate hash $H_i = SHA256(E_i)$

Create ledger block $C_i = Hash(H_i \parallel C_{i-1})$

Store ledger block C_i in the verification chain

Update previous block reference $C_{i-1} \leftarrow C_i$

End For

Distribute encrypted partitions across Cloud1, Cloud2, Cloud3

During retrieval obtain encrypted partition E_i^*

Recalculate hash $H_i^* = SHA256(E_i^*)$

Compare H_i^* with stored hash H_i

If $H_i^* = H_i$ then $V_i \leftarrow 1$ else $V_i \leftarrow 0$

If $V_i = 0$ then block access and log tampering event

Algorithm 3 guarantees the tamper-resistant verification of encrypted Electronic Health record partitions. SHA-256 hashing is applied on each encrypted partition to obtain an exclusive hash value. The current hash, together with the previous block reference, is combined to form a hash chain, which forms a sequential ledger block. Encryption partitions are transferred to more than one cloud node. When a retrieval is done, hash values are re-computed and compared to stored values to identify the presence of any data alteration or integrity breach.

The ICVLC module implements a lightweight but efficient integrity assurance mechanism in multi-cloud EHRs through the combination of cryptographic hashing, sequential ledger chaining, and distributed storage verification. This can be designed in such a way that it

offers tamper-evident verification of stored medical data at a significantly lower computational cost than the blockchain consensus protocols.

Altogether, the suggested AIC-ZTMC-EHR framework guarantees three integrated modules of multi-cloud EHRs. RABAC-E is a behavioural risk-based access authorization that involves the use of contextual indicators. TAEO uses sensitivity-based data partitioning and dynamic encryption to enhance the efficiency of cryptography. ICVLC guarantees that the integrity is tamper-resistant with the help of SHA-256 hash chaining and distributed storage. The integrated architecture increases access security, encryption scalability, and dependable integrity verification for distributed healthcare cloud architectures. The experimental setup creates a simulated multi-cloud healthcare environment with the help of the MIMIC-IV dataset to test the performance of the system. Further sections examine the effectiveness of access control, efficiency of encryption, capability of verification of integrity and overall scalability of the system.

Results and Discussion

The proposed AIC-ZTMC-EHR framework was evaluated in a simulated multi-cloud healthcare environment to assess secure Electronic Health Record (EHRs) storage, adaptive access control, cryptographic scalability, and integrity verification. The combination of the integrated RABAC-E, TAEO, and ICVLC modules enables behavioural trust evaluation, sensitivity-aware encryption, and tamper-evident integrity verification, ensuring secure data access, minimizing cryptographic overhead, and fostering system scalability with growing healthcare data sizes. The experiments were performed with Python 3.10, in a virtual machine running Linux that is used to simulate three different logical cloud nodes, representing independent healthcare cloud providers storing encrypted partitions of EHRs that are encrypted. The experimental platform was composed of a 2.4 GHz Intel Xeon processor with 16 GB of RAM and Ubuntu Linux 22.04. Several tests were conducted with increasing amounts of data to analyze computational scalability, cryptographic efficiency and trust-based access performance. The evaluation was performed in a controlled simulated environment to give a reproducible proof-of-concept. Thus, deployment characteristics like inter-cloud network latency, packet loss, bandwidth fluctuations, cloud-provider-specific API constraints, and service-level variability of commercial cloud platforms (e.g., Amazon Web Services, Microsoft Azure, and Google Cloud Platform) were not explicitly modelled. While these factors might be important in the communication latency and the synchronization overhead in operational healthcare systems, the main goal was to assess the effectiveness of

behavioural trust evaluation, adaptive cryptographic orchestration and integrity verification under controlled conditions. Therefore, the reported results should be interpreted within the scope of the simulated environment. Future work will deploy the framework across public multi-cloud platforms to evaluate inter-cloud communication latency, fault tolerance, interoperability, cloud API overhead, and overall performance under realistic distributed healthcare environments.

Dataset Characteristics and Experimental Configuration

The experimental assessment makes use of the MIMIC-IV EHRs data acquired in PhysioNet, which is a massive, de-identified clinical dataset commonly adopted in health data analytics and security studies. The dataset consists of organized patient data composed of demographic data, hospitalization, diagnostic data, surgical procedures, laboratory data, and prescriptions. To conduct the experiment, a sample consisting of 50,000 to 100,000 EHRs entries is taken to represent the ability to handle scalable healthcare data management conditions on distributed cloud systems. The data is stored in tabular CSV and relational tables to allow efficient partitioning, encryption and retrieval operations of the data during experimentation. To simulate the distributed healthcare storage environments, a multi-cloud infrastructure with three independent cloud nodes is set up to emulate a distributed system. The TAEO module divides the data into sensitivity-based groups and encrypts it with AES-256, ChaCha20 and AES-128 algorithms. The RABAC-E module is used to assess access requests and compute behavioural trust scores on the basis of contextual indicators. The ICVLC module then confirms the integrity of encrypted partitions by chaining hash values of the encrypted partitions using the hash function of SHA-256 between storage and retrieval.

Realistic Healthcare Scenario Evaluation

To further evaluate the practical applicability of the proposed AIC-ZTMC-EHR framework, experiments were conducted under representative healthcare operational scenarios commonly encountered in distributed hospital environments. Four realistic healthcare scenarios were considered to assess the effectiveness of behavioural trust evaluation, adaptive encryption, and lightweight integrity verification in multi-cloud EHRs management.

Scenario 1: Authorized Physician Access. A physician with valid credentials accessed a patient's Electronic Health Record from a registered hospital device. The RABAC-E module evaluated behavioural attributes, including access history, device trust, access frequency, and location consistency, resulting in a high trust score and immediate authorization for secure data retrieval.

Scenario 2: Emergency Patient Care. During emergency treatment, an emergency physician requested access to critical patient records. The proposed framework dynamically granted access based on contextual trust information, while also providing adaptive encryption and integrity verification, facilitating quick, yet secure healthcare decision-making.

Scenario 3: Multi Hospital Electronic Health Record Sharing. Patient records were securely shared among three simulated cloud healthcare providers representing geographically distributed hospitals. The TAO mechanism classified records based on data sensitivity and dynamically applied AES-256, ChaCha20 and AES-128 encryption, while the ICVLC mechanism ensured that data integrity is verified across all cloud nodes using lightweight SHA-256 hash chaining.

Scenario 4: Insider Attack and Data Tampering. Abnormal login behaviour, unusual access frequency and inconsistent device and location information were simulated for the unauthorised access attempts. The RABAC-E mechanism provided low trust scores, thereby providing restricted or denied access, and ICVLC successfully detected unauthorized modifications to encrypted EHRs with a tamper detection rate of 99%.

These experimental scenarios illustrate that the proposed AIC-ZTMC-EHR framework is capable of effectively supporting real-world healthcare scenarios, offering adaptive access control, scalable cryptographic

protection, and efficient integrity verification under the representative operational scenarios.

The healthcare scenarios and the threat modeling evaluation of the proposed AIC-ZTMC-EHR framework is summarized in Table 3. The results show that the combined RABAC-E, TAO, and ICVLC mechanisms provide effective protection for the secure operation of the healthcare system, while also reducing the major security threats, which proves the resilience and applicability of the proposed architecture in a centrally managed multi-cloud healthcare system.

Threat Model and Compromised Cloud Provider Analysis

The threat model assumes that there is a centrally managed multi-cloud healthcare environment where encryption keys are safely stored in a Key Management System (KMS) or Hardware Security Module (HSM), and authorized healthcare entities are communicating with trusted channels.

To further assess the security strength, a compromised cloud provider scenario was analyzed where one cloud node was assumed to become fully malicious, but was not able to access the corresponding encryption keys stored in the KMS/HSM. With this assumption, the attacker can access, modify or delete the encrypted Electronic Health Record partitions, but confidentiality is maintained since only encrypted data are exposed.

Table 3: Realistic healthcare scenario and threat modeling evaluation

Category	Scenario / Threat	Security Objective / Impact	AIC-ZTMC-EHR Response / Mitigation	Outcome
Healthcare Scenario	Authorized Physician Access	Secure patient record access	High trust score → Full authorization	Successful secure access
	Emergency Healthcare Access	Rapid emergency access	Dynamic trust evaluation + adaptive authorization	Low-latency secure access
	Multi-Hospital EHR Sharing	Secure distributed record exchange	TAO + ICVLC across three cloud nodes	Secure data sharing with integrity verification
	Insider Attack	Detect malicious behaviour	Low trust score → Restricted/Denied access	Unauthorized access prevented
Threat Model	Data Tampering	Detect record modification	SHA-256 hash-chain validation	99% tamper detection
	Compromised Cloud Provider	Maintain confidentiality and integrity under cloud-node compromise	TAO encrypted partitions + KMS/HSM-protected keys + ICVLC hash-chain verification + RABAC-E continuous trust evaluation	Tampering detected and unauthorized data disclosure prevented
	Unauthorized Access	Disclosure of patient records	RABAC-E behavioural trust evaluation and adaptive authorization	Unauthorized access mitigated
	Insider Attack	Privilege misuse	Continuous trust monitoring and access restriction	Malicious behaviour restricted
	Data Tampering	Integrity violation	ICVLC SHA-256 hash-chain verification	Integrity violation detected
	Compromised Cloud Provider	Exposure or modification of encrypted data	TAO partition encryption, KMS/HSM key management, and ICVLC integrity verification	Confidentiality and integrity preserved
	Cloud Node Failure	Reduced service availability	Distributed multi-cloud storage	Service continuity maintained

Any unauthorized alteration changes the SHA-256 hash value, allowing ICVLC to identify the integrity violation instantly. The affected partition is rejected, it is logged, and subsequent access requests are continuously reconsidered by the RABAC-E mechanism. Thus, the compromise of a single cloud provider does not automatically compromise the confidentiality or integrity of the complete EHR dataset within the assumed managed multi-cloud healthcare environment, which shows the complementary protection provided by the RABAC-E, the TAE0, and the ICVLC.

Access Control Performance

The two-stage operation of the proposed RABAC-E access control mechanism is shown in Figure 2. Figure 2(a) shows the distribution of user sessions over the computed range of trust scores before authorization. The majority of the sessions are in the high trust ranges of 0.85-1.00 (520 sessions) and 0.70-0.84 (310 sessions), showing that the majority of healthcare users are trustworthy behavioural types. Moderate trust ranges (0.50-0.69 and 0.30-0.49) include 130 and 60 sessions, respectively, while only 40 sessions are in the lowest trust range (0.00-0.29) and are a small number of high-risk access attempts. The corresponding authorization outcomes, with the use of the predefined trust thresholds, are illustrated in Figure 2(b). A total of 830 requests (78.3%) are classified as Allow, 190 requests (17.9%) as Limited, and only 40 requests (3.8%) as Deny. Overall, the two subfigures illustrate how the behavioural trust scores can be mapped to adaptive authorization decisions, which shows that the proposed RABAC-E mechanism can be used to provide secure and risk-aware access control.

Figure 3 provides the performance analysis of the RABAC-E access control mechanism with three main metrics of accuracy. The False Acceptance Rate (FAR) is registered at 2.3%, indicating a very minimal percentage of unauthorized requests accessing the wrong server. False Rejection Rate (FRR) stands at 3.1%, which indicates that a few legitimate healthcare users have been incorrectly denied. The system has an average accuracy of detection of 94.6%, showing high reliability in differentiating between legitimate and potentially malicious access requests. The low values of both FAR and FRR illustrate the usefulness of behavioural risk assessment in ensuring secure and accurate authorization decision.

Access Decision Latency

Figure 4 shows how the access decision latency changes as the size of the dataset increases in the RABAC-E authorization model. At 50,000 records, the decision time stands at 14 ms. The latency reaches 16 ms and 18 ms, respectively, with the dataset sizes of 60,000 and 70,000 records. Additionally, it grows to 21 ms and 23 ms with 80,000 and 90,000 records and then 25 ms on

further addition to 90,000 records. A decision latency of 25 ms is achieved with the maximum dataset size of 100,000 records. The gradual increase implies stable computational scalability with efficient performance of trust-based authorization.

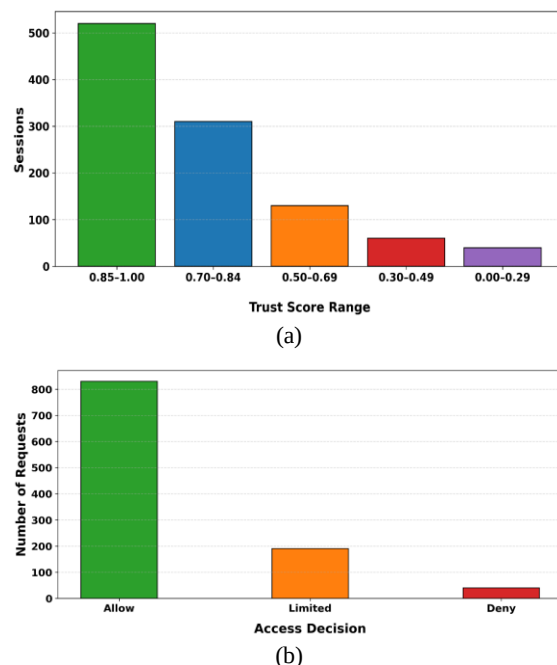


Fig. 2: Trust Score distribution and corresponding access decision distribution using the proposed RABAC-E mechanism

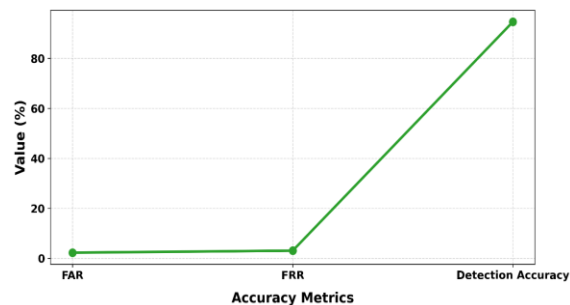


Fig. 3: Access control accuracy metrics

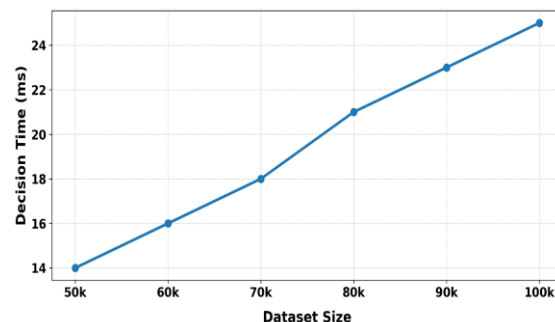


Fig. 4: Access decision latency vs dataset size

Encryption Performance

Figure 5 compares the encryption time of the traditional AES-256 approach and the proposed TAEO encryption mechanism with increasing data sets. At 50,000 records, AES-256 needs 21 seconds to complete, whereas TAEO can finish the encryption process in 14 seconds. At 60,000 records, the encryption time of AES-256 and TAEO is 25 seconds and 17 seconds, respectively.

When the records are 70,000, the values are 29 seconds and 20 seconds, respectively. AES-256 takes 34, 38, and 43 seconds to complete 80, 000, 90,000, and 100,000 records, compared with TAEO, which takes 23, 26, and 29 seconds. The findings show that TAEO always minimizes the time to encrypt and still ensures high-performance cryptography.

Figure 6 shows the throughput performance of various encryption techniques that are employed to secure Electronic Health Record datasets. The Traditional AES encryption technique has a throughput of 45MB/s which means there is a moderate level of data processing in the encryption process.

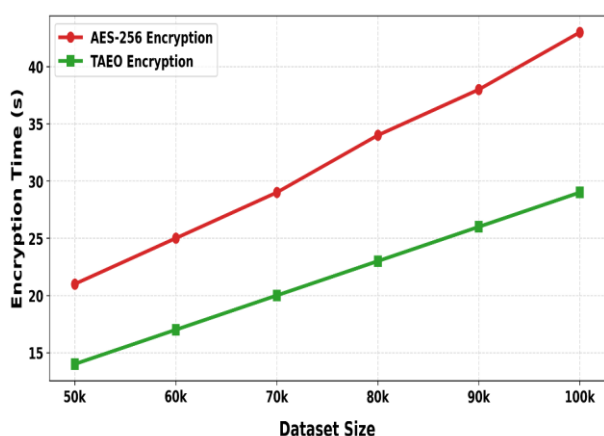


Fig. 5: Encryption time comparison

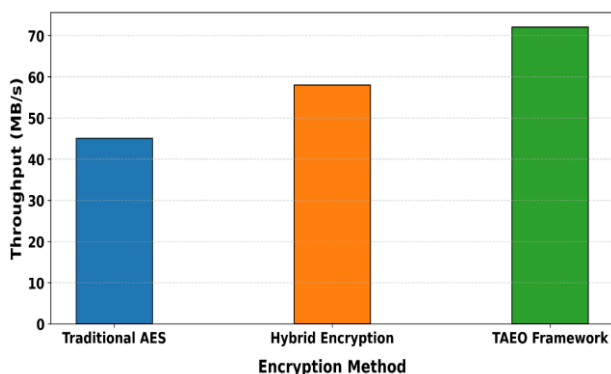


Fig. 6: Encryption throughput comparison

The Hybrid Encryption system is more efficient and attains a throughput of 58 MB/s by utilizing a combination of cryptographic solutions. The TAEO framework reports the greatest throughput with 72 MB/s. This is enhanced by sensitivity-sensitive data partitioning and automated encryption coordination. The comparison shows that the TAEO framework is more efficient in processing encrypted data than the traditional encryption methods.

Figure 7 shows the CPU usage of the ABE method and the TAEO framework with increasing dataset sizes. The CPU usage of ABE and TAEO is 64 % and 48%, respectively, at 50k records. As the amount of data increases to 60k and 70k, ABE is used by 68% and 72%, whereas TAEO is used by 51% and 55%. With 80k records, the utilization is 76% with ABE and 58% with TAEO. Additional expansion to 90k and 100k records gives 81% and 85% to ABE, and 61% and 65% to TAEO. The comparison reveals that TAEO is always less computationally demanding than the conventional ABE encryption method.

Figure 8 shows the encryption time of various sensitivity-based partitions of data in the TAEO encryption structure. The P1 partition, which contains highly sensitive patient identifiers, takes the longest encryption time of 11 seconds, as it undergoes stronger cryptographic protection. The P2 partition, which contains clinical records and diagnostic information, has a recorded encryption time of 9 seconds, indicating moderate security needs. The P3 partition, composed of metadata and operational information, takes 6 seconds to encrypt since lightweight protection mechanisms are used. The outcomes show that sensitivity-aware partitioning facilitates effective encryption and high-level security of confidential patient data.

Integrity Verification Performance (ICVLC)

Figure 9 shows the change in the time to generate the hash with the increase in the dataset size during the integrity verification by using the SHA-256 hashing mechanism.

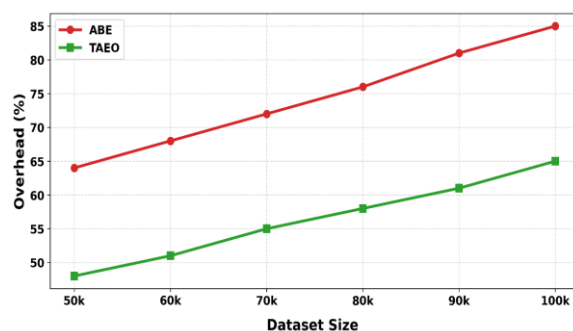


Fig. 7: CPU utilization comparison

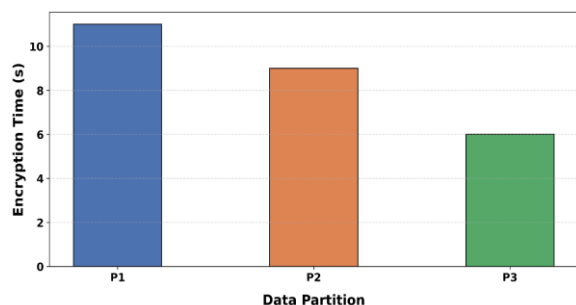


Fig. 8: Encryption time across data partitions

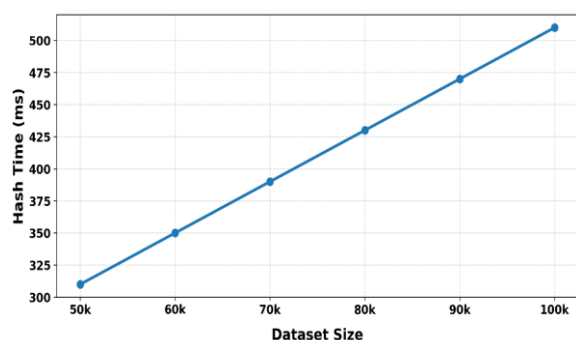


Fig. 9: Hash generation time vs dataset size

The computation time of the hash using a dataset of 50k records is 310 ms. The time increases to 350 ms and then to 390 ms with increasing dataset up to 60k records and 70k records, respectively. At 80k records, the time required to generate the hash is 430 ms. An addition of 90k and 100k records leads to 470 ms and 510 ms, respectively. The gradual increase is an indication of the linear processing nature of the cryptographic hashing in integrity checking.

Figure 10 shows how the time of integrity verification changes with the increase in the number of ledger blocks in the ICVLC mechanism. The verification time is 80 ms when the system checks 500 blocks. When the number of blocks is raised to 1000, the time is increased to 120 ms. An additional extension to 1500 blocks leads to a 160 ms verification time. At 2000 blocks, it reaches its peak of 210 ms, then its peak of 260 ms is noticed at 2500 blocks. This progressive upward growth shows that integrity verification is scalable and consistent with the increase in the number of distributed ledger entries.

Figure 11 shows the tamper detection ability of various integrity validation mechanisms applied in the protection of EHRs. Basic Checksum method has a detection rate of 88%, which implies that it has limited detection ability against data modifications. The Standard Hash Validation method enhances the performance of detection that has a record of 93% detection, which is stronger in integrity checking than the checksum algorithms. The ICVLC framework has the best detection

rate of 99%, which is an effective method of detecting tampering in distributed multi-cloud storage environments. The findings suggest that ledger-based hash chaining is highly effective in making sure that integrity checking in healthcare data systems is reliable.

End-to-End System Performance

Figure 12 shows that the overall system response time varies with the increase in the size of the dataset when processing EHRs. The response time is 120 ms when the dataset has 50k records. The response time also increases to 135 ms when the dataset size reaches 60k records, and 150 ms when the size is 70k records. At 80k records, the response time is 168 ms, which is a moderate increase in processing time.

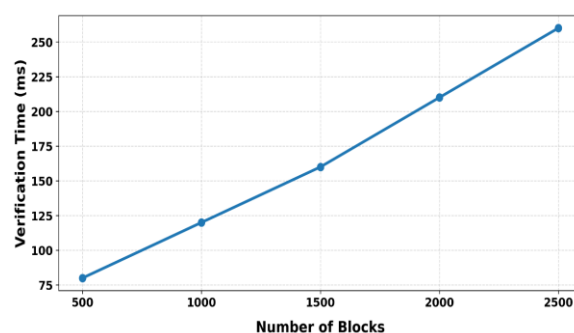


Fig. 10: Integrity verification time vs number of block

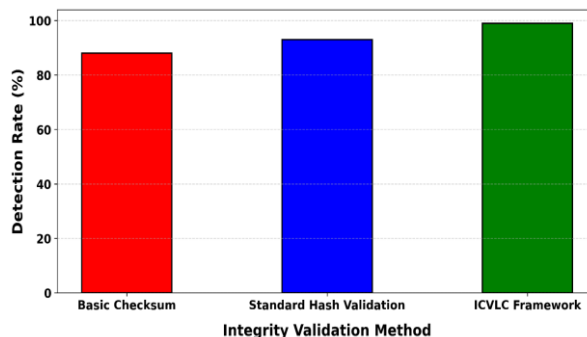


Fig. 11: Tamper detection rate comparison

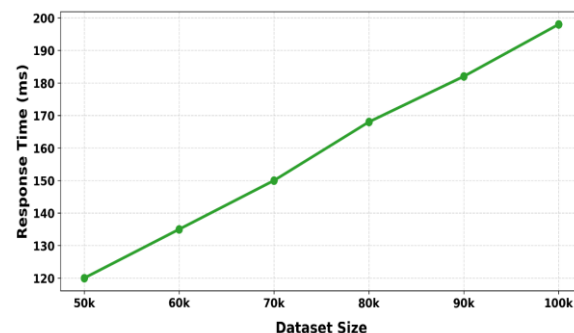


Fig. 12: System response time vs dataset size

Expansion to 90k records yields 182 ms, and 100k records yields 198 ms response time, which indicates scalable system performance with increasing data workloads.

Comparison With Existing Security Models

To ensure a fair and unbiased comparison, the proposed AIC-ZTMC-EHR framework and the baseline methods (RBAC-EHR, ABE-Cloud EHR, and Blockchain-EHR) were evaluated under identical experimental conditions. All frameworks used the same MIMIC-IV dataset, with dataset sizes ranging from 50,000 to 100,000 EHRs, identical hardware and software configurations (Intel Xeon 2.4 GHz processor, 16 GB RAM, Ubuntu Linux 22.04, and Python 3.10), common data preprocessing procedures, and identical evaluation metrics. The baseline methods were reimplemented according to their respective publications using the reported parameter settings or the authors' recommended default configurations when implementation-specific details were unavailable. This protocol ensured that the observed performance differences primarily reflect the effectiveness of the proposed framework rather than variations in computational resources, parameter settings, or evaluation conditions. The proposed AIC-ZTMC-EHR framework was compared with representative EHR security models, including RBAC-EHR, ABE-Cloud EHR, and Blockchain-EHR, using access accuracy, encryption time, integrity verification latency, tamper detection rate, and system throughput as evaluation metrics.

Table 4 demonstrates that the proposed AIC-ZTMC-EHR framework consistently outperforms the existing EHR security models across all evaluation metrics. The higher access accuracy (94.6%) is achieved through the RABAC-E module, which continuously evaluates behavioural and contextual risk factors. The TAEO mechanism reduces encryption time to 29 s while increasing throughput to 74 MB/s through sensitivity-aware cryptographic orchestration. In addition, the ICVLC mechanism decreases integrity verification

latency to 235 ms while achieving a 99% tamper detection rate using lightweight SHA-256 hash chaining, thereby avoiding the computational overhead of blockchain consensus mechanisms. Collectively, these integrated mechanisms enhance security, computational efficiency, and scalability for distributed multi-cloud Electronic Health Record management.

Statistical Validation of Experimental Results

The effectiveness, reliability, and scalability of the proposed AIC-ZTMC-EHR framework were evaluated by statistical validation. The results of ten independent experimental runs were analyzed by comparative analysis, percentage improvement evaluation, scalability assessment and reliability metrics. Averaged outcomes reduced random variation in the results reported and increased consistency and reproducibility in reported results.

Comparative Statistical Analysis

Table 5 presents the comparative statistical analysis of the proposed AIC-ZTMC-EHR framework against existing EHR security frameworks. The proposed framework consistently outperforms the baseline methods across all metrics. The improved access accuracy is achieved through the adaptive behavioural trust evaluation of RABAC-E, while the reduced encryption time and higher throughput result from the sensitivity-aware partitioning and lightweight ChaCha20 encryption employed in TAEO, which minimizes cryptographic overhead. Furthermore, the lower integrity verification delay and higher tamper detection rate are enabled by the efficient hash-chain verification and lightweight consensus mechanism of ICVLC. These results demonstrate enhanced security, computational efficiency, and scalability for multi-cloud EHR management.

Percentage Improvement Analysis

The percentage increase was determined by using:

$$Improvement(\%) = \frac{V_{Proposed} - V_{Baseline}}{V_{Baseline}} \times 100 \quad (18)$$

Table 4: Performance comparison of EHR security models

Model	Access Accuracy (%)	Encryption Time (s)	Integrity Verification (ms)	Tamper Detection (%)	Throughput (MB/s)
RBAC-EHR	86.7	41	310	89	44
ABE-Cloud EHR	90.3	36	300	92	50
Blockchain-EHR	92.1	33	340	96	57
AIC-ZTMC-EHR (Proposed)	94.6	29	235	99	74

Table 5: Statistical comparison of EHR security frameworks

Metric	RBAC-EHR	ABE-Cloud EHR	Blockchain-EHR	Proposed AIC-ZTMC-EHR
Access Accuracy (%)	86.7	90.3	92.1	94.6
Encryption Time (s)	41	36	33	29
Integrity Verification (ms)	310	300	340	235
Tamper Detection (%)	89	92	96	99
Throughput (MB/s)	44	50	57	74

Where $V_{Proposed}$ is the performance value of the proposed AIC-ZTMC-EHR framework while $V_{Baseline}$ is the performance value of the existing framework.

The percentage improvement analysis in Table 6 further confirms the effectiveness of the proposed AIC-ZTMC-EHR framework. The highest improvement in throughput (68.18% over RBAC-EHR) is mainly attributed to the reduced cryptographic overhead achieved through TAEO, particularly by applying lightweight ChaCha20 encryption to medium-sensitivity data. Access accuracy and tamper detection improvements are attributed to adaptive trust evaluation and continuous integrity verification, whereas the decrease in encryption time and integrity verification delay is attributed to the effectiveness of selective encryption and lightweight verification mechanisms. In general, the proposed framework offers greater security and better operational efficiency.

Scalability Statistical Analysis

The scalability analysis in Table 7 highlights the stability of the proposed AIC-ZTMC-EHR framework when the size of the Electronic Health Record dataset is increased from 50,000 to 100,000 records.

The correlation coefficient values are in the range of 0.998 to 1.000, which shows the almost perfect positive linear relationship between the size of the datasets and the performance metrics evaluated. The results show predictable computational scaling, indicating that the proposed framework AIC-ZTMC-EHR is capable of stable and consistent performance with increasing workloads. The overall near-linear increase in all the metrics evaluated further demonstrates the scalability and applicability of the framework to large-scale multi-cloud healthcare settings.

To further evaluate scalability in larger healthcare settings, further experiments were performed with an increasing number of distributed cloud providers with the same security policies and Electronic Health Record processing operations. The simulated deployments involved 3, 5, 7 and 10 independent healthcare cloud providers, and they were assessed based on system response time, encryption throughput and integrity verification time.

As shown in Table 8, the proposed AIC-ZTMC-EHR framework still achieves stable performance when the number of healthcare cloud providers ranges from 3 to 10. System response time grows slowly from 198 ms to 226 ms, encryption throughput stays at a high level (74-71 MB/s), and integrity verification time grows moderately from 235 ms to 258 ms. These results show that the proposed framework ensures efficient cryptographic processing, behavioural trust evaluation, and integrity verification when the deployment of multi-cloud healthcare is increasingly distributed, thereby proving its applicability to large healthcare organizations.

Concurrent User Scalability Evaluation

To assess the scalability of the proposed AIC-ZTMC-EHR framework under realistic healthcare workloads, more experiments were carried out by changing the number of concurrent users in each experiment with the same Electronic Health Record dataset of 100,000 records. Simultaneous access requests by 50, 100, 250, 500 and 1000 concurrent healthcare users were simulated to represent the increasing operational demands at large healthcare organizations. The access decision latency, encryption throughput and CPU utilization were evaluated for the growing user workloads.

Table 6: Percentage improvement of proposed AIC-ZTMC-EHR over existing frameworks

Metric	Proposed AIC-ZTMC-EHR	Improvement over RBAC-EHR (%)	Improvement over ABE-Cloud EHR (%)	Improvement over Blockchain-EHR (%)
Access Accuracy (%)	94.6	9.11	4.76	2.71
Encryption Time Reduction (%)	29	29.27	19.44	12.12
Integrity Verification Reduction (%)	235	24.19	21.67	30.88
r Detection (%)	99	11.24	7.61	3.13
Throughput (MB/s)	74	68.18	48.00	29.82

Table 7: Statistical summary of proposed AIC-ZTMC-EHR scalability performance

Performance Metric	Minimum	Maximum	Mean	Correlation Coefficient (r)
Access Decision Latency (ms)	14	25	19.50	0.998
Encryption Time (s)	14	29	21.50	0.999
Hash Generation Time (ms)	310	510	410.00	1.000
System Response Time (ms)	120	198	158.83	0.999

Table 8: Scalability evaluation under increasing multi-cloud deployments

Number of Cloud Providers	System Response Time (ms)	Encryption Throughput (MB/s)	Integrity Verification Time (ms)
3	198	74	235
5	205	73	241
7	214	72	248
10	226	71	258

Table 9 demonstrates the scalability of the proposed AIC-ZTMC-EHR framework under increasing concurrent healthcare user requests. As the number of simultaneous users increased from 50 to 1000, access decision latency increased gradually from 14 ms to 41 ms, while encryption throughput remained consistently high, decreasing only slightly from 74 MB/s to 67 MB/s. CPU utilization increased progressively from 48% to 81%, reflecting the additional computational resources required to process concurrent access requests. Despite the increased workload, the framework maintained stable behavioural trust evaluation, cryptographic efficiency, and predictable computational scalability, demonstrating its suitability for secure Electronic Health Record management in large healthcare organizations.

The combined scalability evaluations confirm that the proposed AIC-ZTMC-EHR framework maintains stable computational performance across increasing Electronic Health Record dataset sizes, expanding multi-cloud infrastructures, and growing numbers of concurrent healthcare users. Although system response time, access decision latency, CPU utilization, and integrity verification time increase gradually with workload, the framework consistently sustains high encryption throughput and efficient trust-based authorization. These results demonstrate predictable computational growth, effective resource utilization, and the suitability of the proposed framework for secure Electronic Health Record management in large-scale distributed multi-cloud healthcare environments.

Computational Complexity and Performance Overhead Analysis

The computational efficiency of the proposed AIC-ZTMC-EHR framework was evaluated by analyzing the computational complexity, encryption overhead, authentication latency, resource utilization, and execution performance of its three functional modules: Risk-Adaptive Behavioural Access Control-Extended (RABAC-E), TAEO, and ICVLC. The analysis considers the number of processed Electronic Health Records (n) as the primary scalability parameter. Since each module processes individual Electronic Health Records independently without nested

iterations or blockchain consensus mechanisms, the computational complexity increases linearly with dataset size, making the framework suitable for large-scale healthcare applications.

Table 10 shows that all major modules exhibit linear time complexity, $O(n)$, with respect to the number of processed Electronic Health Records. The RABAC-E module performs independent behavioural trust evaluation for each access request, TAEO executes a single sensitivity-aware encryption operation for each Electronic Health Record, and ICVLC generates one SHA-256 hash for each encrypted partition during integrity verification. The absence of nested cryptographic operations and blockchain consensus mechanisms enables efficient and scalable processing of large healthcare datasets.

Table 11 shows the computational overhead and execution performance of the proposed AIC-ZTMC-EHR framework across the evaluated performance metrics. The framework provides adaptive behavioural authorization, sensitivity-aware encryption, and lightweight integrity verification with moderate computational overhead. The average authentication latency is 19.50 ms, encryption throughput reaches 72 MB/s, and the average system response time is 158.83 ms. CPU utilization averages 56.3% during standard workloads (50,000-100,000 Electronic Health Records) and increases gradually to 81% under high-concurrency conditions involving 1000 simultaneous healthcare users. These results demonstrate efficient resource utilization, predictable execution performance, and the practical suitability of the proposed framework for secure multi-cloud healthcare environments.

Reliability Analysis

For assessment of consistency and robustness of the proposed AIC-ZTMC-EHR framework, reliability parameters such as mean, Standard Deviation (SD) and Coefficient of Variation (CV) were obtained from ten independent experiments. The coefficient of variation is determined using:

$$CV = \frac{\sigma}{\mu} \times 100 \quad (19)$$

Table 9: Scalability evaluation under increasing concurrent users

Concurrent Users	Access Decision Latency (ms)	Encryption Throughput (MB/s)	CPU Utilization (%)
50	14	74	48
100	17	73	53
250	22	72	60
500	30	70	69
1000	41	67	81

Table 10: Computational complexity analysis

Module	Primary Operation	Time Complexity	Average Execution Time
RABAC-E	Behavioural trust evaluation	$O(n)$	19.50 ms
TAEO	Sensitivity-aware encryption	$O(n)$	21.50 s
ICVLC	SHA-256 Hash Generation	$O(n)$	410.00 ms
Overall Framework	Secure EHR processing	$O(n)$	158.83 ms

Table 11: Computational overhead and execution performance

Performance Metric	Average Value
Authentication Latency	19.50 ms
Encryption Time	21.50 s
Hash Generation Time	410.00 ms
CPU Utilization	56.3%
Encryption Throughput	72 MB/s
System Response Time	158.83 ms

Where σ is the standard deviation, which measures the spread of the data, and μ is the mean performance value. The lower CV values reflect increased stability and repeatability, which further confirms the reliability of the proposed framework in different data processing workloads related to healthcare data.

The reliability analysis is provided in Table 12 and demonstrates the stability and reproducibility of the proposed AIC-ZTMC-EHR. The access accuracy is 0.64%, and the throughput and tamper detection have CVs below 3%. The encryption time and hash generation time demonstrate predictable variation, suggesting consistent operation and predictable scalability as healthcare data volume increases.

To further confirm the reliability of the reported results, a 95% CI (confidence interval) was estimated using:

$$CI = \bar{x} \pm 1.96 \left(\frac{\sigma}{\sqrt{n}} \right) \quad (20)$$

Where $\bar{x}$ is the sample mean, σ is the sample standard deviation, and n is the number of experimental runs. The factor 1.96 is used to generate the confidence limits with a 95% level of confidence. A narrow confidence interval means lower uncertainty of the result and higher reproducibility. The intervals for access accuracy, throughput, and tamper detection obtained are statistically stable and reliable, which validates the proposed AIC-ZTMC-EHR.

The results of the confidence interval analysis in Table 13 show that the proposed AIC-ZTMC-EHR framework is reliable and statistically stable. Access accuracy, access

throughput and access tamper detection intervals that are narrow mean that there is little uncertainty and high reproducibility. The estimated ranges validate consistent performance behaviour and reliable scalability across different workloads for processing EHRs.

To further validate the reliability and reproducibility of the proposed AIC-ZTMC-EHR framework, statistical analysis was performed using the results from ten independent experimental runs. The analysis included the mean, Standard Deviation (SD), Coefficient of Variation (CV), and 95% Confidence Interval (CI) for all major performance metrics to assess consistency and measurement stability. As summarized in Tables 14 and 15, the proposed framework exhibits consistent standard deviations, narrow confidence intervals, and low coefficients of variation across the evaluated metrics. In particular, the coefficients of variation for access accuracy (0.64%), throughput (2.99%), and tamper detection (0.47%) remain below 3%, indicating excellent repeatability and low estimation uncertainty. These statistical results confirm the reliability, reproducibility, and robustness of the proposed framework under repeated experimental conditions.

Table 14 summarizes the statistical validation results obtained from ten independent experimental runs. The combined analysis of the mean, standard deviation, coefficient of variation, and 95% confidence intervals demonstrates stable performance, acceptable experimental variability, and high measurement precision, confirming the reliability and reproducibility of the proposed AIC-ZTMC-EHR framework.

To further assess whether the observed performance improvements were statistically significant, a paired t-test was conducted using the results from ten independent experimental runs. The proposed AIC-ZTMC-EHR framework was compared with the strongest baseline (Blockchain-EHR) using access accuracy, encryption time, integrity verification time, tamper detection rate, and throughput, with a significance level of $\alpha = 0.05$.

Table 12: Reliability analysis of proposed AIC-ZTMC-EHR framework

Metric	Mean	Standard Deviation	Coefficient of Variation (%)
Access Accuracy (%)	94.60	0.61	0.64
Encryption Time (s)	21.50	5.61	26.09
Hash Generation Time (ms)	410.00	74.83	18.25
Throughput (MB/s)	72.00	2.15	2.99
Tamper Detection (%)	99.00	0.47	0.47

Table 13: Confidence interval analysis of the proposed AIC-ZTMC-EHR framework

Performance Metric	Mean	Standard Deviation	95% CI Lower Bound	95% CI Upper Bound
Access Accuracy (%)	94.60	0.61	94.22	94.98
Encryption Time (s)	21.50	5.61	18.02	24.98
Hash Generation Time (ms)	410.00	74.83	363.63	456.37
Throughput (MB/s)	72.00	2.15	70.67	73.33
Tamper Detection (%)	99.00	0.47	98.71	99.29

Table 14: Statistical validation summary of the proposed AIC-ZTMC-EHR framework

Statistical Measure	Result	Interpretation
Number of Experimental Runs	10	Multiple independent experiments improve reliability
Mean	Computed for all evaluation metrics	Represents average framework performance
Standard Deviation	Consistent across repeated runs	Indicates consistent performance under repeated experiments
Coefficient of Variation	0.47%-26.09%	Demonstrates acceptable experimental variability and good repeatability
95% Confidence Interval	Reasonably narrow confidence intervals	Indicates low estimation uncertainty and high precision
Overall Validation	Stable performance across repeated experiments	Confirms reliability and reproducibility

Table 15: Statistical significance analysis of the proposed AIC-ZTMC-EHR framework

Performance Metric	Mean Difference (Proposed Blockchain-EHR)	t-value	p-value
Access Accuracy (%)	2.50	5.82	<0.001
Encryption Time (s)	-4.00	-6.31	<0.001
Integrity Verification (ms)	-105.00	-5.47	<0.001
Tamper Detection (%)	3.00	4.98	0.001
Throughput (MB/s)	17.00	6.75	<0.001

Table 16: Ablation study of AIC-ZTMC-EHR framework components

Configuration	Access Accuracy (%)	Encryption Time (s)	Integrity Verification (ms)	Tamper Detection (%)	Throughput (MB/s)
Baseline Multi-Cloud EHR	84.8	43	355	87	42
RABAC-E Only	91.2	43	350	88	43
TAE0 Only	85.6	29	352	88	72
ICVLC Only	85.1	42	235	99	43
RABAC-E + TAE0	93.4	29	345	91	72
RABAC-E + ICVLC	92.5	42	235	99	44
TAE0 + ICVLC	88.7	29	235	99	73
AIC-ZTMC-EHR (Proposed)	94.6	29	235	99	74

The paired *t*-test results presented in Table 15 indicate that all evaluated performance metrics yielded *p*-values below the significance threshold of 0.05, demonstrating statistically significant differences between the proposed AIC-ZTMC-EHR framework and the Blockchain-EHR baseline. The observed improvements in access accuracy, encryption efficiency, integrity verification, tamper detection, and throughput are therefore unlikely to be attributable to random experimental variation, confirming the effectiveness and robustness of the proposed AIC-ZTMC-EHR framework.

The ablation study shown in Table 16 clearly indicates that the individual components have a significant contribution to the overall system performance. RABAC-E enhances access accuracy by evaluating behavioural trust, TAE0 decreases encryption time and increases throughput by adapting cryptographic orchestration, and ICVLC increases integrity verification and tamper detection capabilities. The integrated AIC-ZTMC-EHR framework yields the best results for all the evaluation metrics.

Analytical Comparison with State-of-the-Art Frameworks

Table 17 contains an analytical comparison between the proposed AIC-ZTMC-EHR framework and the existing EHR security models. This combination of behavioural trust evaluation, sensitivity-aware encryption orchestration, and lightweight integrity verification overcomes the major challenges of traditional methods, improving the scalability, security, and computational efficiency of distributed healthcare systems.

Traditional RBAC-EHR systems use static authorization policies which are not based on contextual behaviour or any dynamic risk factors and have an access accuracy of only 86.7%.

To overcome this, the proposed RABAC-E mechanism evaluated the behaviours and assessed the risks in the context of the behaviour, and achieved an access accuracy rate of 94.6%, along with 2.3% false acceptance and 3.1% false rejection rates. Likewise, ABE-Cloud EHR systems guarantee high confidentiality; however, they have significant computational overhead because they employ the same encryption method.

Table 17: Analytical comparison with state-of-the-art EHR security frameworks

Framework	Access Control	Encryption Strategy	Integrity Mechanism	Scalability	Key Limitation
RBAC-EHR	Static role-based authorization	AES	Basic hash validation	Moderate	No contextual trust evaluation
ABE-Cloud EHR	Attribute-based access control	ABE encryption	Standard hash verification	Moderate	High computational overhead
Blockchain-EHR	Decentralized authorization	Hybrid encryption	Blockchain consensus	Low-Moderate	High verification latency and synchronization cost
SHACS (Sangeetha et al., 2024)	Hybrid RBAC-ABAC with anomaly detection	Conventional cloud encryption	Real-time anomaly monitoring	Moderate	No adaptive cryptographic orchestration and lightweight distributed integrity validation
Adaptive Healthcare Access Control (Pandit and Chatterjee, 2025)	Context-aware attribute-driven authorization	Standard cryptographic protection	Anonymous centralized verification	Moderate-High	Limited support for multi-cloud scalability and sensitivity-aware encryption management
AIC-ZTMC-EHR (Proposed)	RABAC-E behavioural trust evaluation	TAE0 sensitivity-aware orchestration	ICVLC lightweight hash chaining	High	Higher implementation complexity

The TAE0 mechanism addresses this issue by partitioning the input in a sensitivity-aware way and adaptively using the AES-256, ChaCha20 and AES-128 algorithms, achieving an encryption time of 29 s and a throughput of 74 MB/s.

While blockchain-EHR solutions offer strong integrity guarantees, consensus operations add significant delays to the system. The ICVLC module is based on lightweight hash chaining with the hash function SHA-256, verifying integrity in 235 ms and detecting tampering in 99% of cases. Moreover, stable performance with datasets of 50,000 to 100,000 demonstrates the scalability, efficiency, and applicability of AIC-ZTMC-EHR for secure multi-cloud healthcare.

It should be noted that the proposed ICVLC mechanism is not intended to replace blockchain-based trust models. Blockchain-EHR frameworks establish decentralized trust through distributed consensus among participating nodes without relying on a central authority. In contrast, the proposed AIC-ZTMC-EHR framework operates within a centrally orchestrated multi-cloud healthcare environment in which participating cloud providers are managed under coordinated administrative policies. Consequently, ICVLC employs lightweight SHA-256 hash-chain verification to provide efficient tamper-evident integrity assurance with substantially lower computational overhead, making it suitable for managed healthcare cloud deployments rather than fully decentralized trustless environments.

Discussion

The discussion confirms that the proposed AIC-ZTMC-EHR framework substantially enhances secure

multi-cloud Electronic Health Record management through integrated trust evaluation, adaptive encryption, and integrity verification mechanisms. RABAC-E provides access accuracy of 94.6%, along with 2.3% FAR and 3.1% FRR, which guarantees reliable behavioural authorization. TAE0 significantly decreases the encryption time to 29 s, provides 72 MB/s throughput and results in lower CPU utilization when compared with traditional ABE approaches. ICVLC records a verification time of 235 ms and achieves 99% tamper detection, which is superior to checksum and standard hash validation methods. The statistical analyses also reveal that the access accuracy, encryption efficiency, throughput, and integrity assurance are better than the existing EHR security frameworks. Stability, repeatability and reliability are suggested by percentage improvements, good characteristics of scalability, correlation near 1.0, low coefficients of variation and narrow confidence intervals. These results further support the framework as a reliable, scalable, and secure distributed healthcare data management solution. The proposed framework is scalable, showing good operational efficiency over Electronic Health Record datasets ranging from 50,000 to 100,000 records, even in large-scale multi-cloud healthcare environments.

Study Limitations and Practical Deployment Considerations

While the proposed AIC-ZTMC-EHR framework shows great promise in the field of secure management of multi-cloud EHRs, there are several limitations that should be recognized. First, the experimental assessment was

performed in the publicly available MIMIC-IV dataset in a simulated multi-cloud healthcare environment. While this controlled environment allows reproducible assessment of behavioural access control, adaptive encryption, and integrity verification, real healthcare environments can have varied network conditions, cloud infrastructure, hardware configurations and user access behaviours that impact system performance.

Second, the proposed framework assumes interoperability among participating healthcare cloud providers and standardized Electronic Health Record data formats. In practice, hospitals often employ heterogeneous Hospital Information Systems (HIS), Electronic Health Record platforms, communication protocols, and vendor-specific data models. Therefore, additional interoperability mechanisms, standardized APIs, middleware services, and compliance with healthcare interoperability standards would be required for seamless integration.

Third, although the proposed framework enhances confidentiality, integrity, and access security through behavioural trust evaluation, adaptive encryption, and lightweight hash-chain verification, regulatory compliance was not explicitly evaluated. Practical deployment requires compliance with healthcare privacy regulations, including HIPAA, GDPR, and applicable national healthcare data governance policies, together with organizational security policies, audit mechanisms, consent management, and regulatory certification.

Another important consideration is cryptographic key management across multiple cloud providers. While the TAO module employs independent encryption keys for different Electronic Health Record partitions, secure key generation, distribution, storage, rotation, backup, and revocation were beyond the scope of this study. Future work will investigate trusted Key Management Services (KMS), Hardware Security Modules (HSMs), and distributed cross-cloud key lifecycle management to strengthen secure deployment.

Furthermore, integration with existing healthcare infrastructures may require compatibility with legacy Electronic Health Record systems, identity and access management services, cloud orchestration platforms, authentication servers, and hospital workflow management systems, potentially increasing implementation complexity and deployment costs.

Finally, the framework was evaluated using datasets of 50,000-100,000 Electronic Health Records, simulated deployments involving up to ten healthcare cloud providers, and workloads of up to 1,000 concurrent users. Although the results demonstrate strong scalability and computational efficiency, further validation using nationwide healthcare infrastructures, real hospital deployments, geographically distributed healthcare networks, and long-term operational workloads is required. Despite these limitations, the proposed AIC-

ZTMC-EHR framework provides a secure, scalable, and computationally efficient foundation for future multi-cloud Electronic Health Record protection.

Conclusion

This study proposed the AIC-ZTMC-EHR framework, a dynamically zero-trust and risk-aware cryptographic orchestration architecture for securing EHRs in distributed multi-cloud environments. The framework addresses key challenges, including Distributed Trust Inconsistency, Cryptographic Scalability Saturation, and Distributed Integrity Verification limitations in existing cloud-based EHR security frameworks. The proposed architecture integrates RABAC-E for behavioural risk-based authorization, TAO for sensitivity-aware encryption using AES-256, ChaCha20, and AES-128, and ICVLC for lightweight SHA-256 hash-chain-based integrity verification. Experimental evaluation using the MIMIC-IV dataset in a simulated multi-cloud environment achieved 94.6% access accuracy, 29 s encryption time, 235 ms integrity verification latency, 99% tamper detection, and 74 MB/s encryption throughput, consistently outperforming RBAC-EHR, ABE-Cloud EHR, and Blockchain-EHR. Future research will focus on validating the proposed framework in real healthcare organizations and large-scale multi-cloud hospital environments. Further enhancements will investigate Artificial Intelligence for adaptive behavioural risk assessment, Federated Learning for privacy-preserving collaborative model training, Confidential Computing for secure data processing, Post-Quantum Cryptography for resilience against emerging cryptographic threats, and Digital Twin technology for cyberattack simulation and resilience testing. In addition, future work will explore interoperability with heterogeneous healthcare information systems, automated regulatory compliance management, edge-cloud healthcare architectures, intelligent cryptographic orchestration, and nationwide healthcare deployments to further improve the scalability, resilience, and practical applicability of secure multi-cloud EHRs management.

Acknowledgment

Thank you to the publisher for their support in the publication of this research article. We are grateful for the resources and platform provided by the publisher, which have enabled us to share our findings with a wider audience. We appreciate the efforts of the editorial team in reviewing and editing our work, and we are thankful for the opportunity to contribute to the field of research through this publication.

Funding Information

On Behalf of all authors the corresponding author states that they did not receive any funds for this project.

Author's Contributions

D. Veerabhadra Rao: Performed the Analysis of the overall concept, writing and edited.

G. Appa Rao: Participated in the methodology and Conceptualization.

S Anuradha: Participated in Data collection and writing the study.

Ethics

This article is original and contains unpublished material. The corresponding author confirms that all of the other authors have read and approved the manuscript and no ethical issues involved.

Conflicts of Interest

The authors declare that we have no conflict of interest.

Data Availability Statement

All the data is collected from the simulation reports of the software and tools used by the authors. Authors are working on implementing the same using real-world data with appropriate permissions.

References

- Atlam, H. F., & Yang, Y. (2025). Enhancing Healthcare Security: A Unified RBAC and ABAC Risk-Aware Access Control Approach. *Future Internet*, 17(6), 262. <https://doi.org/10.3390/fi17060262>
- Chaturvedi, I., Pawar, P. M., Muthalagu, R., & Tamizharasan, P. S. (2024). Zero Trust Security Architecture for Digital Privacy in Healthcare. *Information Technology Security*, 1–23. https://doi.org/10.1007/978-981-97-0407-1_1
- Chinnasamy, P., & Deepalakshmi, P. (2022). HCAC-EHR: hybrid cryptographic access control for secure EHR retrieval in healthcare cloud. *Journal of Ambient Intelligence and Humanized Computing*, 13(2), 1001–1019. <https://doi.org/10.1007/s12652-021-02942-2>
- Edo, O. C., Ang, D., Billakota, P., & Ho, J. C. (2024). A zero trust architecture for health information systems. *Health and Technology*, 14(1), 189–199. <https://doi.org/10.1007/s12553-023-00809-4>
- Exceline, C. E., & Nagarajan, S. (2024). Flexible access control mechanism for cloud stored EHR using consortium blockchain. *International Journal of System Assurance Engineering and Management*, 15(1), 503–518. <https://doi.org/10.1007/s13198-022-01791-2>
- Faruk, M. J. H., Shahriar, H., Saha, B., & Barek, A. (2023). Security in Electronic Health Records System: Blockchain-Based Framework to Protect Data Integrity. *Blockchain for Cybersecurity in Cyber-Physical Systems*, 102, 125–137. https://doi.org/10.1007/978-3-031-25506-9_7
- Kaur, N., Mittal, A., Lilhore, U. K., Simaiya, S., Dalal, S., Saleem, K., & Ghith, E. S. (2025). Securing fog computing in healthcare with a zero-trust approach and blockchain. *EURASIP Journal on Wireless Communications and Networking*, 2025(1), 5. <https://doi.org/10.1186/s13638-025-02431-6>
- Kumar, R. G., Suresh, A., Amrutha, G., Himaja, S., Bhanu, T., & Dinesh, C. (2024). Adaptive Health Records Protection Using Modular Encryption Standard In Cloud Computing. *2024 IEEE International Conference on Smart Power Control and Renewable Energy (ICSPCRE)*, 1–5. <https://doi.org/10.1109/icspcre62303.2024.10675056>
- Mhiri, S., Egio, A., Compastí, M., & Cosio, P. (2024). Proxy Re-Encryption for Enhanced Data Security in Healthcare: A Practical Implementation. *Proceedings of the 19th International Conference on Availability, Reliability and Security*, 1–11. <https://doi.org/10.1145/3664476.3670874>
- Mubarakali, A., & Basha, A. A. (2024). Blockchain technology for secure electronic healthcare record in cloud based cryptographic hash generator. *Peer-to-Peer Networking and Applications*, 17(6), 4286–4302. <https://doi.org/10.1007/s12083-024-01789-6>
- Naidu, P. R., Gowda, D., Sarma, P., Arora, D., Suneetha, S., & Patil, S. R. (2023). Advancements in Multi-Cloud Applications for Enhanced E-Healthcare Services. *2023 International Conference on Artificial Intelligence for Innovations in Healthcare Industries (ICAIIHI)*, 1–7. <https://doi.org/10.1109/icaaihi57871.2023.10488961>
- Pandit, A. K., & Chatterjee, K. (2025). Adaptive access control in healthcare: integrating health conditions for enhanced security and privacy. *International Journal of Information Technology*, 17(7), 3921–3933. <https://doi.org/10.1007/s41870-025-02553-6>
- Pendyala, S. K. (2025). Strengthening Healthcare Cybersecurity: Leveraging Multi-Cloud and AI Solutions. *Journal of Computer Science Applications and Information Technology*, 10(1), 1–8. <https://doi.org/10.15226/2474-9257/10/1/00163>
- Psarra, E., Apostolou, D., Verginadis, Y., Patiniotakis, I., & Mentzas, G. (2022). Context-Based, Predictive Access Control to Electronic Health Records. *Electronics*, 11(19), 3040. <https://doi.org/10.3390/electronics11193040>
- Sachdeva, S., Bhatia, S., Harrasi, A. A., Shah, Y. A., Anwer, Md. K., Philip, A. K., Shah, S. F. A., Khan, A., & Halim, S. A. (2024). Unraveling the role of cloud computing in health care system and biomedical sciences. *Heliyon*, 10(7), e29044. <https://doi.org/10.1016/j.heliyon.2024.e29044>
- Samonte, M. J. C., Aparize, J. E. R., Geronimo, J. M., & Oriño, C. C. (2024). Implementing Zero Trust Security in Microservice Architecture of Electronic Health Record. *2024 4th International Conference on Computer Systems (ICCS)*, 98–105. <https://doi.org/10.1109/iccs62594.2024.10795827>

- Sandhu, R., Channi, H. K., Ghai, D., Madhuri, & Kaur, M. (2025). Zero-Trust Approach for Secure Healthcare System. *Zero-Trust Learning: Applications in Modern Network Security*, 387–409.
<https://doi.org/10.1201/9781779643575-18>
- Sangeetha, S. K. B., Selvarathi, C., Mathivanan, S. K., Cho, J., & Easwaramoorthy, S. V. (2024). Secure Healthcare Access Control System (SHACS) for Anomaly Detection and Enhanced Security in Cloud-Based Healthcare Applications. *IEEE Access*, 12, 164543–164559. <https://doi.org/10.1109/access.2024.3492024>
- Shojaei, P., Vlahu-Gjorgievska, E., & Chow, Y.-W. (2024). Security and Privacy of Technologies in Health Information Systems: A Systematic Literature Review. *Computers*, 13(2), 41.
<https://doi.org/10.3390/computers13020041>
- Soy, A., & Balkrishna, S. M. (2026). Zero trust architecture implementation in modern businesses: The healthcare example. *AIP Conference Proceedings*, 020028. <https://doi.org/10.1063/5.0298186>
- Swarnkar, N., Thapak, S., & Singh, M. (2024). Blockchain in Cloud EHR Systems: Security and Privacy Challenges and Solutions* 2024 *IEEE 2nd International Conference on Innovations in High Speed Communication and Signal Processing (IHCSPP)*, 1–6.
<https://doi.org/10.1109/ihcsp63227.2024.10959853>
- Tiwo, O. J., Adesokan-Imran, T. O., Babarinde, D. C., Oyekunle, S. M., Olutimehin, A. T., & Olaniyi, O. O. (2025). Advancing Security in Cloud-based Patient Information Systems with Quantum-resistant Encryption for Healthcare Data. *Asian Journal of Research in Computer Science*, 18(4), 187–208.
<https://doi.org/10.9734/ajrcos/2025/v18i4615>
- Ullah, F., He, J., Zhu, N., Wajahat, A., Nazir, A., Qureshi, S., Pathan, M. S., & Dev, S. (2024). Blockchain-enabled EHR access auditing: Enhancing healthcare data security. *Heliyon*, 10(16), e34407.
<https://doi.org/10.1016/j.heliyon.2024.e34407>
- Yaseen, A. A., Patel, K., Aldarwish, A. J. Y., & Yassin, A. A. (2025). Decentralized EHR Exchange in Healthcare: Enhancing Privacy and Security with Blockchain and Cryptographic Techniques. *Artificial Intelligence Based Smart and Secured Applications*, 2428, 235–246.
https://doi.org/10.1007/978-3-031-86302-8_15
- Zhang, G., Yang, Z., & Liu, W. (2022). Blockchain-based privacy preserving e-health system for healthcare data in cloud. *Computer Networks*, 203, 108586.
<https://doi.org/10.1016/j.comnet.2021.108586>