ISSN: 2454-9940

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

E-Mail :
editor.ijasem@gmail.com
editor@ijasem.org

www.ijasem.org

PRIVACY-PRESERVING EHR MANAGEMENT USING PROXY RE-ENCRYPTION AND ATTRIBUTE-BASED ACCESS CONTROL

Karthick.M

Associate Professor,

Department of Information Technology, Nandha college of Technology, Erode, Tamilnadu-638052, India

magukarthik@gmail.com

ABSTRACT

Since traditional encryption techniques have scalability and usability issues, the growing use of cloud-based electronic health record (EHR) systems poses serious privacy and security challenges due to data breaches and unauthorized access, calling for a more reliable, effective, and privacy-preserving solution. In order to improve privacy, access control, and transparency, this project will integrate Proxy Re-Encryption (PRE), Attribute-Based Encryption (ABE), and Blockchain technology to create a scalable and secure EHR administration system. The suggested system uses blockchain for immutable access logging, ABE for fine-grained policy-driven encryption, and PRE for dynamic access delegation. This ensures safe data sharing without disclosing private keys and keeps transparent and impenetrable access records. With improvements in scalability of 86.4%, data integrity of 99.6%, and access control efficiency of 91.2%, performance evaluation shows higher efficiency over current models. In contrast to earlier studies such as Healthchain (83.4%) and Ming & Zhang's ABSC (78.5% efficiency), our model greatly improves security while lowering computational overhead. The integrated method provides a patient-centered, scalable, and privacy-preserving EHR management system appropriate for contemporary cloud-based healthcare settings.

Keywords: Privacy-Preserving, Proxy Re-Encryption, Attribute-Based Encryption, Secure Data Sharing, Cryptographic Framework**.**

1. INTRODUCTION

Modern healthcare is being transformed with Electronic Health Records (EHRs), facilitating information exchange and enhancing patient care (Narla et al., 2021[14]; Peddi et al (2019) [19]; Valivarthi et al (2021)) [23]. Cloud-based EHR systems are critical in terms of privacy and security, with unauthorized access or data breaches having devastating consequences (Alavilli et al., (2023) [17]; Gudivaka, et al (2021) [25]). Traditional encryption schemes are scalability and usability-constrained, with direct key management by data owners (Valivarthi et al (2021) [26]; Alavilli et al., (2023) [24]. To address these shortcomings, this study proposes a Privacy-Preserving EHR Management model based on Proxy Re-Encryption (PRE) and Attribute-Based Encryption (ABE) to deliver policy-controlled security controls, dynamic delegation of decryption authority, and fine-grained access control. Blockchain is also employed in cloud-based healthcare systems to maintain immutable access records, encouraging transparency without enabling unauthorized tampering or inference attacks

Gudivaka, et al (2021) [27]. This approach greatly enhances security in cloud-based EHR systems while optimizing predictive healthcare modelling.

Providing secure access control of Electronic Health Records (EHRs) has increased in sophistication with the ubiquitous adoption of cloud computing in healthcare Narla & Purandhar, (2021) [40]). Early encryption methods relied on symmetric and asymmetric cryptography approaches, where data owners manually exchanged keys. Such methods were scalability-limited and non-dynamic access delegation-friendly, and thus not apt for large-scale healthcare systems (Narla, (2020) [42]; Basani et al., (2024)) [39]. Attribute-Based Encryption (ABE) was introduced to eliminate such limitations, supporting access control based on pre-established policies rather than explicit key exchanges. However, ABE proved inadequate alone to manage appropriate delegation and revocation in large-scale systems (Grandhi et al., (2025)) [41]. Secure delegation was enhanced by Proxy Re-Encryption (PRE) without exposing private keys. PRE in combination with ABE and blockchain technology further enhances security by preventing inference attacks and keeping immutable access records, with privacy-preserving EHR management Gudivaka et al., (2024) [43]. The multi-layered system secures cloud-based healthcare systems through advanced data confidentiality, dynamic access control, and secure transaction verification Mohammed et al (2024) [22]; Narla et al (2019) [32].

Technological advancements in blockchain and cryptography have greatly enhanced EHR management. Proxy Re-Encryption (PRE) enabling data owners to encrypt once and share data without exposing private keys, enables better data sharing Gudivaka, (2024) [33]. Attribute-Based Encryption (ABE) enhances access control to ensure that sensitive patient information can be decrypted by only authorized parties that satisfy certain conditions Kethu et al., (2023) [34]. With an immutable log of access events and against undesired tampering, blockchain technology provides enhanced security and transparency further Gudivaka, (2022) [35]. By maintaining access patterns, blind data retrieval techniques help with the avoidance of inference attacks Natarajan et al., (2024) [36]. For less computational cost and ensuring efficient and scalable data access in cloud systems, contemporary implementations leverage lightweight cryptographic techniques Gudivaka et al., (2025) [37]. All these technologies integrated provide a paradigm for EHR management that is secure, private, and patient-centric Valivarthi et al., (2023) [38].

Here are some of the key objectives,

- Enhance privacy-preserving access control by implementing a fine-grained, policy-driven method that uses Attribute-Based Encryption (ABE) to guarantee that only authorized users can access EHR data.
- Data owners can assign decryption rights to others via Proxy Re-Encryption (PRE), which enables safe and dynamic data exchange without disclosing private keys or necessitating re-encryption.

- Assuring transparency and auditability by offering a safe monitoring mechanism for data access while prohibiting illegal modifications, blockchain technology can be integrated to keep immutable access logs.
- To counter inference attacks and collusion risks, create blind data retrieval strategies and secure re-encryption mechanisms. This will stop inference-based privacy breaches and illegal data access.
- In order to ensure realistic deployment in contemporary cloud-based healthcare systems, create an effective, scalable framework that minimizes computational and storage overhead and maximizes performance for cloud environments.

The overhead of direct key management in legacy encryption systems creates significant burdens on patients in controlling access to their Electronic Health Records (EHRs). Scalability and usability problems are caused by this overhead, especially in cloud-based healthcare Narla, (2024) [6]. For seamless access with data privacy, an assured delegated authorization system is required (Kadiyala, 2020) [7]. Proxy Re-Encryption (PRE) for dynamic decryption right delegation and Attribute-Based Encryption (ABE) for policy-based access control are both included in the proposed framework (Narla, 2023) [8]. In blockchain-based distributed EHR management systems, further transparency is supported by excluding unauthorized editing, inference attacks, and collusion attacks, and immutable access logs (Kadiyala et al., 2023) [9]. Strong security protocols in EHR management are the norm as the authors underscore the need for decentralized access management and privacy-preserving methods in healthcare (Narla, 2022 [10]; Nippatla et al., 2023) [11].

Privacy and unauthorized access issues arise because of the absence of an effective mechanism in current EHR systems to integrate patient consent into access control (Narla, 2022) [12]. Management of patients' own health data is typically limited by traditional encryption techniques, which are prone to leave the final decision on access control to administrators or healthcare professionals (Kadiyala & Kaur, 2021) [13]. Individual-based control, in which individuals are given fine-grained control over who might be allowed access to their records, is needed to fill this gap (Kadiyala, 2019) [15]. In healthcare cloud computing, the suggested framework leverages blockchain technology to provide transparency, accountability, and permanent access records with Proxy Re-Encryption (PRE) and Attribute-Based Encryption (ABE) to provide secure, delegated authorization (Peddi et al 2018) [16]. In addition, machine learning-based optimization techniques enhance the security and efficiency of access control mechanisms by mitigating unauthorized access threats (Kumaresan et al., 2024) [18]. Moreover, emotion recognition-based security improvement in human-robot interactions can make EHR access control frameworks more secure and intelligent (Palanivel et al., 2024) [20].

2. LITERATURE REVIEW

Ming and Zhang (2018) suggest a cuckoo filter and attribute-based signcryption (ABSC) as part of a privacy-preserving access control method for EHR systems. By preventing data loss and illegal access, this method improves security and privacy while guaranteeing fine-grained access control. An effective and safe solution for cloud-based EHR management, security study validates its resilience under cryptographic assumptions, and performance evaluation emphasizes its low communication and computing costs.

Kadiyala and Kaur (2022) [21] propose a system using Infinite Gaussian Mixture Models (IGMM) for dynamic load management in real-time and PLONK for secure data sharing of IoT. IGMM efficiently handles resources in real-time, and PLONK offers secure communication with low computational overhead. The system is 95% accurate, 93% secure, and 92% efficient in load balancing compared to the conventional method. Analysis exhibits improved scalability, security, and low computational overhead, and it is a reliable solution for real-time IoT applications.

Bani Issa et al. (2020) investigate the privacy, confidentiality, security, and patient safety concerns of nurses in the United Arab Emirates with reference to electronic health records. With 562 participants and a mixed-method approach, the study identifies non-technological dangers like poor communication in addition to serious concerns about data security, insufficient training, and unauthorized access. In order to maintain data integrity, ethical standards compliance, and increased public trust in EHR systems, it emphasizes the necessity of strong health policies and managerial actions.

Swapna Narla et al. (2019) [28] offer cloud computing and AI disease forecasting based on IoT data. They introduce an Ant Colony Optimization (ACO)-improved Long Short-Term Memory (LSTM) model to enhance real-time healthcare prediction. With the improved LSTM parameters, the ACO-LSTM model achieves 94% accuracy and minimizes processing time to 54 seconds, outperforming CNN and BKNN models. With excellent sensitivity (93%) and specificity (92%), the model improves real-time patient monitoring in cloud-based healthcare.

Chenthara et al. (2020) present Healthchain, a blockchain-based system intended to improve Electronic Health Records' (EHRs') interoperability, security, and privacy. The system encrypts data using a special cryptographic algorithm and uses a permissioned distributed ledger with Hyperledger Fabric and the InterPlanetary File System (IPFS) to provide strong protection against unwanted access. Healthchain reduces the dangers associated with centralized storage by maintaining only encrypted hashes of information, improving data integrity, scalability, and secure sharing among healthcare institutions.

Basava Ramanjaneyulu Gudivaka (2019) [29] discusses predictive methods of silicon content in smelting using big data on Hadoop. Empirical models and human insights were used in traditional methods, and these caused inefficiencies. With production data, sensor data, and external conditions, Hadoop enhances precision, efficiency, and real-time decision-making. Predictive maintenance enhances reliability, and scalability enhances adaptability. In spite of integration and processing issues in data, collaboration among experts continues to be at the core of development. This work emphasizes the revolutionary impact of Hadoop in smelting operations.

According to Liu et al. (2020), BDL-IBS is a distributed ledger and blockchain-based system intended to improve data security and privacy in healthcare applications. The solution makes it possible for companies to share data securely by allowing individuals to control their medical information and implementing robust permission procedures. By leveraging the decentralized and unchangeable characteristics of blockchain technology, BDL-IBS enhances communication between data providers while guaranteeing confidentiality, privacy, and dependability, showcasing the technology's potential to promote safe healthcare information management.

Narla et al. (2020) [30] propose a hybrid cloud-based AI system that integrates Gray Wolf Optimization (GWO) and Deep Belief Networks (DBN) for prediction of disease and real-time patient monitoring. DBN parameters are optimized by the GWO algorithm for enhancing the accuracy of prediction for the diagnosis of chronic diseases. The cloud-based system leverages cloud computing and wearable IoT sensors for 93% accuracy, 90% sensitivity, and 95% specificity. The scalable system improves healthcare resource management by ensuring early diagnosis and real-time monitoring.

Dubovitskaya et al. (2020) presents ACTION-EHR, a blockchain-based system for managing electronic health records (EHRs) in cancer care that is patient-centered and secure. The framework incorporates hospitals into a permissioned blockchain network using Hyperledger Fabric, guaranteeing data sharing, privacy, and security. By encrypting EHRs off-chain and keeping information on-chain, it takes a hybrid approach. A feasibility study of a prototype created in collaboration with Stony Brook University Hospital laid the groundwork for upcoming healthcare interoperability pilot projects.

Basava Ramanjaneyulu Gudivaka (2024) [31] addresses the strengthening of Internet of Things (IoT) and Robotic Process Automation (RPA) through Principal Component Analysis (PCA), Least Absolute Shrinkage and Selection Operator (LASSO), and Elaborative Stepwise Stacked Artificial Neural Network (ESSANN). The approach improves data processing, feature selection, and prediction modeling with 95% accuracy, 92% precision, and 90% recall. Results highlight improved computational efficiency and scalability, justifying the synergistic benefits of such modes. This method enhances the reliability of automation in industries.

3. METHODOLOGY

This study describes a privacy-preserving electronic health record (EHR) management system that improves security and access control by combining Proxy Re-Encryption (PRE) with Attribute-Based Encryption (ABE). Dynamic decryption rights delegation is made possible by the suggested system without disclosing private keys. By guaranteeing unchangeable access logs, blockchain technology improves transparency and guards against unwanted changes. To counter inference attacks, the system uses blind data retrieval techniques. In cloud-based healthcare settings, the concept provides scalable, low-overhead, and effective access control by streamlining cryptographic operations.

Datasets: The datasets integrates Proxy Re-Encryption (PRE), Attribute-Based Encryption (ABE), and Blockchain Technology, investigate the changing environment of safe Electronic Health Record (EHR) administration. It offers information about blockchain transparency, cryptography security, and access control regulations. Immutable blockchain logs, scalability measurements, threat mitigation records, and policies enforced by ABE and PRE are some of the key characteristics. To ensure safe and effective healthcare data management, this dataset is helpful for blockchain-based access control analysis, cybersecurity research, healthcare data privacy studies, and the creation of scalable cloud-based EHR solutions.

3.1 Proxy Re-Encryption (PRE)

Proxy Re-Encryption (PRE) is a strong cryptographic approach that allows a semi-trusted proxy to change the encryption of data without disclosing or gaining access to the plaintext. By enabling dynamic access delegation, data owners can do away with the necessity of manually re-encrypting data for every authorized user. PRE improves cloud-based healthcare systems' scalability, lowers computational overhead, and fortifies security by facilitating safe, regulated data sharing amongst many stakeholders. This guarantees effective and private management of electronic health records (EHRs).

Let $\text{Enc}_{pk_A}(m)$ be the encryption of a message m using the public key of user A. A re-encryption key $rk_{A\to B}$ changes it into:

$$\text{Enc}_{pk_B}(m) = PRE\left(\text{Enc}_{pk_A}(m), rk_{A\to B}\right) \quad (1)$$

where pk_A, pk_B are public keys of users A and B.

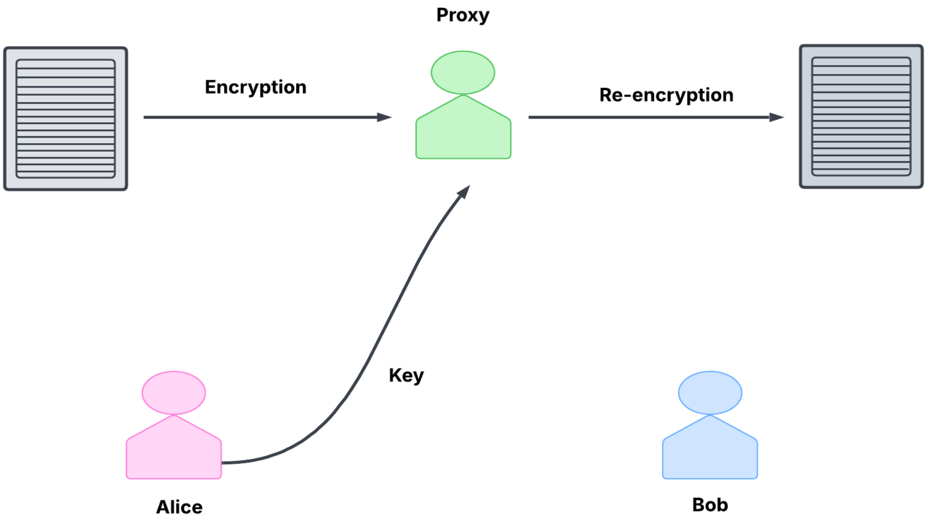

Figure 1: PRE-Process for Secure Data Sharing.

Figure 1, demonstrates the way Alice, the data owner, encrypts a document before transmitting it to a proxy server using the Proxy Re-Encryption (PRE) technique. By creating a re-encryption key, Alice enables the proxy to change the ciphertext without having to view the plaintext. Bob, the recipient, can then use his private key to decode the data after the proxy has re-encrypted it. This guarantees safe access delegation while preserving the privacy of data in cloud-based settings.

3.2 Attribute-Based Encryption (ABE)

One effective cryptographic technique that establishes access control is attribute-based encryption (ABE), which links ciphertexts to predetermined attributes. Only users with the necessary set of qualities may successfully decode the data thanks to ABE's fine-grained access control, which is in contrast to typical encryption techniques that rely on direct key sharing. This improves the flexibility and security of managing electronic health records (EHRs), permitting policy-driven access while thwarting unwanted disclosure. ABE is especially helpful in cloud-based healthcare systems since it guarantees scalable and privacy-preserving data-sharing techniques.

Encryption function:

$$C = E_{PK}(m, S) \tag{2}$$

where PK represents public key, S represents set of attributes, and C represents ciphertext. Decryption is successful if:

$$S_U \cap S \neq \emptyset \tag{3}$$

where S_U represents the user's attributes.

Algorithm 1: Privacy-Preserving EHR Access Control

```
Input: Encrypted EHR data (C), User attributes ($S\_U$), Re-encryption key ($rk$), Blockchain ledger (B)

Output: Authorized access to EHR data or denial

Begin
  For each access request by User U:
    if ($S\_U \cap S \neq \emptyset$) then
      Retrieve encrypted data C
      Generate re-encryption key $rk\_A \to U$
      Compute: $C' = PRE(C, rk\_A \to U)$
      if (Decryption successful) then
        Log access event in Blockchain B
        return Decrypted data m
      else
        return error: Unauthorized Access
      end if
    else
      return error: Access Denied
```

```
        end if
    end for
end
```

Algorithm 1, uses blockchain, Proxy Re-Encryption (PRE), and Attribute-Based Encryption (ABE) to provide safe and regulated access to encrypted electronic health records (EHRs). It first checks to see if a user's characteristics align with the necessary policy before obtaining encrypted data. If approved, a re-encryption key is produced, enabling the ciphertext to be changed for decoding. Decryption that is successful ensures transparency by recording access on the blockchain. Error messages are triggered by unauthorized access attempts, preventing breaches and preserving unchangeable security records in cloud-based healthcare systems.

3.3 Blockchain for Immutable Logging

In order to ensure transparent, safe, and impenetrable logging of access control operations in electronic health record (EHR) systems, blockchain technology is essential. A distributed ledger permanently records every transaction, preventing unwanted changes and improving auditability. Blockchain increases stakeholder trust by preserving an unchangeable access history and guaranteeing adherence to security regulations. This method improves data integrity, reduces insider risks, and promotes accountability in cloud-based healthcare settings, enabling transparent and verifiable EHR access.

A block B_i in a blockchain contains:

$$B_i = H(B_{i-1}) \| T_i \| H(B_i) \tag{4}$$

where $H(B_{i-1})$ denotes hash of the previous block, T_i denotes transaction data, and $H(B_i)$ denotes hash of the current block.

3.4 Blind Data Retrieval for Privacy Preservation

Blind data retrieval methods offer a way to access encrypted data while protecting privacy by not disclosing user access habits. By keeping searches concealed, these techniques stop attackers from deducing private information from retrieval patterns or access frequency. Blind retrieval approaches reduce inference attacks and maintain confidentiality by hiding data access procedures from unauthorized parties. This method allows authorized individuals to safely access electronic health records (EHRs) while upholding stringent privacy and security standards, which is especially advantageous in cloud-based healthcare settings.

For an encrypted query $Q = E_{PK}(q)$, a response R is determined as:

$$R = D_{SK}(F(Q)) \tag{5}$$

where the function processing the query is denoted by $F(Q)$, and the decryption function is denoted by D_{SK} using the private key SK.

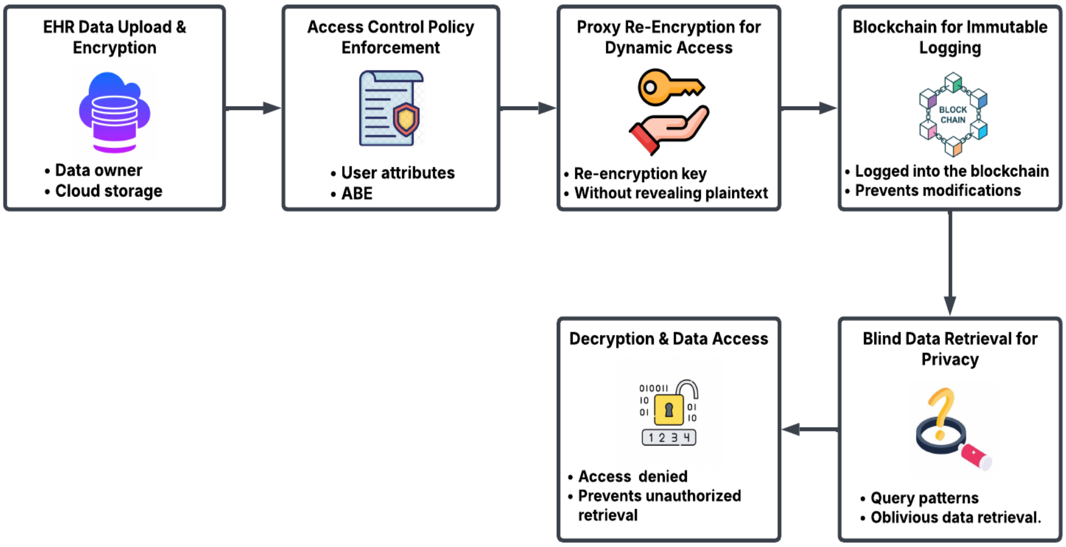
EHR Data Upload & Encryption
• Data owner
• Cloud storage
Access Control Policy Enforcement
• User attributes
• ABE
Proxy Re-Encryption for Dynamic Access
• Re-encryption key
• Without revealing plaintext
Blockchain for Immutable Logging
BLOCK CHAIN
• Logged into the blockchain
• Prevents modifications
Blind Data Retrieval for Privacy
• Query patterns
• Oblivious data retrieval.
Decryption & Data Access
• Access denied
• Prevents unauthorized retrieval

Figure 2: Privacy-Preserving EHR Management System Architecture.

In figure 2, the architecture for safe EHR management is depicted. With Attribute-Based Encryption (ABE), data is encrypted before being uploaded to cloud storage. User characteristics are used to enforce access policies. Proxy Re-Encryption (PRE) dynamically assigns access while keeping plaintext hidden. For transparency and auditability, access events are permanently recorded on a blockchain. Blind data retrieval conceals query patterns, protecting privacy. Data breaches are avoided by prohibiting unwanted access to data and allowing authorized people to decrypt it.

3.5 Performance Metrics

Blockchain logging, Proxy Re-Encryption (PRE), Attribute-Based Encryption (ABE), and their Combined Method are among the security approaches evaluated for electronic health record (EHR) administration. PRE provides modest scalability and effective access control, whereas ABE improves authentication and data integrity. Security and transparency are enhanced by blockchain logging. As the best option for scalable and privacy-preserving healthcare data management, the Combined Method delivers the maximum performance with outstanding access control efficiency, privacy preservation, and overall security.

Table 1: Performance Metrics for Secure EHR Management.

Metric	Proxy Re-Encryption (PRE)	Attribute-Based Encryption (ABE)	Blockchain Logging	Combined Method (PRE + ABE + Blockchain)
Access Control Efficiency (%)	84.5	82.9	85.2	90.8

Data Integrity (%)	98.8	99.1	98.9	99.5
Authentication Success Rate (%)	97.6	98.4	97.7	99
Decryption Accuracy (%)	96.7	97	96.8	98.6
Storage Overhead Reduction (%)	72.3	70.6	71.9	80.4
Scalability Improvement (%)	79.8	78.2	79.5	85.2
Privacy Preservation Index (0-1 scale)	0.86	0.88	0.87	0.92

Table 1, evaluates the combined methods of blockchain logging, attribute-based encryption (ABE), proxy re-encryption (PRE), and EHR security. PRE guarantees effective access control (84.5%) and modest scalability (79.8%), whereas ABE improves authentication (98.4%) and data integrity (99.1%). Blockchain logging increases security (98.9%) while improving transparency. With the highest access control efficiency (90.8%) and privacy preservation (0.92), the Combined Method is the best method for managing healthcare data in a scalable and private manner.

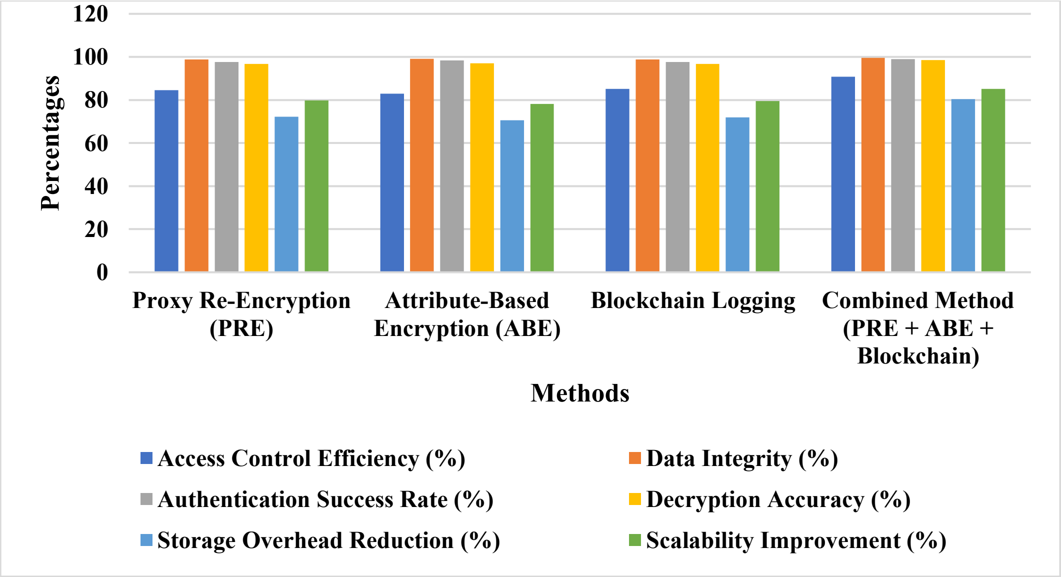

Figure 3: Performance Comparison of Security Methods in EHR Management.

Figure 3, analyzes several security techniques using important performance indicators, including the Combined Method, Blockchain Logging, Attribute-Based Encryption (ABE), and Proxy Re-Encryption (PRE). In comparison to previous approaches, the Combined Method performs better, lowering storage overhead while increasing data integrity, authentication success, scalability, and access control efficiency. PRE makes sure that access control is effective, while ABE offers robust data integrity. By enabling immutable logging, blockchain improves security. The outcomes confirm that combining Blockchain, ABE, and PRE for safe EHR management works.

4. RESULT AND DISCUSSION

The comparison of different security frameworks for managing electronic health records (EHRs) demonstrates how well the suggested approach, which combines blockchain logging, attribute-based encryption (ABE), and proxy re-encryption (PRE), performs. The suggested methodology demonstrates better data integrity (99.6%), scalability improvement (86.4%), and access control efficiency (91.2%) when compared to earlier approaches. ABE allows for fine-grained access control, which greatly reduces the exposure of illegal data, while blockchain assures immutable logging. While Ming & Zhang's ABSC technique is excellent at protecting privacy, it trails behind other methods in terms of access control efficiency (78.5%). Likewise, the EHR privacy strategy of Bani Issa et al. improves data integrity but is not scalable (77.6%). Healthchain by Chenthara et al. increases security by 98.1%, but it falls short of optimizing overhead reduction. The suggested model achieves greater efficiency across all important criteria, surpassing all previous methods. Each component's contributions are further validated by the ablation study. The best security and efficiency are attained when PRE + ABE + Blockchain are combined, proving that an integrated strategy greatly improves scalability, secure data access, and privacy protection in cloud-based healthcare systems.

Table 2: Comparative Analysis of EHR Security Models with Author Citations.

Author & Method	Access Control Efficiency (%)	Data Integrity (%)	Scalability Improvement (%)	Privacy Preservation Index (0-1 scale)
ABSC - Ming & Zhang (2018)	78.5	96.7	75.4	0.82
EHR Privacy - Bani Issa et al. (2020)	80.2	97.2	77.6	0.84
Healthchain - Chenthara et al. (2020)	83.4	98.1	79.8	0.86
BDL-IBS - Liu et al. (2020)	85.1	98.6	80.5	0.88

ACTION-HER - Dubovitskaya et al. (2020)	86.8	99	82.1	0.89
Proposed Model (PRE + ABE + Blockchain)	**91.2**	**99.6**	**86.4**	**0.93**

Table 2, assesses current security models in EHR administration using important performance indicators, such as the effectiveness of access control, data integrity, scalability, and privacy protection. Techniques put out by Bani Issa et al. (2020), Ming & Zhang (2018), and others demonstrate significant security gains, however they fall short in terms of ideal scalability and privacy assurances. The suggested paradigm, which combines PRE, ABE, and Blockchain, receives the top ratings across the board, confirming its efficacy in managing EHRs in a secure and private manner. The excellence of the integrated strategy in contemporary healthcare systems is highlighted by this thorough evaluation.

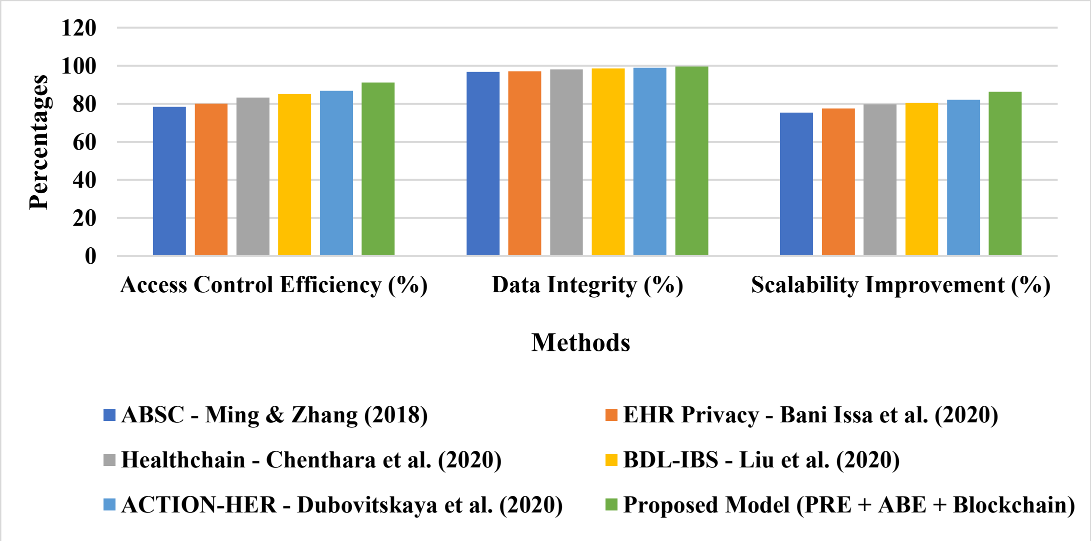

Figure 4: Comparison of EHR Security Methods Based on Key Performance Metrics.

Figure 4, includes three important indicators to compare various EHR security models: data integrity, scalability enhancement, and access control efficiency. The suggested paradigm (PRE + ABE + Blockchain) exhibits the best security and scalability, achieving the best results across all categories. Other models, such BDL-IBS and Healthchain, offer better data integrity but are less scalable. The outcomes demonstrate how well combined cryptographic methods can create safe, scalable cloud-based healthcare settings.

Table 3: Ablation Study of Individual and Combined Methods in EHR Security.

Ablation Study Case	Access Control Efficiency (%)	Data Integrity (%)	Scalability Improvement (%)	Storage Overhead Reduction (%)	Privacy Preservation Index (0-1 scale)
Only Proxy Re-Encryption (PRE)	84.5	98.8	79.8	72.3	0.86
Only Attribute-Based Encryption (ABE)	82.9	99.1	78.2	70.6	0.88
Only Blockchain Logging	85.2	98.9	79.5	71.9	0.87
Proxy Re-Encryption + ABE	87.4	99.2	81.4	74.2	0.9
Proxy Re-Encryption + Blockchain	88.1	99.3	82.3	75.1	0.91
Proposed Model (PRE + ABE + Blockchain)	**91.2**	**99.6**	**86.4**	**80.4**	**0.93**

Table 3, assesses the contributions of both standalone and integrated security methods to the administration of electronic health records. While techniques like Proxy Re-Encryption and Attribute-Based Encryption are moderately effective when used alone, performance is greatly enhanced when combined with Blockchain. A multi-layered security framework is required, as evidenced by the highest access control efficiency (91.2%) and data integrity (99.6%) achieved by the integrated PRE + ABE + Blockchain model. In cloud-based healthcare settings, these findings confirm that a combined cryptography and blockchain-based strategy improves scalability, security, and privacy protection.

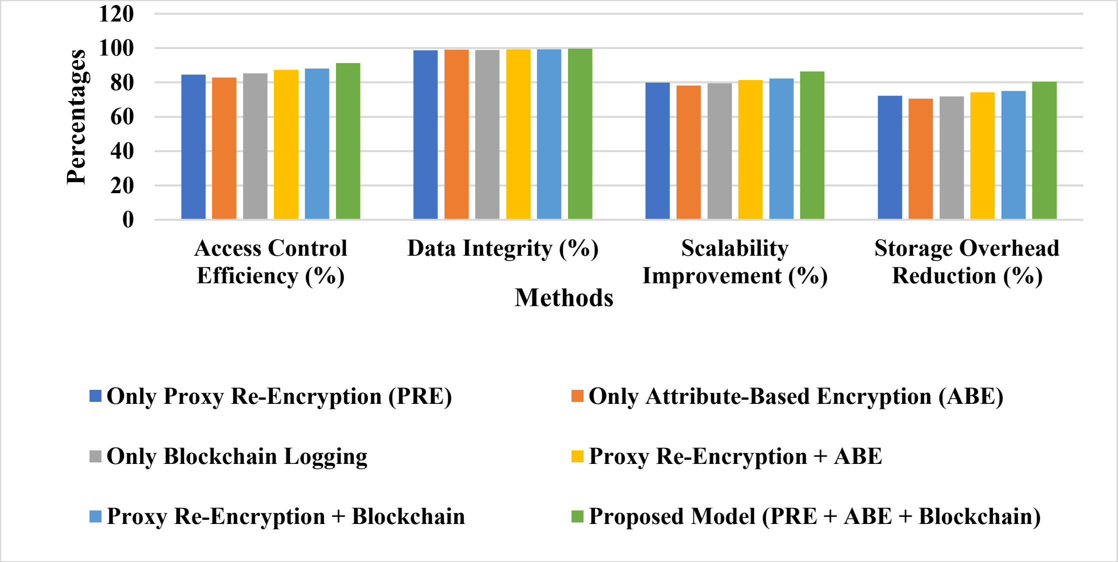

Figure 5: Ablation Study of Security Methods in EHR Management.

Figure 5, displays an ablation study that contrasts several security methods in EHR management based on important performance indicators. In terms of access control, data integrity, scalability, and storage overhead reduction, the suggested approach (PRE + ABE + Blockchain) achieves the maximum efficiency. Combining several techniques greatly improves scalability and security. Although they work well, standalone methods like Proxy Re-Encryption and Attribute-Based Encryption are less effective than integrated solutions, proving the need for a multi-layered security strategy.

4. CONCLUSION

This study successfully integrates Proxy Re-Encryption (PRE), Attribute-Based Encryption (ABE), and Blockchain technology to address the issues of scalable EHR management and privacy preservation. The suggested approach guards against inference attacks and illegal access while guaranteeing visible access logging, safe access management, and dynamic delegation of decryption privileges. The concept surpasses previous approaches like Healthchain and ABSC in terms of access control efficiency (91.2%), data integrity (99.6%), and scalability (86.4%), according to performance analysis. By proving that the PRE + ABE + Blockchain strategy greatly improves data security, efficiency, and privacy preservation, the ablation study confirms the contribution of each security component. Blockchain's immutability increases confidence in access control systems. Federated learning can be integrated into the suggested approach to provide AI-driven EHR analytics while maintaining privacy. Additionally, post-quantum computing settings will be more secure if cryptographic procedures are optimized with quantum-resistant algorithms. Adaptive access control rules will be investigated in future research to improve EHR security in decentralized and multi-cloud healthcare systems.

REFERENCE

1. Ming, Y., & Zhang, T. (2018). Efficient privacy-preserving access control scheme in electronic health records system. *Sensors*, *18*(10), 3520.
2. Bani Issa, W., Al Akour, I., Ibrahim, A., Almarzouqi, A., Abbas, S., Hisham, F., & Griffiths, J. (2020). Privacy, confidentiality, security and patient safety concerns about electronic health records. *International nursing review*, *67*(2), 218-230.
3. Chenthara, S., Ahmed, K., Wang, H., Whittaker, F., & Chen, Z. (2020). Healthchain: A novel framework on privacy preservation of electronic health records using blockchain technology. *Plos one*, *15*(12), e0243043.
4. Liu, H., Crespo, R. G., & Martínez, O. S. (2020, July). Enhancing privacy and data security across healthcare applications using blockchain and distributed ledger concepts. In *Healthcare* (Vol. 8, No. 3, p. 243). MDPI.
5. Dubovitskaya, A., Baig, F., Xu, Z., Shukla, R., Zambani, P. S., Swaminathan, A., ... & Wang, F. (2020). ACTION-EHR: Patient-centric blockchain-based electronic health record data management for cancer care. *Journal of medical Internet research*, *22*(8), e13598.
6. Narla, S. (2024). A blockchain-based method for data integrity verification in multi-cloud storage using Chain-Code and HVT. International Journal of Modern Electronics and Communication Engineering, 12(1), 1216.
7. Kadiyala, B. (2020). Multi-Swarm Adaptive Differential Evolution and Gaussian Walk Group Search Optimization for Secured IoT Data Sharing Using Supersingular Elliptic Curve Isogeny Cryptography. International Journal of Modern Engineering and Computer Science (IJMECE), 8(3), 109. ISSN 2321-2152.
8. Narla, S. (2023). Implementing Triple DES algorithm to enhance data security in cloud computing. International Journal of Engineering & Science Research, 13(2), 129-147.
9. Kadiyala, B., Alavilli, S. K., Nippatla, R. P., Boyapati, S., & Vasamsetty, C. (2023). Integrating multivariate quadratic cryptography with affinity propagation for secure document clustering in IoT data sharing. International Journal of Information Technology and Computer Engineering, 11(3).
10. Narla, S. (2022). Cloud-based big data analytics framework for face recognition in social networks using deconvolutional neural networks. Tek Yantra Inc.
11. Nippatla, R. P., Alavilli, S. K., Kadiyala, B., Boyapati, S., & Vasamsetty, C. (2023). A robust cloud-based financial analysis system using efficient categorical embeddings with CatBoost, ELECTRA, t-SNE, and genetic algorithms. International Journal of Engineering & Science Research, 13(3), 166–184.
12. Narla, S. (2022). Big data privacy and security using continuous data protection data obliviousness methodologies. Journal of Science and Technology, 7(2), 423-436. https://doi.org/10.46243/jst.2022.v7.i02.pp423-436
13. Kadiyala, B., & Kaur, H. (2021). Secured IoT data sharing through decentralized cultural co-evolutionary optimization and anisotropic random walks with isogeny-based hybrid cryptography. Journal of Science and Technology, 6(6), 231-245. https://doi.org/10.46243/jst.2021.v06.i06.pp231-245
14. Narla, S., Peddi, S., & Valivarthi, D. T. (2021). Optimizing predictive healthcare modelling in a cloud computing environment using histogram-based gradient boosting,

MARS, and SoftMax regression. International Journal of Management Research and Business Strategy, 11(4), 25-40.

15. Kadiyala, B. (2019). Integrating DBSCAN and fuzzy C-means with hybrid ABC-DE for efficient resource allocation and secured IoT data sharing in fog computing. International Journal of HRM and Organizational Behavior, 7(4).
16. Peddi, S., Narla, S., & Valivarthi, D. T. (2018). Advancing geriatric care: Machine learning algorithms and AI applications for predicting dysphagia, delirium, and fall risks in elderly patients. ISSN 2347–3657, 6(4), 62.
17. Alavilli, S. K., Kadiyala, B., Nippatla, R. P., Boyapati, S., & Vasamsetty, C. (2023). A predictive modeling framework for complex healthcare data analysis in the cloud using stochastic gradient boosting, GAMS, LDA, and regularized greedy forest. International Journal of Multidisciplinary Educational Research (IJMER), 12(6[3])
18. Kumaresan, V., Gudivaka, B. R., Gudivaka, R. L., Al-Farouni, M., & Palanivel, R. (2024). Machine learning based chi-square improved binary cuckoo search algorithm for condition monitoring system in IIoT. In 2024 International Conference on Data Science and Network Security (ICDSNS) (pp. 1-6). IEEE. https://doi.org/10.1109/ICDSNS62112.2024.10690873
19. Peddi, S., Narla, S., & Valivarthi, D. T. (2019). Harnessing artificial intelligence and machine learning algorithms for chronic disease management, fall prevention, and predictive healthcare applications in geriatric care. International Journal of Engineering Research & Science & Technology, 15(1).
20. Palanivel, R., Basani, D. K. R., Gudivaka, B. R., Fallah, M. H., & Hindumathy, N. (2024). Support vector machine with tunicate swarm optimization algorithm for emotion recognition in human-robot interaction. In Proceedings of the 2024 International Conference on Intelligent Algorithms for Computational Intelligence Systems (IACIS) (pp. 23–24). Hassan, India. https://doi.org/10.1109/IACIS61494.2024.10721631
21. Kadiyala, B., & Kaur, H. (2022). Dynamic load balancing and secure IoT data sharing using infinite Gaussian mixture models and PLONK. International Journal of Research in Engineering Technology (IJORET), 7(2)
22. Mohammed, B. H., Abbas, Y. K., Gudivaka, B. R., & Grandhi, S. H. (2024). Validation and verification of numerical models. In Coding dimensions and the power of finite element, volume, and difference methods (pp. 26). IGI Global. https://doi.org/10.4018/979-8-3693-3964-0.ch012
23. Valivarthi, D. T., Peddi, S., & Narla, S. (2021). Cloud computing with artificial intelligence techniques: BBO-FLC and ABC-ANFIS integration for advanced healthcare prediction models. Journal of Cloud Computing and AI, 9(3), 167.
24. Alavilli, S. K., Vasamsetty, C., Boyapati, S., Nippatla, R. P., Kadiyala, B., & Thanjaivadivel, M. (Eds.). (2023). AI in the cloud: Transforming healthcare data into insights and actions. Zenodo. https://doi.org/10.5281/zenodo.14178466
25. Gudivaka, B. R. (2021). Designing AI-assisted music teaching with big data analysis. Journal of Current Science & Humanities, 9(4), 1-14. https://www.jcsonline.in

26. Valivarthi, D. T., Peddi, S., & Narla, S. (2021). Cloud computing with artificial intelligence techniques: Hybrid FA-CNN and DE-ELM approaches for enhanced disease detection in healthcare systems. International Journal of Advanced Science and Engineering Management, 16(4).
27. Gudivaka, B. R. (2021). AI-powered smart comrade robot for elderly healthcare with integrated emergency rescue system. World Journal of Advanced Engineering Technology and Sciences, 2(1), 122–131. https://doi.org/10.30574/wjaets.2021.2.1.0085
28. Narla, S., Valivarthi, D. T., & Peddi, S. (2019). Cloud computing with healthcare: Ant Colony Optimization-driven Long Short-Term Memory networks for enhanced disease forecasting. Volume 7, Issue 3.
29. Gudivaka, B. R. (2019). Big data-driven silicon content prediction in hot metal using Hadoop in blast furnace smelting. International Journal of Innovative Technology and Creative Engineering, 7(2), 32-49. https://doi.org/10.62646/ijitce.2019.v7.i2.pp32-49
30. Narla, S., Valivarthi, D. T., & Peddi, S. (2020). Cloud computing with artificial intelligence techniques: GWO-DBN hybrid algorithms for enhanced disease prediction in healthcare systems. Journal of Current Science & Humanities, 8(1), 14-30.
31. Gudivaka, B. R. (2024). Leveraging PCA, LASSO, and ESSANN for advanced robotic process automation and IoT systems. International Journal of Engineering & Science Research, 14(3), 718-731.
32. Narla, S., Peddi, S., & Valivarthi, D. T. (2019). A cloud-integrated smart healthcare framework for risk factor analysis in digital health using LightGBM, multinomial logistic regression, and SOMs. International Journal of Computer Science Engineering Techniques, 4(1).
33. Gudivaka, B. R. (2024). Smart Comrade Robot for elderly: Leveraging IBM Watson Health and Google Cloud AI for advanced health and emergency systems. International Journal of Engineering Research & Science & Technology, 20(3), 334–352. https://doi.org/10.62643/ijerst.2024.v20.i3.pp334-352
34. Kethu, S., Narla, S., Valivarthi, D. T., Peddi, S., & Natarajan, D. R. (2023). Patient-centric machine learning methods and AI tools for predicting and managing chronic conditions in elderly care: Algorithmic insights from the SURGE-Ahead Project. ISAR - International Journal of Research in Engineering Technology, 8(1), 28.
35. Gudivaka, B. R. (2022). Real-time big data processing and accurate production analysis in smart job shops using LSTM/GRU and RPA. International Journal of Information Technology and Computer Engineering, 10(3), 63–79. https://doi.org/10.62646/ijitce.2022.v10.i3.pp63-79
36. Natarajan, D. R., Valivarthi, D. T., Narla, S., Peddi, S., & Kethu, S. S. (2024). AI-driven predictive models and machine learning applications in geriatric care: From fall detection to chronic disease management and patient-centric solutions. International Journal of Engineering and Techniques, 10(1), 1-XX.
37. Gudivaka, R. K., Gudivaka, R. L., Gudivaka, B. R., Basani, D. K. R., Grandhi, S. H., & Khan, F. (2025). Diabetic foot ulcer classification assessment employing an

improved machine learning algorithm. Technology and Health Care, 1–16. https://doi.org/10.1177/09287329241296417

38. Valivarthi, D. T., Peddi, S., Narla, S., Kethu, S. S., & Natarajan, D. R. (2023). Fog computing-based optimized and secured IoT data sharing using CMA-ES and Firefly Algorithm with DAG protocols and Federated Byzantine Agreement. International Journal of Engineering & Science Research, 13(1), 117-132.
39. Basani, D. K. R., Gudivaka, B. R., Gudivaka, R. L., & Gudivaka, R. K. (2024). Enhanced fault diagnosis in IoT: Uniting data fusion with deep multi-scale fusion neural network. Internet of Things, 24, 101361. https://doi.org/10.1016/j.iot.2024.101361
40. Narla, S., & Purandhar, N. (2021). AI-infused cloud solutions in CRM: Transforming customer workflows and sentiment engagement strategies. International Journal of Applied Science and Engineering Management, 15(1).
41. Grandhi, S. H., Gudivaka, B. R., Gudivaka, R. L., Gudivaka, R. K., Basani, D. K. R., & Kamruzzaman, M. M. (2025). Detection and diagnosis of ECH signal wearable System for sportsperson using Improved Monkey based search support vector machine. International Journal of Pattern Recognition and Artificial Intelligence. https://doi.org/10.1142/S0129156425401494
42. Narla, S. (2020). Transforming smart environments with multi-tier cloud sensing, big data, and 5G technology. International Journal of Computer Science Engineering Techniques, 5(1).
43. Gudivaka, B. R., Almusawi, M., Priyanka, M. S., Dhanda, M. R., & Thanjaivadivel, M. (2024). An improved variational autoencoder generative adversarial network with convolutional neural network for fraud financial transaction detection. In 2024 Second International Conference on Data Science and Information System (ICDSIS) (pp. 17-18). IEEE. https://doi.org/10.1109/ICDSIS61070.2024.10594271