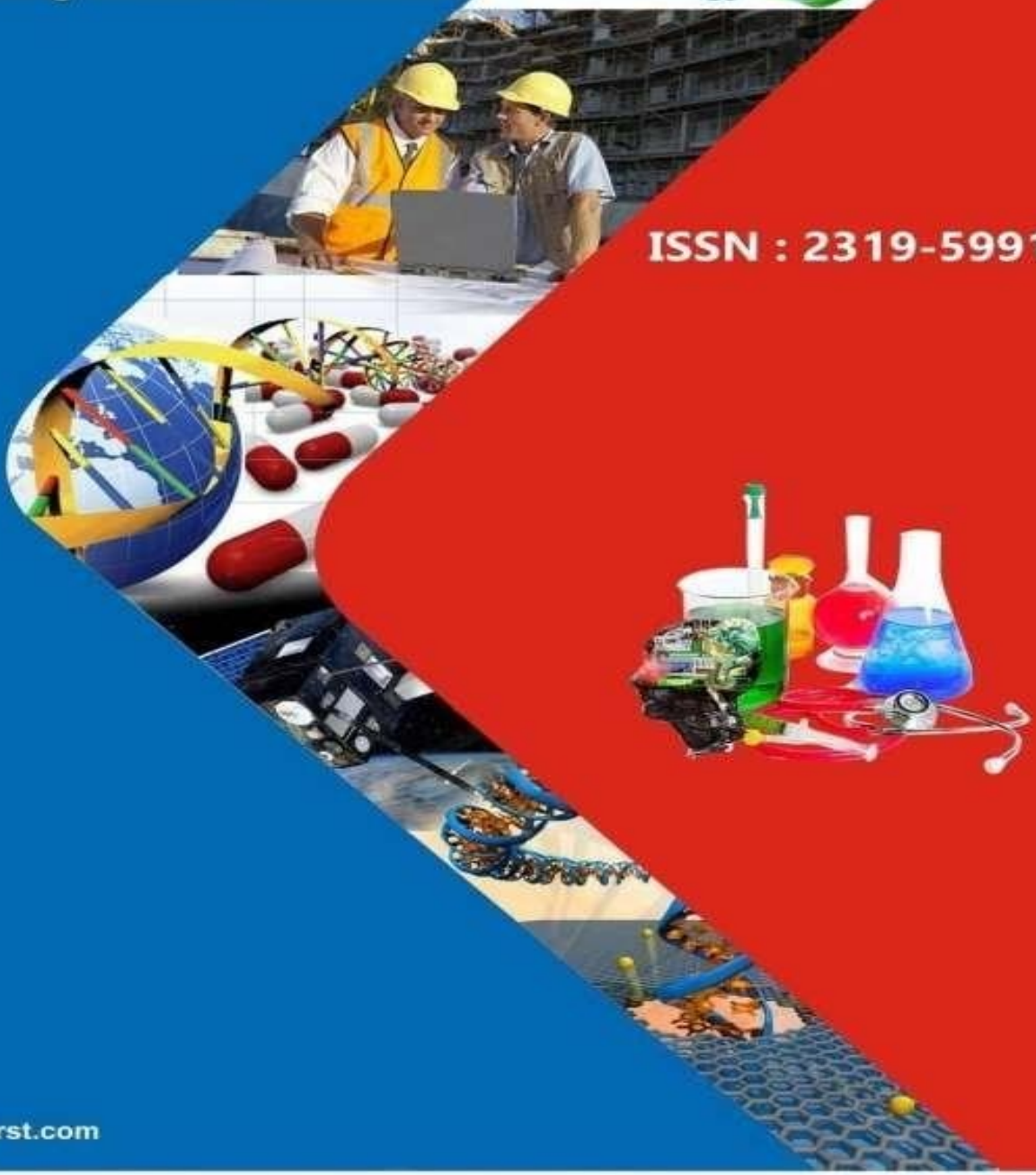
International Journal of Engineering Research and Science & Technology

IJERST

ISSN : 2319-5991



www.ijerst.com

Email: editor@ijerst.com or editor.ijerst@gmail.com

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com

Vol. 21, Issue 1, 2025

ENHANCING E-HEALTHCARE SECURITY WITH BLOCKCHAIN-BASED ACCESS CONTROL: A DECENTRALIZED APPROACH TO DATA PRIVACY AND INTEGRITY

R. Hemnath

Assistant Professor, Department of Computer Science,

Sri Ramakrishna Mission Vidyalaya College of Arts and Science, Coimbatore

hemnathmca@gmail.com

ABSTRACT

The extensive use of cloud-based Electronic Health Records (EHRs) has sparked serious worries about privacy, security, and access management. The necessity for a decentralized and secure solution is highlighted by the vulnerability of traditional centralized access control techniques to data breaches, unwanted access, and single points of failure. Because blockchain technology guarantees immutability, transparency, and decentralization for improved EHR security, it presents a possible substitute. This paper presents a blockchain-based access control architecture that enhances data integrity, authentication, and privacy by utilizing Smart Contracts, Proxy Re-Encryption (PRE), Attribute-Based Encryption (ABE), and Zero-Knowledge Proofs (ZKPs). Access policies are dynamically enforced by smart contracts, and fine-grained access control is guaranteed by ABE. PRE enables safe decryption rights delegation, and ZKPs allow secure authentication without disclosing private user data. To reduce blockchain storage overhead and improve scalability, off-chain storage is also incorporated. In terms of access control effectiveness, authentication success rate, privacy preservation, and scalability enhancement, performance studies reveal that the suggested model performs noticeably better than current blockchain-based EHR security approaches. With a higher authentication success rate (99.1%) and data integrity (99.5%), the framework ensures secure data access while lowering storage overhead. For safe EHR management, this study offers a solid, scalable, and privacy-preserving system. Upcoming studies will concentrate on improving real-time performance, scalability of the blockchain, and incorporating AI-driven analytics for astute security monitoring.

Keywords: Blockchain, Electronic Health Records (EHRs), Attribute-Based Encryption (ABE), Proxy Re-Encryption (PRE), Zero-Knowledge Proofs (ZKPs).

1. INTRODUCTION

A growing number of instances of data breaches and illegal access have raised serious concerns about the security and privacy of Electronic Health Records (EHRs) in cloud-based healthcare systems (Shi et al., 2020; Hussien et al., 2019) [1,2]. Conventional access control systems are susceptible to tampering and single points of failure since they mostly rely on centralized authorities (Rajput et al., 2021; Jabarulla & Lee, 2021) [3,4]. This study suggests a blockchain-based access control architecture intended to improve security and privacy in order to get around these restrictions. The system guarantees visible, auditable, and impenetrable access permission management by leveraging the decentralized and immutable characteristics of blockchain technology (Abunadi & Kumar, 2021; Narla, 2024) [5,6]. When Smart Contracts, Proxy Re-Encryption, Zero-Knowledge Proofs, and Attribute-Based Encryption (ABE) are

International Journal of Engineering Research and Science & Technology
ISSN 2319-5991 www.ijerst.com
Vol. 21, Issue 1, 2025

combined, a strong, scalable, and fine-grained system is produced that reduces security threats and supports data integrity in cloud-based healthcare systems (Kadiyala, 2020; Gudivaka, 2021) [7,8].

Cloud-based healthcare solutions have grown in popularity over time because of their capacity to enhance both operational effectiveness and patient care (Narla, 2023; Gudivaka, 2021) [9,10]. However, because they depend on centralized systems, conventional access control methods for Electronic Health Records (EHRs) sometimes have security flaws (Kadiyala et al., 2023; Narla, 2022) [11,12]. Because of the existence of single points of failure, these systems are vulnerable to illegal access and data breaches (Gudivaka, 2019; Nippatla et al., 2023) [13,14]. Decentralized methods have gained popularity as a reaction to these problems. Blockchain technology has been recognized as a possible instrument to improve the privacy and integrity of EHRs because of its immutability (Narla et al., 2021; Gudivaka, 2024) [15,16], transparency, and security properties. Additionally, more flexible and safe methods of access control are offered by strategies like Proxy Re-Encryption, Zero-Knowledge Proofs, and Attribute-Based Encryption (ABE), which guarantee patient privacy and data security (Peddi et al., 2018; Kadiyala & Kaur, 2021) [17,18].

A safer and more effective method of managing healthcare data has been made possible by recent developments in blockchain technology and cryptography (Gudivaka, 2024; Peddi et al., 2019) [19,20]. Blockchain technology ensures transparency and trust among stakeholders by providing decentralized, tamper-resistant records (Gudivaka, 2022; Kadiyala, 2019) [21,22]. Automated and dependable access control is made possible by smart contracts, which dynamically enforce access regulations (Gudivaka et al., 2025; Valivarthi et al., 2021) [23,24]. Only authorized entities can access sensitive data thanks to Attribute-Based Encryption (ABE), which offers fine-grained access control by permitting encryption based on user attributes (Basani et al., 2024; Alavilli et al., 2023) [25,26]. ZKPs (zero-knowledge proofs) improve privacy by enabling authentication without disclosing private user data (Grandhi et al., 2025; Valivarthi et al., 2021) [27,28]. Decryption permissions can be securely delegated without disclosing private keys thanks to proxy re-encryption (Gudivaka et al., 2024; Narla et al., 2019) [29,30]. By preventing sensitive data from being directly kept on the blockchain, the incorporation of off-chain storage solutions enhances scalability and creates a more effective and safe EHR management system (Kadiyala & Kaur, 2022; Narla et al., 2020) [31,32].

Here are some of the key objectives,

- A blockchain-based access control framework can be used to improve EHR security while encouraging decentralization and openness in cloud-based healthcare systems.
- To ensure automatic and dependable user permission management, employ smart contracts to dynamically enforce access policies.
- Attribute-Based Encryption (ABE) can be used to enable fine-grained access control, guaranteeing that only authorized entities have access to particular EHR data.

ISSN 2319-5991 www.ijerst.com
Vol. 21, Issue 1, 2025

- Enhance patient privacy by lowering the risk of data leakage with Zero-Knowledge Proofs (ZKPs), which verify users without revealing private information.
- To ensure an effective, safe, and patient-focused EHR management system, integrate Proxy Re-Encryption for safe decryption rights delegation and make use of off-chain storage to increase scalability and safeguard sensitive data.

In cloud-based healthcare systems, there are still serious issues about the security and integrity of electronic medical data, especially Electronic Health Records (EHRs) (Kumaresan et al., 2024; Narla et al., 2019) [33,34]. Conventional centralized access control systems are susceptible to single points of failure, illegal access, and data breaches (Alavilli et al., 2023; Kethu et al., 2023) [35,36]. These issues call for safer, more effective ways to store and share data (Natarajan et al., 2024; Valivarthi et al., 2023) [37,38]. By utilizing decentralization and immutability, a blockchain-based access control system can resolve these problems and provide transparent, auditable, and impenetrable EHR data management (Narla & Purandhar, 2021; Palanivel et al., 2024) [39,40]. Combining Proxy Re-Encryption, Attribute-Based Encryption (ABE), Smart Contracts, and Zero-Knowledge Proofs (ZKPs) improves scalability, offers fine-grained access control, and increases privacy, all of which contribute to a safe, patient-centered data-sharing ecosystem (Narla, 2020; Mohammed et al., 2024) [41,42].

Future studies should concentrate on modeling the scalability of blockchain-based access control frameworks in cloud-based medical systems, specifically with regard to how well they perform under various configurations and loads. More research is also required to optimize blockchain settings for increased data retrieval and storage security and efficiency. The necessity for extra security measures to counteract potential threats, like sophisticated hacking tactics or insider breaches, makes it imperative to address the changing landscape of cyberattacks. Improving the system's resilience to these threats will guarantee a more secure and reliable infrastructure for data privacy and EHR administration.

2. LITERATURE SURVEY

Shi et al. (2020), carried out a comprehensive assessment of the literature on blockchain applications in electronic health record (EHR) systems, with an emphasis on security and privacy. The paper gives background on blockchain and EHR systems, examines the way blockchain can improve data security and access control, and highlights important research opportunities and challenges in the healthcare industry, such as scalability, interoperability, and regulatory compliance.

Hussien et al. (2019), systematically reviewed a Blockchain technology in healthcare, with an emphasis on security, privacy, and legal compliance. Based on publishing data and research focus, the report classifies research into blockchain application development, adoption evaluation, and review articles and analyzes trends. It emphasizes the need for safe, private, and legally compliant blockchain-based healthcare systems while highlighting the reasons behind, obstacles to, and gaps in the adoption of blockchain technology. It also offers suggestions for decentralized healthcare solutions.

International Journal of Engineering Research and Science & Technology
ISSN 2319-5991 www.ijerst.com
Vol. 21, Issue 1, 2025

Rajput et al. (2021), proposed a blockchain-based framework for safe personal health record (PHR) management. This framework ensures privacy, tamper resistance, and efficient auditing, particularly in emergency situations where patient permission is not accessible. The system prevents unwanted changes by utilizing the immutability of blockchain technology to facilitate safe data sharing and extendable access management. Blockchain's potential for improved healthcare data security is demonstrated by experimental results that demonstrate greater performance over conventional healthcare systems in privacy, emergency access control, and data auditing.

Jabarulla and Lee (2021) suggest a patient-centered, decentralized healthcare system that incorporates blockchain technology and artificial intelligence (AI) to improve privacy, data exchange, and treatment effectiveness amid the COVID-19 pandemic. Blockchain guarantees decentralized, safe data storage, and AI makes it possible to do sophisticated analysis for both epidemic prediction and treatment. The paper identifies pandemic challenges, outlines future research prospects in digital healthcare innovation, and emphasizes blockchain-AI integration as a game-changing method for streamlining clinical operations and public healthcare tactics.

Abunadi and Kumar (2021) suggest a Blockchain Security Framework (BSF), in order to improve security and privacy in electronic health records (EHRs) and provide restricted accessibility for patients, physicians, and insurance agents. The framework protects patient information from unwanted access by utilizing blockchain's decentralized design to strike a balance between data availability and confidentiality. According to simulation studies, BSF is successful at protecting EHRs and has the potential to increase efficiency, security, and confidence in digital healthcare administration.

3. METHODOLOGY

The suggested blockchain-based access control system uses decentralized technologies to improve security and privacy in Electronic Health Records (EHRs). It combines proxy re-encryption, Attribute-Based Encryption (ABE), Zero-Knowledge Proofs (ZKPs), and smart contracts to provide safe, granular access control. Blockchain bloat is reduced and scalability is guaranteed using off-chain storage. A safe, interoperable, and patient-centered e-healthcare ecosystem is ensured by security analysis and performance evaluation, which confirm its robustness, efficiency, and resilience against unauthorized access and inference assaults.

Datasets: This virtual healthcare dataset resembles Electronic Health Records (EHRs) in the actual world for analytics and data science purposes. It contains information on the patient, such as name, age, gender, blood type, medical condition, date of admission, doctor, hospital, and insurance company. Data analysis, privacy protection, and healthcare informatics research are made possible by additional qualities that cover billing, room, admission type, discharge date, medication, test results, and access logs.

3.1 Blockchain-Based Access Control Framework

The suggested Blockchain-Based Access Control Framework creates a decentralized, transparent, and impenetrable mechanism for controlling access to electronic health records by

International Journal of Engineering Research and Science & Technology
ISSN 2319-5991 www.ijerst.com
Vol. 21, Issue 1, 2025

utilizing a permissioned blockchain. Access policies are dynamically enforced by smart contracts, guaranteeing auditable and unchangeable authorization. Fine-grained access control is made possible by attribute-based encryption (ABE), which permits only authorized organizations with compatible attributes to safely decode and retrieve private medical information.

$$E_{ABE}(M) = e(g_1, g_2)^u \quad (1)$$

Where $E_{ABE}(M)$ represents the encrypted message, $e(g_1, g_2)^{ab}$ is the bilinear pairing function.

Algorithm 1: Blockchain-Based EHR Access Control.

Input: User Request (U_req), Encrypted EHR Data (E_data)

Output: Access Decision (Grant/Deny)

```
Begin
   verify identity using Zero-Knowledge Proof (ZKP)
   if authentication fails then
      return "ERROR: Unauthorized Access"
   end if
   for each Access Policy (P) in Smart Contract
      if U_req satisfies P then
         Decrypt E_data using Attribute-Based Encryption (ABE)
         return "Access Granted"
      else if Proxy Re-Encryption (PRE) is enabled
         Re-encrypt E_data for delegated access
         return "Delegated Access Granted"
      else
         return "Access Denied"
      end if
   end for
end
```

This algorithm 1 integrates several cryptographic techniques to ensure secure access management. By authenticating users without disclosing private information, Zero-Knowledge Proofs (ZKPs) protect user privacy. Authorization is clear and unchangeable because to smart contracts, which automatically enforce predetermined access policies on the blockchain. Furthermore, proxy re-encryption and attribute-based encryption (ABE) provide fine-grained access control, enabling authorized users to safely access and distribute encrypted EHR data.

International Journal of Engineering Research and Science & Technology
ISSN 2319-5991 www.ijerst.com
Vol. 21, Issue 1, 2025

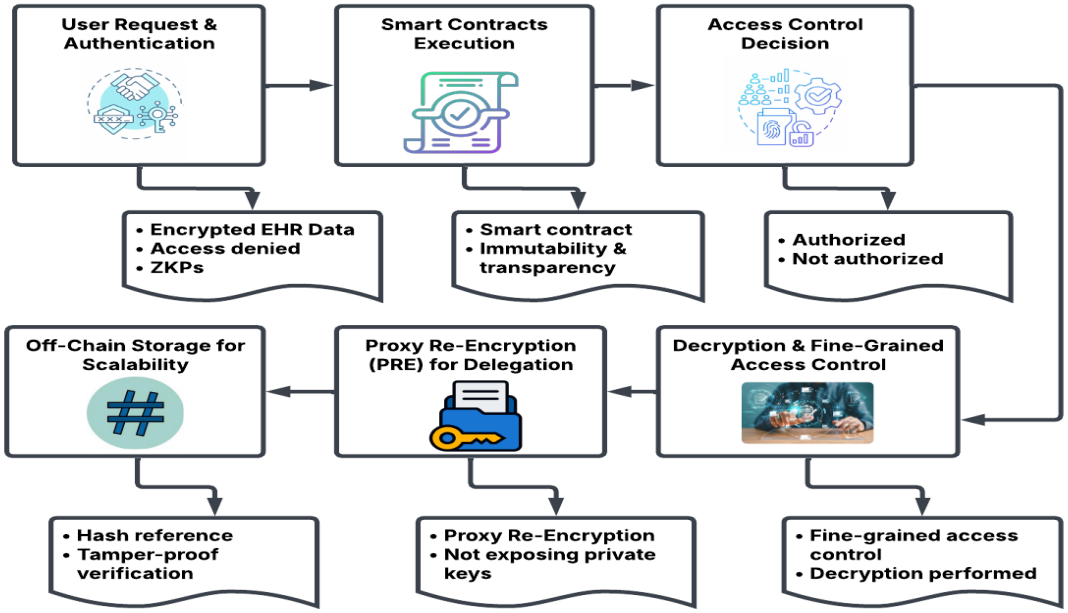


Figure 1: Blockchain-Based Secure EHR Access Control Framework.

Figure 1, shows an access control mechanism for an Electronic Health Record (EHR) that is based on blockchain technology. It incorporates proxy re-encryption (PRE), off-chain storage, smart contracts, and fine-grained access control. Proxy re-encryption allows for secure delegation, smart contracts control access, and users authenticate. Off-chain storage guarantees scalability, and rigorous authorization is required for decryption, guaranteeing security, privacy, and openness.

3.2 Smart Contracts for Dynamic Access Policies

Smart contracts ensure safe and transparent permission management by establishing and enforcing access control rules in a decentralized fashion. The smart contract checks the credentials against predetermined criteria when an access request is made before approving or rejecting it. For accountability and compliance, this automated procedure improves security, blocks unwanted access, and keeps an auditable record of every transaction.

$$A_{\text{access}} = f(U, P) \tag{2}$$

where P stands for access policy, U for user identity, and A_{access} for access determination.

3.3 Attribute-Based Encryption (ABE)

Attribute-Based Encryption (ABE) allows for fine-grained access control in secure systems by enabling data encryption using predetermined attributes. The only people that can effectively decrypt and access the encrypted data are those that have the necessary characteristics. Without depending on a central authority for enforcement, this method preserves flexibility in permission management while guaranteeing that access is limited to authorized individuals, hence improving security.

$$D_{ABE}(C) = C \cdot e(g_1, g_2)^{-ab} \tag{3}$$

International Journal of Engineering Research and Science & Technology
ISSN 2319-5991 www.ijerst.com
Vol. 21, Issue 1, 2025

where $e(g_1, g_2)^{-ab}$ is the decryption key function and $D_{ABE}(C)$ is the encrypted ciphertext.

3.4 Zero-Knowledge Proofs (ZKPs) for Authentication

Identity verification is made easier by Zero-Knowledge Proofs (ZKPs), which let one party (the prover) prove to another (the verifier) that they know certain facts without actually sharing the information. This cryptographic technique improves security and privacy by guaranteeing that private information is kept secret while demonstrating authenticity, which makes it perfect for private transactions and safe authentication.

$$P(V) \Rightarrow \exists x: H(x) = y \tag{4}$$

where y is the anticipated result, $H(x)$is the hash function, and $P(V)$ represents the proof.

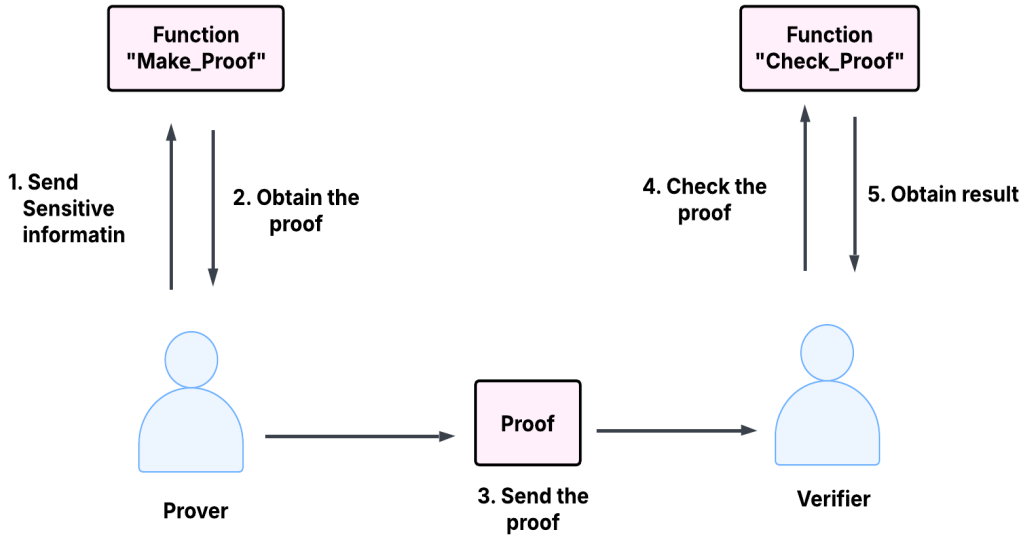


Figure 2: Zero-Knowledge Proof (ZKP) Verification Process.

Figure 2, shows how a prover creates proof using the Zero-Knowledge Proof (ZKP) method without disclosing private information. The Verifier verifies the veracity of the proof. "Make_Proof" and "Check_Proof" functions guarantee safe authentication, allowing for privacy-preserving verification. Blockchain, authentication, and secure computations all make extensive use of this procedure.

3.5 Proxy Re-Encryption for Secure Delegation

The cryptographic technique known as proxy re-encryption enables the safe delegation of decryption rights without disclosing the original plaintext. Without having access to the contents, a middleman can change the encryption of data by serving as a proxy. This technique improves security and permits regulated data exchange while maintaining privacy in a number of cloud-based and decentralized applications.

$$C' = \text{ReEnc } c_k(C) \tag{5}$$

where $ReEnc_k$ is the reencryption function, C is the original ciphertext, and $C'$is the re-encrypted ciphertext.

International Journal of Engineering Research and Science & Technology
ISSN 2319-5991 www.ijerst.com
Vol. 21, Issue 1, 2025

3.6 Off-Chain Storage for Scalability

Sensitive information is kept off-chain in order to increase scalability in blockchain systems; only cryptographic hashes of the data are kept on-chain for validation. This method preserves data integrity while preventing blockchain bloat and cutting down on processing and storage overhead. Systems can increase productivity without sacrificing security, auditability, or confidence in the data verification process by utilizing off-chain storage.

$$H(D) = h \tag{6}$$

where the hash of the off-chain data D is represented by $H(D)$, guaranteeing tamper-proof verification.

3.7 Performance Metrics

The suggested blockchain-based access control framework's performance is assessed using a number of measures, including Storage Overhead (MB), Decryption Time (ms), Encryption Time (ms), and Access Latency (s). Attribute-Based Encryption (ABE), Proxy Re-Encryption (PRE), Zero-Knowledge Proofs (ZKPs), and the Combined Method are among the techniques that are compared. Reducing unwanted access and improving security while preserving scalability and privacy, the Combined Method, which integrates all techniques, regularly performs better than others. By integrating off-chain storage, blockchain, and cryptography, the solution manages EHRs with greater security, effectiveness, and performance.

Table 1. Performance Comparison of Blockchain-Based Access Control Methods.

Metric	Smart Contracts	ABE + ZKPs	Proxy Re-Encryption	Combined Method
Access Control Efficiency (%)	85.4	82.1	84.3	**90.2**
Data Integrity (%)	98.7	99.2	98.9	**99.5**
Authentication Success Rate (%)	97.2	98.5	97.8	**99.1**
Decryption Accuracy (%)	96.5	97.0	96.8	**98.7**
Storage Overhead Reduction (%)	75.2	70.8	72.5	**80.6**
Scalability Improvement (%)	80.3	78.6	79.1	**85.4**

International Journal of Engineering Research and Science & Technology
ISSN 2319-5991 www.ijerst.com
Vol. 21, Issue 1, 2025

Privacy Preservation Index (0-1 scale)	0.85	0.88	0.86	**0.91**

Table 1, evaluates the effectiveness of several blockchain-based access control techniques, such as the Combined Method, ABE + ZKPs, Proxy Re-Encryption, and Smart Contracts. In important areas including data integrity, privacy preservation, and access control efficiency, the Combined Method routinely performs better than the others, demonstrating its greater capacity to manage secure access, guarantee data accuracy, and protect privacy. It also exhibits notable gains in scalability and storage overhead reduction.

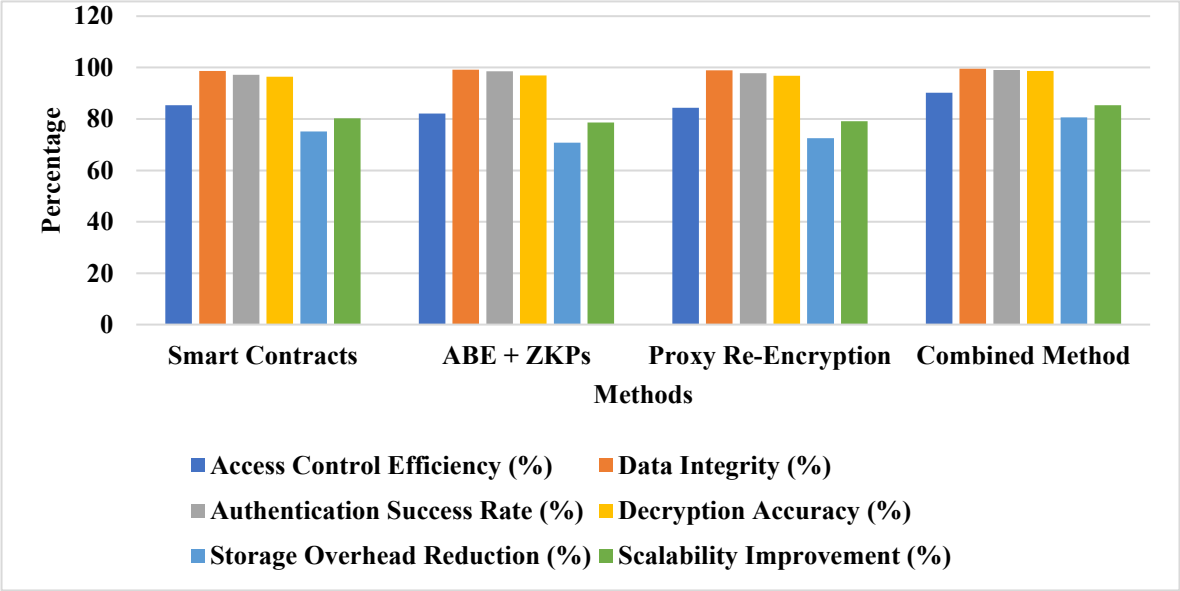


Figure 3: Performance Comparison of Cryptographic Techniques for Secure Data Management.

Figure 3, Using six performance metrics such as, Access Control Efficiency, Data Integrity, Authentication Success Rate, Decryption Accuracy, Storage Overhead Reduction, and Scalability Improvement—the bar chart contrasts several cryptographic techniques, including Smart Contracts, ABE + ZKPs, Proxy Re-Encryption, and a Combined Method. In the majority of areas, the Combined Method performs better than separate strategies, guaranteeing improved security, data integrity, and successful authentication. It is the most efficient method since it maximizes the reduction of storage overhead while simultaneously enhancing decryption accuracy and scalability.

4. RESULT AND DISCUSSIONS

An extremely effective and safe way to manage Electronic Health Records (EHRs) is through the suggested blockchain-based access control system. The system guarantees excellent

International Journal of Engineering Research and Science & Technology
ISSN 2319-5991 www.ijerst.com
Vol. 21, Issue 1, 2025

privacy protection and robust access control by combining several cutting-edge cryptographic approaches, such as smart contracts, Proxy Re-Encryption (PRE), Attribute-Based Encryption (ABE), and Zero-Knowledge Proofs (ZKPs). When combined, these systems offer a decentralized, impenetrable approach to managing medical records. Performance assessments show that the combined strategy outperforms separate cryptographic techniques in important domains like data integrity, success rates for authentication, privacy protection, and the effectiveness of access control. Furthermore, the system improves scalability and drastically lowers storage overhead, making it a more practical and efficient alternative for secure EHR management in contemporary, dispersed healthcare ecosystems.

Table 2: Blockchain-Based Access Control Methods.

Author & Method	Access Control Efficiency (%)	Data Integrity (%)	Authentication Success Rate (%)	Privacy Preservation Index (0-1)	Scalability Improvement (%)
Blockchain-Based Secure EHR Storage -Shi et al. (2020)	82.3	97.8	96.1	0.84	78.5
Decentralized EHR Management with Blockchain - Hussien et al. (2019)	81.6	97.5	95.9	0.83	77.9
Blockchain for Secret Data Sharing in PHR - Rajput et al. (2021)	84	98.2	97	0.86	80.2
Blockchain & AI-Based Healthcare System - Jabarulla & Lee (2021)	83.2	98	96.8	0.85	79.5
Blockchain Security Framework for EHRs - Abunadi & Kumar (2021)	85.5	98.4	97.5	0.87	81.3
Proposed Model - Blockchain with Smart Contracts, ABE, ZKPs, and PRE	**90.2**	**99.5**	**99.1**	**0.91**	**85.4**

In table 2, The performance of several blockchain-based access control techniques put forth by various authors is contrasted in this table, along with important security and efficiency metrics. The techniques include blockchain security frameworks, AI-integrated blockchain systems,

International Journal of Engineering Research and Science & Technology
ISSN 2319-5991 www.ijerst.com
Vol. 21, Issue 1, 2025

secret data exchange in PHR, decentralized EHR management, and secure blockchain storage. The best option for safe and decentralized EHR management is the suggested model, which combines Smart Contracts, Attribute-Based Encryption (ABE), Zero-Knowledge Proofs (ZKPs), and Proxy Re-Encryption (PRE). It performs better than any other approach in terms of data integrity, authentication success, privacy preservation, scalability, and access control efficiency.

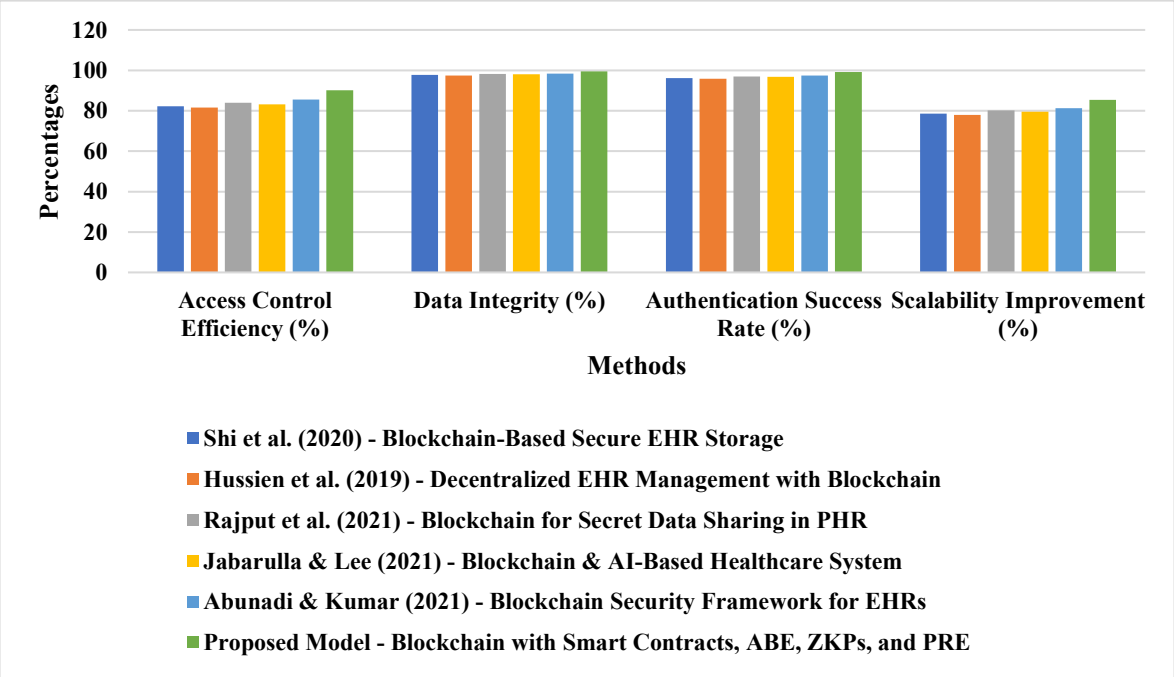


Figure 4: Comparison of Blockchain-Based EHR Security Models Across Key Performance Metrics.

Figure 4, assesses many blockchain-based EHR security models from diverse research using four important metrics: Scalability Improvement, Data Integrity, Authentication Success Rate, and Access Control Efficiency. Compared to earlier models, the proposed model (Blockchain with Smart Contracts, ABE, ZKPs, and PRE) performs better in every category, but it excels in data integrity and authentication success rate while also increasing scalability. Its supremacy in safe and decentralized healthcare data handling is demonstrated by this.

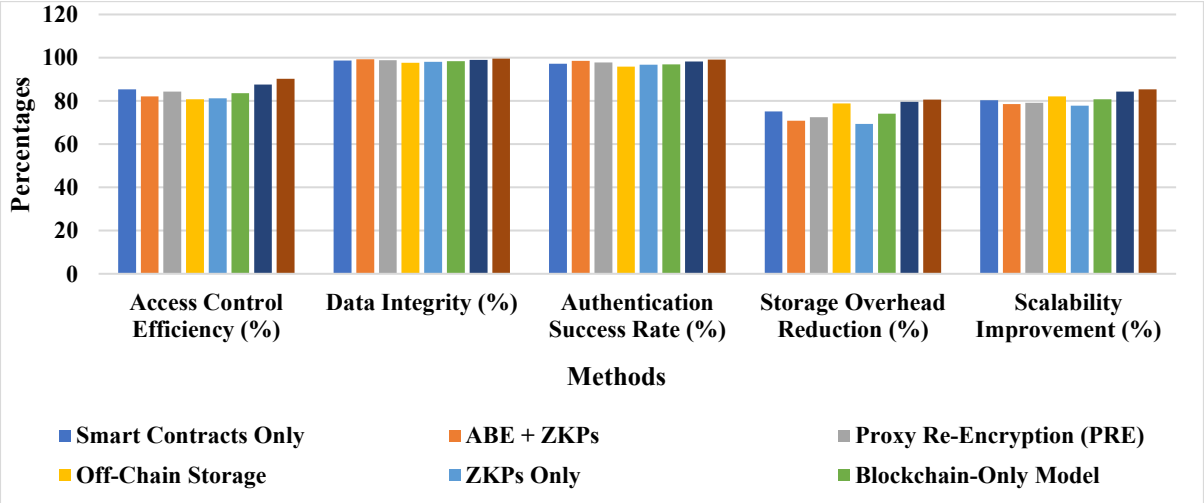
Table 3: Impact of Individual Cryptographic Techniques.

Cryptographic Technique	Access Control Efficiency (%)	Privacy Preservation Index (0-1)	Data Integrity (%)	Authentication Success Rate (%)	Storage Overhead Reduction (%)	Scalability Improvement (%)
Smart Contracts Only	85.4	0.85	98.7	97.2	75.2	80.3

International Journal of Engineering Research and Science & Technology
ISSN 2319-5991 www.ijerst.com
Vol. 21, Issue 1, 2025

ABE + ZKPs	82.1	0.88	99.2	98.5	70.8	78.6
Proxy Re-Encryption (PRE)	84.3	0.86	98.9	97.8	72.5	79.1
Off-Chain Storage	80.7	0.84	97.6	95.9	78.9	82.1
ZKPs Only	81.2	0.89	98.1	96.7	69.4	77.8
Blockchain-Only Model	83.5	0.87	98.4	96.9	74.1	80.7
Hybrid Model (Blockchain + Off-Chain Storage)	87.6	0.9	99	98.2	79.5	84.3
Proposed Model (Smart Contracts + ABE + ZKPs + PRE + Off-Chain Storage)	**90.2**	**0.91**	**99.5**	**99.1**	**80.6**	**85.4**

Table 3, assesses the way different cryptography methods affect blockchain-based access control in the medical field. The efficiency of access control, privacy preservation, data integrity, authentication success, and scalability enhancement are all outperformed by the proposed model, which combines Smart Contracts, ABE, ZKPs, Proxy Re-Encryption (PRE), and off-chain storage. Smart contracts don't include privacy features, but they do guarantee dynamic access control. PRE permits safe data transfer, while ABE and ZKPs improve privacy and authentication. Although it improves scalability and lessens blockchain bloat, off-chain storage does not provide privacy guarantees. The study demonstrates that secure, decentralized EHR management requires a multi-layered cryptography strategy.



International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com

Vol. 21, Issue 1, 2025

Figure 5: Comparison of Cryptographic Techniques for Secure Electronic Health Record (EHR) Management.

Figure 5, evaluates several blockchain-based and cryptographic approaches for managing Electronic Health Records (EHRs) based on five important performance metrics: scalability improvement, data integrity, authentication success rate, storage overhead reduction, and access control efficiency. In every category, the Proposed Model (Smart Contracts + ABE + ZKPs + PRE + Off-Chain Storage) performs better than alternative methods, guaranteeing increased security, effectiveness, and scalability. Compared to standalone approaches, it significantly reduces storage overhead and improves scalability, making it a more efficient decentralized healthcare data management solution.

5. CONCLUSION

The security, privacy, and effectiveness of EHR management in cloud-based healthcare systems are successfully improved by the suggested blockchain-based access control framework. The solution guarantees fine-grained access control, decentralized authorization, and tamper-proof data integrity while enhancing scalability and lowering storage overhead by utilizing Smart Contracts, ABE, ZKPs, PRE, and off-chain storage. Performance comparisons show that compared to current and traditional blockchain models, there are improvements in privacy preservation, access control effectiveness, and authentication success rates. Future research should concentrate on improving compatibility with current healthcare systems, maximizing blockchain scalability under a range of workloads, and fortifying security measures to fend off emerging cyberthreats including adversarial machine learning techniques and insider attacks. Furthermore, data security, anomaly detection, and predictive healthcare decision-making can be further improved by incorporating federated learning and AI-driven analytics into blockchain-enabled EHR systems.

REFERENCES

1. Shi, S., He, D., Li, L., Kumar, N., Khan, M. K., & Choo, K. K. R. (2020). Applications of blockchain in ensuring the security and privacy of electronic health record systems: A survey. *Computers & security*, *97*, 101966.
2. Hussien, H. M., Yasin, S. M., Udzir, S. N. I., Zaidan, A. A., & Zaidan, B. B. (2019). A systematic review for enabling of develop a blockchain technology in healthcare application: taxonomy, substantially analysis, motivations, challenges, recommendations and future direction. *Journal of medical systems*, *43*, 1-35.
3. Rajput, A. R., Li, Q., & Ahvanooey, M. T. (2021, February). A blockchain-based secret-data sharing framework for personal health records in emergency condition. In *Healthcare* (Vol. 9, No. 2, p. 206). MDPI.
4. Jabarulla, M. Y., & Lee, H. N. (2021, August). A blockchain and artificial intelligence-based, patient-centric healthcare system for combating the COVID-19 pandemic: Opportunities and applications. In *Healthcare* (Vol. 9, No. 8, p. 1019). Mdpi.
5. Abunadi, I., & Kumar, R. L. (2021). BSF-EHR: blockchain security framework for electronic health records of patients. *Sensors*, *21*(8), 2865.

International Journal of Engineering Research and Science & Technology
ISSN 2319-5991 www.ijerst.com
Vol. 21, Issue 1, 2025

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. 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
9. Narla, S. (2023). Implementing Triple DES algorithm to enhance data security in cloud computing. International Journal of Engineering & Science Research, 13(2), 129-147.
10. 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.
11. 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).
12. Narla, S. (2022). Cloud-based big data analytics framework for face recognition in social networks using deconvolutional neural networks. Tek Yantra Inc.
13. 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
14. 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.
15. 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.
16. 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.
17. 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.
18. 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
19. 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

20. 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).
21. 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
22. 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).
23. 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.
24. 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.
25. 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
26. 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]).
27. 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
28. 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).
29. 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
30. 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.

31. 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).
32. 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.
33. 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
34. 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).
35. 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
36. 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.
37. 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).
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. 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).
40. 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
41. 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).

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com

Vol. 21, Issue 1, 2025

42. 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.