International Journal of Engineering & Extended Technologies Research (IJEETR)

| ISSN: 2322-0163 | www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802436

Blockchain-Based Decentralized Cloud Storage with Privacy-Preserving Access Control using IPFS and ECC

Mohanraj P[1], HarishR[2], JaikumarM[2], Kathirvel R[2] and Kiruthish S[2]

Assistant Professor, Department of Computer Science and Engineering, Muthayammal Engineering College, Rasipuram, Namakkal, Tamil Nadu, India[1]

UG Scholar, Department of Artificial Intelligence and Data Science, Muthayammal College of Engineering, Rasipuram, Namakkal, Tamil Nadu, India[2]

Publication History: Received: 25.02.2026; Revised: 20.03.2026; Accepted: 25.03. 2026; Published: 28.03.2026.

ABSTRACT: Cloud storage has become essential for modern data management, yet centralized architectures introduce critical security and privacy concerns such as data breaches, unauthorized access, and reliance on third-party providers. Centralized systems store sensitive information in a single location, increasing vulnerability and limiting user control over data. To overcome these limitations, this paper presents a decentralized framework for secure and privacy-preserving data storage and sharing. The proposed approach integrates blockchain technology, InterPlanetary File System (IPFS), and advanced cryptographic techniques to ensure data confidentiality, integrity, and transparency. Files are securely encrypted and stored in a distributed manner using IPFS, while blockchain maintains immutable records of access control and transactions. Cryptographic mechanisms, including proxy re-encryption and zero-knowledge proofs, enable secure data sharing and user authentication without exposing sensitive information. This architecture eliminates single points of failure and reduces dependency on centralized authorities. The framework enhances user control over data while ensuring secure access and efficient management. Overall, the proposed solution provides a scalable and trustworthy environment for cloud data storage, addressing key challenges in security, privacy, and transparency in modern digital systems.

KEYWORDS: Blockchain, Cloud Security, Data Privacy, Decentralized Storage, Elliptic Curve Cryptography, IPFS, Zero-Knowledge Proof

I. INTRODUCTION

The rapid growth of digital technologies has significantly increased the reliance on cloud storage for managing and sharing data across various domains. Despite its convenience and scalability, traditional cloud infrastructure is primarily based on centralized architectures, which introduce critical security and privacy challenges. Sensitive information, including user credentials and access records, is typically stored in centralized servers, making them attractive targets for cyberattacks and data breaches. In addition, limited transparency in data handling processes creates trust concerns, as users must depend on service providers for data protection without direct control or visibility. To address these limitations, this paper explores a decentralized approach to secure data storage and access control. By integrating blockchain technology with distributed storage systems such as IPFS, the proposed framework enhances data integrity, availability, and transparency. Advanced cryptographic techniques, including Elliptic Curve Cryptography, proxy re-encryption, and zero-knowledge proofs, are employed to ensure secure data sharing and privacy preservation. This approach eliminates single points of failure, strengthens user control over data, and establishes a more resilient and trustworthy environment for cloud-based services.

i) Problem statement

The increasing dependence on centralized cloud storage systems has introduced significant challenges related to data security, privacy, and user control. Sensitive information is commonly stored and managed by third-party providers, creating a single point of failure that is highly vulnerable to cyberattacks, data breaches, and unauthorized access. Limited transparency in access control mechanisms further weakens trust, as users lack visibility into how data is stored, accessed, and shared. In addition, existing systems provide inadequate support for secure data sharing, efficient

| ISSN: 2322-0163 | www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802436

key management, and privacy-preserving authentication. These limitations highlight the need for a robust and decentralized solution that ensures secure, transparent, and user-controlled data storage and access management.

ii) Dataset details

The evaluation of the proposed framework is conducted using a combination of synthetic and sample user-generated datasets that simulate real-world cloud storage scenarios. The dataset includes encrypted files of varying sizes, user credentials, access permission records, and transaction logs to represent typical data storage and sharing activities. Metadata such as file hashes and access control policies are also incorporated to validate blockchain-based recording and verification processes. The dataset is structured to assess system performance in terms of secure data upload, retrieval, sharing, and authorization under different user roles. This setup enables comprehensive analysis of security mechanisms, data integrity, and access control efficiency within a decentralized environment.

iii) Objectives

The primary objective of this research is to develop a decentralized framework that ensures secure, privacy-preserving, and efficient data storage and sharing in cloud environments. The study aims to eliminate reliance on centralized authorities by integrating blockchain and distributed storage mechanisms, thereby reducing security vulnerabilities and single points of failure. Another key objective is to enhance data confidentiality and integrity through the use of advanced cryptographic techniques such as Elliptic Curve Cryptography, proxy re-encryption, and zero-knowledge proofs. The framework also focuses on providing transparent and tamper-resistant access control while enabling users to retain full ownership and control over their data. Additionally, the research seeks to establish a scalable and trustworthy system capable of supporting secure data access, sharing, and verification in modern cloud-based applications.

II. RELATED WORK

Xiaoguang Liu, et al. [1] proposed a blockchain-assisted electronic medical record system that enhances data security and privacy through the integration of proxy re-encryption and multisignature techniques. The approach focuses on enabling secure sharing of medical records without exposing sensitive patient information. Proxy re-encryption allows controlled delegation of access, ensuring that only authorized users can decrypt the data without revealing original encryption keys. The multisignature mechanism strengthens authentication by requiring multiple approvals before granting access, thereby reducing the risk of unauthorized entry. Blockchain technology is utilized to store transaction logs and access records in an immutable and transparent manner, ensuring traceability and accountability. The system also improves data integrity by preventing tampering of stored medical records. Furthermore, decentralized storage reduces dependency on centralized authorities and minimizes the risk of single-point failures. The proposed method demonstrates improved efficiency in secure data sharing while maintaining patient privacy. The integration of cryptographic techniques with blockchain ensures a robust and scalable healthcare data management solution. Overall, the study highlights the effectiveness of combining encryption and decentralized technologies for secure electronic medical record systems.

Abdullah Alabdulatif, et al. [2] proposed a cloud-enabled access control model designed to preserve the security and privacy of medical big data. The model introduces a fine-grained access control mechanism that allows data owners to define and manage permissions based on user roles and attributes. The system emphasizes protecting sensitive healthcare information from unauthorized access while maintaining efficient data sharing. Advanced encryption techniques are applied to ensure confidentiality during storage and transmission. The framework also integrates privacy-preserving mechanisms to prevent exposure of user identities and sensitive attributes. Scalability is addressed by enabling the system to handle large volumes of medical data without performance degradation. The proposed solution reduces reliance on centralized authorities by incorporating distributed control features. Additionally, the model enhances transparency in access management, allowing better monitoring of user activities. The approach demonstrates improved flexibility and adaptability in dynamic cloud environments. Overall, the study provides an effective solution for secure and privacy-aware management of medical big data in cloud systems.

D. Dhinakaran, et al. [3] presented a comprehensive survey on privacy-preserving techniques in IoT-based cloud systems, with a focus on integrating artificial intelligence methods. The study analyzes various existing approaches for securing data generated by IoT devices and stored in cloud environments. It highlights the challenges associated with data privacy, including unauthorized access, data leakage, and lack of user control. The survey explores encryption-based methods, anonymization techniques, and blockchain integration as potential solutions for enhancing security. It also examines the role of AI in improving threat detection and adaptive security mechanisms. The research identifies

| ISSN: 2322-0163 | www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802436

limitations in current systems, such as high computational complexity and scalability issues. Furthermore, the study emphasizes the need for efficient key management and secure communication protocols. The integration of AI is shown to improve decision-making and automate security processes. The survey provides valuable insights into emerging trends and future research directions in privacy-preserving cloud systems. Overall, it serves as a foundation for developing advanced secure frameworks in IoT-cloud environments.

Weizheng Wang, et al. [4] proposed a smart contract-based access control system for the Industrial Internet of Things, focusing on privacy preservation and secure data sharing. The system leverages blockchain technology to implement token-based authentication and authorization mechanisms. Smart contracts are used to automate access control policies, ensuring that permissions are enforced without human intervention. The token-based approach enhances security by providing dynamic and flexible access rights to users. Blockchain ensures transparency and immutability of access records, preventing unauthorized modifications. The system also addresses challenges related to data integrity and trust in industrial environments. By decentralizing access control, the framework eliminates reliance on centralized authorities and reduces vulnerability to attacks. The approach improves scalability and supports efficient management of large-scale IoT networks. Additionally, privacy is preserved by limiting exposure of sensitive information during authentication processes. Overall, the study demonstrates an effective solution for secure and automated access control in industrial IoT systems.

HananNaserAlsuqaih, et al. [5] proposed a blockchain-based privacy-preserving access control mechanism tailored for e-health applications. The system aims to secure sensitive healthcare data while enabling efficient and controlled sharing among authorized users. Blockchain technology is employed to maintain immutable records of data access and transactions, ensuring transparency and traceability. The framework incorporates encryption techniques to protect patient data during storage and transmission. Access control policies are designed to provide fine-grained authorization, allowing only permitted users to access specific information. The decentralized architecture reduces the risk of data breaches and eliminates single points of failure. The study also focuses on improving system efficiency and reducing computational overhead. Privacy preservation is achieved by minimizing exposure of sensitive data during authentication and access processes. The proposed solution demonstrates enhanced security, reliability, and scalability in e-health systems. Overall, the research highlights the potential of blockchain technology in developing secure and privacy-focused healthcare data management systems.

Reetu Gupta, et al. [6] proposed a secure and privacy-preserving multi-authority access control system for cloud-based healthcare data sharing. The framework distributes access control responsibilities among multiple authorities, reducing dependency on a single entity and enhancing system reliability. Attribute-based encryption is utilized to enforce fine-grained access policies, ensuring that only authorized users can access sensitive healthcare information. The system improves privacy by preventing unauthorized exposure of patient data during access and transmission. It also addresses key management challenges by distributing control across different authorities, thereby reducing the risk of key compromise. The architecture enhances scalability, making it suitable for large-scale healthcare environments. Security mechanisms are designed to resist common attacks such as collusion and unauthorized data access. Additionally, the model ensures flexibility in defining access permissions based on dynamic user roles. The approach demonstrates improved efficiency in managing secure data sharing across multiple domains. Overall, the study highlights the effectiveness of multi-authority systems in strengthening cloud healthcare security.

HernánVanegas, et al. [7] proposed a privacy-preserving method for computing edit distance using secret-sharing-based two-party computation. The approach enables two parties to collaboratively compute the similarity between datasets without revealing their private inputs. Secret-sharing techniques divide sensitive data into shares, ensuring that no single party can reconstruct the original information independently. The system is designed to protect data confidentiality during computation, making it suitable for applications such as secure data matching and biometric verification. Cryptographic protocols are employed to ensure correctness and security of the computation process. The method addresses privacy concerns in data comparison tasks, where revealing raw data is not acceptable. Efficiency is also considered, with optimizations to reduce computational and communication overhead. The approach demonstrates strong resistance to data leakage and inference attacks. Furthermore, it provides a foundation for secure multi-party computations in distributed systems. Overall, the study contributes to the development of advanced privacy-preserving computational techniques.

Amit Kumar Jakhar, et al. [8] proposed a blockchain-based privacy-preserving and access-control framework for electronic health records management. The system leverages blockchain to store access logs and enforce secure data sharing policies in a decentralized environment. Encryption techniques are applied to protect patient records, ensuring

| ISSN: 2322-0163 | www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802436

confidentiality during storage and transmission. The framework introduces efficient access control mechanisms that allow data owners to define permissions for different users. Blockchain ensures immutability and transparency of transactions, enabling traceability of data access activities. The approach eliminates reliance on centralized authorities, reducing vulnerability to attacks and data breaches. Scalability is addressed through optimized storage and processing strategies. The system also integrates mechanisms to ensure secure key management and data retrieval. Privacy preservation is achieved by restricting access to sensitive information based on predefined policies. Overall, the research demonstrates an effective solution for secure and decentralized healthcare data management.

Omar Hasan, et al. [9] presented a comprehensive survey on privacy-preserving reputation systems based on blockchain and cryptographic techniques. The study analyzes various methods used to build secure and trustworthy reputation systems in decentralized environments. It highlights the role of blockchain in ensuring transparency, immutability, and resistance to tampering. Cryptographic building blocks such as zero-knowledge proofs and secure multiparty computation are discussed as key enablers of privacy preservation. The survey identifies challenges related to scalability, data anonymity, and performance overhead in existing systems. It also explores different design approaches for balancing transparency and user privacy. The research provides insights into how reputation systems can be securely implemented without exposing sensitive user data. Furthermore, it outlines future directions for improving efficiency and robustness in decentralized reputation frameworks. The study serves as a valuable reference for designing secure and privacy-aware systems. Overall, it emphasizes the importance of integrating blockchain with advanced cryptographic methods for privacy protection.

Sejong Lee, et al. [10] proposed a blockchain-based system for privacy preservation in patient information exchange. The framework focuses on securely sharing medical data among healthcare providers while maintaining patient confidentiality. Blockchain technology is used to store access records and ensure transparency in data transactions. Encryption techniques are implemented to protect sensitive patient information from unauthorized access. The system introduces mechanisms for controlled data sharing, allowing only authorized entities to access specific records. It also enhances trust among participants by providing verifiable and immutable logs of data exchanges. The architecture reduces dependency on centralized systems, improving security and reliability. Efficiency considerations are addressed to ensure smooth operation in real-world healthcare environments. Privacy is maintained by minimizing exposure of sensitive data during communication processes. Overall, the study demonstrates the potential of blockchain in enabling secure and privacy-preserving patient data exchange systems.

III. EXISTING METHODLOGY

Traditional cloud storage systems rely on centralized architectures in which a single authority, typically the service provider, is responsible for managing data storage, authentication, and access control. Common techniques include username–password authentication, role-based access control (RBAC), and centralized key management for encrypting sensitive information. Data is usually stored in large data centers, where encryption may be applied either at rest or during transmission. Access permissions and user activities are maintained in centralized databases, enabling administrators to control and monitor system operations. While these approaches simplify management and provide high availability, they concentrate control within a single entity. Despite the use of standard security mechanisms, centralized systems exhibit several inherent limitations. Storing critical information such as encryption keys, credentials, and access logs in a single repository creates a significant vulnerability, making the system an attractive target for cyberattacks. If the central server is compromised, unauthorized entities may gain access to sensitive data, leading to privacy breaches and potential data manipulation. Additionally, traditional encryption techniques often depend on trusted intermediaries for key distribution and management, which introduces further risks. Limited transparency in how data is accessed and shared also reduces user confidence, as verification of data integrity and access history is not always possible. Scalability and flexibility present further challenges in existing approaches. As the volume of data and number of users increase, centralized infrastructures may struggle to efficiently handle access control, key revocation, and permission updates. Processes such as session management, token validation, and access revocation can become complex and prone to delays or inconsistencies. Furthermore, users have minimal control over their own data, as policies are enforced by the service provider rather than the data owner. These constraints highlight the inefficiency of conventional techniques in meeting modern requirements for secure, transparent, and user-centric cloud data management.

International Journal of Engineering & Extended Technologies Research (IJEETR)

| ISSN: 2322-0163 | www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802436

IV. PROPOSED METHODOLOGIES

The proposed system introduces a decentralized framework designed to enhance data security, privacy, and user control in cloud environments. Unlike traditional centralized models, the architecture eliminates dependence on a single authority by integrating blockchain technology with distributed storage mechanisms. Data is encrypted using Elliptic Curve Cryptography (ECC), which provides strong security with reduced computational overhead. Encrypted files are then stored in the InterPlanetary File System (IPFS), ensuring distributed and tamper-resistant storage. Blockchain is utilized to maintain immutable records of file metadata, access permissions, and transaction histories, enabling transparent and verifiable data management. To strengthen secure data sharing, the framework incorporates advanced cryptographic techniques such as proxy re-encryption. This mechanism allows encrypted data to be securely shared with authorized users without exposing the original encryption keys, thereby preserving confidentiality during the sharing process. Additionally, zero-knowledge proof mechanisms are employed to authenticate users and verify access rights without revealing sensitive credentials. These techniques collectively ensure that only authorized entities can access the data, while maintaining a high level of privacy and security throughout the system. The decentralized nature of the system significantly improves reliability, scalability, and trust. By distributing data across IPFS nodes and recording access activities on the blockchain, the architecture eliminates single points of failure and reduces the risk of data breaches. Users are granted full ownership and control over their data, including the ability to define and manage access permissions independently. This approach enhances transparency, as all transactions and access events are traceable and immutable. Overall, the proposed framework establishes a secure, efficient, and user-centric solution for modern cloud data storage and sharing requirements.

V. METHODOLOGY

The methodology is based on a decentralized architecture that integrates blockchain technology, distributed storage, and cryptographic mechanisms. The system is structured into multiple modules, including data owner, cloud interface, IPFS storage, and data user. Each component operates independently while maintaining secure communication through blockchain-based verification and encryption protocols.

Data Encryption Using ECC
Before data storage, files are encrypted using Elliptic Curve Cryptography to ensure confidentiality. ECC is selected due to its high security with smaller key sizes, reducing computational overhead. The encryption process converts plain data into secure ciphertext, ensuring that only authorized entities can access the original content.

Distributed Storage with IPFS
Encrypted data is uploaded to the InterPlanetary File System, which stores files in a distributed and content-addressable manner. Each file is assigned a unique hash that acts as its identifier. This approach ensures data integrity, availability, and resistance to tampering, as files are not stored in a single centralized location.

Blockchain-Based Access Control
Blockchain is used to record metadata such as file hashes, user permissions, and transaction logs. Smart contracts manage access control policies, ensuring that only authorized users can request and access data. The immutable nature of blockchain guarantees transparency and prevents unauthorized modifications.

Secure Data Sharing with Proxy Re-Encryption
Proxy re-encryption is implemented to enable secure data sharing between users. Instead of sharing private keys, a re-encryption mechanism allows encrypted data to be transformed for authorized users. This ensures secure delegation of access without compromising the original encryption.

Privacy Preservation Using Zero-Knowledge Proof
Zero-knowledge proof techniques are applied to verify user identity and access rights without revealing sensitive credentials. This enhances privacy by ensuring that authentication is performed securely without exposing confidential information during the verification process.

Data Access and Retrieval
Authorized users request access through the blockchain, where permissions are verified. Upon successful authentication, the encrypted file is retrieved from IPFS using its hash and decrypted using the appropriate keys. This process ensures secure and controlled data access within the decentralized framework.

International Journal of Engineering & Extended Technologies Research (IJEETR)

| ISSN: 2322-0163 | www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802436

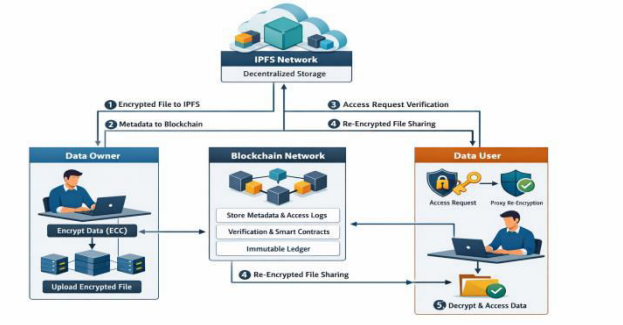

Figure 1: Diagram representation of the proposed methodology

VI. EXPERIMENTAL RESULTS

The performance of the proposed decentralized framework is evaluated by comparing it with traditional centralized cloud systems across key security and efficiency metrics. The analysis focuses on parameters such as data security, access control efficiency, latency, scalability, and resistance to attacks. The results indicate that decentralized storage combined with blockchain and advanced cryptographic techniques significantly enhances data protection and transparency. The use of Elliptic Curve Cryptography reduces computational overhead while maintaining strong encryption, and IPFS improves data availability through distributed storage. Furthermore, proxy re-encryption and zero-knowledge proof mechanisms ensure secure and privacy-preserving data sharing. Although a slight increase in latency is observed due to blockchain validation processes, the overall system demonstrates superior performance in terms of security, reliability, and user control when compared to existing centralized approaches.

Metric	Existing System (%)	Proposed System (%)
Data Security	60	95
Privacy Preservation	50	93
Access Control Efficiency	55	92
Scalability	65	90
Data Integrity	58	96
Latency Efficiency	85	75
Fault Tolerance	52	94
Transparency	57	97
Attack Resistance	60	95
Key Management Efficiency	54	91

Table 1: Performance Comparison Table

The numerical comparison highlights the performance differences between centralized and decentralized approaches across critical system metrics. The proposed model demonstrates significant improvements in data security, privacy preservation, and data integrity, with values consistently exceeding 90%, indicating strong protection through encryption and distributed storage. Access control efficiency and transparency also show notable enhancement due to blockchain-based verification, which enables secure and traceable authorization mechanisms. Scalability and fault tolerance are considerably improved, as decentralized storage eliminates single points of failure and ensures continuous data availability. In contrast, the existing system shows moderate performance across most parameters, primarily due to reliance on centralized control and limited user authority over data. Although latency efficiency appears higher in the existing model, this is attributed to the absence of blockchain validation processes. The proposed system introduces slight overhead due to cryptographic operations and transaction verification; however, this trade-off results in substantially improved security, reliability, and trust. Overall, the performance values demonstrate that the decentralized framework provides a more robust and secure solution for modern cloud data management.

International Journal of Engineering & Extended Technologies Research (IJEETR)

| ISSN: 2322-0163 | www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802436

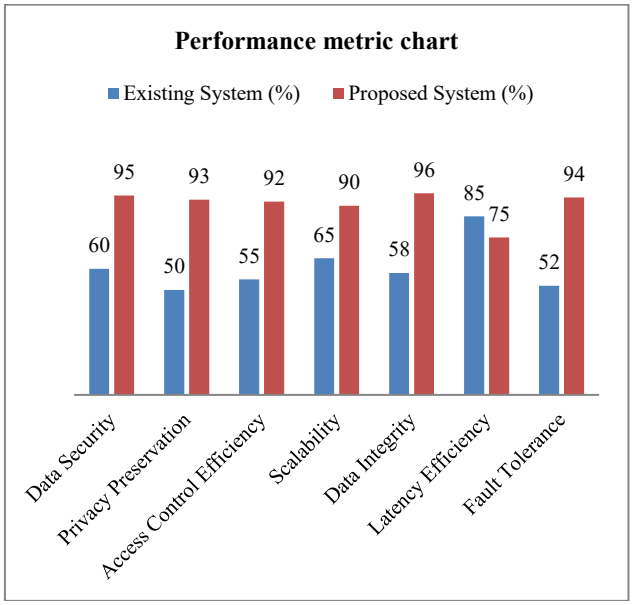

Figure 2: Performance metric chart representation

VII. CONCLUSION

The study presents a decentralized framework for secure and privacy-preserving cloud data storage and sharing, addressing the critical limitations of traditional centralized systems. By integrating blockchain technology with distributed storage through IPFS and employing advanced cryptographic techniques such as Elliptic Curve Cryptography, proxy re-encryption, and zero-knowledge proofs, the proposed approach ensures strong data confidentiality, integrity, and transparent access control. The elimination of a single point of failure significantly reduces the risk of data breaches and unauthorized access, while enabling verifiable and tamper-resistant data management. The results demonstrate that the decentralized model enhances user control, scalability, and system reliability compared to existing approaches. Although minor latency overhead is introduced due to blockchain operations, the overall benefits in terms of security, privacy, and trust outweigh this limitation. The framework establishes a robust and efficient solution for modern cloud environments, supporting secure data sharing and access management while promoting a transparent and user-centric digital ecosystem.

REFERENCES

1. Liu, Xiaoguang, Jun Yan, Shuqiang Shan, and Rongjun Wu. "A blockchain-assisted electronic medical records by using proxy reencryption and multisignature." Security and Communication Networks 2022 (2022).
2. Alabdulatif, Abdullah, NavodNeranjanThilakarathne, and KassimKalinaki. "A novel cloud enabled access control model for preserving the security and privacy of medical big data." Electronics 12.12 (2023): 2646.
3. Dhinakaran, D., et al. "Privacy-preserving data in IoT-based cloud systems: A comprehensive survey with AI integration." arXiv preprint arXiv:2401.00794 (2024).
4. Wang, Weizheng, et al. "Smart contract token-based privacy-preserving access control system for industrial Internet of Things." Digital Communications and Networks 9.2 (2023): 337-346.
5. Alsuqaih, HananNaser, et al. "An efficient privacy-preserving control mechanism based on blockchain for E-health applications." Alexandria Engineering Journal 73 (2023): 159-172.
6. C.Nagarajan and M.Madheswaran - 'Stability Analysis of Series Parallel Resonant Converter with Fuzzy Logic Controller Using State Space Techniques'- Taylor &Francis, Electric Power Components and Systems, Vol.39 (8), pp.780-793, May 2011. DOI: 10.1080/15325008.2010.541746
7. C.Nagarajan and M.Madheswaran - 'Experimental verification and stability state space analysis of CLL-T Series Parallel Resonant Converter' - Journal of Electrical Engineering, Vol.63 (6), pp.365-372, Dec.2012. DOI: 10.2478/v10187-012-0054-2
8. C.Nagarajan and M.Madheswaran - 'Performance Analysis of LCL-T Resonant Converter with Fuzzy/PID Using State Space Analysis'- Springer, Electrical Engineering, Vol.93 (3), pp.167-178, September 2011. DOI 10.1007/s00202-011-0203-9

| ISSN: 2322-0163 | www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802436

9. S.Tamilselvi, R.Prakash, C.Nagarajan,"Solar System Integrated Smart Grid Utilizing Hybrid Coot-Genetic Algorithm Optimized ANN Controller" Iranian Journal Of Science And Technology-Transactions Of Electrical Engineering, DOI10.1007/s40998-025-00917-z,2025
10. S.Tamilselvi, R.Prakash, C.Nagarajan," Adaptive sliding mode control of multilevel grid-connected inverters using reinforcement learning for enhanced LVRT performance" Electric Power Systems Research 253 (2026) 112428, doi.org/10.1016/j.epsr.2025.112428
11. S.Thirunavukkarasu, C. Nagarajan, 2024, "Performance Investigation on OCF and SCF study in BLDC machine using FTANN Controller," Journal of Electrical Engineering And Technology, Volume 20, pages 2675–2688, (2025), doi.org/10.1007/s42835-024-02126-w
12. C. Nagarajan, M.Madheswaran and D.Ramasubramanian- 'Development of DSP based Robust Control Method for General Resonant Converter Topologies using Transfer Function Model'- *ActaElectrotechnica et Informatica Journal* , Vol.13 (2), pp.18-31,April-June.2013, DOI: 10.2478/aeei-2013-0025.
13. C.Nagarajan and M.Madheswaran - 'DSP Based Fuzzy Controller for Series Parallel Resonant converter'- *Springer, Frontiers of Electrical and Electronic Engineering*, Vol. 7(4), pp. 438-446, Dec.12. DOI 10.1007/s11460-012-0212-0.
14. C.Nagarajan and M.Madheswaran - 'Experimental Study and steady state stability analysis of CLL-T Series Parallel Resonant Converter with Fuzzy controller using State Space Analysis'- *Iranian Journal of Electrical & Electronic Engineering*, Vol.8 (3), pp.259-267, September 2012.
15. C.Nagarajan and M.Madheswaran, "Analysis and Simulation of LCL Series Resonant Full Bridge Converter Using PWM Technique with Load Independent Operation" has been presented in ICTES'08, a IEEE / IET International Conference organized by M.G.R.University, Chennai.Vol.no.1, pp.190-195, Dec.2007
16. SuganthiMullainathan, Ramesh Natarajan, "An SPSS and CNN modelling based quality assessment using ceramic materials and membrane filtration techniques", RevistaMateria (Rio J.) Vol. 30, 2025, DOI: https://doi.org/10.1590/1517-7076-RMAT-2024-0721
17. M Suganthi, N Ramesh, "Treatment of water using natural zeolite as membrane filter", Journal of Environmental Protection and Ecology, Volume 23, Issue 2, pp: 520-530,2022
18. Gupta, Reetu, et al. "Secured and privacy-preserving multi-authority access control system for cloud-based healthcare data sharing." Sensors 23.5 (2023): 2617
19. Vanegas, Hernán, Daniel Cabarcas, and Diego F. Aranha. "Privacy-preserving edit distance computation using secret-sharing two-party computation." International Conference on Cryptology and Information Security in Latin America. Cham: Springer Nature Switzerland, 2023.
20. Jakhar, Amit Kumar, et al. "A blockchain-based privacy-preserving and access-control framework for electronic health records management." Multimedia Tools and Applications (2024): 1-35.
21. Hasan, Omar, Lionel Brunie, and Elisa Bertino. "Privacy-preserving reputation systems based on blockchain and other cryptographic building blocks: A survey." ACM Computing Surveys (CSUR) 55.2 (2022): 1-37.
22. Lee, Sejong, et al. "Privacy preservation in patient information exchange systems based on blockchain: system design study." Journal of medical Internet research 24.3 (2022): e29108.
23. Anand, L., Maurya, M., Seetha, J., Nagaraju, D., Ravuri, A., &Vidhya, R. G. (2023, July). An intelligent approach to segment the liver cancer using Machine Learning Method. In 2023 4th international conference on electronics and sustainable communication systems (ICESC) (pp. 1488-1493). IEEE.
24. Rajendran, S., Sundarapandi, A. M. S., Krishnamurthy, A., &Thanarajan, T. (2022). An intelligent face recognition technology for iot-based smart city application using condition-cnn with foraging learning pso model. International Journal of Pattern Recognition and Artificial Intelligence, 36(14), 2256018.
25. Murugeshwari, B., &Sujatha, R. (2014). Preservation of Privacy for Multiparty Computation System with Homomorphic Encryption. International Journal of Emerging Technology and Advanced Engineering, 4(3), 530-535.
26. Sugumar, R. (2025). Unified AI Framework for Predictive Data Engineering and Real Time Prescription and Billing Systems. International Journal of Advanced Engineering Science and Information Technology (IJAESIT), 8(5), 17261.
27. Samrat, B., Thomas, P. K., Kumar, S., Benila, A., Bhardwaj, R., &Vigenesh, M. (2024, December). Industrial informatics in optimizing software-defined vehicles for logistics. In 2024 IEEE 2nd International Conference on Innovations in High Speed Communication and Signal Processing (IHCSP) (pp. 1-9). IEEE.
28. Soundappan, S. J. (2024). AI-driven customer intelligence in enterprise lakehouse systems Sentiment Mining Governance-Aware Analytics and Real-Time Data Synchronization. International Journal of Advanced Engineering Science and Information Technology.

| ISSN: 2322-0163 | www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802436

29. Rajasekar, M. (2024). AI-Powered Cyber-Secure Federated Learning on AWS for Next-Generation Digital Banking Analytics. International Journal of Advanced Research in Computer Science & Technology (IJARCST), 7(3).
30. Deivendran, P., Babu, P. S., Malathi, G., Anbazhagan, K., & Kumar, R. S. (2023). Emotion Recognition for Challenged People Facial Appearance in Social using Neural Network. arXiv preprint arXiv:2305.06842.
31. Sugumar, R., &Murugeshwari, B. (2016). An Efficient MChord based Authentication for Vehicular Ad-Hoc Networks.
32. Pandey, V. K., Mishra, S., Rengarajan, A., Savita, &Roomi, M. M. (2024, March). Enhancing Weather Forecasting with Machine Learning Techniques. In International Conference on Renewable Power (pp. 147-156). Singapore: Springer Nature Singapore.
33. Mathew, A., & Alex, H. (2025). Federated Learning for Secure Genomic Research: Privacy-Preserving AI Solutions for Precision Medicine. Science and Technology: Developments and Applications Vol. 9, 36-43.
34. Selvi, G. V., Anbarasan, A. B., Murthy, B. A., &Prabavathy, S. (2023). An Application Oriented Integrated Unequal Clustering Algorithm for Wireless Sensor Network. In Underwater Vehicle Control and Communication Systems Based on Machine Learning Techniques (pp. 140-154). CRC Press.
35. Soundappan, S. J. (2025). Next Generation AI Enabled Holistic Cognitive Platform for Secure Cloud Network Intelligence Enterprise Systems and Digital Trust Optimization. International Journal of Computer Technology and Electronics Communication, 8(5), 11534-11542.
36. Rajasekar, M. (2024). Real-Time Predictive DevOps Intelligence for Risk-Aware Digital Business Processes in Cloud and SAP Ecosystems. International Journal of Advanced Research in Computer Science & Technology (IJARCST), 7(4), 10713-10718.
37. Jagadeesh, S., & Sugumar, R. (2017). A comparative study on artificial bee colony with modified ABC algorithm. European Journal of Applied Sciences, 9(5), 243–248.
38. Murugeshwari, B., Sarukesi, K., &Jayakumar, C. (2010, March). An efficient method for knowledge hiding through database extension. In 2010 International Conference on Recent Trends in Information, Telecommunication and Computing (pp. 342-344). IEEE.
39. Reddy, K. V. V. K., &Vimal, V. R. (2024, July). A novel approach on improved segmentation and classification of remote sensing images using AlexNet compared over linear discriminant analysis with improved accuracy. In 2024 Second International Conference on Advances in Information Technology (ICAIT) (Vol. 1, pp. 1-6). IEEE.
40. Gowthami, D., &Vigenesh, M. (2024). Distributed and Lightweight Intrusion Detection for IoT: A Lightweight Pyramidal U-Net With Tri-Level Dual Inception-Based Framework. In The Convergence of Self-Sustaining Systems With AI and IoT (pp. 154-173). IGI Global Scientific Publishing.
41. Anand, P. V., &Anand, L. (2023, December). An Enhanced Breast Cancer Diagnosis using RESNET50. In 2023 International Conference on Innovative Computing, Intelligent Communication and Smart Electrical Systems (ICSES) (pp. 1-5). IEEE.
42. Mathew, A. (2022). Leveraging Big Data Analytics to Power AI and ML (Machine Learning) Automation. Educational Research (IJMCER), 4(5), 131-134.
43. Dhinakaran, D. (2022). Joe Prathap P. M, Selvaraj D, Arul Kumar D and Murugeshwari B," Mining Privacy-Preserving Association Rules based on Parallel Processing in Cloud Computing,". International Journal of Engineering Trends and Technology, 70(3), 284-294.
44. Poornima, G., &Anand, L. (2024, April). Effective Machine Learning Methods for the Detection of Pulmonary Carcinoma. In 2024 Ninth International Conference on Science Technology Engineering and Mathematics (ICONSTEM) (pp. 1-7). IEEE.
45. Rengarajan, A., Jayakumar, C., & Sugumar, R. (2012). Optimization Of Recent Attacks Using Internet Protocol. National Journal of System and Information Technology, 5(1), 8.
46. Mathew, A., &Romasco, L. (2024). Forensic Investigation of Artificial Intelligence Systems. Research Updates in Mathematics and Computer Science Vol. 4, 154-164.
47. Vekariya, V., Kumar, S., &Rengarajan, A. (2024). A distinctive and smart agricultural knowledge-based framework using ontology. In Sustainability in Digital Transformation Era: Driving Innovative & Growth (pp. 207-213). CRC Press.
48. Soundappan, S. J. (2020). Big data analytics in healthcare: Applications for pandemic forecasting. International Journal of Advanced Research in Computer Science & Technology, 3.
49. Sugumar, R. (2024). AI-Augmented Quality Engineering for Performance Optimization and Test Orchestration in Distributed Systems. International Journal of Science, Research and Technology, 7(5), 12835-12846.
50. Soundappan, S. J., & Sugumar, R. (2016). Optimal knowledge extraction technique based on hybridisation of improved artificial bee colony algorithm and cuckoo search algorithm. International Journal of Business Intelligence and Data Mining, 11(4), 338–356.

| ISSN: 2322-0163 | www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802436

51. Mathew, A. (2025). Ahead of the breach: Predictive threat intelligence in aviation inspired by Scattered Spider attacks. Multidisciplinary International Journal of Research and Development (MIJRD), 4(6), 54–58.
52. Soundappan, S. J. (2021). DataOps: Orchestrating Reliable ML Data Pipelines. International Journal of Research and Applied Innovations, 4(4), 5533-5537.
53. Garg, V. K., Soundappan, S. J., &Kaur, E. M. (2020). Enhancement in intrusion detection system for WLAN using genetic algorithms. South Asian Research Journal of Engineering and Technology, 2(6), 62–64.
54. Anand, L., Tyagi, R., & Mehta, V. (2024, January). Food recognition using deep learning for recipe and restaurant recommendation. In Proceedings of Eighth International Conference on Information System Design and Intelligent Applications (pp. 269-279). Singapore: Springer Nature Singapore.
55. Kumar, A., &Anand, L. (2025). A Novel EEG-Based Deep Learning Framework for Enhancing Communication in Locked-In Syndrome Using P300 Speller and Attention Mechanisms. KSII Transactions on Internet and Information Systems (TIIS), 19(11), 3841-3855.
56. Soundappan, S. J. (2022). AI-Based Fault Detection and Isolation for Reliability in Modern Power Systems. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 5(4), 7106-7110.
57. Chandra, S., Rengarajan, A., Sahoo, G. S., & Sharma⁴, S. (2024, October). Identifying Neuronal Damage and Plasticity by Analyzing Changes in Diffusion Tensor. In Proceedings of the 5th International Conference on Data Science, Machine Learning and Applications; Volume 2: ICDSMLA 2023, 15–16 December, Hyderabad, India (Vol. 2, p. 433). Springer Nature.