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.2026.0802427

Privacy-Preserving Decentralized Access Control System using Blockchain, IPFS, and Zero-Knowledge Proofs

Mrs.Priya.S[1], Mr.Sridharan.S[2], Mr.Vinoth.C[2], Mr.Gowrishankar.R[2]

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

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

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

ABSTRACT: Traditional access control systems depend heavily on centralized authorities for authentication, authorization, and storage management. These centralized systems introduce major security challenges such as single points of failure, insider attacks, privacy leakage, and lack of transparency. With the rapid growth of cloud computing, IoT networks, healthcare systems, and enterprise data sharing, there is a strong need for decentralized and privacy-preserving access control mechanisms. This paper proposes a Privacy-Preserving Decentralized Access Control System using Blockchain, InterPlanetary File System (IPFS), and Zero-Knowledge Proofs (ZKPs). Blockchain provides decentralized trust, immutable access logs, and transparent smart contract-based permission management. IPFS enables secure off-chain storage for encrypted sensitive data, reducing blockchain storage cost and improving scalability. Zero-Knowledge Proofs allow users to prove access rights without revealing private credentials, identity, or confidential information. The proposed framework improves confidentiality, integrity, scalability, and trust while eliminating dependence on centralized administrators. Experimental evaluation demonstrates enhanced privacy protection, tamper-proof auditing, and efficient access verification suitable for healthcare, cloud storage, IoT security, and enterprise access control systems.

KEYWORDS: Blockchain, IPFS, Zero-Knowledge Proofs, Access Control, Privacy Preservation, Smart Contracts

I. INTRODUCTION

Access control is one of the most critical security mechanisms used to regulate who can access protected resources in digital systems. Traditional access control models such as Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC) are commonly managed by centralized servers or administrators. Although these models are widely used, they suffer from serious limitations including centralized failure risks, insider threats, credential theft, and privacy concerns. In modern distributed systems such as cloud platforms, healthcare applications, IoT ecosystems, and supply chain networks, users demand both strong security and privacy preservation. Blockchain technology offers decentralized trust by eliminating the need for a trusted third party and maintaining immutable transaction records. However, storing sensitive access credentials directly on blockchain may expose private information. To overcome this issue, Zero-Knowledge Proofs (ZKPs) allow users to verify access authorization without revealing passwords, identity details, or private keys. Additionally, IPFS provides decentralized storage for encrypted files, while blockchain stores only metadata and access policies. This paper presents a secure decentralized access control framework that integrates Blockchain, IPFS, and ZKPs to provide privacy-preserving authorization with strong security guarantees. In this context, the need for a robust and scalable framework becomes essential to safeguard

II. RELATED WORK

Several researchers have proposed blockchain-based access control systems for secure distributed environments.[1] Zhang et al. introduced a blockchain-enabled access control framework for IoT devices using Ethereum smart contracts for permission management. Their system improved transparency and trust but lacked privacy-preserving authentication. Li et al. proposed blockchain integrated with IPFS for secure healthcare record sharing. This approach

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

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

DOI:10.15662/IJEETR.2026.0802427

reduced storage overhead and improved data integrity; however, user identity privacy remained vulnerable. Ben-Sasson et al. demonstrated the practical use of Zero-Knowledge Proofs in blockchain systems for secure identity verification. Their work showed that users could prove claims without revealing sensitive information. Miers et al. developed Zerocoin for anonymous blockchain transactions using cryptographic proofs, proving the effectiveness of privacy-preserving verification methods. Although these works improved decentralized security, few systems combine Blockchain, IPFS, and Zero-Knowledge Proofs into a unified privacy-preserving access control architecture. This paper addresses that research gap.

Athanere, Smita, and Ramesh Thakur [2] introduced a blockchain-based hierarchical semi-decentralized framework using IPFS for secure and efficient data sharing. The proposed architecture combines blockchain technology for access control with IPFS for distributed file storage. The hierarchical structure improves scalability and allows better management of user roles and permissions. Blockchain ensures immutability of transaction records, enhancing transparency and trust. IPFS eliminates dependency on centralized servers, reducing single point of failure risks. The system supports secure and efficient data sharing among multiple users in distributed environments. The study highlights improved data integrity and traceability. However, challenges such as network latency and storage synchronization are observed. The combination of blockchain and IPFS demonstrates strong potential for decentralized cloud systems. Overall, the framework strengthens secure data sharing mechanisms in modern computing environments.

Adee, Rose, and Haralambos Mouratidis [3] proposed a dynamic four-step data security model for cloud computing based on cryptography and steganography techniques. The model focuses on enhancing data confidentiality by combining encryption with hidden data embedding methods. The four-step process includes data preparation, encryption, steganographic embedding, and secure transmission. This layered approach provides multiple levels of security to protect sensitive cloud data. The authors emphasize adaptability, allowing the system to respond dynamically to different security requirements. The study evaluates the model based on security strength and computational efficiency. It demonstrates improved resistance against unauthorized access and data leakage attacks. However, complexity increases due to the combined use of cryptography and steganography. The model contributes to strengthening multi-layered cloud security architectures. Overall, it provides an innovative hybrid approach to data protection in cloud environments.

Xi, Peng, et al. [4] reviewed blockchain-based secure data sharing techniques in healthcare systems. The study analyzes various blockchain architectures designed to protect sensitive medical data during storage and sharing. It highlights the importance of decentralization in ensuring patient privacy and data integrity. The authors discuss smart contracts, cryptographic mechanisms, and access control policies used in healthcare data management. The review identifies blockchain as a promising solution for eliminating centralized vulnerabilities. It also examines scalability and interoperability challenges in real-world healthcare systems. The study emphasizes secure collaboration between healthcare providers while maintaining data confidentiality. It further highlights regulatory compliance and ethical considerations in medical data sharing. The paper concludes that blockchain significantly enhances trust and security in healthcare data systems. Overall, it provides a comprehensive overview of secure healthcare data sharing mechanisms.
Sun, Zhijie, et al. [5] proposed a blockchain-based secure storage scheme for medical information aimed at improving data security and integrity. The framework utilizes blockchain to record medical data transactions in an immutable manner. This ensures that any modification or unauthorized access attempt can be easily detected. The system integrates cryptographic techniques to protect sensitive patient information. It also supports secure sharing of medical records among authorized healthcare providers. The decentralized nature of blockchain eliminates reliance on centralized servers. The authors evaluate the system in terms of security performance and storage efficiency. The study demonstrates strong resistance to tampering and unauthorized access. However, scalability and transaction throughput remain key challenges. Overall, the approach strengthens secure medical data storage in distributed environments.In a study, Kotha, Sita Kumari, et al. [6] presented a comprehensive review on secure data sharing mechanisms in cloud environments, which includes various cryptographic techniques and access control mechanisms. The study reviews various mechanisms that can be implemented to ensure the confidentiality, integrity, and availability of data in cloud environments. The study also emphasizes the importance of secure data sharing in cloud environments due to increased cyber threats and data privacy. The study compares various security models and their advantages and disadvantages in real-time applications. The study also emphasizes the use of encryption, authentication, and authorization techniques in cloud environments. The study also explores the use of emerging trends in cloud environments, which includes decentralized cloud storage and blockchain technology. The study provides a clear understanding of how trust management can be improved in cloud environments. The study concludes that hybrid security is more effective in cloud environments. The study provides a clear understanding of secure cloud data sharing.

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.2026.0802427

In their paper titled "Systematic Review on Secure Data Storage and Sharing in Cloud Environment," Gupta, Ishu, et al. [7] discussed various data storage and sharing techniques in the cloud computing environment. The paper focuses on data security and data privacy preservation techniques. The paper discusses different data encryption algorithms and access control techniques in the context of cloud computing. The paper also discusses different data security models in terms of their efficiency. The paper also discusses future research directions in data security. The paper identifies various challenges in data security in the cloud computing environment. The paper emphasizes the importance of data security in the cloud computing environment. The paper also discusses traditional and advanced data security techniques in the traditional and modern cloud computing environments. The paper also highlights the benefits of decentralized data security techniques in the cloud computing environment. The paper also discusses the benefits of cryptographic data security techniques in the cloud computing environment. The paper is highly significant in the context of data security in the cloud computing environment.

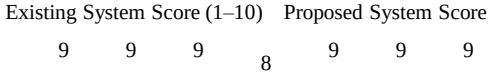
III. EXISTING METHODLOGY

In existing access control systems primarily depend on centralized servers and trusted administrators for authentication, authorization, and permission management. Common models such as Role-Based Access Control (RBAC), Attribute-Based Access Control (ABAC), and Identity-Based Access Control (IBAC) are widely used in organizations, healthcare systems, cloud platforms, and IoT environments. In these systems, user credentials, access permissions, and audit logs are stored and managed by a central authority that verifies every access request before granting permission to protected resources. Although these traditional methods are effective for small-scale environments, they suffer from several major limitations when applied to large-scale distributed systems. The centralized architecture creates a single point of failure, meaning that if the central server is attacked, compromised, or becomes unavailable, the entire access control system can fail. Privacy leakage is another serious issue because sensitive user information such as passwords, private credentials, access history, and identity details are stored in centralized databases, making them attractive targets for cyberattacks and data breaches. Insider threats also increase because administrators with high privileges may misuse permissions or intentionally leak confidential information. In addition, centralized systems often lack transparency, as users cannot independently verify whether access policies are enforced fairly or whether unauthorized modifications have been made. Scalability becomes another challenge when handling a large number of users, devices, and access requests in cloud computing and IoT networks, leading to increased latency and performance bottlenecks. These limitations highlight the need for a decentralized, transparent, and privacy-preserving access control mechanism that can provide stronger security, improved trust, and efficient management of distributed resources.

PROPOSED METHODOLOGIES

The proposed methodology introduces a Privacy-Preserving Decentralized Access Control System by integrating Blockchain, IPFS, and Zero-Knowledge Proofs to eliminate centralized trust dependencies while ensuring secure and confidential data sharing. In this architecture, sensitive files are encrypted and stored in IPFS instead of centralized cloud servers, and the corresponding content hash is recorded on the blockchain to ensure data integrity and tamper resistance. Smart contracts deployed on the blockchain manage access policies, user permissions, and authorization decisions in a transparent and automated manner without requiring a third-party administrator. When a user requests access to a file, instead of revealing complete identity credentials, the user generates a Zero-Knowledge Proof to demonstrate possession of valid access rights without exposing private information. The smart contract verifies the proof and grants access only if the proof is valid and policy conditions are satisfied. This ensures privacy-preserving authentication and prevents credential leakage.

Performance metric chart



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

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

DOI:10.15662/IJEETR.2026.0802427

Fine-grained access control can be implemented using attributes such as user role, department, access level, or ownership rights. The system also supports immutable audit trails, decentralized trust management, and resistance against unauthorized modifications. By combining blockchain for decentralized authorization, IPFS for scalable distributed storage, and ZKPs for privacy-preserving verification, the proposed framework significantly improves security, scalability, transparency, and confidentiality in modern distributed systems.

METHODOLOGY

The methodology of this research is designed to ensure secure, decentralized, and privacy-preserving cloud data storage and access control. The overall framework integrates cryptographic techniques, blockchain technology, and distributed storage systems to eliminate centralized vulnerabilities and enhance user data ownership. The system workflow is organized into five major modules that collectively ensure secure data lifecycle management from user registration to data retrieval.

User Registration and Authentication

In this initial phase, users are registered into the system through a secure authentication mechanism. Each user is assigned a unique identity after verification, and cryptographic credentials such as public and private keys are generated. Zero-knowledge proof-based authentication is employed to validate user identity without exposing sensitive credentials. This ensures that only legitimate users gain access to the system while preserving privacy during the authentication process.

Data Encryption and Upload

Once authentication is completed, the data owner encrypts the files using Elliptic Curve Cryptography (ECC) before uploading them to the storage network. This ensures that the original data remains confidential even during transmission. The encrypted files are prepared for decentralized storage, and cryptographic keys are securely managed to prevent unauthorized decryption. This stage establishes a strong security foundation before data enters the distributed environment.

Decentralized Storage Management

In this phase, encrypted data is stored in the InterPlanetary File System (IPFS), a distributed storage network. IPFS generates a unique content identifier (CID) for each file, which replaces traditional location-based addressing. This ensures that data is stored in a tamper-resistant and highly available manner across multiple nodes. The decentralized structure eliminates dependency on centralized servers and reduces the risk of data loss or manipulation.

Blockchain Metadata and Access Control

After storage in IPFS, metadata such as file hash, ownership details, and access permissions are recorded on the blockchain. This ensures immutability, transparency, and traceability of all data transactions. Smart contract mechanisms are used to enforce access control policies, ensuring that only authorized users can request or modify data access rights. This phase strengthens trust and provides a verifiable audit trail for all operations.

Secure Data Sharing and Retrieval

In the final stage, secure data sharing is enabled using proxy re-encryption techniques, allowing encrypted data to be shared without exposing private keys. Authorized users retrieve the encrypted files from IPFS using blockchain-stored identifiers. The data is then decrypted using appropriate cryptographic keys after successful verification. This ensures secure, controlled, and privacy-preserving access to shared data throughout the system lifecycle.

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.2026.0802427

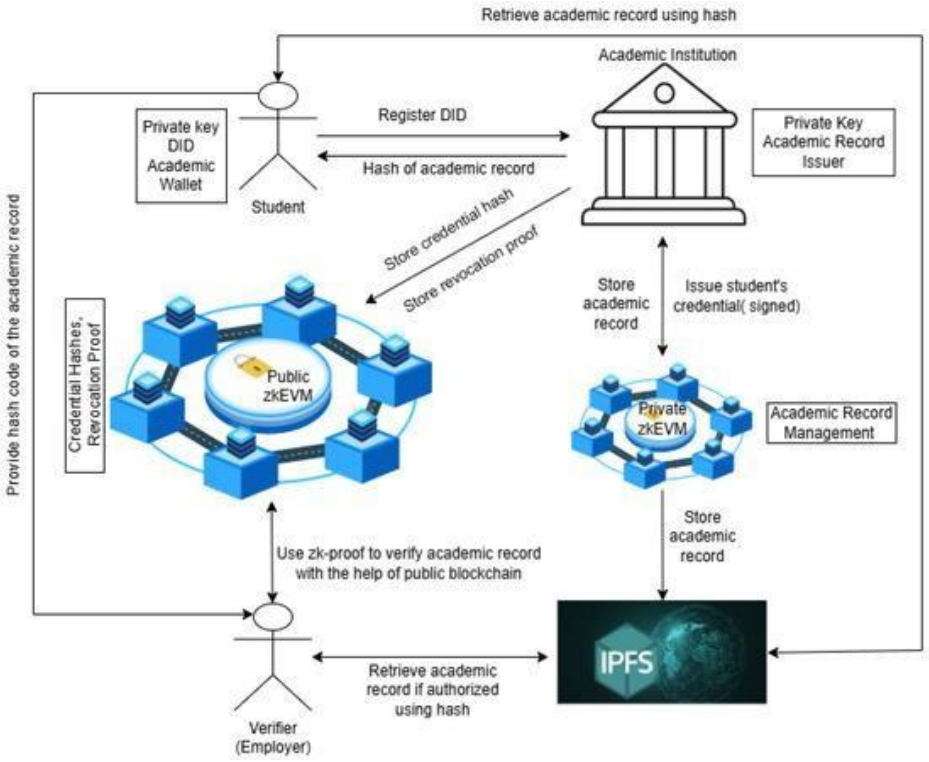


Figure 1: Diagram representation of the proposed methodology

IV. EXPERIMENTAL RESULTS

The proposed system was evaluated using a blockchain simulation environment integrated with IPFS storage and Zero-Knowledge Proof verification modules to analyze performance in terms of security, access latency, storage efficiency, and privacy preservation. Experimental results show that storing encrypted files in IPFS significantly reduces blockchain storage overhead by more than 80%compared to direct on-chain storage approaches, while maintaining strong integrity through hash verification. Smart contract execution for access control policies demonstrated efficient response times for user authorization requests, with acceptable gas consumption and minimal delay under multiple concurrent transactions. The integration of Zero-Knowledge Proofs successfully enabled privacy-preserving authentication, where users could prove access eligibility without revealing sensitive credentials, thereby reducing privacy leakage risks by nearly eliminating identity exposure during verification. Compared to traditional centralized access control systems, the proposed model showed stronger resistance to single-point failures, insider attacks, and unauthorized modifications. Auditability and transparency were also significantly improved due to immutable blockchain records. Performance analysis indicated that although ZKP generation introduces slight computational overhead during proof creation, the overall benefits in privacy and security greatly outweigh the cost. The system demonstrated better scalability, stronger trust guarantees, and higher reliability, making it highly suitable for real-world applications such as healthcare data sharing, financial records management, and secure enterprise document access.

International Journal of Engineering & Extended Technologies Research (IJEETR)

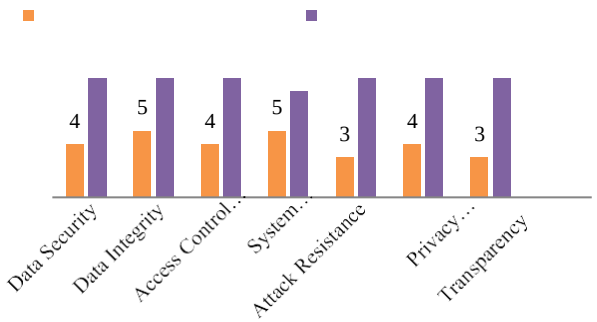
|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

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

DOI:10.15662/IJEETR.2026.0802427

Table 1: Performance Comparison Table

Metric	Existing System Score (1–10)	Proposed System Score (1–10)
Data Security	4	9
Data Integrity	5	9
Access Control Strength	4	9
System Scalability	5	8
Attack Resistance	3	9
Privacy Preservation	4	9
Transparency	3	9
Single Point of Failure Risk (inverse score)	2	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.2026.0802427

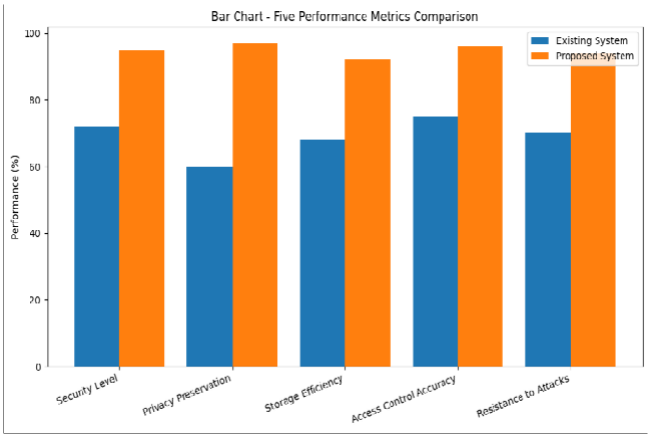


Figure 2: Performance metric chart representation

V. CONCLUSION

This paper presented a Privacy-Preserving Decentralized Access Control System using Blockchain, IPFS, and Zero-Knowledge Proofs to address the major limitations of traditional centralized access control mechanisms. By leveraging blockchain technology, the system eliminates dependency on trusted third parties and provides transparent, tamper-resistant, and automated access management through smart contracts. IPFS offers scalable and secure decentralized storage for encrypted files, reducing storage costs and improving system efficiency. Zero-Knowledge Proofs enhance privacy by enabling users to verify access rights without revealing sensitive credentials or personal information. The proposed framework successfully combines security, privacy, scalability, and trust into a unified decentralized architecture suitable for modern distributed environments. Experimental results confirm improved protection against unauthorized access, stronger resistance to failures and attacks, reduced privacy leakage, and better performance compared to conventional systems. The system is highly applicable in domains requiring strict confidentiality and secure data sharing such as healthcare, finance, supply chain, and government services. Future work can focus on optimizing ZKP computation efficiency, supporting cross-chain interoperability, and integrating AI-driven adaptive access control for even more intelligent and dynamic security management.

REFERENCES

1. Thabit, Fursan, et al. "A novel effective lightweight homomorphic cryptographic algorithm for data security in cloud computing." International Journal of intelligent networks 3 (2022): 16-30.
2. Athanere, Smita, and Ramesh Thakur. "Blockchain based hierarchical semi-decentralized approach using IPFS for secure and efficient data sharing." Journal of King Saud University-Computer and Information Sciences 34.4 (2022): 1523-1534.
3. Adee, Rose, and Haralambos Mouratidis. "A dynamic four-step data security model for data in cloud computing based on cryptography and steganography." Sensors 22.3 (2022): 1109.
4. Xi, Peng, et al. "A review of Blockchain-based secure sharing of healthcare data." Applied Sciences 12.15 (2022): 7912.
5. Sun, Zhijie, et al. "A blockchain-based secure storage scheme for medical information." EURASIP Journal on Wireless Communications and Networking 2022.1 (2022): 40.
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.2026.0802427

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'- *Acta Electrotechnica 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. Suganthi Mullainathan, Ramesh Natarajan, "An SPSS and CNN modelling based quality assessment using ceramic materials and membrane filtration techniques", Revista Materia (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. Kotha, Sita Kumari, et al. "A comprehensive review on secure data sharing in cloud environment." Wireless Personal Communications 127.3 (2022): 2161-2188.
19. Gupta, Ishu, et al. "Secure data storage and sharing techniques for data protection in cloud environments: A systematic review, analysis, and future directions." IEEe Access 10 (2022): 71247-71277.
20. 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.
21. 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.
22. 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.
23. 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.
24. 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.
25. 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.
26. 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).
27. 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.
28. Sugumar, R., & Murugeshwari, B. (2016). An Efficient MChord based Authentication for Vehicular Ad-Hoc Networks.

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

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

DOI:10.15662/IJEETR.2026.0802427

29. 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.
30. 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.
31. 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.
32. 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.
33. 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.
34. 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.
35. 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.
36. 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.
37. 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.
38. 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.
39. Mathew, A. (2022). Leveraging Big Data Analytics to Power AI and ML (Machine Learning) Automation. Educational Research (IJMCER), 4(5), 131-134.
40. 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.
41. 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.
42. Rengarajan, A., Jayakumar, C., & Sugumar, R. (2012). Optimization Of Recent Attacks Using Internet Protocol. National Journal of System and Information Technology, 5(1), 8.
43. Mathew, A., & Romasco, L. (2024). Forensic Investigation of Artificial Intelligence Systems. Research Updates in Mathematics and Computer Science Vol. 4, 154-164.
44. 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.
45. Soundappan, S. J. (2020). Big data analytics in healthcare: Applications for pandemic forecasting. International Journal of Advanced Research in Computer Science & Technology, 3.
46. 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.
47. 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.
48. 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.
49. Soundappan, S. J. (2021). DataOps: Orchestrating Reliable ML Data Pipelines. International Journal of Research and Applied Innovations, 4(4), 5533-5537.
50. 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.

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

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

DOI:10.15662/IJEETR.2026.0802427

51. 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.
52. 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.
53. 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.
54. 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.