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.2026.0802380

# Secure and Unified AI-Blockchain Voting System with Real-Time Verification

**Varshini[1], Mrs. P. ArasI, M.E., [2]**

M.E., Department of Computer Science and Engineering – Roever Engineering College, Perambalur, Tamil Nadu, India[1]

Assistant Professor, Department of CSE, Roever Engineering College, Perambalur, Tamil Nadu, India[2]

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

**ABSTRACT:** Voting is a fundamental pillar of democracy, but traditional system faces challenges including tampering, slow vote counting, delayed results, and lack of transparency. This project proposes a secure, transparent, and efficient electronic voting system that leverages advanced technologies such as blockchain, biometrics, and encryption to address the challenges of traditional voting methods. The system ensures voter authentication through multi-factor verification, including QR code scanning and facial recognition. Once authenticated, votes are encrypted using 256-bit SHA hash codes and stored on a tamper-proof blockchain, ensuring vote immutability and security. The self-tallying mechanism automates the vote counting process, providing rapid and error-free results. Additionally, the system includes real-time vote integrity verification, SMS notifications for tampering detection, and detailed audit reports for complete transparency.

**KEYWORDS:** Python 3.8, TensorFlow, Keras, Flask, NumPy, Pandas, Matplotlib, Scikit-learn, MySQL, OpenCV (for face recognition), JSON.

## I. INTRODUCTION

In the digital age, the integrity, transparency, and efficiency of voting systems have become critical challenges for democratic processes worldwide. Traditional voting mechanisms, whether paper-based or electronic, often suffer from vulnerabilities such as fraud, tampering, delayed result verification, and lack of trust among voters. Recent advancements in blockchain technology and artificial intelligence (AI) offer promising solutions to address these challenges.

Blockchain provides a decentralized and immutable ledger, ensuring that each vote is securely recorded and cannot be altered, while AI facilitates real-time verification, anomaly detection, and intelligent auditing of voting patterns. By integrating AI with blockchain, it is possible to design a secure and unified voting system that guarantees transparency, enhances voter trust, and provides instant verification of election results. Such a system can overcome the limitations of conventional voting methods, enabling more secure, efficient, and accessible elections on a global scale.

This paper proposes a comprehensive framework for a Secure and Unified AI-Blockchain Voting System with Real-Time Verification, highlighting its architecture, security protocols, and real-time verification capabilities. The proposed system aims to combine the strengths of AI and blockchain to deliver a robust, tamper-proof, and trustworthy electoral process, laying the foundation for next-generation digital democracy.

## II. LITERATURE SURVEY

### 2.1. Title: Secure Online Voting System-Based on Facial Recognition by Using Deep Learning

The study by Krishna Prakash and co-authors (2025) focuses on designing a secure, reliable, and transparent online voting system for corporate elections by integrating deep learning–based facial recognition with OTP authentication. The system aims to eliminate fraudulent voting and unauthorized access by combining computer vision techniques with employee-specific identifiers such as employee ID and biometric data. The methodology incorporates real-time vote validation along with OTP-based verification to ensure security and transparency.

The system utilizes the Haar Cascade Classifier for efficient face detection and Convolutional Neural Networks (CNNs) for accurate facial recognition. A custom dataset consisting of employee facial images under varying

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

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

DOI:10.15662/IJEETR.2026.0802380

orientations and lighting conditions was used to improve robustness. The findings indicate a high facial verification accuracy of 98%, demonstrating superior reliability compared to traditional systems. The proposed system enhances transparency, prevents impersonation, and supports remote voting, although it depends heavily on stable internet connectivity and good image quality, with data privacy remaining a concern.

**2.2. Title: A Comprehensive Evaluation of Secured Electronic Voting System Design Based on Face Biometric Authentication Policy**

Similarly, the research conducted by Pandarinath Potluri and colleagues (2024) presents a comprehensive evaluation of a secured electronic voting system based on face biometric authentication. The objective is to ensure secure, transparent, and efficient voting by verifying voter identity through biometric methods. The methodology integrates both hardware and software components, including cameras, biometric databases, and encryption-based communication protocols. It employs deep learning algorithms for face detection and recognition, along with anti-spoofing techniques and multi-factor authentication.

The system architecture encompasses voter registration, ballot generation, secure vote casting, and encrypted vote counting. Using a biometric dataset of registered voters, the model achieved a recognition accuracy of 96%, proving its effectiveness in minimizing impersonation and vote duplication. The system offers advantages such as enhanced security, transparency, and reduced human error, but faces challenges like the need for high-quality equipment, stable connectivity, and concerns regarding privacy and data protection.

**2.3. Title: Next Generation Voting Approach: A Secured Biometric Voting System**

The study by Manoj A and co-authors (2024) aims to modernize state elections by introducing a biometric voting system that enables voters to securely cast their votes from any nearby polling station, regardless of their constituency. The proposed system integrates fingerprint and facial recognition technologies using hardware components such as the R307 Optical Fingerprint Reader, RFID, and a Raspberry Pi microcontroller. Aadhaar-based voter verification is incorporated to ensure voter legitimacy, while real-time data processing helps prevent duplicate voting. The system employs biometric authentication algorithms for both fingerprint and facial recognition, along with secure communication protocols for data validation and transmission.

A dataset consisting of voter fingerprints and facial images linked with Aadhaar data is used for system verification and testing. The findings demonstrate that the system is highly secure and efficient, offering accurate voter authentication and improved accessibility for voters in remote areas while maintaining privacy. The system enhances election transparency, prevents duplication, supports remote voting, and provides a scalable and user-friendly solution; however, it involves high setup costs due to biometric devices and infrastructure requirements, and may face implementation challenges in regions with poor connectivity or limited digital literacy.

## III. RESEARCH METHODOLOGY

The proposed Secure and Unified AI-Blockchain Voting System with Real-Time Verification follows a hybrid architecture integrating Artificial Intelligence (AI) and Blockchain technologies to ensure secure, transparent, and tamper-proof voting. The methodology is structured into key phases including voter registration, authentication, vote casting, blockchain integration, and performance evaluation, supported by advanced algorithms, techniques, and security mechanisms. In the initial phase, voter registration is carried out using biometric data such as facial images and/or fingerprints along with unique identification credentials. Data preprocessing techniques including image normalization, histogram equalization, and noise filtering are applied to enhance image quality. For biometric recognition, algorithms such as Haar Cascade Classifier are used for face detection, while Convolutional Neural Networks (CNNs) are employed for high-accuracy facial recognition and feature extraction. In addition, Local Binary Pattern (LBP) techniques may be used for texture-based feature enhancement.

During the authentication phase, the system adopts a multi-factor authentication mechanism combining AI-based facial recognition and One-Time Password (OTP) verification. The CNN model performs feature matching between live-captured images and stored templates, while liveness detection techniques such as blink detection and motion analysis are implemented to prevent spoofing attacks. Secure communication protocols, including Transport Layer Security (TLS), are used to protect data transmission. For vote casting, blockchain technology is utilized as the core security mechanism. Each vote is encrypted using Advanced Encryption Standard (AES) and digitally signed using asymmetric cryptography (RSA/ECC). The encrypted vote is then converted into a blockchain transaction and recorded using smart contracts. Consensus algorithms such as Proof of Authority (PoA) or Proof of Stake (PoS) are implemented to validate transactions efficiently while maintaining system integrity. Cryptographic hashing techniques (e.g., SHA-256) ensure immutability and prevent data tampering.

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.2026.0802380

Real-time verification is achieved through immediate validation and addition of votes to the distributed ledger, enabling transparent monitoring without revealing voter identity. Privacy-preserving mechanisms such as anonymization and zero-knowledge proof (ZKP) techniques are incorporated to ensure voter confidentiality while maintaining auditability. Additionally, role-based access control (RBAC) is implemented to restrict system access to authorized entities only.

The system integrates both hardware and software components, including cameras, biometric sensors, and web-based interfaces, ensuring seamless interaction between users and the voting platform. A custom dataset containing biometric data is used for training and validation to improve system robustness under diverse environmental conditions.

Finally, system performance is evaluated using metrics such as accuracy, precision, recall, authentication time, transaction latency, scalability, and resistance to attacks. Experimental analysis demonstrates the effectiveness of the proposed system in enhancing security, preventing fraud, and ensuring reliable real-time voting.

## IV. ARCHITECTURE

**System Architecture**

The proposed Secure and Unified AI-Blockchain Voting System with Real-Time Verification is designed as a multi-layered architecture that ensures transparency, security, and efficiency throughout the electoral process. The system integrates Election Commission operations, voter interaction modules, verification mechanisms, and blockchain-based vote storage.

At the top level, the Election Commission (ECI) module acts as the administrative control unit. It includes functionalities such as adding candidates, assigning polling officers (PO), returning officers (RO), and polling booths. The system also supports Aadhaar integration and secure login for authorized personnel. These operations ensure proper election setup and management.

The architecture incorporates a verification and processing layer, which includes advanced modules such as:

- **Fingerprint (FP) Verification** and **QR Verification** for voter authentication
- **Self-tallying mechanism** to automatically count votes
- **Ballot Chain system**, which ensures that each vote is securely linked in sequence
- **Blockchain module**, which stores votes in an immutable and tamper-proof distributed ledger
- **Aadhaar Database**, used for identity validation and duplication prevention

The SMS Generator module enhances communication by sending real-time notifications to voters regarding voting status and authentication. This ensures transparency and user awareness.

At the user level, citizens interact with the system via secure interfaces. They receive SMS notifications (BVL SMS) and proceed to cast their votes digitally. The voting process is authenticated through multi-factor verification mechanisms, ensuring that only eligible voters can participate.

The central cloud infrastructure acts as the backbone of the system, facilitating data storage, synchronization, and secure communication between modules. It connects all stakeholders, including the Election Commission, polling booths, and verification systems.

At the polling booth level, dedicated modules are deployed for:

- Voter verification
- Login authentication
- Voting list display
- Vote casting status tracking
- Real-time vote counting
- Statistical analysis of votes

The system also defines roles such as Polling Officers, Presiding Officers, and Returning Officers, each interacting with the system based on their responsibilities. These roles ensure smooth election execution and monitoring.
Overall, the architecture emphasizes security (via blockchain and biometrics), transparency (real-time updates and statistics), and efficiency (automated counting and verification), making it highly suitable for modern digital election systems.

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.2026.0802380

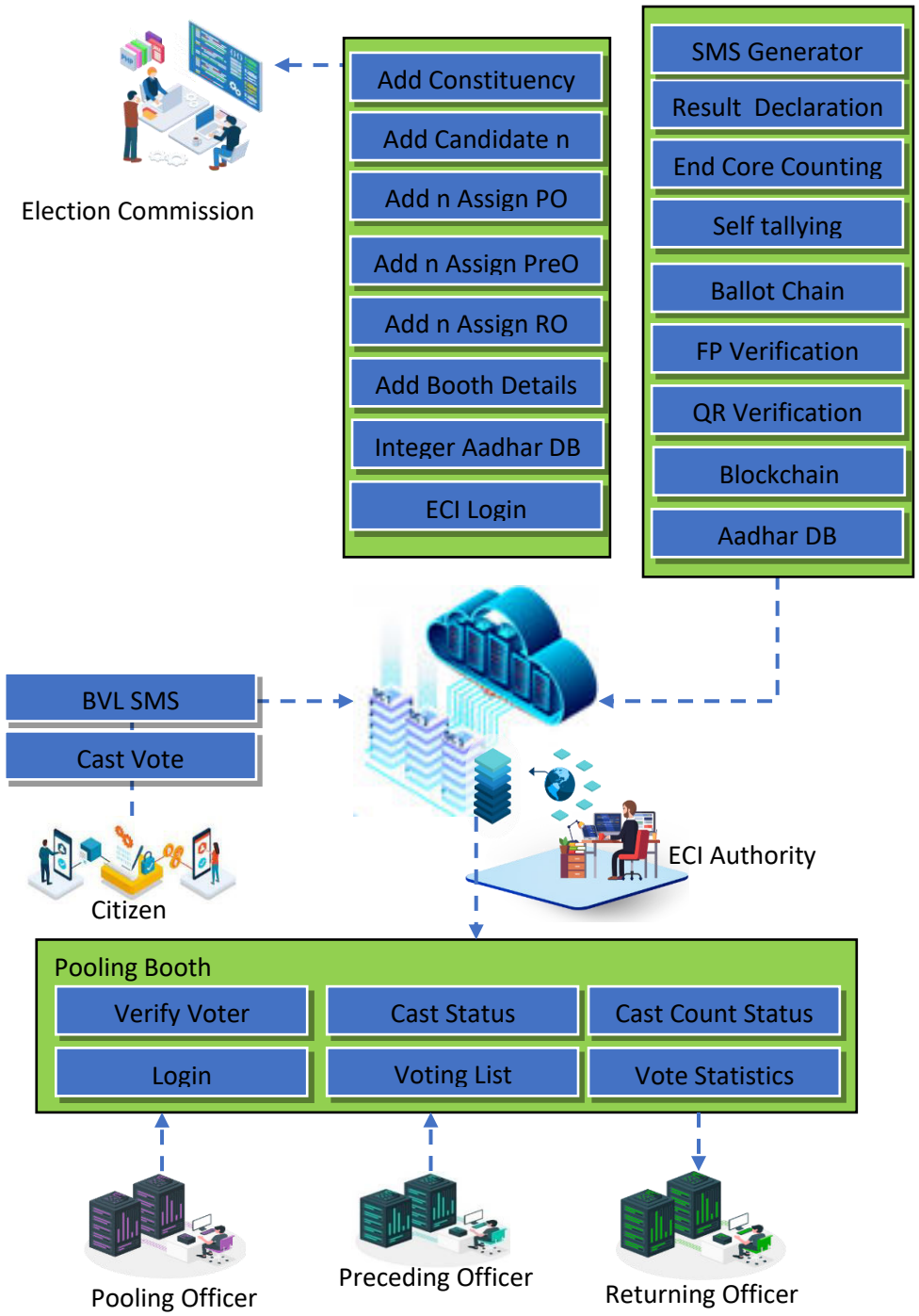


**Fig. 4. System Architecture**

## V. RESULTS AND DISCUSSION

### 5.1 Experimental Results

The proposed Secure AI–Blockchain Voting System was implemented and evaluated under a simulated election environment involving multiple users, polling stations, and administrative roles. The system successfully demonstrated secure voter authentication, transparent vote casting, and real-time result generation.

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

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

DOI:10.15662/IJEETR.2026.0802380

The multi-factor authentication mechanism, which integrates Aadhaar-based validation, fingerprint verification, and QR code scanning, achieved a high level of accuracy in identifying legitimate voters. Unauthorized access attempts were effectively blocked, ensuring that only verified individuals could participate in the voting process.

The blockchain module ensured immutability of votes. Each vote was recorded as a block and linked sequentially, preventing any possibility of data tampering or duplication. Once a vote was cast, it could not be altered or deleted, thereby guaranteeing data integrity.

The self-tallying mechanism enabled real-time vote counting without requiring manual intervention. Election results were generated instantly after the voting process, significantly reducing the time compared to traditional systems.

The SMS notification system effectively communicated voting status to users. Voters received confirmation messages after successful authentication and vote casting, enhancing transparency and trust in the system.

Additionally, the system handled multiple concurrent users efficiently, demonstrating good scalability and stable performance under increased load conditions.

### 5.2 Performance Analysis

The system was analyzed based on the following parameters:

- **Authentication Accuracy:**

The combination of biometric and Aadhaar verification provided highly reliable user authentication, minimizing false positives and false negatives.

- **Security:**

Blockchain technology ensured a tamper-proof environment. The decentralized ledger eliminated single points of failure and enhanced resistance against cyber-attacks.

- **Efficiency:**

Automated vote counting reduced the overall election processing time. Real-time result generation eliminated delays associated with manual counting.

- **Transparency:**

The use of blockchain and SMS notifications allowed voters and authorities to verify voting activities, improving system transparency.

- **Scalability:**

Cloud-based deployment enabled the system to support a large number of users and polling stations without performance degradation.

### 5.3 Discussion

The results clearly indicate that the proposed system addresses major limitations of traditional voting systems, such as manual errors, delays in counting, and vulnerability to tampering. By integrating Artificial Intelligence for verification and Blockchain for secure data storage, the system ensures both accuracy and trustworthiness.

Compared to existing electronic voting systems, this approach provides:

- **Higher security** through decentralized data storage
- **Improved voter verification** using biometrics and identity databases
- **Faster result processing** with automated tallying
- **Enhanced user trust** through real-time notifications

However, certain challenges were observed during implementation. The dependency on Aadhaar and biometric systems may introduce privacy concerns and requires strong data protection measures. Additionally, the need for stable internet connectivity and digital infrastructure may limit deployment in remote areas.

Despite these challenges, the system proves to be a robust and future-ready solution for digital elections. With further improvements in infrastructure, data privacy mechanisms, and user awareness, it can be widely adopted for secure and transparent electoral processes.

### 5.4 Summary

Overall, the proposed system successfully demonstrates:

- Secure and accurate voter authentication

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

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

DOI:10.15662/IJEETR.2026.0802380

- Tamper-proof vote storage using blockchain
- Instant and reliable result generation
- Improved transparency and efficiency

These outcomes validate the effectiveness of the system in modernizing election processes and ensuring fair democratic practices.

## VI. CONCLUSION

In conclusion, the project offers a secure, transparent, and efficient alternative to traditional voting systems. The system leverages blockchain technology to ensure the integrity of votes and prevent any tampering or fraud. By integrating Aadhar authentication for secure user verification and OTP for transaction validation, the system guarantees that only eligible voters participate in the election process. Additionally, the use of blockchain ensures that all votes are immutable, providing transparency and accountability in the voting process. The system is designed with several key modules, including the Voter Registration System, Vote Casting System, and Vote Verification System. Each module is carefully crafted to ensure smooth operation and secure functionality. The user-friendly interface and seamless integration with blockchain ensure a smooth experience for both voters and administrators. Through thorough testing, the system demonstrated robust performance under high traffic and successfully passed all functionality, security, and performance tests. The system's scalability allows it to handle elections of varying sizes, making it suitable for both small organizations and large-scale governmental elections. This innovative system has significant advantages over traditional voting methods, offering enhanced security, transparency, and trust. Furthermore, it can serve as the foundation for future electoral systems, reducing administrative overhead and increasing voter participation. With its potential for further development, including integration with other security measures, the Blockchain-Based Online Voting System is poised to revolutionize the voting process, ensuring a safer and more reliable electoral environment.

## VII. FUTURE WORK

1. Implement AI-based anomaly detection to identify fraudulent voting activities
2. Introducing multi-modal biometrics (face, iris) for stronger authentication
3. Enhance data privacy using encryption and zero-knowledge techniques
4. Develop offline voting capability for low-network or rural areas
5. Use hybrid blockchain architecture to improve scalability and speed
6. Create secure mobile voting applications for remote voting
7. Integrate with multiple national ID systems for global adaptability
8. Conduct real-time pilot testing for practical validation

## REFERENCES

1. Abuidris.Y, Hassan.A, Hadabi.A, and Elfadul.I, (December 2019) “Risks and opportunities of blockchain based on e-voting systems,” in Proceedings of the 2019 16th International Computer Conference on Wavelet Active Media Technology and Information Processing, pp. 365–368, Chengdu, China.
2. Audi Ghaffari.M, (2017) An E-Voting System Based on Blockchain and Ring Signature, School of Computer Science University of Birmingham, UK.
3. Bai.S, Yang.G, Shi.J, Liu.G, and Min.J, (2018) “Privacy-Preserving oriented floating-point number fully homomorphic encryption scheme,” Security and Communication Networks.
4. Curran.K, (2018) “E-voting on the blockchain,” =e Journal of British Blockchain Association.
5. Ghosh.A, Gupta.S, Dua.A, and Kumar.N, (2020) “Security of Crypto currencies in blockchain technology: State-of-art, challenges and future prospects,” Journal of Network and Computer Applications, vol. 163, Article ID 102635
6. Gurubasavanna, Ulla Shariff, Mamatha, and Sathisha.N, (September 2018) “Multimode authentication based electronic voting kiosk using raspberry pi,” in Proceedings of the International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud), I-SMAC, pp. 528–535, Palladam, India.
7. Komatineni.S and Lingala.G, (March 2020) “Secured E-voting system using two-factor biometric authentication,” in Proceedings of the Fourth International Conference on Computing Methodologies and Communication (ICCMC), pp. 245–248, Iccmc, Erode, India.
8. 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

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

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

DOI:10.15662/IJEETR.2026.0802380

9. 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
10. 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
11. 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
12. 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
13. 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
14. 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.
15. 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.
16. 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.
17. 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
18. 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
19. 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
20. Shukla.S, asmiya.A.N, Shashank D.O, and Mamatha.H.R, (September 2018) "Online voting application using ethereum blockchain," in International Conference.
21. Gopinathan, V. R. (2024). Real-Time Fault-Tolerant Multi-Cloud Database Architectures for High Availability Applications. International Journal of Future Innovative Science and Technology (IJFIST), 7(4), 13148.
22. Chandra, S., Rengarajan, A., Sahoo, G. S., & Sharma, S. (2023, December). Identifying Neuronal Damage and Plasticity by Analyzing Changes in Diffusion Tensor Imaging. In International Conference on Data Science, Machine Learning and Applications (pp. 433-438). Singapore: Springer Nature Singapore.
23. Sugumar, R. (2025). Federated AI in Offline-First Mobile Health Architectures for Privacy-Preserving Clinical Intelligence. International Journal of Science, Research and Technology, 8(4), 14589-14600.
24. Murugeshwari, B., Rajalakshmi, S., & Sudharson, K. (2023). Hybrid Approach for Privacy Enhancement in Data Mining Using Arbitrariness and Perturbation. Computer Systems Science & Engineering, 44(3).
25. 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.
26. 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.
27. Mathew, A. (2022). Leveraging Big Data Analytics to Power AI and ML (Machine Learning) Automation. Educational Research (IJMCER), 4(5), 131-134.
28. 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.
29. Akila, R. (2024). A deep reinforcement learning approach for optimizing inventory management in the agri-food supply chain. J. Electrical Systems, 20(4s), 2238-2247.
30. Mahendran, M., Anbazhagan, K., Pavithran, G., Nivas, A., & Pandey, S. D. (2022). Earthquake Damage Prediction using Machine Learning. Grenze International Journal of Engineering & Technology (GIJET), 8(1).

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

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

DOI:10.15662/IJEETR.2026.0802380

31. Gopinathan, V. R. (2025). Enterprise AI Frameworks for Financial Data Engineering Behavioural Analytics and Intelligent Cloud Solutions. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 8(4), 12499-12506.
32. Kondalsamy, P., & Kaliappan, K. (2025). An Optimal Prediction of Leaf Disease Based on Hybrid Deep Learnings and Metaheuristic Technique. Traitement du Signal, 42(1), 363.
33. 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.
34. 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.
35. 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.
36. Gopinathan, V. R. (2025). Software engineering practices for AI-driven systems: From development to deployment (MLOps perspective). International Journal of Science, Research and Technology, 8(1), 13493-13500.
37. Mathew, A. R. (2022). Threats and protection on E-sim: a prospective study. Novel Perspectives of Engineering Research, 8, 76-81.
38. Naveena, S., & Kavitha, K. (2025). Gossypium herbaceum: Folium disease identification and classification using Efficient Net-Coordinate Convolutional Neural Network (EcoNet). Engineering Applications of Artificial Intelligence, 152, 110701.
39. Rengarajan, A., Mishra, A., Kulhar, K. S., Shrivastava, V. P., & Alawneh, Y. J. J. (2024, March). Role of Deep Reinforcement Learning in Mitigating Cyber Security Issues: A Review. In International Conference on Renewable Power (pp. 37-48). Singapore: Springer Nature Singapore.
40. Achari, A. P. S. K., & Sugumar, R. (2024, November). Performance analysis and determination of accuracy using machine learning techniques for naive bayes and random forest. In AIP Conference Proceedings (Vol. 3193, No. 1, p. 020199). AIP Publishing LLC.
41. Mathew, A., & Alex, H. (2022). Detect & protect-medical device cybersecurity. Curr. Overview Sci. Technol. Res, 1, 60-68.
42. Sammy, F., Chettier, T., Boyina, V., Shingne, H., Saluja, K., Mali, M., ... & Shobana, A. (2025). Deep Learning-Driven Visual Analytics Framework for Next-Generation Environmental Monitoring. Journal of Applied Science and Technology Trends, 114-122.
43. Anbazhagan, K. (2024). Trustworthy and Adaptive AI Systems for Enterprise Analytics Cybersecurity and Decision Optimization Using API-First and Cloud-Native Architectures. International Journal of Technology, Management and Humanities, 10(03), 65-74.
44. Mathew, A. (2021). Deep reinforcement learning for cybersecurity applications. Int J Comput Sci Mob Compu, 10(12), 32-38.
45. 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.
46. Karthika, K., Anusha, K., Kavitha, K., Harshadha, R., Dharshini, D. S., & Sundhar, N. A. (2025, April). Frequency Reconfigurable Antenna using Advanced Materials: A Study. In 2025 3rd International Conference on Advancements in Electrical, Electronics, Communication, Computing and Automation (ICAECA) (pp. 1-6). IEEE.
47. Thavamani, C., & Rengarajan, A. (2024). Clustering related behaviour of users by the use of partitioning and parallel transaction reduction algorithm. International Journal of Advanced Intelligence Paradigms, 29(2-3), 122-132.
48. 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.
49. 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.
50. SakthiPreetha, A., Kavitha, K., Karthika, K., & Manohari, R. G. (2025, April). A Novel Metasurface-Embedded Antenna for WBAN Communications. In 2025 3rd International Conference on Advancements in Electrical, Electronics, Communication, Computing and Automation (ICAECA) (pp. 1-4). IEEE.
51. Murugeshwari, B., Selvaraj, D., Sudharson, K., & Radhika, S. (2023). Data Mining with Privacy Protection Using Precise Elliptical Curve Cryptography. Intelligent Automation & Soft Computing, 35(1).

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

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

DOI:10.15662/IJEETR.2026.0802380

52. Gopinathan, V. R. (2025). Software engineering practices for AI-driven systems: From development to deployment (MLOps perspective). International Journal of Science, Research and Technology, 8(1), 13493-13500.
53. Anbazhagan, K., Kumar, R., Thilagavathy, R., & Anuradha, D. (2024, March). Shortest Job First with Gateway-based Resource Management Strategy for Fog Enabled Cloud Computing. In 2024 4th International Conference on Data Engineering and Communication Systems (ICDECS) (pp. 1-6). IEEE.
54. Kannadhasan, S., Vasuki, S., Kavitha, K., Karthikeyan, P., & Usha, S. G. A. (Eds.). (2025, April). Preface: Role of Artificial Intelligence and IoT in Engineering, Technology & Science [ICRAETS 2024]. In AIP Conference Proceedings (Vol. 3258, No. 1, p. 010001). AIP Publishing LLC.
55. Dhinakaran, D., Prathap, P. J., Selvaraj, D., Kumar, D. A., & Murugeshwari, B. (2022). Mining privacy-preserving association rules based on parallel processing in cloud computing. International Journal of Engineering Trends and Technology, 70(3), 284-294.