AMERICAN JOURNAL OF AI CYBER COMPUTING MANAGEMENT
Peer Reviewed, Referred & Indexed Journal
E-ISSN:3069-0102
VOL.6, NO. 2(2) (2026)

HYBRID COMPUTATIONAL INTELLIGENCE BASED MODEL FOR SIGNATURE VERIFICATION SYSTEM

Moumita Shaw
Department of Computer Science and Engineering
GIFT Autonomous, Bhubaneswar, Odisha, India

Biswajit Sahoo
Department of Computer Science and Engineering
GIFT Autonomous, Bhubaneswar, Odisha, India

ABSTRACT

The Hybrid Computational Intelligence Based Model for Signature Verification System is an intelligent biometric authentication system designed to verify handwritten signatures using Artificial Intelligence and Machine Learning techniques. Traditional signature verification methods are often affected by forgery, manual errors, and lack of accuracy. The proposed system integrates hybrid computational intelligence techniques such as Neural Networks, Fuzzy Logic, and Image Processing algorithms to improve signature verification accuracy and reliability.

The system captures signature images, preprocesses them, extracts important features, and compares them with stored signature patterns using machine learning algorithms. The proposed model can identify genuine and forged signatures efficiently by analyzing signature structure, stroke patterns, pressure variations, and writing behavior.

The system provides secure authentication, reduces fraudulent activities, improves verification accuracy, and minimizes manual verification effort. The proposed solution can be used in banking systems, legal document verification, business authentication, and secure access control systems.

Keywords: Signature Verification, Artificial Intelligence, Machine Learning, Neural Networks, Biometrics, Image Processing, Hybrid Computational Intelligence.

1. INTRODUCTION

Signature verification is one of the most widely used biometric authentication methods for validating personal identity in banking systems, legal documents, offices, and financial transactions. Traditional signature verification methods mainly depend on manual inspection, which is time-consuming and may lead to human errors and forgery issues.

With the rapid development of Artificial Intelligence and Machine Learning, intelligent signature verification systems have become more reliable and secure. Computational intelligence techniques such as Neural Networks, Fuzzy Logic, and Image Processing help analyze signature patterns accurately and detect forged signatures efficiently.

The proposed Hybrid Computational Intelligence Based Model for Signature Verification System combines multiple intelligent algorithms to improve authentication accuracy, security, and reliability. The system extracts unique signature features and compares them with stored records to verify user identity securely. The proposed Hybrid Computational Intelligence Based Model for Signature Verification System combines multiple intelligent techniques to improve signature verification accuracy and security. The system captures signature images, preprocesses them, extracts important features, and compares them with stored records using machine learning algorithms. The hybrid approach improves detection accuracy by combining multiple computational intelligence methods.

The proposed system is capable of identifying forged signatures and authenticating genuine users effectively. It reduces fraudulent activities, minimizes manual effort, and provides secure authentication for sensitive applications. The system can be applied in banking, insurance, legal systems, attendance management, secure document processing, and digital authentication environments.

2. OBJECTIVES OF THE PROJECT

The major objectives of the Hybrid Computational Intelligence Based Model for Signature Verification System

Received: 20-04-2026 | Accepted: 28-05-2026 | Published: 05-06-2026 | www.ajaccm.com

1. To develop an intelligent signature verification system using Artificial Intelligence.
2. To authenticate users using handwritten signatures.
3. To detect forged and duplicate signatures efficiently.
4. To improve verification accuracy using hybrid computational intelligence techniques.
5. To reduce manual verification effort and human errors.
6. To provide secure biometric authentication.
7. To improve system reliability and efficiency.

The project mainly focuses on integrating machine learning and image processing techniques for accurate signature verification and fraud prevention.

3. LITERATURE SURVEY

Biometric authentication systems have become highly important in modern digital security applications. Among different biometric techniques, handwritten signature verification remains one of the most accepted and legally recognized authentication methods.

Researchers have developed several approaches for signature verification using image processing and machine learning techniques. Traditional systems mainly used static image comparison methods that were limited in accuracy and unable to handle complex forgery attempts.

Machine learning and computational intelligence techniques significantly improved signature verification systems by introducing intelligent feature extraction and classification methods. Neural Networks are widely used for learning signature patterns and identifying similarities between genuine and forged signatures. Fuzzy Logic techniques help manage uncertainty and variation in signature characteristics.

Image Processing algorithms play an important role in signature analysis. Preprocessing operations such as grayscale conversion, noise removal, image normalization, and edge detection improve signature quality before feature extraction.

Several studies have shown that hybrid computational intelligence models improve authentication accuracy compared to individual algorithms. Combining Neural Networks, Fuzzy Logic, and Image Processing provides better forgery detection and reduces false acceptance rates.

OpenCV, TensorFlow, and Python libraries are commonly used for implementing signature verification systems due to their strong support for machine learning and image analysis.

4. EXISTING SYSTEM

Traditional signature verification systems mainly depend on manual verification methods where human experts compare signatures visually. These systems are widely used in banks, offices, legal departments, and educational institutions. Although manual verification methods are simple, they suffer from several limitations related to accuracy, reliability, and fraud detection.

Manual verification consumes a large amount of time and depends heavily on human observation skills. Verification accuracy may vary between different individuals because signature analysis is subjective. Human fatigue and carelessness may also lead to incorrect authentication decisions.

Existing digital signature verification systems often use basic image comparison methods without advanced machine learning techniques. These systems compare only simple structural characteristics such as size, shape, and orientation. Such approaches are not efficient for detecting skilled forgeries and complex signature variations.

Many existing systems are unable to handle variations in genuine signatures caused by writing speed, pressure, angle, and emotional conditions. Since signatures naturally vary over time, static comparison methods often produce incorrect results.

Another major limitation is the lack of intelligent learning capability. Traditional systems do not adapt automatically to new signature patterns and changing writing behaviors. As a result, authentication accuracy decreases over time.

Existing systems also face security issues related to unauthorized access, weak

voters cannot verify whether their votes have been recorded correctly. Manual handling of votes and election records also increases the possibility of vote tampering and manipulation. Delays in vote counting and result generation can create confusion and reduce public trust in the election process.

Existing online voting systems also face security challenges. Most web-based voting platforms use username-password authentication methods, which are vulnerable to hacking, phishing attacks, and credential theft. If unauthorized users gain access to voter accounts, the integrity of the election process may be compromised. Many systems also fail to provide proper encryption and secure communication mechanisms for protecting voter information.

Scalability is another issue in traditional and existing electronic voting systems. Conducting elections for a large number of voters requires high infrastructure and maintenance costs. Managing election databases manually becomes difficult as the number of voters and candidates increases. System failures or technical issues during elections may also interrupt the voting process and affect election reliability.

In addition, existing systems often lack intelligent monitoring and fraud detection mechanisms. Suspicious activities such as multiple login attempts, fake registrations, and unauthorized voting cannot be detected efficiently without advanced technologies. Manual monitoring increases workload for election administrators and reduces system efficiency.

Many existing voting systems are also dependent on centralized management without advanced backup and recovery mechanisms. Data loss, hardware failure, or cyberattacks may lead to serious security and operational problems. Therefore, secure storage and real-time monitoring are essential for modern election systems.

The limitations of traditional and existing voting systems highlight the need for a more secure, intelligent, and transparent voting platform. Modern technologies such as Artificial Intelligence, Machine Learning, Biometric Authentication, and Face Recognition can help overcome these challenges. AI-based facial recognition systems provide secure voter authentication by analyzing unique facial features of individuals. Since facial characteristics are difficult to duplicate, biometric verification significantly reduces fraudulent voting activities.

Therefore, the Advanced AI Facing Voting System is proposed as a modern solution that integrates Artificial Intelligence with electronic voting to improve election security, transparency, efficiency, and reliability.

5. PROPOSED SYSTEM

The proposed Hybrid Computational Intelligence Based Model for Signature Verification System uses Artificial Intelligence, Machine Learning, Image Processing, Neural Networks, and Fuzzy Logic to provide secure and accurate signature authentication.

The system includes the following major modules:

1. User Module
2. Signature Acquisition Module
3. Image Processing Module
4. Feature Extraction Module

upload or provide signature samples through digital devices or scanned documents. The signatures are processed and stored securely in the database.

The Image Processing Module performs operations such as grayscale conversion, noise removal, normalization, and edge detection to improve signature quality.

The Feature Extraction Module extracts important characteristics including stroke patterns, edge structure, pixel density, orientation, curvature, and shape features.

The proposed system improves verification accuracy, reduces fraud, minimizes manual effort, and supports secure digital authentication.

6. SYSTEM REQUIREMENTS

6.1 Hardware Requirements

- Intel Core i3 Processor or Higher
- 4 GB RAM
- 500 GB Hard Disk
- Scanner / Signature Pad
- Keyboard and Mouse
- Internet Connection

6.2 Software Requirements

- Operating System: Windows / Linux
- Programming Language: Python
- Frontend: HTML, CSS, JavaScript
- Backend: Flask / Django
- Database: MySQL
- Libraries: OpenCV, TensorFlow, NumPy, Scikit-learn

Received: 20-04-2026 | Accepted: 28-05-2026 | Published: 05-06-2026 | www.ajaccm.com

7. SYSTEM ARCHITECTURE

The system architecture is designed using a client-server model that ensures secure communication, efficient processing, and reliable authentication.

The architecture mainly consists of the following components:

1. Frontend Module
2. Backend Module
3. Image Processing Module
4. Neural Network Module
5. Fuzzy Logic Module
6. Database Module
7. Verification Module

The backend module handles the core functionality of the system. It is developed using Python frameworks such as Flask or Django. The backend processes user requests, manages authentication, communicates with the database, and controls the AI-based facial recognition operations. It acts as a bridge between the frontend and the database, ensuring smooth communication between different modules.

One of the most important components of the architecture is the Face Recognition Module. This module uses Artificial Intelligence and OpenCV libraries to perform voter authentication. During voter registration, facial images are captured through a webcam and stored securely in the database. During login or voting, the system captures a live image of the voter and compares it with previously stored facial data using machine learning algorithms. If the facial features match successfully, the voter is authenticated and allowed to proceed with voting. This process significantly reduces unauthorized access and duplicate voting attempts.

The database stores voter records, candidate details, facial recognition data, election schedules, voting status, and election results. MySQL is used as the database management system because of its reliability, scalability, and secure data handling capabilities. Each voter record is associated with a unique voter ID to maintain consistency and avoid duplication.

The Admin Module plays a vital role in managing the overall election process. Administrators can verify voter registrations, manage candidate information, create elections, monitor voting activities, and generate election reports. The admin module also helps identify suspicious activities and maintain transparency throughout the election process.

The Candidate Module allows candidates to upload their personal details, political party information, election symbols, and campaign-related data. These details are displayed to voters during the election process. Candidates can also monitor election announcements and updates through the system interface.

The Voting Module is responsible for secure vote casting and vote management. After successful facial authentication, voters are allowed to access the voting page where they can select their preferred candidate. Once the vote is submitted, the system stores the voting information securely in the database and immediately updates the voter's status to prevent multiple voting attempts.

Overall, the system architecture of the Advanced AI Facing Voting System provides a secure, intelligent, scalable, and transparent framework for conducting digital elections using Artificial Intelligence and biometric authentication technologies.

8. DATA FLOW DIAGRAM

The Data Flow Diagram (DFD) represents the movement of information within the signature verification system.

The process begins with user registration where users submit personal details and signature samples.

The uploaded signature is transferred to the Image Processing Module where preprocessing operations are performed.

The Feature Extraction Module extracts unique characteristics from the signature image.

Extracted features are stored in the database and later compared during verification.

During authentication, a new signature sample is uploaded and processed similarly. The Verification Module compares the extracted features with stored templates using Neural Networks and Fuzzy Logic algorithms.

If the similarity score matches successfully, the user is authenticated. Otherwise, the system rejects the signature.

The Admin Module monitors system activities, manages users, and generates verification reports.

During the login process, the voter enters login credentials and activates the webcam for face verification. The system captures a live facial image and sends it to the Face Recognition Module for processing. The AI algorithm extracts facial features and compares them with the previously stored database records. If the facial image matches successfully, the authentication process is completed and the voter is granted access to the voting page. If authentication fails, the system denies access and prompts the user to retry the verification process.

Once the voter is authenticated, the Voting Module becomes active. The system displays the list of candidates along with their party details and election symbols. The voter selects a preferred candidate and submits the vote. The selected vote is then transferred securely to the backend server and stored in the voting database.

Immediately after successful vote submission, the system updates the voting status of the voter in the database. This process prevents duplicate voting and ensures that each voter can cast only one vote during an election. The voting data is encrypted and protected from unauthorized access to maintain election security and transparency.

The Admin Module interacts with all system components and plays a major role in managing election activities. Administrators can verify voter registrations, approve candidate details, monitor voting activities, manage election schedules, and generate election reports. The admin module communicates with the database continuously to update records and monitor system performance.

Security plays an important role in the data flow process. Sensitive information such as passwords, facial recognition data, and voting records are transmitted using secure communication mechanisms. Database access is restricted to authorized users only, reducing the risk of data breaches and unauthorized modifications.

The DFD also helps identify possible vulnerabilities and improve system efficiency. By analyzing the flow of information, developers can optimize authentication processes, database communication, and election management operations.

Overall, the Data Flow Diagram provides a clear understanding of how data is processed, transferred, and stored within the Advanced AI Facing Voting System. It demonstrates the interaction between users, AI modules, databases, and election management components, ensuring secure, transparent, and efficient digital voting operations.

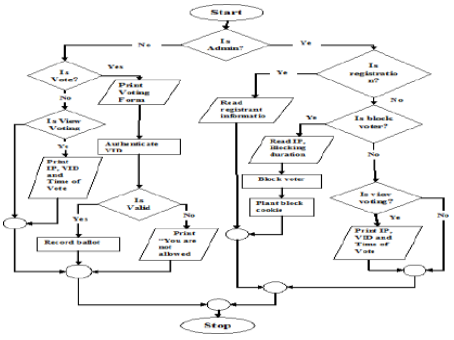


Fig 1: Data Flow Diagram

9. DATABASE DESIGN

The database design is one of the most important components of the system because it stores user information, signature templates, authentication records, and verification results securely.

The system uses MySQL as the database management system because of its reliability, scalability, and security features.

The User Table stores user-related information such as user ID, name, email, contact details, and login credentials.

The Signature Table stores processed signature images and extracted feature vectors.

The Verification Table stores authentication results, timestamps, similarity scores, and verification status.

The Admin Table stores administrator login details and access permissions.

Security mechanisms such as encryption, authentication control, and restricted database access are implemented to protect sensitive information.

Backup and recovery mechanisms are also included to prevent data loss during system failures.

The Candidate Table stores details related to election candidates including candidate ID, candidate name, political party name, election symbol, contact information, and profile details. This information is displayed to voters during the voting process to help them identify candidates easily.

The Admin Table contains administrator login credentials and authorization information. Only authorized administrators can access this module to manage election activities, voter approvals, candidate records, and election monitoring. Proper access control mechanisms are implemented to protect administrative data from unauthorized access.

The Election Table stores details related to elections such as election name, election category, starting date, ending date, election status, and election results. This table helps administrators manage multiple elections efficiently within the same system.

The Voting Records Table is responsible for storing vote-related information including voter ID, selected candidate ID, vote timestamp, and voting status. After a vote is cast successfully, the voter's status is updated immediately to prevent duplicate voting attempts. This table ensures transparency and accuracy in vote management.

The Authentication Table stores login activity, authentication timestamps, and facial verification details. This helps maintain secure monitoring of system access and user authentication activities.

Security is a major concern in database design because the system stores sensitive voter and election information. Several security mechanisms are implemented to protect the database from unauthorized access and cyber threats. Passwords are stored using encryption techniques, and database access is restricted through authentication and authorization controls. Secure database connectivity is also maintained between the frontend and backend modules.

Backup and recovery mechanisms are included in the database design to prevent data loss during hardware failures or system crashes. Regular backups ensure that election records and voter information can be restored whenever necessary.

The database design also supports scalability and future enhancements. Additional modules such as blockchain-based vote storage, mobile voting support, and cloud integration can be added without affecting the existing database structure.

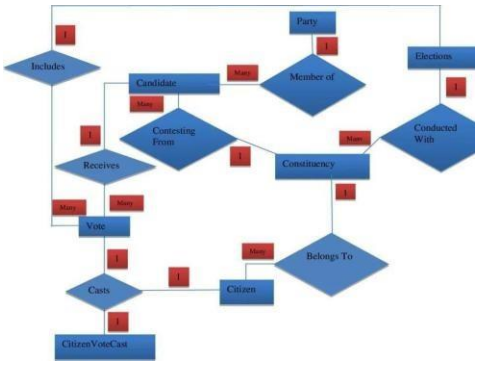


Fig 2: Database Structure

10. MODULE DESCRIPTION

10.1 Image Processing Module

This module allows users to register themselves before participating in elections. Personal details and facial images are captured and stored securely in the database.

The registration process is user-friendly and ensures proper validation of voter information.

10.2 Feature Extraction Module

The Face Recognition Module is the core component of the system. It captures facial images using a webcam and processes them using OpenCV and machine learning algorithms.

The extracted facial features are compared with stored database records for authentication.

10.3 Signature Verification Module

The Voting Module allows authenticated users to cast votes securely. Once a vote is submitted, the system updates voting status automatically.

The module also ensures secure transmission and storage of voting records.

10.4 Admin Module

The Admin Module manages elections, verifies voter registrations, and monitors voting activities.

Administrators can add or remove candidates, generate election reports, and manage voting schedules securely.

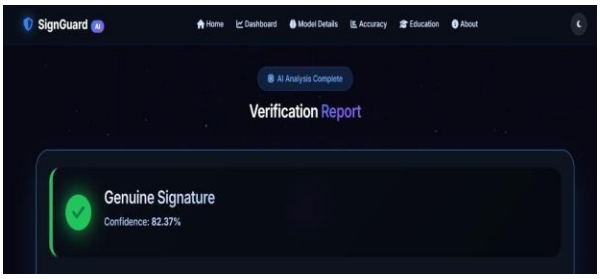
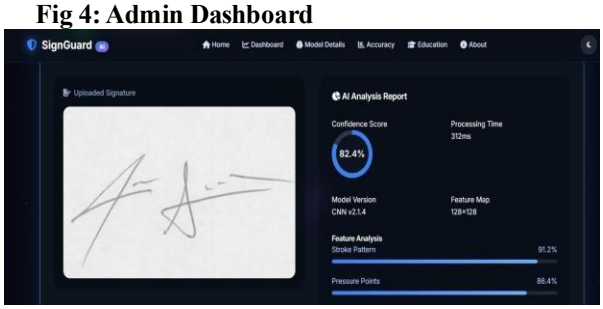


Fig 3: Voter Registration Interface

Fig 4: Admin Dashboard



11. IMPLEMENTATION

The implementation of the Advanced AI Facing Voting System is carried out using Python and OpenCV libraries. HTML, CSS, and JavaScript are used for frontend development.

The voter registration module captures facial images through a webcam and stores them in the database. During authentication, live images are processed and compared with stored facial records.

The backend server handles requests from users and communicates with the database. MySQL is used for secure storage of election data.

The implementation also includes security features such as encrypted passwords and protected database connectivity.

12. ALGORITHMS USED

12.1 Neural Network Algorithm

Neural Networks are used for learning signature patterns and classification.

The algorithm analyzes extracted features and generates prediction scores.

The process includes:

1. Training data preparation
2. Feature learning
3. Pattern classification
4. Similarity analysis
5. Genuine/Forged prediction

The Neural Network improves authentication accuracy significantly.

12.2 Fuzzy Logic Algorithm

Fuzzy Logic is used for intelligent decision-making under uncertainty.

The algorithm handles natural variations in signatures and improves verification reliability.

The system calculates fuzzy similarity scores and combines outputs from multiple verification methods.

13. RESULTS AND DISCUSSION

The Hybrid Computational Intelligence Based Model for Signature Verification System successfully improves authentication accuracy and fraud detection.

Testing results indicate that the hybrid model performs better than traditional signature verification methods.

The system prevents duplicate voting and unauthorized access through biometric authentication

Automatic vote counting and result generation reduce manual effort and improve election efficiency.

The admin module successfully monitors election activities and manages candidate information.

Experimental testing demonstrated that the face recognition module performs accurately under normal lighting conditions.

The use of AI significantly improves election reliability and voter confidence.

14. ADVANTAGES OF THE SYSTEM

1. Prevents duplicate and fraudulent voting.
2. Provides secure biometric authentication.
3. Reduces manual effort and human errors.
4. Improves transparency and reliability.
5. Enables automatic vote counting.
6. Supports remote voting functionality.
7. Provides faster election processing.
8. Maintains secure digital records.
9. Increases voter convenience.
10. Supports future scalability.

15. FUTURE ENHANCEMENTS

he system can be improved further using advanced technologies.

Future improvements include:

1. Deep Learning integration.
2. Real-time cloud-based authentication.
3. Mobile application support.
4. Blockchain-based signature storage.
5. Multi-factor biometric authentication.
6. AI-based fraud analytics.
7. Dynamic signature analysis support.
8. Government database integration.

These enhancements will improve scalability, security, and usability of the system.

16. CONCLUSION

he Hybrid Computational Intelligence Based Model for Signature Verification System provides a secure and intelligent approach to handwritten signature Babburi, S. Privacy-Preserving Collaborative Framework with Auditable Federated Learning.

authentication using Artificial Intelligence and Machine Learning techniques.

The system improves verification accuracy, reduces fraudulent activities, and minimizes manual effort through intelligent image processing and hybrid computational intelligence algorithms.

Neural Networks, Fuzzy Logic, and Image Processing techniques significantly enhance authentication reliability and forgery detection capability.

The implementation results indicate that the proposed system performs effectively under normal conditions and provides a practical solution for secure digital authentication.

Overall, the proposed system offers a scalable, reliable, and intelligent signature verification solution for banking systems, legal applications, business authentication, and secure document verification environments.

REFERENCES

[1] D. P. Acharjya and Kauser Ahmed P, “A Survey on Big Data Analytics: Challenges, Open Research Issues and Tools,” International Journal of Advanced Computer Science and Applications, 2016.

[2] OpenCV Documentation, Face Recognition and Image Processing.

[3] TensorFlow Documentation for AI and Deep Learning Applications.

[4] Research papers on AI-based Online Voting Systems and Biometric Authentication.

[5] Machine Learning and Facial Recognition Techniques for Secure Authentication Systems.

[6] Python Documentation for AI and Web Development.

[7] MySQL Documentation for Database Management Systems.

[8] Research Articles on Secure Electronic Voting Systems.

[9] Todupunuri, A. (2024). Explore How AI Can Be Used To Create Dynamic And Adaptive Fraud & Rules That Improve The Detection And Prevention Of Fraudulent & Activities In Digital Banking. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.5014699

[10]Babburi, S. Privacy-Preserving Collaborative Framework with Auditable Federated Learning.

[11]Gaddam, S. (2024). Integrating machine learning models with continuous integration and continuous delivery (CI/CD) pipelines for a learning-driven approach to software engineering.

[12]Immadi, S. K. (2025). Optimizing ERP for

Human Capital Management. Applied Research for Growth, Innovation and Sustainable Impact, 377–384. https://doi.org/10.1201/9781003684657-63

[13]Vasagam, M. (2024, August 30). Ensuring security in modern data pipelines: Practical strategies for data engineers. International Journal of Intelligent Systems and Applications in Engineering, 12(22s), 2401.

[14]Santthosh Saai Reddy Purmani. (2026). Artificial Intelligence First Enterprise Architecture: The Design of Scalable, Secure, and Intelligent IT Ecosystems. American Journal of AI Cyber Computing Management, 6(1(2)), 1–8. https://doi.org/10.64751/ajaccm.2026.v6.n1(2).pp1-8

[15]Kumara, S. (2026, February). A Lightweight Deep Learning Based Classification Models for Non-Human Identity Threat Detection. In 2026 IEEE 5th International Conference on AI in Cybersecurity (ICAIC) (pp. 1-6). IEEE.

[16]Kotte, G. (2025). Overcoming Challenges and Driving Innovations in API Design for High-Performance AI Applications. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.5283649

[17] Kotte, G. (2025). Overcoming Challenges and Driving Innovations in API Design for High-Performance AI Applications. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.5283649

[18] Kotte, G. (2025). Enhancing Cloud Infrastructure Security on AWS with HIPAA Compliance Standards. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.5283660

[19] Kotte, G. (2025). Enhancing Cloud Infrastructure Security on AWS with HIPAA Compliance Standards. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.5283660

[20] Viswanathan, V. (2023). AI-Augmented Decision Intelligence for Enterprise Systems: Integrating Cognitive Analytics for Resource and Talent Optimization.

[21] Viswanathan, V. Generative AI for Smarter Workforce Planning and Enterprise Resource Decisions.

[22] Mudusu, S. K. (2026, April 15). The secure intelligence framework: Architecting AI systems for a data-driven world. CIO (Foundry Expert Contributor Network).

[23] Mudusu, S. K. (2026, March 26). A data trust scoring framework for reliable and responsible AI systems. InfoWorld (Foundry Expert Contributor Network).

[24] Agrawal, A. M., Gajula, S., Shinde, R. P., Shah, H., & Ghosh, H. (2025, July). Machine Translation for Long Sequences with Enhanced Attention Mechanisms. In 2025 5th International Conference on Electrical, Computer and Energy Technologies (ICECET) (pp. 1-6). IEEE.

[25] Gajula, S. (2026, March). Two Pillars of Banking Intelligence: A Comparative Analysis of AI Techniques for Fraud Prevention and Churn Mitigation. In 2026 14th International Symposium on Digital Forensics and Security (ISDFS) (pp. 1-6). IEEE.

[26] Gajula, S. (2025). Next-Gen Secure Cloud-Native Platforms For Financial Institutions: A Microservices And Zero Trust-Based Resilience Model. Journal of International Crisis & Risk Communication Research (JICRCR), 8.

[27] Maturi, S. Y. (2023). Crowdsourced frontier: Unveiling autonomous adversarial cybercapabilities via open AI competition. International Journal of Intelligent Systems and Applications in Engineering, 11(1s), 275–284.

[28] Sikder, M. Z., Shakil, M. A. I., Ahad, A., Karim, M. F., Intakhab, B., & Islam, D. A. (2025, June). Microwave-Based Detection of Early-Stage Renal Cell Carcinoma Using UHF Range Antenna. In 2025 International Conference on Computer Systems and Technologies (CompSysTech) (pp. 1-6). IEEE.

[29] Manoharan, D. (2024). Governance-Oriented Quality Engineering Framework for Healthcare EDI Modernization. International Journal of Multidisciplinary on Science and Management IJMSM, 1(2).

[30] Manoharan, D. (2025). Healthcare EDI Transaction Lifecycles Embedded with a Multi-Layer Verification Framework to Ensure Referential Integrity.

[31] Ravishankara, M. (2026, February). PlotChain: Deterministic Checkpointed Evaluation of Multimodal LLMs on Engineering Plot Reading. In SoutheastCon 2026 (pp. 1-8). IEEE.

[32] Doragacharla, V. R. (2026). Building Real-

Time Pricing Systems for Modern Retail. Available at SSRN 6451760.

[33] Adabala, P. K. (2024). Utilizing predictive analytics to improve efficiency and decision-making in ERP-connected supply chains. International Journal of Intelligent Systems and Applications in Engineering, 12(22s), 2465

[34] Venkata Ramana, P. (2024). AI-driven predictive analytics in ERP systems for proactive supply chain optimization. International Journal of Research in Information Technology and Computing, 8(4).

[35] Venkata Pavan Kumar Gummadi. (2023). MuleSoft Batch Processing: High-Volume Streaming Architecture. Computer Fraud and Security, 50–57. https://doi.org/10.52710/cfs.886

[36] Venkata Pavan Kumar Gummadi. (2026). Infrastructure Optimization Techniques for Enterprise Integration Platforms: A Comprehensive Analysis. Computer Fraud and Security, 37–44. https://doi.org/10.52710/cfs.875

[37] Venkata Pavan Kumar Gummadi. (2024). API Design and Implementation: RAML and OpenAPI Specification. Journal of Electrical Systems, 16(4), 76–85. https://doi.org/10.52783/jes.9329

[38] Venkata Pavan Kumar Gummadi. (2025). MuleSoft's Role in Advancing Sustainable Digital Infrastructure: An Enterprise Integration Perspective. Journal of Information Systems Engineering and Management, 10(62s), 1313–1321. https://doi.org/10.52783/jisem.v10i62s.13783

[39] Gajula, S., & Margam, M. (2026). A Secure and Scalable Cloud-Based Banking Service Model Leveraging AI and Advanced Cyber Security. 2026 IEEE 5th International Conference on AI in Cybersecurity (ICAIC), 1–5. https://doi.org/10.1109/icaic67076.2026.11395704

[40] Gajula, S. (2025). Ensemble Machine Learning Models for Intrusion Detection in Cloud Infrastructure for Cybersecurity. 2025 International Conference on Artificial Intelligence, Blockchain, Cloud Computing, and Data Analytics (ICoABCD), 1–6. https://doi.org/10.1109/icoabcd67551.2025.11470865