International Journal of
LAW, ARTS AND HUMANITIES
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0523 www.zesterapublications.com Original Research Paper

ADVANCED AI FACING VOTING SYSTEM

Bellana Rohit
Department of Computer Science and Engineering (Artificial Intelligence)
GIFT Autonomous, Bhubaneswar, Odisha, India

Kajal Kumari Thakur
Department of Computer Science and Engineering
GIFT Autonomous, Bhubaneswar, Odisha, India

Debaprasad Nanda
Department of Computer Science and Engineering
GIFT Autonomous, Bhubaneswar, Odisha, India

ABSTRACT

The Advanced AI-Facing Voting System is an intelligent electronic voting solution that utilizes artificial intelligence and facial recognition technology to enhance the security, transparency, and efficiency of digital elections. Traditional voting systems face several challenges such as duplicate voting, impersonation, vote tampering, and manual errors. The proposed system integrates AI-based biometric authentication to verify voter identity before vote casting, thereby ensuring that only authorized individuals can participate in the election process.

The system consists of voter, candidate, and admin modules. Facial images captured during voter registration are stored securely in the database. During voting, live facial images are verified using OpenCV and machine learning algorithms. After successful authentication, voters can securely cast their votes. The system also provides automatic vote counting, result generation, and election monitoring.

The Advanced AI Facing Voting System improves election reliability, reduces manual effort, minimizes fraud, and increases transparency. The proposed solution provides a modern and secure approach for future digital election environments.

Keywords: Artificial Intelligence, Face Recognition, Electronic Voting, Biometric Authentication, Digital Election, Machine Learning.

1. INTRODUCTION

Voting is one of the fundamental rights in a democratic society. Traditional voting systems such as paper ballots and Electronic Voting Machines (EVMs) have been used for many years. However, these systems often face problems including vote duplication, identity fraud, ballot manipulation, and delayed result processing.

Electronic voting systems were introduced to improve election efficiency and reduce manual effort. Although e-voting systems provide faster processing, they still face security challenges related to voter authentication and transparency. Password-based authentication methods are not sufficient to ensure secure identity verification.

Artificial Intelligence (AI) has emerged as an effective technology for solving modern security problems. Face recognition is one of the most widely used biometric technologies for authentication. Since every individual has unique facial features, face recognition provides a reliable and secure method of identity verification.

The proposed Advanced AI Facing Voting System integrates facial recognition with electronic voting to improve election security and reliability. The system verifies voter identity using AI algorithms before allowing vote casting. This reduces the possibility of duplicate voting and unauthorized access.

The system also provides transparency by maintaining digital voting records and automatic

Received: 05-04-2026 | Accepted: 28-05-2026 | Published: 04-06-2026

International Journal of
LAW, ARTS AND HUMANITIES
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0523 www.zesterapublications.com Original Research Paper

result generation. The use of AI improves election accuracy and reduces operational costs. The proposed model is suitable for educational institutions, organizations, and future government election systems.

2. OBJECTIVES OF THE PROJECT

The major objectives of the Advanced AI Facing Voting System are:

1. To develop a secure electronic voting system using AI technology.
2. To authenticate voters using facial recognition.
3. To prevent duplicate and fraudulent voting.
4. To improve transparency in election management.
5. To reduce manual effort and operational cost.
6. To provide automatic vote counting and result generation.
7. To maintain secure storage of voter and election data.
8. To improve accessibility through digital voting platforms.
9. To support future scalability and enhancements.
10. To increase election reliability and security.

The project mainly focuses on integrating biometric authentication with digital voting to improve election integrity and efficiency.

3. LITERATURE SURVEY

Artificial Intelligence and biometric authentication systems have become popular in modern security applications. AI-based face recognition systems are widely used in banking, surveillance, attendance systems, and digital authentication.

Researchers have explored electronic voting systems to improve accessibility and reduce manual effort. However, many existing systems lack strong authentication mechanisms. Password-based systems are vulnerable to hacking and identity theft.

Face recognition systems use machine learning and image processing techniques to identify individuals based on facial features. The process involves image capture, face detection, feature extraction, and face matching.

OpenCV and TensorFlow are commonly used libraries for implementing face recognition systems. Machine learning algorithms improve recognition accuracy under different lighting conditions and facial expressions.

Several studies show that biometric authentication improves election security by reducing impersonation and duplicate voting. AI-based systems also improve transparency and efficiency in election management.

Although AI-based voting systems provide several advantages, challenges such as privacy concerns, data security, and scalability still require further research.

4. EXISTING SYSTEM

Traditional voting systems have been used for many years in schools, organizations, institutions, and government elections. These systems mainly depend on paper ballots and Electronic Voting Machines (EVMs) for conducting elections. Although these methods are widely accepted and implemented in many countries, they still suffer from several limitations related to security, transparency, efficiency, and reliability.

In the traditional paper ballot system, voters are required to visit polling booths physically and cast their votes manually using ballot papers. After completion of the voting process, election officials manually count the votes. This process consumes a large amount of time and manpower. Human involvement at every stage increases the chances of errors and manipulation. In many cases, invalid votes occur due to improper marking of ballot papers by voters. Managing large-scale elections using paper ballots also requires huge financial resources for printing, transportation, storage, and security of ballot boxes.

Received: 05-04-2026 | Accepted: 28-05-2026 | Published: 04-06-2026

International Journal of
LAW, ARTS AND HUMANITIES
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0523 www.zesterapublications.com Original Research Paper

Electronic Voting Machines were introduced to overcome some of the limitations of paper ballot systems. EVMs reduce paper usage and improve vote counting speed. However, they still depend heavily on physical polling stations and manual voter verification processes. Voters are required to carry identification documents and stand in long queues to cast their votes. This reduces voter convenience and accessibility, especially for elderly people, disabled individuals, and people living in remote locations.

One of the major problems in existing voting systems is voter impersonation and duplicate voting. Traditional authentication methods such as voter ID cards, passwords, or manual verification are not fully secure. Fake identities, forged documents, and unauthorized access may lead to fraudulent voting activities. Since these systems do not use advanced biometric verification, it becomes difficult to ensure that only authorized individuals are participating in elections.

Another major limitation is the lack of transparency in election management. In many traditional systems, 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 Advanced AI Facing Voting System uses Artificial Intelligence and facial recognition technology to provide secure and transparent digital voting.

The system includes three major modules:

1. Voter Module
2. Candidate Module
3. Admin Module

Received: 05-04-2026 | Accepted: 28-05-2026 | Published: 04-06-2026

International Journal of
LAW, ARTS AND HUMANITIES
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0523 www.zesterapublications.com Original Research Paper

During voter registration, personal details and facial images are stored securely in the database. During login, the system captures live facial images and compares them with stored records using AI algorithms.

If authentication is successful, the voter can cast the vote securely. The system updates voting status automatically to prevent duplicate voting.

The proposed system improves election security, transparency, and efficiency while reducing manual effort and operational cost. The architecture also supports future enhancements such as mobile voting and blockchain integration.

6. SYSTEM REQUIREMENTS

6.1 Hardware Requirements

- Intel Core i3 Processor or Higher
- 4 GB RAM
- 500 GB Hard Disk
- Webcam
- 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

7. SYSTEM ARCHITECTURE

The Advanced AI Facing Voting System is designed using a client-server architecture model that ensures secure communication, efficient data management, and reliable election processing. The architecture consists of multiple interconnected modules that work together to perform voter registration, facial authentication, vote casting, election monitoring, and result generation. The modular design of the system improves flexibility, scalability, and maintainability while ensuring secure handling of sensitive voter information.

The system architecture mainly consists of the following components:

1. Frontend Module
2. Backend Module
3. Face Recognition Module
4. Database Module
5. Admin Module
6. Candidate Module
7. Voting Module

The frontend module provides an interactive user interface for voters, administrators, and candidates. It is developed using HTML, CSS, and JavaScript to create a responsive and user-friendly environment. Through this interface, voters can register themselves, log into the system, verify their identity using facial recognition, and cast their votes securely. The frontend also allows candidates to upload their information and administrators to monitor election activities.

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.

International Journal of
LAW, ARTS AND HUMANITIES
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0523 www.zesterapublications.com Original Research Paper

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.

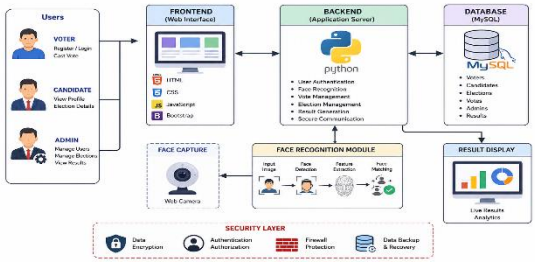


Fig 1: System Architecture Diagram

8. DATA FLOW DIAGRAM

The Data Flow Diagram (DFD) represents the flow of information within the Advanced AI Facing Voting System. It illustrates how data moves between different modules, processes, users, and the database. The DFD helps in understanding the functioning of the system by showing the interaction between various components involved in the voting process. It also provides a clear representation of how voter information, authentication data, election details, and voting records are processed and stored securely.

The main entities involved in the system are the Voter, Admin, Candidate, Face Recognition Module, Voting Module, and Database. Each entity exchanges information with the system to perform specific operations related to election management and voting activities.

The data flow process begins with the voter registration stage. During registration, the voter enters personal details such as name, voter ID, contact information, email address, and login credentials through the registration interface. Along with these details, the system captures facial images using a webcam. The captured facial data is processed using OpenCV and Artificial Intelligence algorithms before being stored securely in the database.

After successful registration, the voter data is transferred to the database module where all information is stored securely. The database maintains records of voter details, facial recognition data, voting status, and authentication information. Each voter is assigned a unique identifier to avoid duplication and maintain consistency within the system.

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

International Journal of
LAW, ARTS AND HUMANITIES
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0523 www.zesterapublications.com Original Research Paper

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.

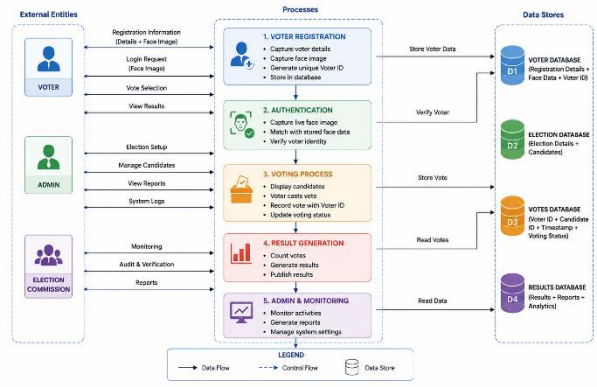


Fig 2: Data Flow Diagram

9. DATABASE DESIGN

The database design is one of the most important components of the Advanced AI Facing Voting System because it manages and stores all information related to voters, candidates, elections, authentication records, and voting results. A well-structured database ensures efficient data storage, fast retrieval, secure communication, and reliable election management. The database acts as the backbone of the entire system by maintaining consistency and integrity of election data.

The system uses MySQL as the database management system due to its reliability, scalability, security features, and support for structured data handling. The database is designed using relational tables that are connected through unique identifiers

International Journal of
LAW, ARTS AND HUMANITIES
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0523 www.zesterapublications.com Original Research Paper

and relationships. Proper normalization techniques are applied to reduce redundancy and improve database performance.

The Voter Table stores all voter-related information such as voter ID, name, contact details, email address, password, age, gender, and facial recognition data. Each voter is assigned a unique voter ID to prevent duplication and maintain proper identification. The facial images captured during registration are processed and linked with voter records for biometric authentication during login and voting.

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.

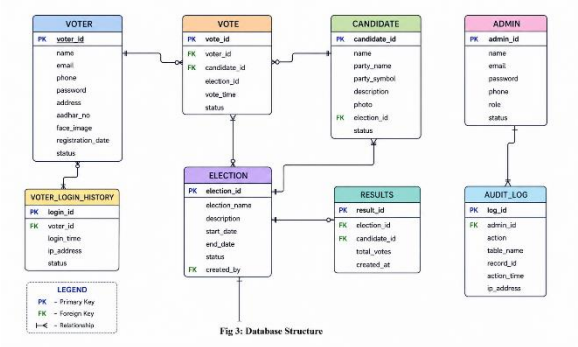


Fig 3: Database Structure

10. MODULE DESCRIPTION

10.1 Voter Registration 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.

International Journal of
LAW, ARTS AND HUMANITIES
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0523 www.zesterapublications.com Original Research Paper

10.2 Face Recognition 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 Voting 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.

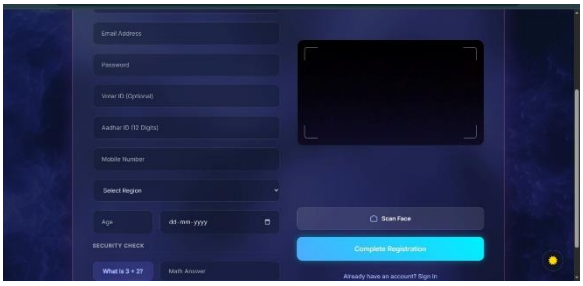


Fig 4: Voter Registration Interface

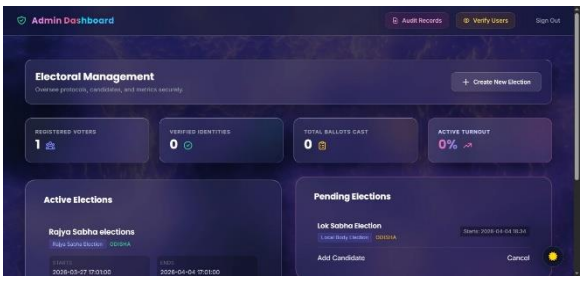


Fig 5: Admin Dashboard

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 Face Detection Algorithm

Face detection is performed using OpenCV Haar Cascade Classifier. The algorithm detects human faces in real-time using webcam input.

The process includes:

1. Capturing image frames
2. Converting images into grayscale
3. Detecting face regions
4. Extracting facial features

The algorithm provides fast and accurate facial detection.

12.2 Face Recognition Algorithm

The face recognition process compares facial features with stored database records.

Machine learning techniques analyze facial structures and generate feature vectors. If the similarity score matches successfully, the voter is authenticated.

The algorithm improves election security by preventing unauthorized access.

13. RESULTS AND DISCUSSION

The Advanced AI Facing Voting System successfully improves election security and

International Journal of
LAW, ARTS AND HUMANITIES
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0523 www.zesterapublications.com Original Research Paper

transparency. Testing results indicate accurate facial recognition and efficient vote management.

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

The system can be enhanced further using advanced technologies.

Future improvements include:

1. Blockchain integration for secure vote storage.
2. Mobile application support.
3. Cloud-based deployment.
4. Multilingual interfaces.
5. Fingerprint and iris recognition support.
6. AI-based fraud detection systems.
7. Real-time analytics dashboards.
8. Government database integration.

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

16. CONCLUSION

The Advanced AI Facing Voting System provides a secure and intelligent approach to digital elections by integrating Artificial Intelligence and biometric authentication.

The system improves election security, transparency, and efficiency while reducing fraud and manual intervention. Facial recognition technology ensures secure voter authentication and prevents unauthorized voting activities.

The project demonstrates how AI can improve modern election systems through automation and biometric verification.

The implementation results indicate that AI-based authentication significantly enhances election reliability and user confidence.

Overall, the proposed system provides a practical and scalable solution for future digital voting 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.

International Journal of
LAW, ARTS AND HUMANITIES
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0523 www.zesterapublications.com Original Research Paper

7. MySQL Documentation for Database Management Systems.
8. Research Articles on Secure Electronic Voting Systems.
9. Babburi, S. Privacy-Preserving Collaborative Framework with Auditable Federated Learning.
10. Gaddam, S. (2024). Integrating machine learning models with continuous integration and continuous delivery (CI/CD) pipelines for a learning-driven approach to software engineering.
11. Reddy, S. K. R. Developing a Modular AI Framework to Enhance Scalability and Personalization in Next-Generation Reward Platforms.
12. Poojari, R. INTELLIGENT SYSTEMS+B108 AND APPLICATIONS IN ENGINEERING.
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. Purmani, S. S. R. (2025). Streamlining IT operations and service management with agile frameworks. European Journal of Advances in Engineering and Technology, 12(4), 76–81.
16. Kotte, G. (2025). Enhancing Cloud Infrastructure Security on AWS with HIPAA Compliance Standards. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.5283660
17. 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.
18. 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
19. Mahtabi, M., Roshan, M., Muhit, M. M. I., Behvar, A., & Haghshenas, M. (2026). Cryogenic ultrasonic fatigue: Mechanisms, advancements, and insights. Cryogenics, 153, 104257. https://doi.org/10.1016/j.cryogenics.2025.104257
20. Viswanathan, V. (2023). AI-Augmented Decision Intelligence for Enterprise Systems: Integrating Cognitive Analytics for Resource and Talent Optimization.
21. Viswanathan, V. (2025). Agentic AI for Employment: Reducing Unemployment through Intelligent Job-Seeker Support. LEX LOCALIS–Journal of Local Self-Government.
22. Mudusu, S. (2025). Health Insurance Fraud Detection: The Role Of Advanced It Systems In Preventing And Identifying Fraud. International Journal, 16(1), 3769-3777
23. Mudusu, S. K. (2026, February 9). AI-augmented data quality engineering. 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. 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.
26. Sikder, M. Z., Shakil, M. A. I., Ahad, A., Karim, M. F., Intakhab, B., & Islam, D. A.

International Journal of
LAW, ARTS AND HUMANITIES
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0523 www.zesterapublications.com Original Research Paper

(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.

27. Manoharan, D. (2024). Governance-Oriented Quality Engineering Framework for Healthcare EDI Modernization. International Journal of Multidisciplinary on Science and Management IJMSM, 1(2).
28. Ravishankara, M. (2026, February). PlotChain: Deterministic Checkpointed Evaluation of Multimodal LLMs on Engineering Plot Reading. In SoutheastCon 2026 (pp. 1-8). IEEE.
29. Doragacharla, V. R. (2026). Building Real-Time Pricing Systems for Modern Retail. Available at SSRN 6451760.
30. 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
31. Kavuri, S. (2026). An Explainable Machine Learning Framework for Predicting Software Defects in Large-Scale Software Systems. 2026 IEEE 5th International Conference on AI in Cybersecurity (ICAIC), 1–6. https://doi.org/10.1109/icaic67076.2026.11395777
32. 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
33. Gummadi, V. P. K., Chilamkurthi, L. S., & Kavuri, S. (2026). Securing APIs in Government Clouds and Runtime Fabric Using FIPS-Enabled MuleSoft. 2026 International Conference on Artificial Intelligence, Systems, and Emerging Technologies (ICAISET), 1–6. https://doi.org/10.1109/icaiset66439.2026.11542099
34. 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