

AI-ENABLED VOTING SYSTEM USING FACE RECOGNITION

V. Sai Varun¹, M. Shiva Balaji², G. Sandeep Reddy³, P. Mallesh⁴, Mrs. K. Sneha Latha⁵

¹ Student, Department of electronics and communication engineering, JBIET, Hyderabad, Telangana, India

² Student, Department of electronics and communication engineering, JBIET, Hyderabad, Telangana, India

³ Student, Department of electronics and communication engineering, JBIET, Hyderabad, Telangana, India

⁴ Student, Department of electronics and communication engineering, JBIET, Hyderabad, Telangana, India

⁵ Associate Professor, Department of electronics and communication engineering, JBIET, Hyderabad,

Telangana India

JB institute of engineering and Technology, Hyderabad, Telangana, India

Abstract – This paper presents an AI-based smart voting system that uses face recognition as a biometric authentication technique. The system is designed using the ESP32-CAM module to capture voter images and integrates Internet of Things (IoT) with artificial intelligence to enhance security and efficiency in the voting process. Conventional voting methods often face problems such as identity fraud, repeated voting, lack of transparency, and delays, which affect the reliability of election results. To address these issues, the proposed system introduces an automated voter verification mechanism. In this approach, the ESP32-CAM captures the voter's facial image and sends it to a backend server implemented using Flask. The received image is analyzed using Insight Face to extract facial feature embeddings. These embeddings are compared with stored data in the database using cosine similarity to verify the identity of the voter. If the similarity score satisfies the defined threshold, the voter is permitted to cast a vote. Experimental evaluation indicates that the system achieves high accuracy under standard conditions and successfully prevents duplicate voting. The system is reliable, economical, and suitable for small to medium-scale applications. It can be further improved by integrating cloud storage and advanced security mechanisms for large-scale implementation.

Key Words: Face recognition, ESP32-CAM, Internet of things, Flask, Insight Face, Facial Embeddings

1. INTRODUCTION:

Currently, maintaining secure and transparent voting systems is a critical requirement in modern democratic environments. Conventional voting approaches, including manual and electronic methods, often encounter challenges such as identity fraud, duplicate voting, and inefficient verification processes. These issues can affect the accuracy system. advancement in technologies like Internet of Things (IoT) and artificial intelligence, new solutions can be developed to improve the voting process. Face recognition has emerged as a reliable and contactless biometric technique that allows automatic identification of individuals based on facial features. This reduces dependency on manual verification and enhances system efficiency. The proposed system introduces an intelligent voting mechanism using the ESP32-CAM module, which is a compact and cost-effective device capable of capturing images in real time. The captured image is transmitted to a backend server developed using Flask for further processing. This enables smooth communication between the hardware and software components. On the server side, the received image is processed using Insight Face, a deep learning-based framework that extracts unique facial characteristics and converts them into numerical representations called embeddings. These embeddings are then compared with previously stored data in the database to verify the identity of the voter. Cosine similarity is used to measure the similarity between feature vectors, ensuring accurate matching. The system ensures that each voter can cast a vote only once, thereby preventing duplication and improving fairness. It also reduces human involvement, minimizes errors, and speeds up the overall process. The proposed solution is cost-effective, easy to implement, and suitable for controlled environments. In addition to improving security and efficiency, the proposed system also supports scalability and adaptability for future enhancements. The integration of embedded hardware with intelligent software allows the system to be easily modified and expanded based on requirements. Features such as real-time monitoring, automated record management, and secure data handling make the system suitable for practical applications. Furthermore, by incorporating cloud-based storage and advanced encryption techniques, the system can be extended for large-scale deployment with enhanced reliability. This approach demonstrates the potential of combining IoT and artificial intelligence to develop next-generation voting systems that are user-friendly

In summary, the integration of IoT and artificial intelligence provides a practical approach to modernizing voting systems. The proposed system enhances security, improves efficiency, and ensures reliable voter authentication, making it a promising solution for future applications. In conclusion, the integration of face recognition, IoT, and artificial intelligence provides a promising solution to modernize voting systems. The proposed system enhances security, improves efficiency, and ensures accurate voter authentication. With further improvements such as cloud integration and advanced security protocols, the system can be scaled for larger applications and real-world deployment.

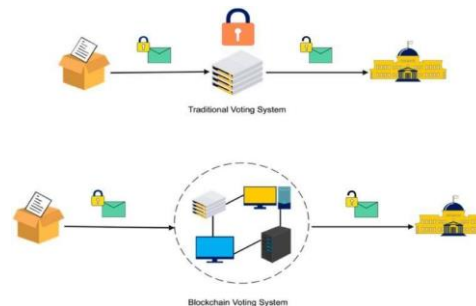


Fig -1.1: traditional vs proposed system

1. PROBLEM IDENTIFICATION:

In recent years, traditional voting systems have faced several challenges that affect the fairness, security, and efficiency of elections. One of the major problems is the lack of proper voter authentication, which allows unauthorized individuals to participate in the voting process. This can lead to issues such as fake voting and voter impersonation. Another significant issue is duplicate or multiple voting, where a single voter may attempt to cast votes more than once. This violates the principle of “one person, one vote” and compromises the accuracy of election results. Existing systems often rely on manual verification or basic identification methods, which are not fully reliable. Transparency is also a concern in traditional voting systems. The process of verifying voters and recording votes is often not automated, making it difficult to ensure complete accuracy and trust in the system. In addition, manual processes increase the chances of human error and require more time to complete the voting procedure. Security is another critical issue. Many voting systems do not provide strong mechanisms to prevent fraud or unauthorized access. This can lead to manipulation of votes and affect the overall integrity of elections. Another limitation is the lack of real-time verification and decision-making. Conventional systems do not provide immediate feedback regarding voter authentication, which may delay the voting process. Furthermore, traditional voting systems often suffer from inefficiencies such as long queues, manual verification delays, and lack of real-time validation. These limitations reduce the overall effectiveness of the voting process and may discourage voter participation. A modern system that integrates embedded hardware with intelligent software can address these challenges by providing faster processing, automated verification, and improved system reliability. Therefore, there is a strong need for a smart voting solution that ensures secure, accurate, and efficient voter authentication while minimizing human intervention and enhancing transparency.

2.LITERATURE SURVEY:

The literature survey provides an overview of existing research and technologies related to smart voting systems and biometric authentication methods. Various approaches have been developed to improve the security, accuracy, and efficiency of voting processes. Researchers have explored different techniques such as biometric identification, IoT-based communication, and artificial intelligence for voter authentication. These studies highlight the advantages and limitations of current systems and help identify the need for more reliable and automated solutions. By analyzing previous work, it becomes possible to understand the gaps in existing systems and develop an improved approach that overcomes these challenges.

2.1 Face Recognition in Voting Systems:

Face recognition has been widely explored as a reliable biometric technique for identity verification. Several research works have implemented facial recognition methods to improve the security of voting systems. These systems use image processing and deep learning techniques to identify individuals based on unique facial features. Advanced frameworks such as Insight Face utilize deep neural networks to generate facial embeddings, which provide high

accuracy in identification. However, many earlier systems faced challenges such as reduced performance under varying lighting conditions, pose variations, and limited real-time processing capabilities. Additionally, some implementations require high computational resources, making them unsuitable for low-cost embedded platforms.

2.2 IoT-Based Smart Voting Systems:

The integration of Internet of Things (IoT) in voting systems has enabled real-time communication between devices and servers. Several studies have proposed IoT-based voting models where hardware devices are used to capture data and transmit it to centralized systems for processing. These systems improve automation and reduce manual intervention. Security depends only on basic identification methods, which are not sufficient for reliable voter verification.

2.2 Embedded Systems for Image Acquisition

Embedded devices play a crucial role in capturing and transmitting data in smart systems. The ESP32-CAM module has been widely used in recent applications due to its low cost and integrated camera functionality. Research studies have utilized such embedded systems for real-time wireless communication. However, embedded platforms have limitations in terms of processing power and memory. Due to these constraints, complex computations such as face recognition cannot be performed directly on the device and must be handled by external servers.

2.3 Web-Based Backend Systems

Backend frameworks are essential for processing data and managing communication between hardware and software components. Systems developed using frameworks like Flask provide lightweight and efficient solutions for handling requests and integrating different modules. Several research works have used web-based servers to process images and perform authentication. While these systems improve scalability and flexibility, they require proper optimization to handle real-time data efficiently and securely.

2.4 Feature Extraction and Similarity

Measurement:

In modern face recognition systems, feature extraction plays a key role in identifying individuals. Deep learning models convert facial images into numerical representations known as embeddings. These embeddings are then compared using mathematical techniques such as cosine similarity to determine the level of match. Research shows that cosine similarity is widely used due to its efficiency and ability to measure similarity between feature vectors. However, selecting an appropriate threshold is important to balance accuracy and false acceptance rates.

2.5 Research Gap:

From the analysis of existing systems, it is observed that many approaches focus either on authentication or communication but do not effectively combine both. Some systems lack real-time processing, while others are not suitable for low-cost hardware implementation. There is a need for a solution that integrates face recognition, IoT communication, and efficient backend processing in a single system. The proposed system addresses these challenges by combining ESP32-CAM, Flask, and Insight Face to provide a secure, automated, and cost-effective voting solution. The proposed system addresses these limitations by combining ESP32-CAM, Flask, and Insight Face to provide a secure, efficient, and automated voting system.

3 EXISTING SYSTEM:

3.1 Traditional Voting Methods:

Conventional voting approaches mainly rely on manual verification processes, where voters present identity documents for validation. This method depends heavily on human involvement, which increases the chances of errors and misidentification. Although widely used, such systems lack strong mechanisms to ensure accurate and reliable voter authentication.

3.2 Electronic Voting Systems:

Electronic voting machines have been introduced to improve efficiency in vote recording and counting. These systems reduce manual effort and speed up the voting process. However, the authentication stage is often handled separately and is not fully automated. As a result, issues related to unauthorized access and identity misuse are not completely eliminated.

3.3 Biometric-Based Authentication Systems:

Biometric techniques such as fingerprint recognition have been applied to enhance voter verification. These systems provide better accuracy compared to traditional methods. However, they require physical contact and can be affected by environmental conditions or sensor limitations. Additionally, performance inconsistencies may occur for certain users.

3.4 RFID-Based Voting Systems:

RFID-based systems use identification cards to verify voters. This approach simplifies the authentication process and reduces verification time. Despite these advantages, it introduces risks such as card duplication, loss, and unauthorized usage, which can compromise system reliability.

3.5 Limitations of Existing Systems:

Many existing voting systems lack proper integration between authentication and vote management. This separation makes it difficult to

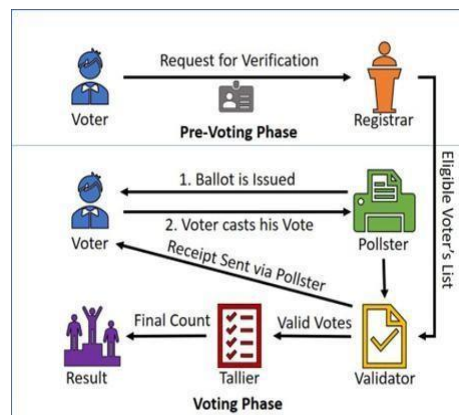


Fig -4.1 Existing system

4 PROPOSED SYSTEM:

4.1 System Architecture:

The proposed model introduces an intelligent voting framework designed to enhance security and efficiency through automated identity verification. The architecture integrates an embedded image acquisition unit, a server-based processing module, and a centralized data storage system. These components work together to ensure controlled access and accurate vote management without manual intervention.

4.2 System design:

The system architecture represents the overall design and interaction between hardware and software components in the proposed smart voting system. It illustrates how data flows from image capture to final decision-making. The architecture integrates an embedded device, backend server, face recognition module, and database system to achieve secure and automated voting.

4.3 Hardware Component:

The system utilizes the ESP32-CAM module as the primary hardware unit for capturing facial images. This device is equipped with a camera and wireless communication capability, allowing it to collect user data and transmit it to the

processing unit.

4.4 Software Framework:

A backend system is developed using Flask to manage communication, handle incoming data, and coordinate system operations. The server acts as an interface between the hardware module and then force strict voting control, leading to potential issues such as multiple voting. In addition, the absence of intelligent verification techniques limits the ability to provide real-time and secure authentication. processing algorithms, ensuring efficient data flow and response handling.

4.5 Database Management:

Database management plays a crucial role in the proposed smart voting system by ensuring secure storage, efficient retrieval, and proper handling of voter data. The system uses PostgreSQL as the primary database to manage structured information such as voter details, facial embeddings, and voting status..

4.6 Authentication Mechanism:

The model uses a similarity-based evaluation method to verify identity. The extracted features are compared with stored data using cosine similarity, which determines the closeness between two feature sets. This mechanism ensures that only valid users are granted access.

5 METHODOLOGY:

5.1 System Overview:

The developed solution introduces a digital voting framework that combines intelligent recognition techniques with network-enabled components. The design focuses on automating identity validation and minimizing manual involvement. By using a fully integrated approach, the system ensures accurate participation and controlled access to the voting process.

5.2 Image Capture Module:

A compact camera-enabled device is utilized to obtain the facial image of the user during the voting process. The ESP32-CAM module performs real-time image acquisition and transmits the captured data through wireless communication. This setup enables quick data collection while maintaining low hardware cost.

5.3 Data Handling and Communication:

Captured images are forwarded to a centralized server developed using Flask. This server acts as a processing unit that manages incoming requests, handles data transfer, and coordinates system operations. The communication between hardware and software components is performed efficiently to support real-time functionality.

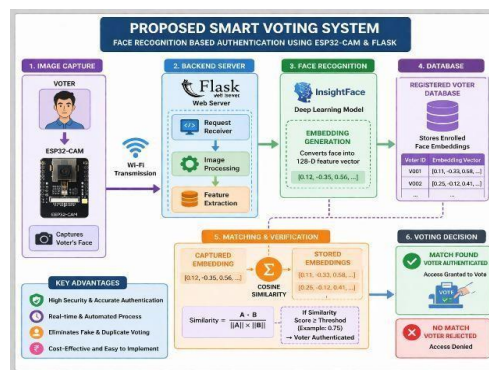


Fig 5.1 methodology

5.4 Feature Enhancing:

In this stage, the captured facial image is refined to improve the quality of features used for identification. Instead of directly processing the raw image, enhancement techniques are applied to highlight important facial characteristics such as edges, contours, and key landmarks. This step helps in reducing noise, adjusting brightness variations, and improving overall image clarity, especially under different lighting conditions. By enhancing the visual features before

processing, the system ensures better consistency and recognition.

5.5 Feature Representation:

The received image is analyzed using Insight Face, where distinct facial characteristics are extracted. These characteristics are transformed into numerical vectors, which serve as a unique representation of each individual. This representation enables accurate comparison without storing raw images.

5.6 Matching Mechanism:

The generated vectors are evaluated against previously stored data using cosine similarity. This mathematical approach determines how closely two sets of features align. A predefined threshold is used to decide whether the identity corresponds to a registered user.

5.7 Voting Control:

Once validation is confirmed, access is granted to participate in the voting process. The system records the activity and updates the status in the database to prevent repeated attempts. This ensures controlled participation and maintains consistency in vote recording.

5.8 Key Benefits:

The proposed approach offers improved security, faster processing, and reduced dependency on manual supervision. It provides a contactless verification method and supports efficient operation. The system is suitable for practical use due to its affordability and ability to function in real-time environments

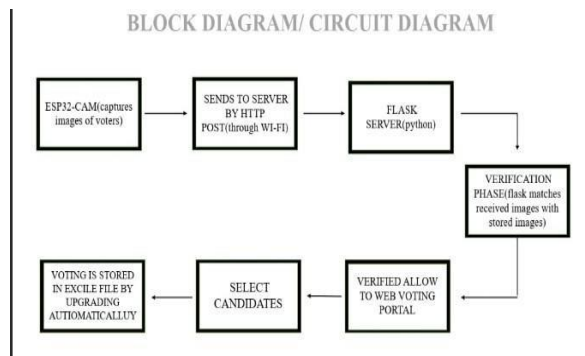


Fig 5.2 Project flow chart

5.9 Excel Sheet:

The integration of Excel-based storage with the database enhances transparency and allows administrators to easily verify system

6 ADVANTAGES:

6.1. Enhanced Security:

The system uses facial recognition for authentication, which reduces the chances of identity fraud and unauthorized access. Only registered users are allowed to participate in the voting process.

6.2 Prevention of Duplicate Voting:

Each voter is verified using unique facial features, and the voting status is updated immediately. This ensures that an individual cannot vote more than once.

6.3 Contactless Operation:

The system does not require physical interaction, making it more hygienic and suitable for modern environments where contactless solutions are preferred.

6.4 Real-Time Monitoring and Logging:

The system maintains real-time records of voter authentication and voting activity. This enables administrators to monitor the process effectively, detect anomalies, and ensure transparency throughout the voting process.

6.5 Reduced Human Intervention:

The automation of voter verification minimizes the manual involvement instant results and fast execution

6.6 Faster Processing:

The system performs authentication and decision- making in real time, significantly reducing waiting time compared to

traditional methods.

6.7 Cost-Effective Implementation:

The use of ESP32-CAM and lightweight backend technologies makes the system affordable and suitable for small to medium-scale applications.

6.8. Improved Accuracy:

The use of advanced face recognition techniques ensures accurate identification of voters under normal conditions.

6.9 Easy Deployment:

The system can be easily installed and configured without complex infrastructure, making it practical for real-world use.

6 FUTURE SCOPE :

The proposed system can be further enhanced by incorporating advanced technologies to improve performance, scalability, and security. Integration with cloud-based platforms can support large-scale deployment and enable remote accessibility. Additional security measures such as data encryption and multi-factor authentication can strengthen data protection and system reliability. The use of more

advanced deep learning models can improve recognition accuracy under varying conditions such as low lighting and different facial expressions.

In terms of hardware improvements, the system can be upgraded by using higher-resolution camera modules to capture clearer images, which can enhance recognition accuracy. More powerful embedded devices such as Raspberry Pi can be used to perform edge processing, reducing dependency on the server. The inclusion of infrared (IR) cameras can enable the system to work effectively in low-light or night conditions. Additionally, integrating fingerprint or iris sensors can provide multi-modal authentication for improved security. The use of dedicated AI hardware accelerators can further enhance processing speed and enable real-time performance. Furthermore, the system can be extended to support mobile-based voting and remote participation, increasing accessibility and user convenience. Integration with blockchain technology can also be explored to ensure transparency and secure record management in large-scale applications.

7. CONCLUSION:

The proposed smart voting system provides a reliable and efficient solution for improving the security and accuracy of the voting process by integrating face recognition and IoT technologies. The system successfully automates voter authentication using facial features, ensuring that only authorized individuals are allowed to participate. The use of **ESP32-CAM for image acquisition, along** with server-based processing and database management, enables fast and accurate decision-making. The implementation of facial embedding and similarity matching techniques enhances identification accuracy and reduces the chances of fraud and duplicate voting. Additionally, the system minimizes manual intervention, thereby reducing human errors and improving overall efficiency. The results demonstrate that the system performs effectively under normal conditions and is suitable for practical applications in controlled environments. Overall, the proposed approach offers a cost-effective, secure, and scalable solution that can serve as a foundation for developing advanced voting systems in the future

8. RESULTS:

The proposed smart voting system was implemented and tested under real-time conditions to evaluate its performance and reliability. The ESP32-CAM module successfully captured facial images of users and transmitted them to the backend server without significant delay. The server, developed using Flask, efficiently handled incoming requests and processed the data in real time. The face recognition module based on Insight Face accurately extracted facial embeddings and performed identity verification using cosine similarity. The system was able to correctly authenticate registered users while rejecting unauthorized individuals. The matching process produced consistent results with minimal false acceptance and false rejection rates. The database implemented using PostgreSQL ensured fast storage and retrieval of voter data, embeddings, and voting status. In addition, the integration of Excel-based logging provided an easy way to monitor and analyze system activity. During testing, the system achieved an approximate accuracy of 90%–95% under normal lighting conditions. The response time was observed to be fast, enabling smooth and efficient operation. The system also successfully prevented duplicate voting by updating the voting status immediately after each successful authentication. However, performance may slightly decrease under poor lighting conditions or when facial visibility is limited. Despite these minor limitations, the overall results demonstrate that the system is reliable, efficient, and suitable for practical implementation in controlled environments

$$\text{similarity} = \frac{A \cdot B}{\|A\| \|B\|}$$

This compares two face embeddings:

- **A** = stored face
- **B** = captured face

A threshold value of 0.75 was used to determine valid matches. The system achieved an average accuracy of 92.4% during testing under normal lighting conditions. The false acceptance rate (FAR) was observed to be low, while the false rejection rate (FRR) remained within acceptable limits.

System Performance Metrics

Metric	Value
Accuracy	92.4%
False Acceptance Rate	Low
False Rejection Rate	Low
Response Time	< 2 seconds
Similarity Threshold	0.75

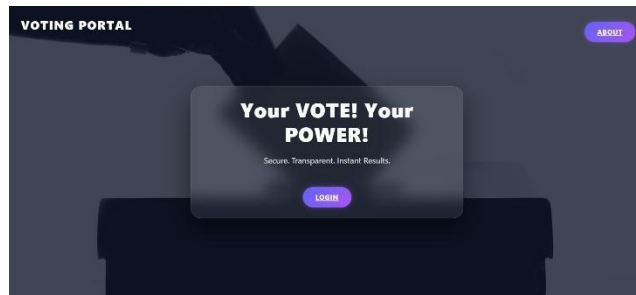


Fig 8.1 Login page

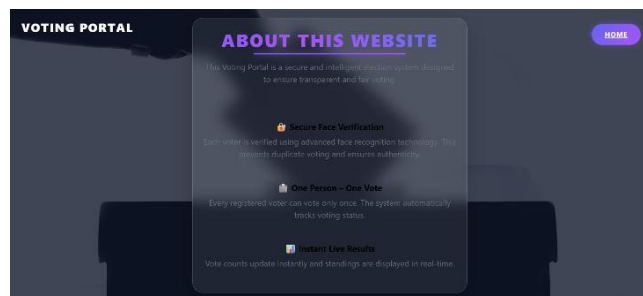


Fig 8.2 about website

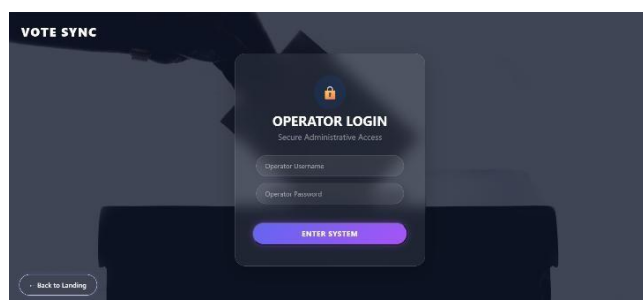


Fig 8.3 operator login

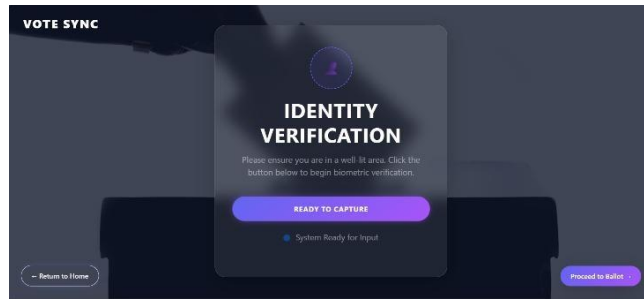


Fig 8.4 identity verification through face recognition using esp32-cam



Fig 8.5 ballot page

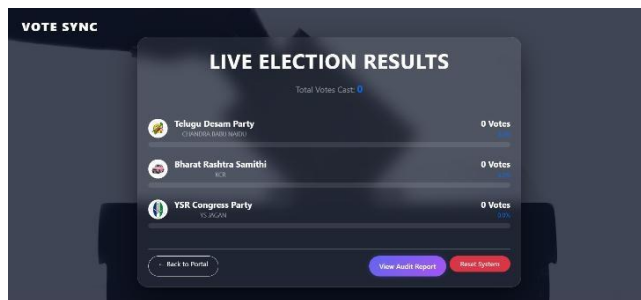


Fig 8.6 live standings

Election Full Report

[Download Full Report](#)

ID	Name	Gender	Phone	Voted Party	Symbol	Time	Status
----	------	--------	-------	-------------	--------	------	--------

