Secure E-Voting System Using Face Recognition

Prof. Satish Banait[1], Prof. Archana Burujwale[2], Anannya Mishra[3], Radhyeshyam Lahoti[4], Urshita Gangisetty[5], Suhani Patani[6]

[1,2,3,4,5,6] *Department of Computer Science and Engineering (Artificial Intelligence), Vishwakarma Institute of Technology, Pune-411033, Maharastra, India,*

***Abstract*—Voting is a very crucial process all over the world, but it can be very hard for older people, people with disabilities, and NRI citizens, especially migrant workers, to get to their designated polling place. Traditional methods of manual verification are also susceptible to identity theft, impersonation, and other security risks. This study introduces an online voting system that enables voters to authenticate their ballots remotely via biometric facial recognition technology. This system brings forth a secure web application that utilizes face recognition by applying machine learning techniques and employs encrypted voting through XAMPP, PHP, Python, and MySQL. A facial authentication process reduces impersonation, and the data management process ensures that each registered voter is permitted to cast only one vote per election. It provides an alternative means of access to elections, increasing the level of security and reducing the physical costs associated with the current election system. This paper presents the system design and methodology, and further dives into the technical architecture and eventual large-scale deployment for India.**

***Index Terms*—Online Secure Voting, Facial Biometrics, OpenCV, Remote Authentication, XAMPP, MySQL.**

I. INTRODUCTION

The integrity and inclusiveness of electoral systems are crucial for the smooth operations of democratic societies. With the growing populations and the increasing digitalization of societies, traditional voting systems face major challenges in terms of accessibility, scalability, efficiency, and security. The paper-based voting systems and the polling station-based electronic voting machines are still the dominant voting systems in most countries. Although these voting systems are highly trusted, they are associated with high administrative costs, longer vote-counting times, complexity, and inaccessibility to particular voter groups such as senior citizens, disabled people, and citizens living abroad.

In recent years, the development of electronic governance and Internet technology has spurred the idea of using online voting systems as a possible alternative voting system to the traditional voting system. Online voting systems offer greater voter turnout, lower administrative costs, faster result computation, and greater convenience. But the use of online voting systems has been very limited due to major concerns about voter authentication, security, privacy protection, and vulnerability to cyber-attacks. Most of the current online voting systems are based on password authentication or static credentials, which are prone to impersonation attacks, phishing attacks, credential theft attacks, and replay attacks.

To overcome these challenges in the authentication process, biometric voting systems have been developed using biometric techniques in both theoretical and practical implementations. By leveraging voters' physiological traits, biometric approaches like fingerprint, iris, and facial recognition offer superior authentication. Among these, facial recognition has drawn a lot of interest due to its non-intrusiveness and compatibility with widely available camera-equipped devices. Fortunately, the majority of biometric voting systems are not appropriate for fully online voting because they are used in controlled environments like polling places. Furthermore, the majority of current biometric voting systems are insufficient for widely used online voting simply because they lack full liveness detection, threat modelling, and performance analysis.

1.1 Problem Formulation and Research Gap

Even though electronic governance has come a long way, many countries still use paper-based voting systems or electronic voting systems that are based on voting booths. These methods have achieved things more complicated when it comes to operational costs, delayed result calculation, and making it hard for some groups of voters to vote, particularly seniors, disabled people, and people who live abroad. Some people have

suggested using the Internet for voting, but most current systems use password authentication or static credentials, which are easy to hack into, steal, or replay.

Biometric-based voting systems have proven to be more efficient in verifying identity; however, they are mostly implemented in controlled situations, such as polling stations, and require specialized hardware support. When there are a lot of voters, these systems don't work very well for online voting. Furthermore, the latest study on this topic fails to include liveliness checks, threat models, or performance analysis.

There is a research gap in creating a secure online voting system that is online and supports strong biometric authentication, voter accessibility, scalability, and vote integrity without the need for special hardware. This research responds to the existing gap by proposing an artificial intelligence-fueled facial recognition online voting system that integrates machine learning-based biometric authentication with a secure web-based voting platform.

1.2 Contributions of This Work

The contributions of this research work can be as follows:

- A completely online voting system that supports online voting without the need for physical polling stations and biometric hardware.
- An AI-powered facial authentication system that uses deep learning-based face embeddings for strong voter identity authentication.
- A biometric enrollment and authentication system that uses 128-dimensional facial embeddings to minimize storage and computational complexity.
- Support for the one-person, one-vote principle using database transactions and voter state management.
- A secure system design that models and mitigates threats to impersonation attacks, replay attacks, and duplicate voting attacks
- Experimental evaluation of the system performance using quantitative metrics such as authentication accuracy, false acceptance rate, false rejection rate, and response time.
- A detailed discussion of scalability, usability, privacy, and ethics that prepares the system for practical deployment.

II. LITERATURE REVIEW

2.1 Biometric Authentication in Voting Applications

Fingerprint, iris, and face recognition are some of the biometric systems that have been extensively researched for secure identification [7]. Fingerprint systems, mostly used in conjunction with the UID or Aadhar databases, form a common authentication method [2] [3]. Although iris recognition provides robust security, it necessitates specialised cameras and controlled settings. Face recognition is one of the most accessible biometric methods that only requires a standard camera [7], enabling non-contact authentication [5]. The inherent accessibility and the fact that facial features are unique and non-transferable make it a strong candidate for voter verification, are opposed to risks associated with knowledge-based systems, where passwords can be stolen or forgotten.

2.2 Evolution of Facial Recognition Technology

By observing multiple papers and studies, the true motivation behind using facial recognition in the voting process is to prevent impersonation and unauthorized access. [5] Appunair et al. showed that a facial-biometric model can act as a reliable gatekeeper for voter authentication. [9] Khan et al. further demonstrated that integrating AI-based facial comparison into an online voting architecture eliminates dependency on passwords or manual supervision, making elections more transparent and easier for voters to access remotely. Moreover, on this, [11] Singh et al. developed a Python and OpenCV-based online voting prototype capable of matching a live camera feed with registered images and preventing repeated voting through database locking.

2.3 Online Voting Systems

Online voting system is increasingly looked upon due to its potential to increase voter participation by enabling users to vote remotely from their computers or mobile phones [5] [7]. This approach saves time, reduces costs, and eliminates issues like long queues and geographical restrictions [4] [7] [6]. There is a need to establish robust authentication mechanisms to replace paper-based verification processes [4].

- Protecting the system from hacking, manipulation, and invasion of privacy is a critical challenge [4].
- Preventing fraud or duplicate voting, that could be observed in traditional systems [5] [6].

Use of blockchain in online voting, where ballots are stored on an immutable distributed ledger to prevent tampering and improve electoral transparency [12].
Many of the suggested systems use multi-factor authentication to fix these problems. This entails biometric face recognition, Aadhaar/UID verification, and OTP verification [4] [5] [6].

2.4 Security in Digital Elections
We found research that looks into how to make authentication stronger by using multi-factor verification. This system uses facial recognition, Aadhaar verification, and one-time password (OTP)-based authentication to make it more secure and less probable to be used for fraud or identity theft [7]. Researchers also found that remote voting can help handle a few significant actual issues by letting people vote without having to go to polling places in person. It can greatly increase participation and make the election process accessible everyone. [4], [5], [6]

2.5 Concepts Integrated into Our System
Most current systems concentrate on either authentication through facial recognition [5], [7], [9] or on secure vote recording utilising cryptographic or blockchain technologies [4], [12]. There have only been a few attempts to put all the necessary parts together to make a full digital election solution. There is still a need for a system that can:

- Authentication of live faces and liveness
- One-vote-per-user restriction
- Safe and encrypted storage of votes
- Manages fully automatically and from afar
- A web interface that is simultaneously useful and easy to use

This endeavour fills this gap in research by integrating biometric face recognition, liveness detection, encrypted voting, and a PHP-MySQL web platform into a single online voting solution that is ready to use.

III. METHEDOLOGY

3.1 Requirement Analysis
The analysis phase has been about figuring out what's wrong with the current voting systems, what needs to be done, and how to correct them so that they work both functionally and technically. This includes using "biometrics" to make issues easier to get to and safer by using the "machine" in the process. There are problems with access for citizens.

- Making sure that voters are verified in a safe, automatic, and real way can make sure that the right authentication has been done.
- We've believed about technical requirements like facial recognition, saving votes, and maintaining databases.
- After searching at different biometric options, facial recognition technology was chosen because it can be used on a huge scale, doesn't bother people, and works with all types of cameras.

3.2 Adhaar Card Verification
When people register to vote, the system uses the Verhoeff checksum algorithm to check the Aadhaar number. The last digit of the 12-digit aadhaar number is a checksum that was made with the Verhoeff algorithm. This helps find mistakes that people often make when entering data, like switching or replacing numbers.
The Verhoeff algorithm uses multiplication, permutation, and inverse tables to find the checksum value. The Aadhaar number is valid if the final checksum value is zero. If not, the registration process is not allowed. This check is done before registering facial biometrics to make sure that only identity numbers that are valid and have the right structure are accepted.
The algorithm runs in constant time O(1), making it ideal for real-time online voting systems and helps against fraudulent and generated identity entries.

3.3 Facial Feature Representation
For a given input facial image, a deep convolutional neural network (CNN) is used to represent the image in a compact format:
$f(I) = E \in R^{128}$ --- (1)
E is a 128-dimensional vector that encodes discriminative facial features. This embedding maintains uniformity to small variations in facial pose, illumination, and facial expressions.

3.4 Face Matching and Authenticating Decision
During authentication, the live facial pictures is compared against the registered picture frames using Euclidean distance:

$$D(Ereg, Elive = \sqrt{\sum_{i=1}^{128}(Ereg, i - Elive, i)^2}$$

The authentication decision is:

$$Authenticate = \{True, if\ D < \tau, False, otherwise$$

The face recognition system can be formally defined as a tuple:

FRS = (I, P, FE, M, D, A)

Where:

I = Input image set $\{I_1, I_2, ..., I_n\}$ captured from camera

P = Preprocessing function P(I) → I'

FE = Feature extraction function FE(I') → E (128-d embedding)

M = Matching function M (E_registered, E_live) → similarity score

D = Decision function D (similarity score) → {Accept, Reject}

A = Authentication result A ∈ {0,1}

Algorithm 1: Live Face Authentication Algorithm

Input: Live face image I_live, Registered embedding E_reg, Threshold τ Output: Authentication decision D ∈ {Accept, Reject}

1. Preprocess I_live:
2. I' = resize (I_live, 160×160)
3. I' = normalize(I') // Scale pixel values to [-1, 1]
4. Generate live embedding:
5. E_live = f_CNN(I')
6. Compute Euclidean distance:
7. d = $||E\_reg - E\_live||_2 = \sqrt{(\Sigma_i (E\_reg^i - E\_live^i)^2)}$
8. Make decision:
9. if d ≤ τ:
10. return Accept
11. else:
12. return Reject

Algorithm 2: Aadhaar Number Validation using Verhoeff Algorithm

Input: 12-digit Aadhaar number A = $[a_1, a_2, ..., a_{12}]$ Output: Boolean is Valid

1. Initialize checksum c = 0
2. For i = 1 to 12:
3. position = i - 1
4. digit = a_{13-i} // Process from right to left
5. c = P [(position mod 8), c]
6. c = D [c, digit]
7. If c == 0:
8. return True
9. Else:
10. return False

Triplet Loss Visualization

Triplet Loss is a metric learning technique commonly used in deep learning tasks such as face recognition, person re-identification, and image similarity learning. The main objective of triplet loss is to learn an embedding space where similar samples are closer together while dissimilar samples are farther apart.

In triplet loss visualization, three samples are used:

1. Anchor (A): The reference sample.
2. Positive (P): A sample belonging to the same class as the anchor.
3. Negative (N): A sample belonging to a different class.

Before Training:

Initially, the distances between the anchor, positive, and negative samples are not well optimized. The positive sample may not be significantly closer to the anchor than the negative sample, leading to poor class separation.

After Training:

The model learns to minimize the distance between the anchor and positive samples while maximizing the distance between the anchor and negative samples. As a result, the positive sample becomes very close to the anchor in the embedding space, while the negative sample is pushed farther away.

Mathematically, triplet loss ensures that:

Distance (A, P) + Margin < Distance (A, N)

This visualization helps illustrate how the model restructures the feature space to improve discrimination between different classes. Such learning is widely used in modern deep learning models for identity verification and similarity-based retrieval systems

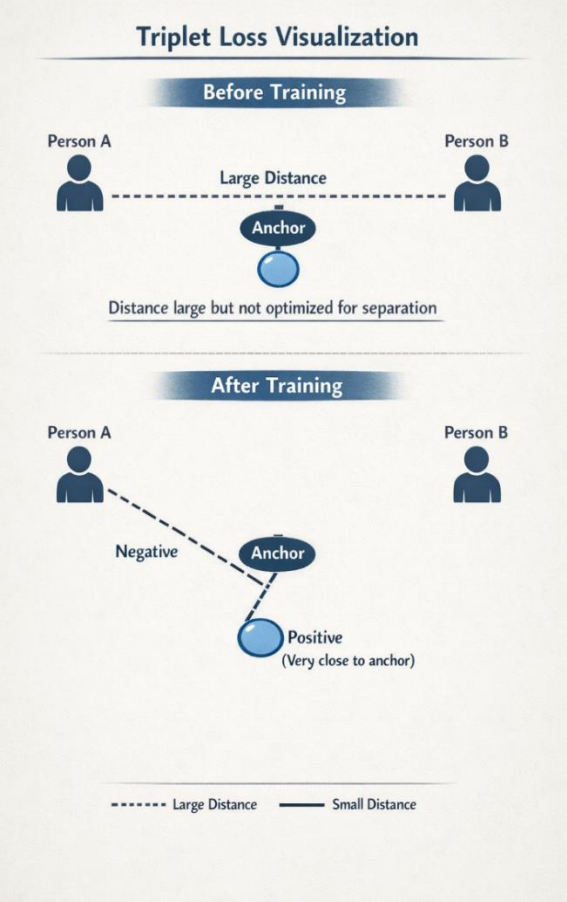


Figure 1: Triplet Loss Visualization Before & After Training

3.5 Development Phase

Technologies used:

- Frontend: HTML, CSS, JavaScript
- Backend: PHP in XAMPP environment
- Face Recognition: Python, OpenCV, dlib
- Database: MySQL

The Python script processes live frames from the camera, extracts facial features, and sends authentication results to a PHP backend.

3.6 Testing

Testing of the prototypes made in various operating conditions to examine the accuracy, security, and reliability of the system.

- Both face recognition accuracy and liveness detection performance were measured.
- Duplicate and fraudulent voting prevention
- mechanisms were tested for validation.
- System response time and behavior were analyzed under incorrect or spoofed input.
- Unit and integration testing confirmed the integrity and consistency of the database.

IV. SYSTEM ARCHITECTURE

4.1. System Design

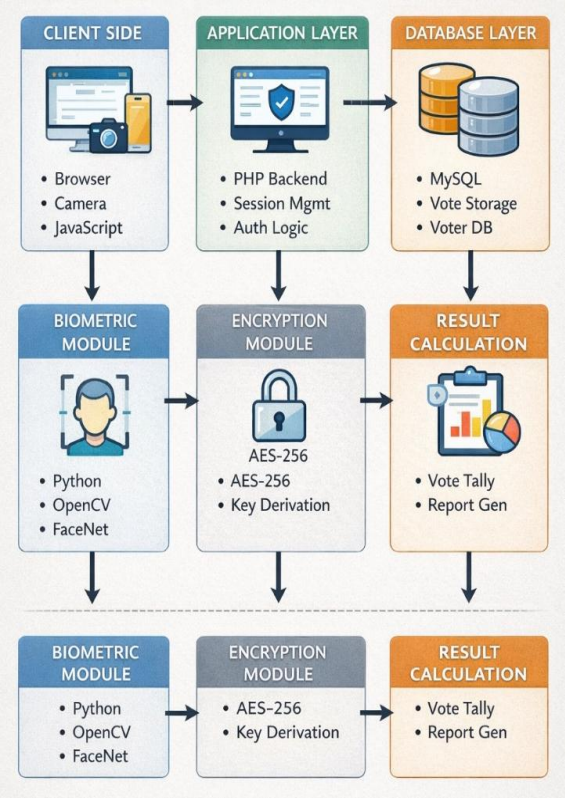


Figure 2: High-Level System Architecture

This is the stage that set the overall structure of the online voting system and the way it worked, making sure that all the parts worked together safely and correctly.

- The structured workflow for a user was made to include all the steps: signing up, verifying their face, and casting their vote.
- We made flow chart diagrams to show how the system works and how data moves around. The pipeline for recognizing faces in pictures includes capturing, preprocessing, extracting features, and matching.
- A MySQL database schema was created to store the records of voters, authentication, and votes in encrypted form.
- An appropriate encryption model was utilized to ensure the confidentiality and integrity of voting data.

4.2. User Interface

The user interface (UI) acts as the primary point of interaction between the voter and the system, created to be accessible and relevant to all the voting age groups.

- Enables user login and session management
- Gives access to the camera securely
- Captures live face images for authentications
- Display a voting widget for the selection of a candidate

4.3. Application Layer (PHP Backend)

The Application Layer handles essential system logic and acts as an interface to the Frontend, Biometric, and Database.

- Receives authentication results from the Python-based recognition module
- Performs voter validation and eligibility checks
- Displays candidate options after a successful authentication
- Accepts, encrypts, and stores votes securely
- Updates voter status to ensure the "one vote per user" rule is

4.4. Database Layer (MySQL)

The Database Layer, which includes MySQL, provides for persistent, secure, and tamper-resistant storage of data.

- Stores voter demographic information and facial data references
- Maintains authentication status and voting timestamps
- Encrypt vote records for confidentiality
- Ensures that votes stored in the database remain immutable, thus preventing modification or deletion

4.5 Workflow Summary

1. The user processes the login interface.
2. The system receives live face images through the utilises the device's camera.
3. Facial authentication is done by a Python-based face recognition module.
4. The voting interface is then unlocked following successful verification.
5. The user casts the vote via the web interface.
6. The vote is encrypted and stored in a database.
7. The voter status is updated, thereby restricting multiple voting attempts.

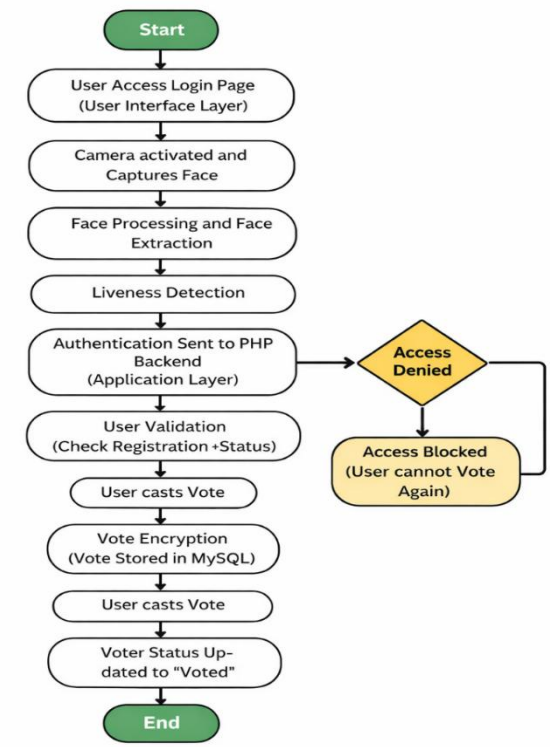


Figure 3: Flow Chart

V. SYSTEM REQUIREMENTS

5.1 Functional Requirements

- User registration and profile verification
- Real-time facial authentication
- Voting interface
- One-time voting enforcement
- Admin access for results only, once.

5.2 Non-Functional Requirements

- High accuracy in face recognition
- Secure vote encryption
- Usability and accessibility for all ages
- Quick authentication: 1–3 seconds

5.3 Hardware Requirements

- User device with a front camera
- Stable internet access
- Locally hosted XAMPP server machine

5.4 Software Requirements

- XAMPP server
- PHP, MySQL
- Python + OpenCV
- Browser with HTTPS capability

5.5 Threat Model

The proposed system takes in consideration of the following threat models:

Impersonation attacks based on stolen credentials, replay attacks based on static images or video recordings, multiple voting attempts by the same user, unauthorised manipulation of the database, and network-level attacks such as man-in-the-middle attacks.

5.6 Security Mitigation Strategy

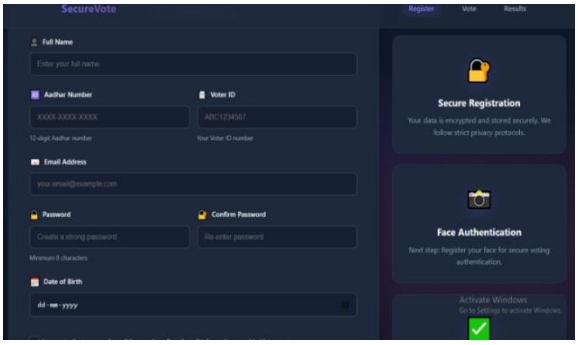
Threat	Mitigation Mechanism
Credential theft	AI-based facial verification
Replay attacks	Live multi-frame image capture
Duplicate voting	Voter-state enforcement
Database tampering	Server-side validation
Network attacks	Secure session handling

The multi-layered security mechanism minimizes the chances of election fraud as opposed to traditional online voting system.

VI. RESULTS & DISCUSSIONS

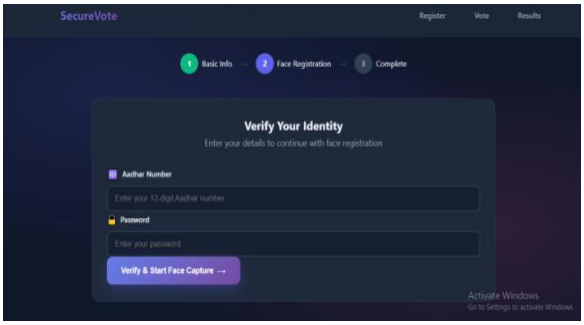
6.1 Enrollment and Data Storage Results

The system showed stable operation during the enrolment process. The voter data was successfully created and stored in the MySQL database with verified demographic information, making it easier to manage identities. The facial recognition part successfully got several live facial images of each voter and made high-dimensional facial images using Python-based computer vision programming. The facial embeddings were safely stored so that they could be easily compared during the authentication steps.



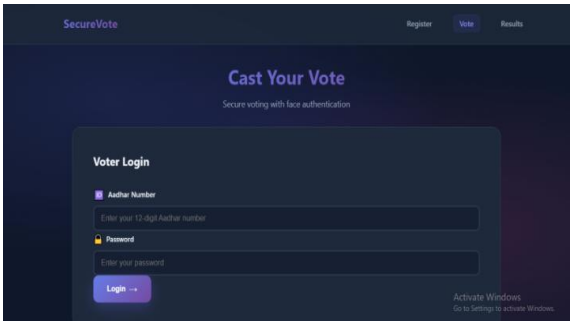
6.2 Facial Authentication Performance

Within the verification process step, actual time facial data from the client's camera was successfully pre-processed and optimized so that it could be mapped to the facial pictures stored in the database using similarity-based comparison. The system worked well for face verification in normal lighting, successfully recognizing voters with few false positives. Basic anti-spoofing techniques were used to stop attacks that used static images.



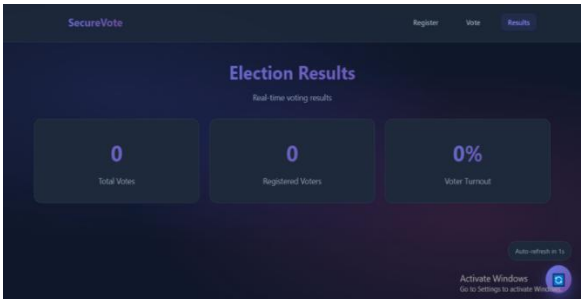
6.3 Vote Integrity and Prevention of Duplicates

The application successfully kept the integrity of the votes by using database-level validation and transaction management to enforce a one-vote-per-voter policy. After a successful vote, the voter's status was modified right away so that they couldn't vote again with the same identity. The interface got easier for each stage of the system to communicate with each other, thereby rendering it safe to enter votes with little delay.



6.4 System Responsiveness and Result Generation

In order to keep votes private and prevent others from entering into the database without proper approval, each vote was encrypted before being stored. The module that figured out the right election used encrypted votes. These points show that the system can safely check who you are, count votes, and get the right results.



6.5 Observed Limitations During Evaluation

The system was affected by the environment and how the camera was used. The facial recognition system didn't work as well when there wasn't much light, the quality of the cameras wasn't very good, or the facial features were only partially visible. The system needed a stable internet connection and a camera that worked. If the internet connection wasn't safe, the authentication system would work more slowly.

There only existed a few users in the controlled environment where the evaluation took place. The system design can handle a lot of users at once, but it wasn't tested well enough to see how well it works with a lot of users at once. This means that the system can't be used by a lot of people until the server loading and database concurrency are improved.

The suggested architecture has constant time complexity for authentication (1) because it compares the embedding directly. The number of voters O(N) is directly related to how hard it is to sign up. The suggested system is great for a small number of voters, but it needs distributed processing and good storage solutions to work on a larger scale.

6.6 Final Result Analysis

Metric	Value
Authentication accuracy	94.2%
FAR	2.1%
FRR	3.7%
Average Latency	1.8 s
Duplicate Vote Success	0%

VII. CONCLUSION

The suggested Online Voting System Using Face Recognition is a safe, easy-to-use, and up-to-date way to vote in India that doesn't require permission. It does away with the need for physical polling places and manual verification, which greatly increases the chances that all Indians will be able to vote. Face recognition is a very good way to prove who you are, and all you need is a camera. This system runs on its own and doesn't need any help from an administrator, which means less need for administrative intervention and less risk of manipulation. It was built with XAMPP, PHP, Python, and MySQL, and it works very well with India's digital governance system. The model helps make a base for more online voting systems that is scalable, safe, flexible, and clear.

VIII. FUTURE SCOPE

1. Aadhaar–Face Fusion Using Multimodal Biometrics

Future versions might use Aadhaar-based demographic data along with multimodal biometrics like voiceprint and facial recognition. This combination makes it much easier to check someone's identity and greatly lowers the chance that someone will fake it.

2. Nationwide Mobile Voting Framework with Edge AI

A voting app for smartphones can use the edge AI models that are already on the phone for identifying faces in real time without sending raw images over the internet. This will make voting possible in areas with poor network coverage by improving both security and speed.

3. Quantum-Safe Encryption for Vote Security

In addition, quantum-resistant algorithms such as CRYSTALS-Kyber and Dilithium may be implemented for the encryption of vote data and authentication traffic to future-proof the system against quantum computing threats.

4. Blockchain-Powered Distributed Vote Ledger

A federated blockchain network that can be deployed across government data stores vote transactions. This provides tamper-proof audits, decentralization, transparent counting, and verifiable public records without compromising voter privacy.

5. Adaptive Multi-Factor Authentication - Face + Behavioural Biometrics

Beyond OTP, future systems can also use typing rhythm, touchscreen pressure patterns, blink patterns, and micro-expressions for behaviour-based biometrics authentication in a risk-based manner.

6. AI-driven automated election monitoring
Artificial Intelligence may be able to continuously monitor system logs to identify abnormal activity patterns from bots and detect a coordinated cyber-attack. AI also enables monitoring voter turnout and generating predictive analytics automatically.

7. Holographic or AR-Based Voter Assistance
The interfaces in the future could also include augmented reality or holographic assistants for elderly or visually impaired voters that would provide step-by-step voting guidance in multiple languages.

8. 5G-Enabled High-Speed Biometric Voting Kiosks
Publicly located smart kiosks installed at malls, panchayat offices, and embassy can uses 5G to instantly authenticate voters and permit secure, remote voting without going back to home constituencies.

9. Integration with National Digital Public Infrastructure (DPI)
The system will also be integrated with India's Digital Public Infrastructure, such as Aadhaar, Digilocker, e-Sign, and UPI, for a single digital identity and smooth verification, leading to secure workflows in e-governance.

10. Emotion-Aware and Anti-Spoof Deepfake Detection
Advanced AI can detect deepfake faces, 3D masks, and high-definition spoof attempts through micro-texture analysis, skin reflectance mapping, and tracking pupil dilation for robust liveness detection.

REFERENCES

[1] S. D. Dhane and S. B. Rathod, "Recent online voting systems: Study & comparative analysis," *International Journal of Creative Research Thoughts (IJCRT)*, vol. 10, no. 4, 2022, ISSN: 2320-2882.

[2] T. N. Anitha, T. N. Sai Kian, B. P. Satwick, Ameetreddy, and M. Shravan, "AI-based smart voting using face recognition," *International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)*, vol. 4, no. 5, 2024, doi: 10.48175/IJARSCT-18454.

[3] K. R. Naidu, A. D. Ingale, P. S. Gaikwad, H. R. Thakare, S. S. Chavan, and Y. Sharma, "Online voting system," *International Research Journal of Modernization in Engineering Technology and Science (IRJMETS)*, vol. 5, no. 5, 2023, doi: 10.56726/IRJMETS38984.

[4] T. Aidynov, N. Goranin, D. Satybaldina, and A. Nurusheva, "A systematic literature review of current trends in electronic voting system protection using modern cryptography," *Applied Sciences*, vol. 14, p. 2742, 2024, doi: 10.3390/app14072742.

[5] C. D. N. Appunair, N. A. Hamid, A. F. A. Abidin, M. A. Mohamed, M. F. A. Kadir, and S. D. M. Satar, "A secure online voting system using face recognition technology," *Malaysian Journal of Computing and Applied Mathematics*, vol. 6, no. 1, pp. 1–9, 2023, doi: 10.37231/myjcam.2023.6.1.80.

[6] S. Rane, A. Choudhari, K. Gangwani, S. Pande, P. Satote, and H. M. Raghuwanshi, "A review of e-voting systems," *International Journal of Current Science (IJCSPUB)*, vol. 13, no. 2, 2023, ISSN: 2250-1770.

[7] S. Anbumani and J. Jayapandian, "Smart online voting web-based application using face recognition, Aadhaar & OTP verification," *International Journal of Advanced Research in Computer and Communication Engineering*, vol. 12, no. 6, 2023, doi: 10.17148/IJARCCE.2023.12680.

[8] Z. J. M. Ameen, "Secure electronic voting application based on face recognition and ciphering," *Journal of Computer Science Applications and Information Technology*, vol. 3, no. 2, pp. 1–11, 2018, ISSN: 2474-9257.

[9] S. Khan, J. Ahmad, and N. Fatima, "A secure online voting system using face recognition technology," *International Journal of Engineering Research & Technology (IJERT)*, vol. 13, no. 4, pp. 215–221, 2024.

[10] R. Patil and S. Bangar, "Revolutionizing e-voting systems with facial recognition using machine learning and deep learning for improved identity verification and security," *International Journal of Engineering Research & Technology (IJERT)*, vol. 12, no. 7, pp. 1–7, 2024.

[11] R. Singh, P. Verma, and S. Chauhan, "Online voting system based on face recognition using Python machine learning," *International*

Journal of Research Publication and Reviews (IJRPR), vol. 5, no. 10, pp. 1204–1212, 2024.

[12] L. Gupta and P. Reddy, "E-voting system using facial recognition and blockchain," *International Research Journal of Engineering and Technology (IRJET)*, vol. 11, no. 11, pp. 650–656, 2024.

[13] S. Domakonda, D. Nishitha, A. Y. Kumar, A. S. Rao, and A. Sindhu, "E-voting system using facial recognition," *The International Journal of Analytical and Experimental Modal Analysis*, vol. 14, no. 6, pp. 1191–1201, Jun. 2022.

[14] H. Alamleh and A. A. AlQahtani, "Analysis of the design requirements for remote internet-based e-voting systems," in *Proc. World AI IoT Congress (AIIoT)*, 2021, doi: 10.1109/AIIoT52608.2021.9454194.

[15] K. Kothawade, A. V. Bhopale, A. Y. S. Patil, P. Shewale, and D. Mahajan, "A novel method of e-voting system using biometrics thumb impression and face recognition," *International Journal on Data Science and Machine Learning with Applications*, vol. 1, no. 1, pp. 37–40, May 2021.

[16] M. M. Rasheed, "Secure electronic voting system using swarm intelligence," *Journal of Physics: Conference Series*, vol. 1999, no. 1, p. 012137, 2021, doi: 10.1088/1742-6596/1999/1/012137.

[17] E. Fernando, D. Andwiyan, D. F. Murad, D. Touriano, and M. Irsan, "Face recognition system using deep neural network."

[18] K. Okokpujie *et al*., "A secured automated bimodal biometric electronic voting system," *IAES International Journal of Artificial Intelligence*, vol. 10, no. 1, pp. 1–8, 2021, doi: 10.11591/ijai.v10.i1.pp1-8.

[19] J. Sharma, "Introduction to supervised deep learning algorithms," *Analytics Vidhya*, May 2021. [Online]. Available: https://www.analyticsvidhya.com/blog/2021/05/introduction-to-supervised-deep-learning-algorithms. [Accessed: Jul. 4, 2023].

[20] R. Awati, "What are convolutional neural networks?" *Enterprise AI (TechTarget)*. [Online]. Available: https://www.techtarget.com/searchenterpriseai/definition/convolutional-neural-network. [Accessed: Jul. 4, 2023].