A Secure And Transparent Electronic Voting System Using Blockchain, Facial Recognition, And OTP Authentication

1st.Prof. Ashwini Pawale
Information Technology JSPM's
Bhivarabai Sawant Institute Of Technology
And Research Wagholi Pune, India.

2nd.Sanket Subhash Kale
Information Technology JSPM's
Bhivarabai Sawant Institute Of Technology
And Research Wagholi Pune, India

3rd..Akash Rajendra Kale
Information Technology JSPM's
Bhivarabai Sawant Institute Of Technology
And Research Wagholi Pune, India

4th .Meghraj Maruti Korade
Information Technology JSPM's
Bhivarabai Sawant Institute Of Technology
And Research Wagholi Pune, India

5th .Anand Deshmukh
Information Technology JSPM's
Bhivarabai Sawant Institute Of Technology
And Research Wagholi Pune, India

***Abstract*— The Real-Time Facial Recognition Electronic Voting System is an advanced solution aimed at improving the security, accuracy, and transparency of electronic voting. It leverages deep learning-powered facial recognition to identify registered voters by analyzing their unique facial characteristics [1]. This reduces the chances of errors, such as mistaken identity, and ensures that only legitimate voters can participate. To add an extra layer of security, the system sends a one-time password (OTP) to the voter's registered mobile number after successful facial recognition [2]. This step helps prevent unauthorized access and minimizes the risk of voter fraud. Once both facial recognition and OTP authentication are verified, the voter gains access to the voting platform, where they can securely cast their vote. Each vote is instantly recorded on a blockchain ledger, making it tamper-proof and ensuring that no one can alter or manipulate the results. Because blockchain is decentralized, it also enhances transparency, allowing voters, election officials, and auditors to verify the election outcomes independently, without relying on a single central authority [3]. With its real-time processing, the system works efficiently with minimal delays, making it an ideal choice for large-scale elections and other real-world voting scenarios [4].**

***Keywords*— Facial Recognition, Electronic Voting, Deep Learning, OTP Security, Blockchain, Cybersecurity, Transparent Elections.**

I. INTRODUCTION

As the need for secure, transparent, and efficient voting systems continues to rise, ensuring election security has become more critical than ever. Traditional voting methods, which rely on physical identification cards, PINs, or passwords, are often susceptible to fraud and manipulation, raising concerns about the integrity of elections [3]. While electronic voting systems offer a faster and more convenient alternative, they also come with risks such as hacking, vote tampering, and system failures, which can weaken public trust in the electoral process [4].

To address these challenges, the Real-Time Face Recognition Electronic Voting System integrates advanced technologies to create a secure, user-friendly, and tamper-proof voting mechanism. This system is built around three key components: facial recognition powered by neural networks, OTP-based authentication, and blockchain-based vote recording. Neural networks enable precise voter identification, significantly reducing the chances of misidentification or fraud [1]. Once a voter's face is successfully recognized, the system sends a one-time password (OTP) to their registered mobile device, ensuring an additional layer of security that prevents unauthorized access [2].

Blockchain technology further enhances the security and transparency of the voting process by recording each vote on a decentralized ledger. Since blockchain records cannot be altered or deleted, the risk of data manipulation is eliminated, ensuring that every vote remains secure and verifiable [3]. This decentralized approach allows voters, election officials, and auditors to independently confirm election results, fostering greater trust in the system and improving overall electoral integrity [4].

This paper examines the design, implementation, and advantages of the Real-Time Face Recognition Electronic Voting System. By combining facial recognition, OTP-based authentication, and blockchain technology, the system effectively addresses security and transparency concerns present in both traditional and electronic voting methods [5]. The proposed system offers a scalable and reliable framework suitable for both local and national elections, contributing to the modernization of the voting process while ensuring fair and fraud-free elections.

II. LITERATURE REVIEW

In recent years, the adoption of emerging technologies like blockchain and biometric systems has transformed the landscape of electronic voting (e-voting), particularly within the context of smart cities. Traditional voting systems face critical issues such as lack of security, transparency, and reliable voter authentication—problems that are effectively addressed by blockchain's decentralized and tamper-proof architecture. According to Zheng et al. [3], blockchain provides a secure, distributed ledger in which each transaction (or vote) is recorded immutably, making it highly resistant to fraud or tampering. Pilkington [4] further explains that blockchain relies on cryptographic principles and consensus mechanisms, eliminating the need for a central authority and ensuring that participants trust the system through mathematical verification. This decentralization significantly enhances the reliability and transparency of digital electoral processes.

The integration of blockchain with biometric authentication systems is particularly promising for enhancing voter verification and preventing impersonation or double voting. Sadeghi et al. [5] proposed a hybrid model that uses blockchain for secure vote storage and biometrics for voter authentication. This dual-layered approach not only strengthens overall system security but also supports the automation and scalability required for large-scale elections in urban environments. Among various biometric technologies, facial recognition has gained popularity due to its non-intrusive and real-time verification capabilities. Schroff et al. [1] introduced FaceNet, a deep learning model that maps facial features into a high-dimensional embedding space, enabling accurate identity recognition and clustering. This model has proven effective in various security applications and is ideal for integration into e-voting systems for fast and accurate user verification.

Earlier research into image-based authentication systems, such as the study by Dhamija and Perrig [2], laid the groundwork for modern biometric methods by evaluating the usability and effectiveness of visual recognition in authentication tasks. Their findings emphasized that users are more likely to adopt systems that strike a balance between security and ease of use—an important factor when implementing voting systems on a large scale. The progression from basic image-based logins to advanced deep learning-powered facial recognition represents significant advancements in user authentication technology

III. EXISTING SYSTEM

Traditional voting systems, including ballot papers and Electronic Voting Machines (EVMs), require a considerable amount of manpower and financial investment to function efficiently. In EVM-based voting, voters simply press a button next to their chosen candidate's name and symbol, and the machine records their selection automatically. In contrast, the ballot paper system requires voters to manually mark their choice on a printed sheet listing all candidates, after which the votes are collected and counted by election officials. This manual process is both time-consuming and labor-intensive [2].

Voter verification in traditional elections is usually done by election officials, who check ID documents and mark voters' fingers with indelible ink to prevent multiple voting. However, this manual verification method lacks advanced security features. Since the process relies on human judgment rather than automated systems, it increases the chances of errors, fraud, or manipulation. Weak security measures can allow unauthorized voting, tampering with votes, or even multiple votes cast by the same person, ultimately undermining the credibility of the election process.

Disadvantages:

1. **Slow and Error-Prone Counting**– Counting votes manually takes a long time and is vulnerable to human errors, which may cause delays and inaccuracies in election results.

2. **Risk of Election Fraud** – Traditional voting methods are susceptible to fraud, including ballot box stuffing, vote tampering, and manipulation of EVMs, threatening the fairness of the election.

3. **Human Dependency and Bias** – The system relies heavily on election officials for verification and vote counting, making it prone to human errors and potential biases that can affect election fairness.

4. **Risk of Lost or Damaged Votes** – Paper ballots can be lost, misplaced, or damaged due to mishandling or external factors such as weather conditions or natural disasters.

IV. PROPOSED SYSTEM

The Real-Time Face Recognition Electronic Voting System is designed to make elections more secure, transparent, and efficient by integrating facial recognition, OTP verification, and blockchain technology. Traditional voting methods often face issues like fraud and manipulation, making it essential to adopt more secure solutions.

In this system, facial recognition is used to verify a voter's identity, eliminating the need for physical ID cards or passwords. Once the system confirms a match, it sends a One-Time Password (OTP) to the voter's registered mobile number for additional authentication. This extra step ensures that only legitimate voters can cast their votes, reducing the chances of impersonation or unauthorized access.

After authentication, the voter gains access to a simple and user-friendly voting interface where they can securely cast their vote. Each vote is stored on a blockchain, ensuring that it cannot be changed or tampered with. Since blockchain operates in a decentralized manner, election results remain trustworthy and verifiable by independent auditors, reducing reliance on a single authority. To further strengthen the process, an audit module allows officials to verify votes, ensuring fairness, while a security module protects sensitive voter information through encryption. The system also includes a voter registration and management module, preventing duplicate or unauthorized voting by ensuring only registered individuals can participate.

This approach offers multiple advantages, such as higher security, improved transparency, reduced operational costs, and greater accessibility. By eliminating paper ballots and manual vote counting, it lowers election costs and simplifies the entire process. Additionally, the digital nature of the system makes remote or mobile voting a practical option for the future.

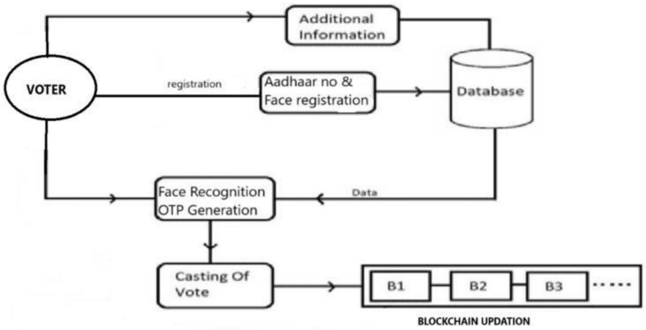


Fig : System Architecture

WORKFLOW:

1. **Voter Registration:** Voters sign up by submitting their facial data, which is securely stored and linked to their mobile number.

2. Facial Recognition Authentication: On election day, the system captures a live image of the voter and matches it with the stored data to verify their identity.

3. OTP Verification: To add an extra layer of security, an OTP is sent to the voter's registered mobile number, which they must enter to proceed.

4. Voting Process: Once authenticated, the voter accesses the digital voting interface, selects their candidate, and casts their vote.

5. Blockchain Vote Recording: Every vote is securely recorded on a blockchain ledger, ensuring it cannot be altered or tampered with.

6. Result Declaration: The system automatically counts the votes, providing fast and accurate election results without manual intervention.

Benefits

1. High Security: The system prevents fraud by using facial recognition and OTP verification, ensuring only authorized voters can cast their votes.
2. Transparency**:** Blockchain technology makes every vote verifiable and tamper-proof, increasing trust in the election process.
3. Faster Results: Since votes are counted digitally, election results are generated quickly without delays.
4 Remote Voting Possibility: With secure digital verification, the system can be adapted for online voting, allowing people to vote from anywhere.
5. Reduces Human Errors**:** Automating the process minimizes mistakes that can occur in manual voting and counting.

V. Modules and Methodology

MODULES

Voter (User): The voter is the key participant in the election, selecting their preferred candidate. Before voting, each voter must go through a registration process where they are verified and approved by the system administrator to ensure only authorized individuals can vote.

Machine Learning Process: This part of the system is responsible for recognizing voter faces. It uses machine learning techniques to train and identify faces accurately, making sure that only registered voters can cast their votes.

Face and OTP Verification: To improve security, the system uses a two-step authentication process. First, it scans the voter's face and checks if it matches the records in the system. If the face is verified, the second step sends a One-Time Password (OTP) to the voter's registered mobile number. The voter must enter the correct OTP to proceed, adding an extra layer of protection against fraud.

Blockchain Module (SHA-256 Algorithm): To ensure votes remain secure and unchangeable, the system stores them using blockchain technology with SHA-256 encryption. Once a vote is recorded, it becomes permanent and cannot be modified or tampered with. This guarantees election integrity, builds trust in the results, and makes the voting process transparent.

ALGORITHM USED

1. Haar Classifier Algorithm for Face Detection

The Haar Classifier is a widely used face detection algorithm in computer vision. Instead of analyzing individual pixels, it detects brightness variations between rectangular regions, identifying facial features like eyes, nose, and mouth. Its cascading system filters out unnecessary areas, improving speed and accuracy. Developed by Viola and Jones, it achieves around 95% accuracy using 200 optimized features.

Fig: face Detection using Haar Algorithm

Trained with AdaBoost, it selects key features for better performance but requires large datasets and high computational power. OpenCV provides pre-trained Haar cascades, making implementation easier. While fast and efficient, it struggles with lighting, angles, and expressions. Modern face detection now favors deep learning models like CNNs for higher accuracy and robustness.

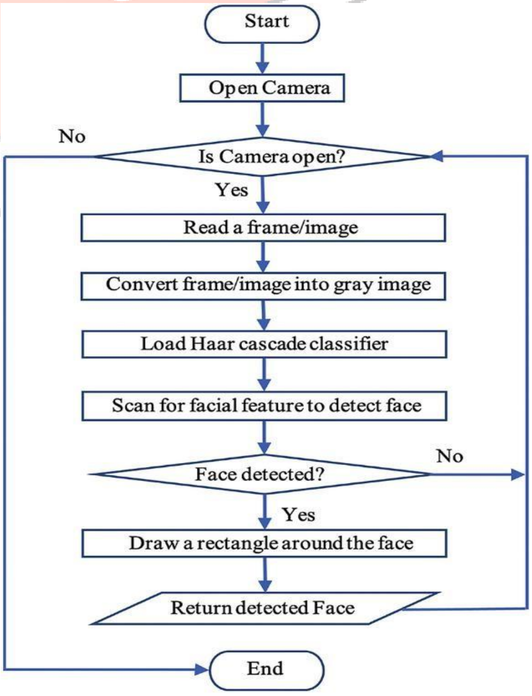

Start
Open Camera
Is Camera open?
No
Yes
Read a frame/image
Convert frame/image into gray image
Load Haar cascade classifier
Scan for facial feature to detect face
Face detected?
No
Yes
Draw a rectangle around the face
Return detected Face
End

Fig: Haar

1.1 Face Detection Approach

a. Haar Feature Computation

Each Haar feature is designed to capture variations in brightness between two regions of the image. Mathematically, for the *i*th feature, it can be expressed as:

$$Hi = \text{sum } (x,y) \text{ in } R\ d1\ I(x, y) - \text{sum } (x,y) \text{ in } R\ d2\ I(x,y)$$

- I(x,y) refers to the intensity value of the pixel at coordinate (x,y).
- R_{i1} and R_{i2} are two neighboring rectangular sections over which pixel intensities are summed.

This difference helps identify edges and textures essential for face detection.

b. Integral Image Technique

To speed up the process of summing pixel values over rectangles, an intermediate image known as the Integral Image is created. It is defined as:

Using S(x,y), the total sum over any rectangular area RRR becomes:

$$I(x,y)=S(x2,y2)-S(x1-1,y2)-S(x2,y1-1)+S(x1-1,y1-1)$$

where (x1,y1) and (x2,y2) are the top-left and bottom-right points of the rectangle.

c. Final Score Calculation

After extracting all features, they are combined into a single score by assigning each feature a specific weight, learned during training:

$$F=1\sum n\ wiHi$$

where:

n is the total number of features.

wi is the weight of feature i.

d. Decision Condition for Face Detection

The detection decision relies on comparing the final score F against a predefined threshold T. The condition is simple:

$$\text{If } F \geq T \text{ then Face Detected.}$$

If the score doesn't meet the threshold, the window is rejected.

e. Cascade Classifier Structure

To make the system faster and more efficient, the classifier is split into multiple stages. Each stage has its own set of features and weights, and the score for the jth stage is calculated as:

where:

$$Fj=w_{j1}H_{j1}+w_{j2}H_{j2}+w_{j3}H_{j3}+\cdots+w_{jnj}H_{jnj}$$

nj is the number of features in stage j.

$$Fj \geq Tj$$

Only if this condition is true, the window moves to the next stage. Otherwise, it's immediately discarded.

f. Feature Training

During the training process, the AdaBoost algorithm is employed to fine-tune the weights wi assigned to each feature and to set appropriate thresholds Tj for every classifier stage. The objective is to prioritize the most relevant features and systematically lower the classification error with each iteration.

1.2 Face Matching Approach

a. Extracting Facial Features with CNN

After detecting a face, the next critical step is to represent it in a way that can be compared accurately. This is done by using a Convolutional Neural Network (CNN), which is highly effective at learning important facial patterns. The CNN processes the input face image and converts it into a numerical feature vector.

The extraction process can be described as:

$$F = CNN(I)$$

Here:

- I refers to the face image provided as input.
- f is the output feature vector containing the unique characteristics of the face.

These feature vectors serve as a compact representation of the person's facial details, enabling reliable comparisons during recognition.

b. Face Comparison Methods

To identify or verify the face, the feature vector fff is compared with the stored feature vectors from the database. Two commonly used comparison methods are described below:

Euclidean Distance Method

This method calculates the straight-line distance between two feature vectors. The formula is:

$$d = \| f - f_{db} \|$$

Where:

- f is the feature vector from the input image.
- f_{db} is the feature vector from the database.
- d indicates the distance between them.

A smaller value of ddd means the two faces are more similar.

c. Final Recognition Criteria

The decision on whether the input face matches a known face depends on the results of the above methods. The system follows this rule:

- If the Euclidean distance ddd is less than a set threshold is greater than a defined threshold, then the face is recognized as belonging to a known individual.

If neither condition is met, the face is classified as unknown.

2. OTP Authentication Using Twilio

Twilio is a cloud-based communication service that allows developers to easily add messaging, voice, and email features to their applications through simple APIs. One of Twilio's key services is its SMS gateway, which is commonly used for sending One-Time Passwords (OTPs) to users' mobile phones.

In this work, Twilio's API is integrated to handle the generation and delivery of OTPs. When a user attempts to authenticate, the system uses Twilio to send a unique OTP directly to their registered phone number. Twilio ensures the message is delivered quickly and securely, regardless of the user's location.

Twilio's platform is highly scalable and reliable, supporting millions of messages worldwide with strong security measures in place. This makes it ideal for adding an extra layer of verification in authentication systems, helping to protect against unauthorized access.

a. User Identification:

$$ui=(Pi)$$

Where:
ui = User,
Pi = User's phone number.

b. OTP Generation:

$$OTP_i = G(L,C)$$

Where:
G = Twilio's random generator,
L = OTP length (e.g., 6 digits),
C = Character set (0-9).

c. OTP Delivery via Twilio:

$$Twilio\_Send(Pi,OTPi)$$

Twilio sends OTP_i to P_i.

d. User Verification:

$\delta=1$, if $OTP_{input} = OTP_i$ and valid
$\delta= 0$, otherwise

e. Final Authentication:

Auth(ui)= Granted, $\delta= 1$
Auth(ui)= Denied, $\delta= 0$

3. SHA Algorithm for Blockchain

To securely store votes in a blockchain-based voting system, the SHA-256 algorithm is used. When a voter casts their vote, the system converts it into a unique hash using SHA-256. This hash is a fixed 64-character string that represents the vote in an encrypted form. Since SHA-256 ensures that even a small change in the input creates a completely different hash, it becomes impossible to alter votes without detection.

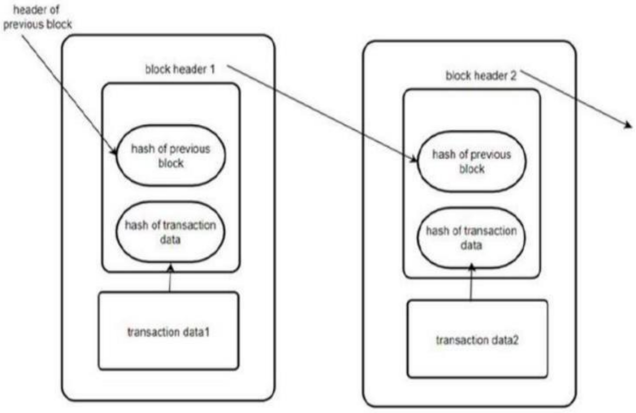


Fig: Blockchain Architecture

Each vote's hash is then linked to the previous vote's hash, forming a secure chain of records. This structure guarantees that votes remain unchanged and tamper-proof. Additionally, since blockchain operates on a decentralized network, no single person or authority can modify or manipulate the stored votes. By using SHA-256, the voting system ensures high security, transparency, and protection against fraud, making the election process trustworthy and reliable.

Block Hash Formula

Each block in the blockchain has a unique hash calculated as:

$$H(Bi)=SHA\text{-}256(Pi||Ti||H(Bi-1)||Ni)$$

Where:

- H(Bi) = Hash of the current block.
- Pi = Public information (timestamp, block number, etc.).
- Ti = Votes stored in the current block.
- H(Bi−1) = Hash of the previous block (linking blocks).
- Ni = Nonce (random number used in mining).
- || = Means combining all data together.

Vote Hashing

Each vote inside the block is also hashed:

$$Ti=SHA\text{-}256(V_{i1}||V_{i2}||V_{i3}||\ldots||V_{in})$$

Where:

- Vij = Individual vote.

All vote data is concatenated first and then hashed together.

Chain Security

If someone tries to change any vote V_{ij}, it will change:

$$\Delta V_{ij}\rightarrow\Delta T_i\rightarrow\Delta H(B_i)\rightarrow\Delta H(B_k)\ \forall k > i$$

This means all future block hashes will be broken, and tampering will be detected easily.

Final Block Check

The block is added to the blockchain only if:

$$H(B_i)<\text{Target Difficulty}$$

This condition makes sure the block is valid

VI. EASE OF USE

A. User-Friendly Interface:

The voting system has a simple, easy-to-use design that works well on desktops, mobile devices, or special voting kiosks. Clear instructions guide every step, so voters of any technical skill can use it without hassle.

B. Secure and Efficient Authentication:

Instead of physical ID cards or passwords, the system uses facial recognition and one-time passwords (OTP) for a secure, automated check. This not only boosts security but also speeds up the voting process.

C. Easy Setup and Integration:

The system is designed to work smoothly with current election setups. Registering voters is straightforward, and administrators can manage voter information and security protocols without needing advanced technical skills.

D Low Maintenance Requirements:

Powered by advanced machine learning and blockchain technology, the system updates automatically and stores data securely with encryption. This means it runs efficiently with very little manual maintenance.

E. Transparent and Tamper-Proof Voting:

Votes are recorded on a blockchain, creating an unchangeable, transparent ledger. This method makes it nearly impossible to tamper with the votes, thereby building trust in the electoral process.

F. Training and Support:

Detailed training materials and responsive support are available for both election officials and system administrators. This ensures that everyone can easily learn and troubleshoot the system if needed.

G. Real-Time Monitoring and Instant Results:

The system allows election officials to keep an eye on the entire voting process as it happens. They can easily check voter turnout, monitor how the system is performing, and quickly spot any unusual activity. Once voting ends, the results are calculated immediately and accurately, eliminating the need for manual counting. This not only speeds up the process but also ensures everything runs smoothly and transparently.

RESULTS AND DISCUSSIONS

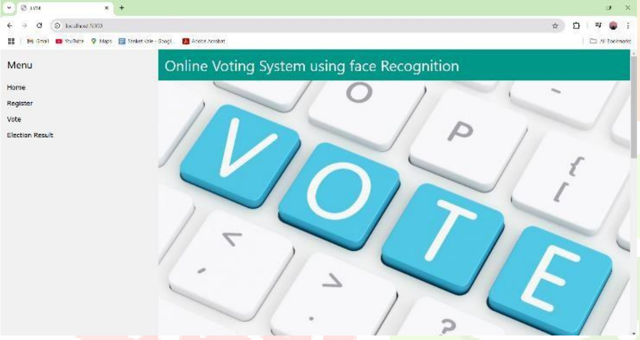
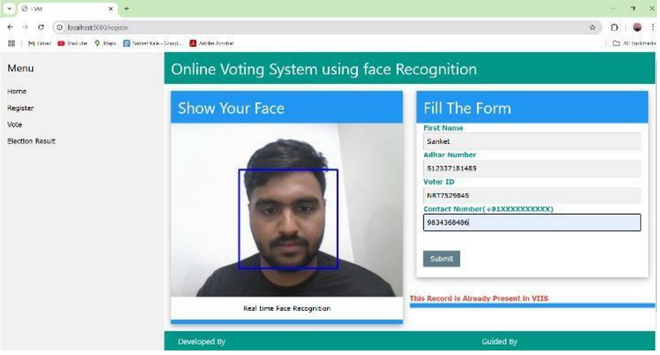


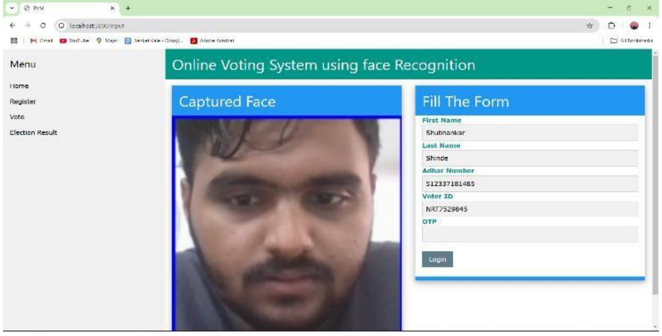
Fig 1: Home page



First Name: Sanket
Adhar Number: 512337181485
Voter ID: NRT7529845
Contact Number(+91XXXXXXXXXX): 9834368486

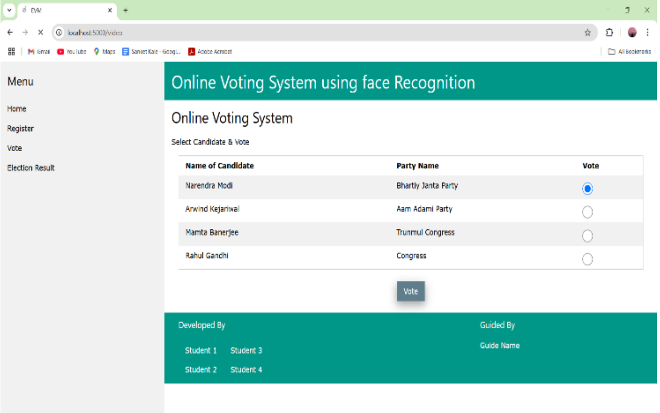
This Record is Already Present in VIIS

Fig 2: Registration Page



First Name: Shubhankar
Last Name: Shinde
Adhar Number: 512337181485
Voter ID: NRT7529845
OTP:

Fig 3: Face Recognition and OTP Authentication



Online Voting System

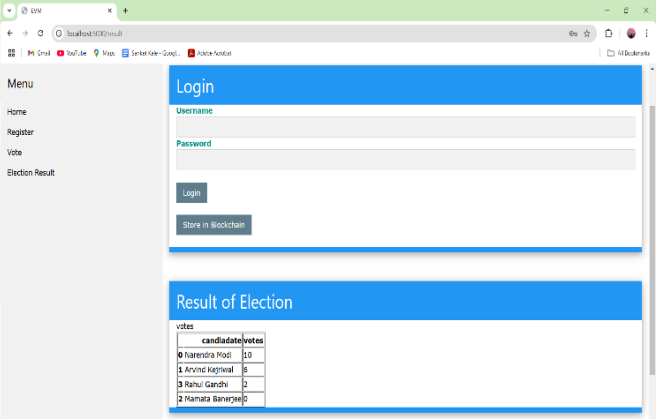
Select Candidate & Vote

Name of Candidate	Party Name	Vote
Narendra Modi	Bhartiy Janta Party	●
Arwind Kejariwal	Aam Adami Party	○
Mamta Banerjee	Trunmul Congress	○
Rahul Gandhi	Congress	○

Developed By
Student 1 Student 3
Student 2 Student 4

Guided By
Guide Name

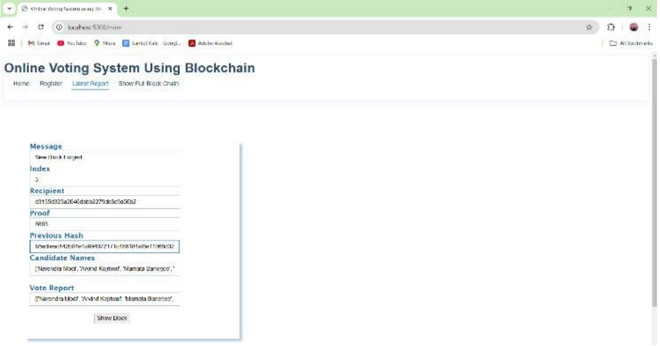
Fig 4: Voting Page



votes

	candiadate	votes
0	Narendra Modi	10
1	Arvind Kejriwal	6
3	Rahul Gandhi	2
2	Mamata Banerjee	0

Fig 5: Result



Message: New Block Forged
Index: 3
Recipient: d3135d323a2646dabb2279dc8c9a56b2
Proof: 8883
Previous Hash: [illegible]
Candidate Names: ['Narendra Modi', 'Arvind Kejriwal', 'Mamata Banerjee', '
Vote Report: [['Narendra Modi', 'Arvind Kejriwal', 'Mamata Banerjee',

Fig 6: Blockchain Stored

VII. Conclusion

The Real-Time Face Recognition Electronic Voting System transforms both traditional and digital voting by incorporating facial recognition, OTP authentication, and blockchain technology. This advanced system enhances security, boosts transparency, and increases efficiency. It ensures that only authenticated voters can participate, preserves an unalterable record of votes, and allows for public verification, reducing the chances of fraud and interference. Built to manage large-scale elections, it streamlines vote counting and reinforces confidence in the electoral process, establishing a new standard for secure and modern voting solutions.

VIII. ACKNOWLEDGMENT

The authors sincerely express their gratitude to Prof. Ashwini Pawale, our project mentor, for her invaluable guidance, support, and encouragement throughout the research and development of this project. Her expertise and insights were essential to its successful completion.

We also extend our appreciation to the faculty and staff of the Department of Information Technology at JSPM's Bhivarabai Sawant Institute of Technology and Research for their continuous support and cooperation. A special thanks to our colleagues and friends for their valuable contributions and assistance during this project.

Finally, we acknowledge the unwavering encouragement from our families, whose constant support and motivation played a crucial role in the successful completion of this work.

References

[1] Schroff, F., Kalenichenko, D., & Philbin, J. (2015). FaceNet: A Unified Embedding for Face Recognition and Clustering. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (pp. 815-823).

[2] Dhamija, R., & Perrig, A. (2000). Déjà Vu: A User Study Using Images for Authentication. In Proceedings of the 9th USENIX Security Symposium.

[3] Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2018). An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. In IEEE International Congress on Big Data (pp. 557-564).

[4] Pilkington, M. (2016). Blockchain Technology: Principles and Applications. In Research Handbook on Digital Transformations. Edward Elgar Publishing.

[5] Sadeghi, A. R., Bocek, T., & Kießling, W. (2018). Secure Electronic Voting Using Blockchain and Biometrics. IEEE Access, 6, 56899-56909.

[6] Sun, Y., Wang, X., & Tang, X. (2014). Deep Learning Face Representation by Joint Identification-Verification. IEEE Transactions on Pattern Analysis and Machine Intelligence, 38(12), 2280-2292.

[7] Jain, A. K., Nandakumar, K., & Ross, A. (2018). 50 Years of Biometric Research: Accomplishments, Challenges, and Opportunities. Pattern Recognition Letters, 81, 1-20.

[8] Crosby, M., Pattanayak, P., Verma, S., & Kalyanaraman, V. (2016). Blockchain Technology: Beyond Bitcoin. Applied Innovation Review, 2, 6-10.

[9] Mills, L., Xie, L., & Viswanath, B. (2020). Blockchain for Secure Voting Systems: A Case Study of Voatz. IEEE Transactions on Engineering Management, 67(4), 1012-1021

[10] Khan, M. A., & Salah, K. (2018). IoT Security: Review, Blockchain Solutions, and Open Challenges. Future Generation Computer Systems, 82, 395-411.

[11] Kok, S., & Postma, E. (2005). Using Triplet Half-Face Designs for Facial Expression Recognition. Proceedings of the 17th Belgium-Netherlands Conference on Artificial Intelligence, 195-202.

[12] Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. White Paper.

[13] Zyskind, G., Nathan, O., & Pentland, A. (2015). Decentralizing Privacy: Using Blockchain to Protect Personal Data. 2015 IEEE Security and Privacy Workshops, 180-184.

[14] R.Suganya, Khan Farina, Alfiya Abid Shahbad, Neelam LabhadeKumar, Mangala S Biradar, Ashvini Narayan Pawale,"Reinforcement Learning-Based Deep FEFM for Blockchain Consensus Mechanism Optimization with Non-Linear Analysis"Journal of Computational Analysis and Applications, Vol. 33 No. 05 (2024)