Iris Recognition Based Modern Voting System Using Deep Learning

Goma E[1], Manasa G[2], Manjula B[3] And Sanchana S[4]

[1]Assistant Professor, Adhiyamaan College of Engineering, Hosur.
[2,3,4]UG Students, Adhiyamaan College of Engineering, Hosur.

ABSTRACT

The adoption of online voting systems has grown significantly in recent years, providing greater accessibility and convenience for voters. However, ensuring the security, accuracy, and integrity of these systems remains a critical challenge. This project proposes a Face and Iris Recognition-Based Voting System utilizing Convolutional Neural Networks (CNNs) to enhance voter authentication and prevent fraudulent activities. The system captures a voter's face and iris via a webcam and employs a CNN-based model trained on a database of registered voters' biometric data to verify their identity. Additionally, fingerprint verification is incorporated as an extra layer of security. Once the authentication process is successfully completed, a One-Time Password (OTP) is sent to the voter's registered mobile number for final verification before granting access to the voting interface. This multi-layered security approach combining facial recognition, iris scanning, fingerprint authentication, and OTP verification ensures that only legitimate voters can participate in the election, significantly reducing risks such as impersonation, multiple voting, and unauthorized access. Furthermore, the system employs a secure database to store voter details and ballots, ensuring data confidentiality and integrity. A user-friendly interface is designed to streamline the voting process, making it accessible even to individuals with limited technical knowledge. By integrating advanced biometric authentication with a secure and efficient voting mechanism, this system offers a reliable solution for online elections, improving accessibility while maintaining the privacy, security, and integrity of the electoral process.

KEYWORDS: Online voting system, biometric authentication, face recognition, iris recognition, fingerprint verification, Convolutional Neural Networks (CNNs), voter authentication, fraud prevention, OTP verification, multi-layered security, secure database, data confidentiality, electoral integrity, secure voting mechanism, artificial intelligence, machine learning, webcam-based authentication, election security, voter identity verification, real-time authentication, deep learning, online elections, digital democracy.

INTRODUCTION

The Iris and Face Recognition-Based Voting System enhances security and efficiency in the electoral process, addressing issues like voter fraud, ballot tampering, and accessibility challenges. As digital platforms gain prominence, modernizing voting methods is essential to ensure convenience, security, and transparency. Traditional systems face challenges such as long wait times and impersonation risks, especially in regions with limited resources. This system leverages biometric authentication through iris, face, and fingerprint recognition, providing a highly accurate and tamper-proof verification method. The combination of biometric authentication and OTP verification ensures that only legitimate voters participate. Face and iris recognition algorithms analyse unique physical traits, significantly improving security over traditional password-based systems. Additionally, a one-time password (OTP) sent to the voter's registered phone number adds an extra layer of protection, confirming their physical presence before allowing them to vote. This multi-factor authentication approach prevents unauthorized access and enhances election integrity. Designed with user-friendliness in mind, the system allows voters to authenticate using a webcam and fingerprint scanner, eliminating the need for specialized equipment. The simple and intuitive interface displays candidate names and party symbols, making the process accessible even to users with limited technological expertise. This ease of use promotes higher voter participation, particularly in remote areas where traditional voting facilities are scarce. To ensure data security and election transparency, all biometric data and votes are stored in a secure, encrypted database, preventing unauthorized access or tampering. Real-time monitoring and auditing help election authorities detect anomalies and maintain a fair and transparent process. By adopting this scalable and secure biometric voting system, governments can enhance election security, increase voter trust, and minimize fraud, paving the way for a new era of digital voting.

LITERATURE SURVEY

Lombardi et al. (2012) proposed a deep learning-based model for enhancing the performance of smart city voting systems. Their research highlighted the integration of biometric authentication technologies, such as iris and face recognition, to ensure secure and efficient electronic voting processes in urban environments. The model showed promising results in increasing the trustworthiness and scalability of smart voting solutions. [1]

Neirotti et al. (2014) examined the current trends in smart city initiatives, with a particular focus on the use of biometric technologies for secure online voting. Their work emphasized the potential of face and iris recognition systems in improving voter identification and preventing fraud in e-voting scenarios. [2]

Mehmood et al. (2017) explored the role of the Internet of Things (IoT) in smart cities, including its application in secure e-voting systems using biometric authentication. Their study demonstrated how IoT devices, paired with advanced deep learning techniques like convolutional neural networks (CNNs), can significantly enhance the security of voting systems. [3]

Cayamcela and Lim (2018) provided a survey on artificial intelligence (AI) integration in 5G technology, with implications for secure e-voting systems. They discussed how 5G networks, combined with AI-based biometric authentication methods like face and iris recognition, could support efficient and secure voting systems in smart cities. [4]

Al-Turjman (2019) reviewed the role of 5G-enabled devices and social IoT in enhancing smart-spaces and secure voting platforms. The study focused on biometric identification technologies, particularly facial and iris recognition, in providing accurate and tamper-proof voter verification in modern elections. [5]

Molina-Masegosa and Gozalvez (2017) investigated LTE-V and V2X communications in the context of vehicular networks, drawing parallels to secure e-voting systems. Their research highlighted the potential of deep learning-based face and iris recognition techniques in ensuring secure, real-time voter authentication and communication. [6]

Tarasov and Tewari (2017) discussed the future of electronic voting systems, proposing the incorporation of biometric features like face and iris recognition for voter authentication. Their research concluded that these technologies could address several security challenges faced by traditional voting systems. [7]

Kshetri and Voas (2018) examined the potential of blockchain-enabled e-voting systems, focusing on secure identity verification through biometric technologies. Their work emphasized the combination of blockchain and deep learning-based iris and face recognition systems for tamper-proof elections. [8]

Xie et al. (2019) conducted a survey on blockchain applications in smart cities, with a focus on secure online voting systems. The study proposed the use of advanced face and iris recognition technologies, enhanced by deep learning models, to ensure secure voter identification in decentralized voting systems. [9]

Monrat et al. (2019) surveyed blockchain technologies from an application perspective, highlighting their use in secure e-voting systems. The research suggested combining blockchain with biometric identification methods, such as facial and iris recognition, to enhance election security and transparency. [10]

Curran (2018) explored e-voting on the blockchain, proposing the use of biometric technologies like iris and face recognition for secure voter authentication. Their work demonstrated how deep learning algorithms can improve the accuracy and efficiency of biometric-based identification methods in electronic voting. [11]

Shafiq et al. (2020) investigated the application of machine learning techniques in IoT-based malicious traffic identification. They highlighted the use of these techniques, particularly in biometric-based voting systems, to improve voter identification and prevent cyberattacks in e-voting processes. [12]

Khan and Salah (2018) reviewed IoT security challenges and blockchain solutions, with an emphasis on biometric identification for secure voting systems. Their study focused on face and iris recognition techniques to address the security risks in IoT-enabled voting platforms. [13]

Gandhi et al. (2018) developed an IoT-based surveillance system to protect against recent threats. Their work included integrating biometric technologies, such as facial and iris recognition, to safeguard the integrity of e-voting systems and ensure secure voter authentication. [14]

Rathee et al. (2019) presented a blockchain framework for securing connected and autonomous vehicles, which was extended to cover e-voting systems. Their study emphasized the potential of deep learning-based biometric methods, particularly iris and face recognition, to improve the security and reliability of voting processes. [15]

METHODOLOGY

1.User Management Module

1.1 User Registration

- The registration module allows the user to create login Voter Id, Name and Face by submitting their information like mail id.
- By registering in the network, the user can gain access to the resources stored in the server.

1.2 Login / Logout

- In this module the user can login by using their unique Vote Id and Face.
- The login module verifies the user given Vote Id and Face with the stored Vote Id and Face in the server.
- If the Vote Id and Face is matched then the user can access the resources.
- If it does not match, then the user does not allow to access the resources.

2. Authentication & Verification Module

2.1 Face Verification

- In this module verified to your registered face.
- The current face is matched to the registered voter id face then allowed to generate the OTP to the candidate.
- The face not matched to voter id the system is not allowed to user.

2.2 OTP Verification

- This module is extra verification to the candidates after complete the face verification then OTP will generate and send to the user email.
- Enter the correct OTP on the user only allowed to vote. If doesn't match the OTP the system is stopped.

3.Voting Process Module

3.1 Add Vote

- Displays party names and allows the user to cast their vote after successful verification.

4. Admin Management Module

4.1 Admin Login

- Admin can only access view the voter list and voting count.admin_login endpoint first checks if a POST request has been made. If so, it takes the username and password from the request.compares it to the password stored in the admin function. If the hashes match, the admin is redirected to the admin index. If the password does not match, an "Incorrect password" message is returned. The admin_login endpoint simply returns a welcome message.

4.2 View Voters

- View Voters module is displayed the how many voters are vote to the election.
- It can see the voter details as like voter id, name and email those are visible on table.
- This module can access only admin.

4.3 View Voting Count

- This module is working for parties get how many votes in the election.
- It can see the party name and they are getting how many votes.
  This module can access only admin.

ARCHITECTURAL DESIGN

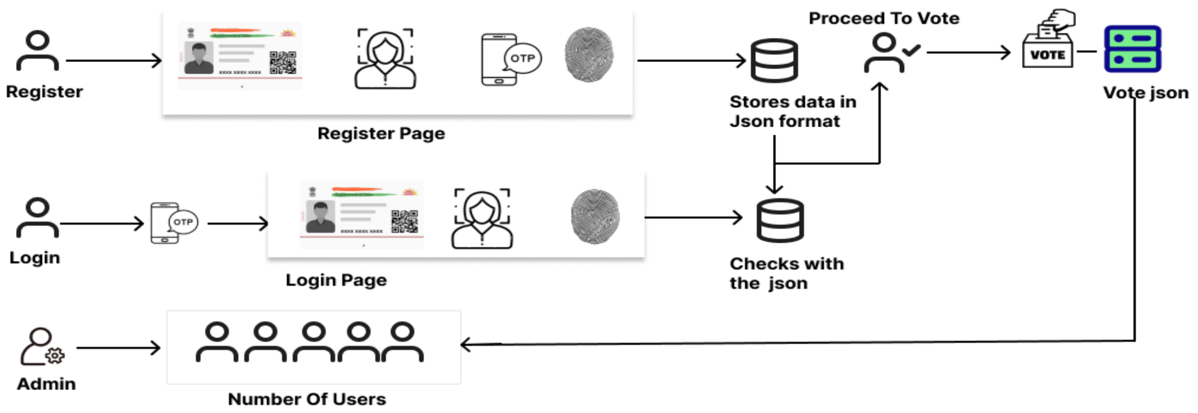


FIGURE 1: ARCHITECTURE DIAGRAM

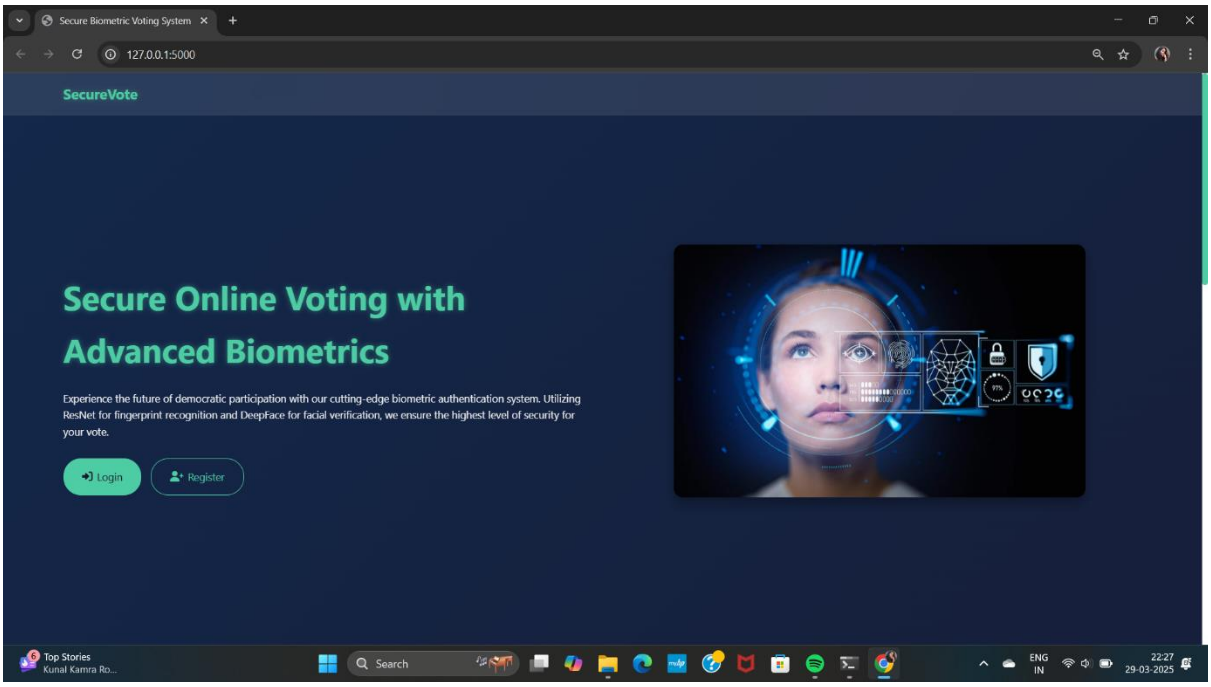
IMPLEMENTATION AND RESULT

The proposed voting system integrates multi-factor authentication methods, including facial recognition, mobile number verification, and fingerprint authentication, to enhance security and prevent fraudulent activities. The implementation consists of two primary components: the admin panel and the user interface.In the admin panel, authorized personnel can add candidate details using a dedicated form that captures essential information such as name and avatar. This data is stored in a structured JSON format instead of a traditional database, ensuring lightweight and flexible data management. The admin dashboard also includes a table to monitor vote counts dynamically.

On the user side, the election card replaces the EPIC number for voter identification. The vote.html page displays all candidates retrieved from the admin panel, each accompanied by a 'Vote' button. When a voter selects a candidate, the system records their vote securely in the JSON file, ensuring integrity and accuracy. The authentication process ensures that only eligible voters can participate, leveraging biometric and mobile verification mechanisms.

The voting system demonstrates improved security and accessibility. The elimination of EPIC number-based input simplifies the voting process while ensuring a seamless experience for users. The real-time vote count update in the admin dashboard provides transparency and ease of monitoring election progress. Testing of the system indicates high reliability and accuracy in vote recording, with authentication mechanisms successfully preventing unauthorized access. The use of JSON for data storage ensures efficient processing and retrieval, making the system lightweight and scalable.

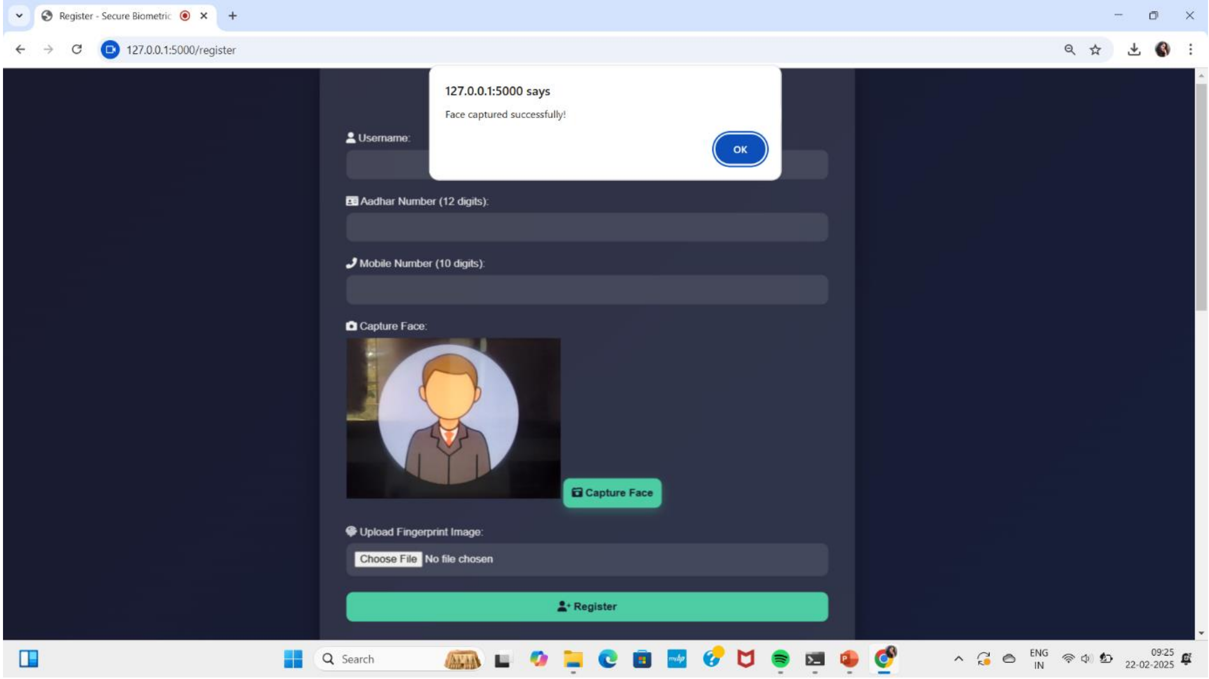
Overall, the proposed approach enhances voter confidence by providing a secure, user-friendly, and fraud-resistant digital voting experience.



Secure Online Voting with Advanced Biometrics

Experience the future of democratic participation with our cutting-edge biometric authentication system. Utilizing ResNet for fingerprint recognition and DeepFace for facial verification, we ensure the highest level of security for your vote.

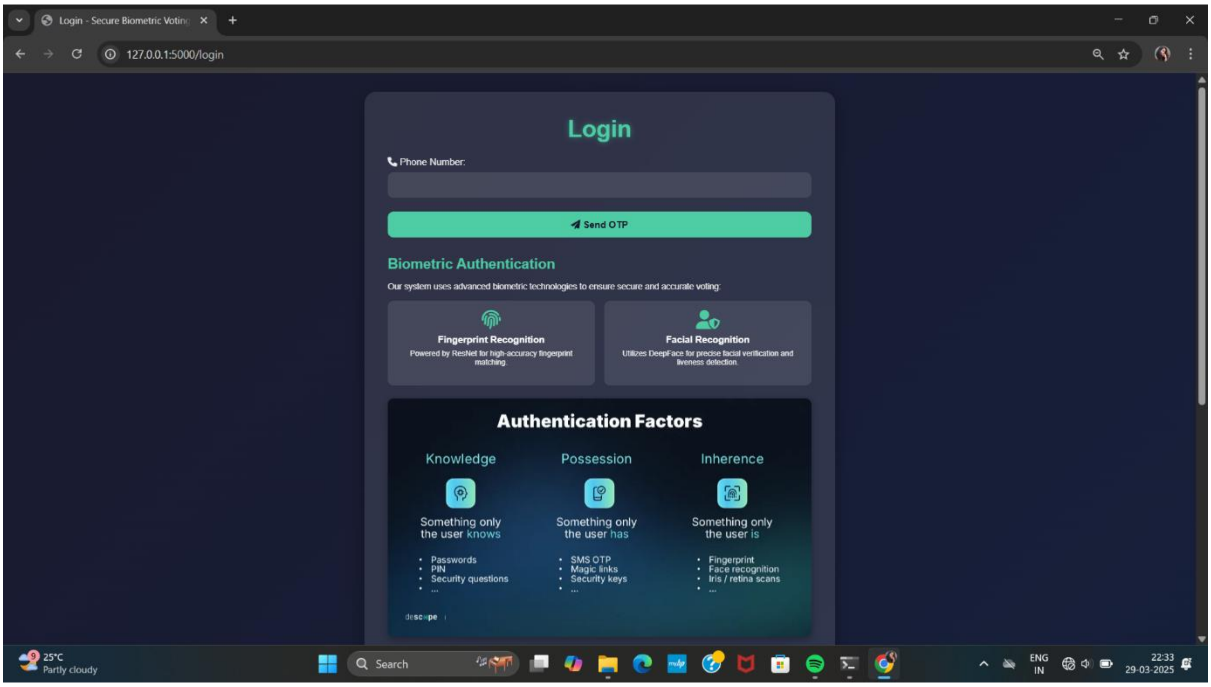
FIGURE 2: LANDING PAGE



127.0.0.1:5000 says

Face captured successfully!

FIGURE 3: USER REGISTER PAGE



Our system uses advanced biometric technologies to ensure secure and accurate voting:

Powered by ResNet for high-accuracy fingerprint matching.

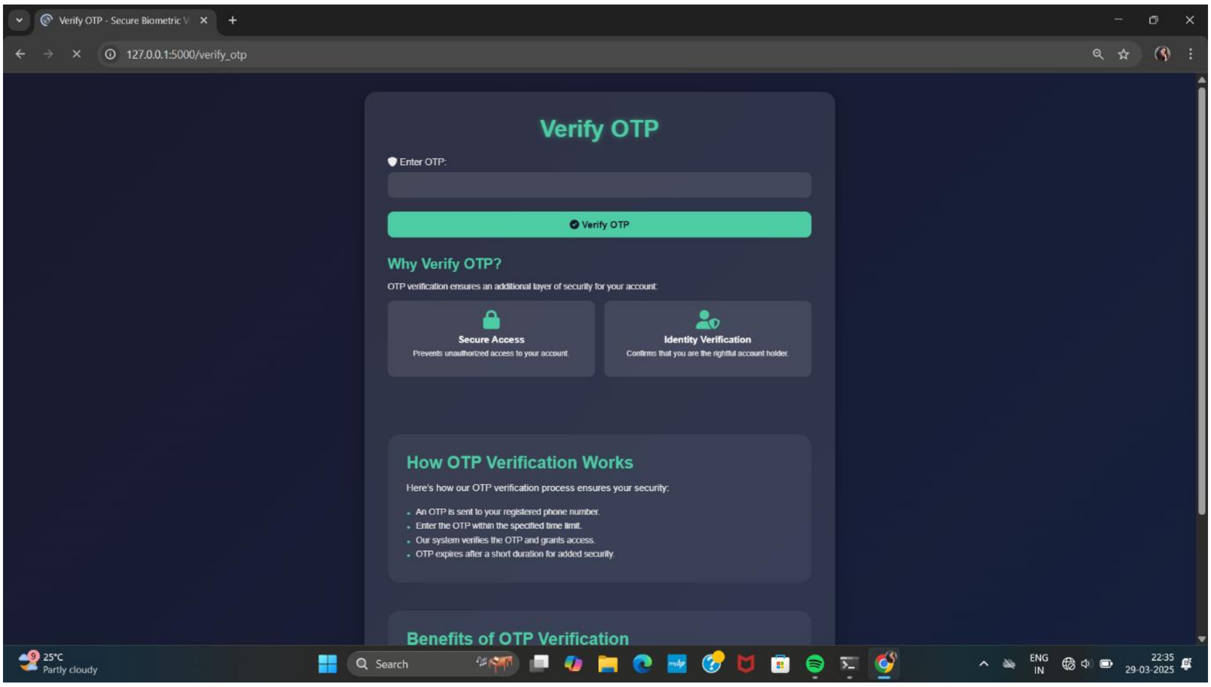
Utilizes DeepFace for precise facial verification and liveness detection.

Something only the user knows
- Passwords
- PIN
- Security questions
- ...

Something only the user has
- SMS OTP
- Magic links
- Security keys
- ...

Something only the user is
- Fingerprint
- Face recognition
- Iris / retina scans
- ...

FIGURE 4: LOGIN PAGE



Verify OTP

Enter OTP:

Verify OTP

Why Verify OTP?

OTP verification ensures an additional layer of security for your account:

Secure Access
Prevents unauthorized access to your account.

Identity Verification
Confirms that you are the rightful account holder.

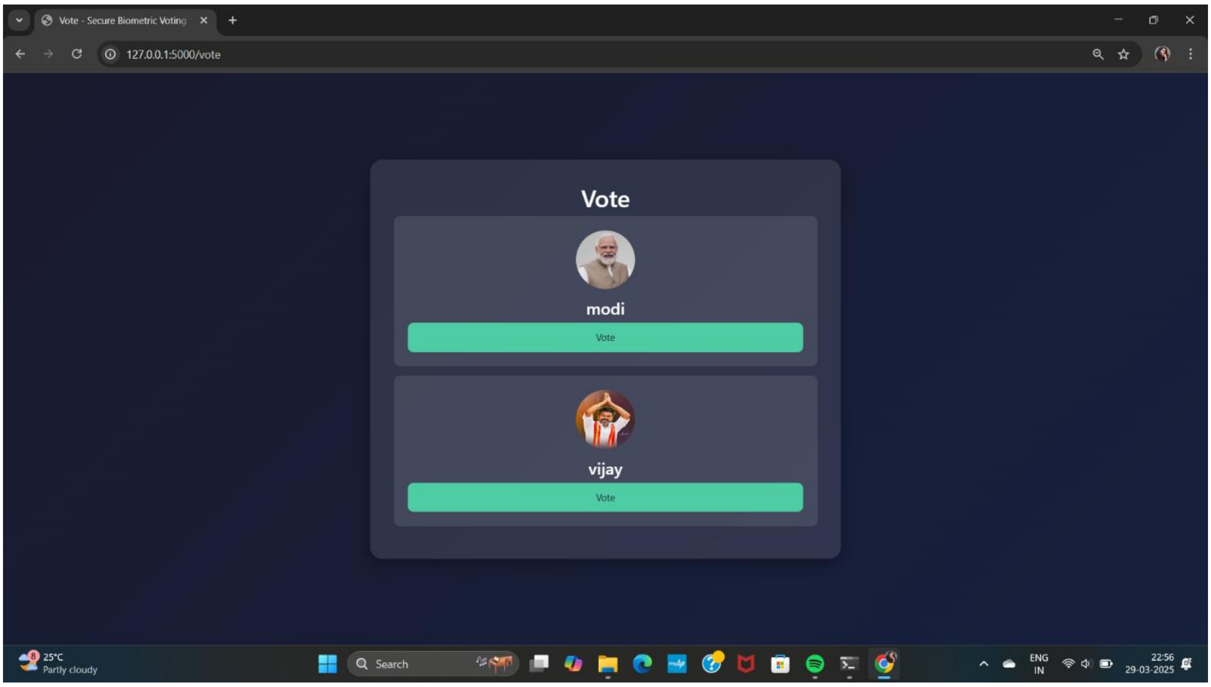
How OTP Verification Works

Here's how our OTP verification process ensures your security:

- An OTP is sent to your registered phone number.
- Enter the OTP within the specified time limit.
- Our system verifies the OTP and grants access.
- OTP expires after a short duration for added security.

Benefits of OTP Verification

FIGURE 5: VERIFYING OTP



Vote

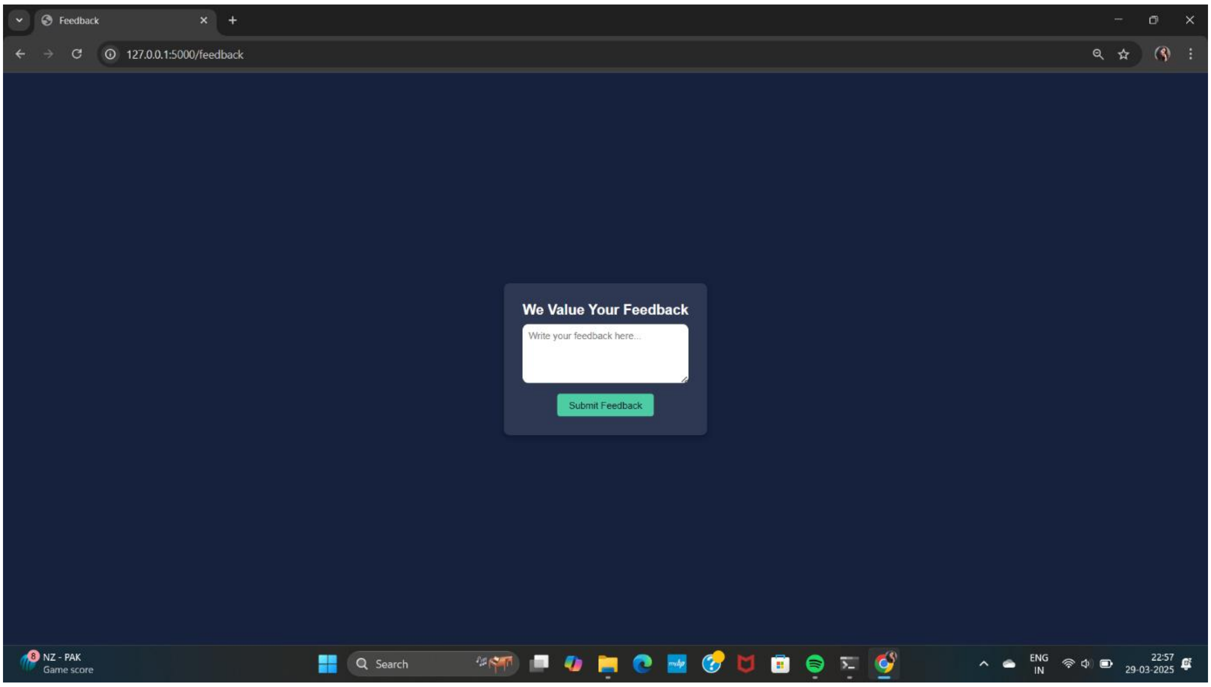
modi

Vote

vijay

Vote

FIGURE 6: CASTING THE VOTE

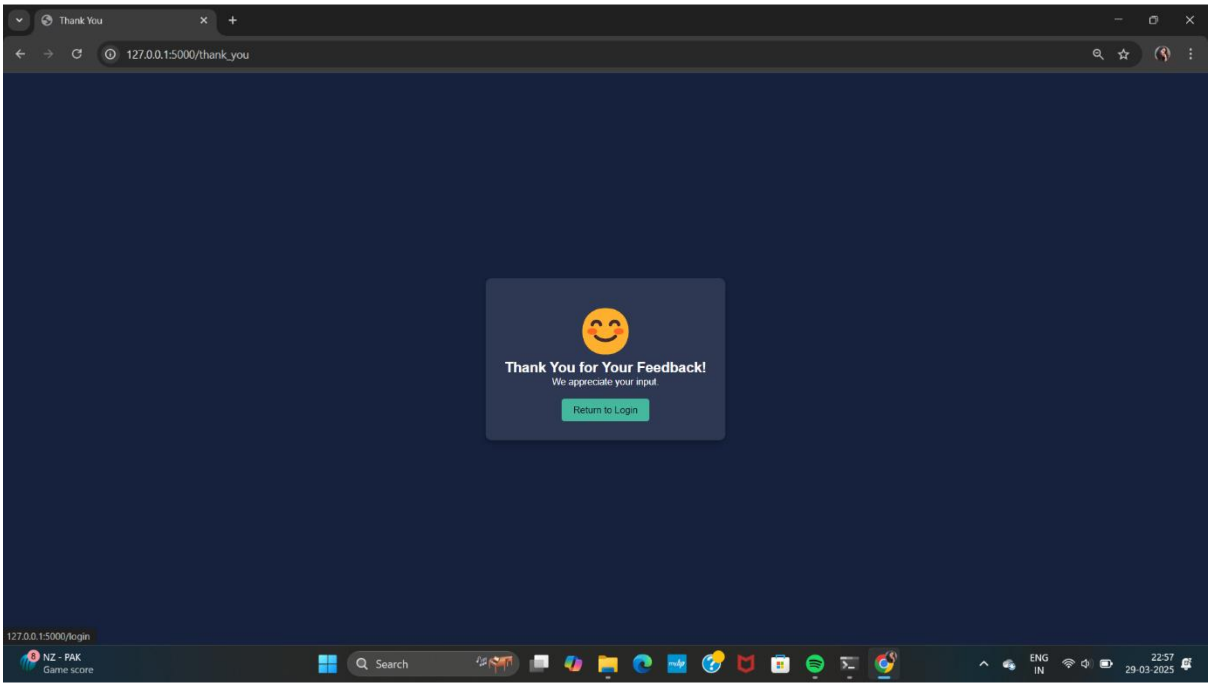


127.0.0.1:5000/feedback

We Value Your Feedback

Write your feedback here...

FIGURE 7: FEEDBACK



127.0.0.1:5000/thank_you

Thank You for Your Feedback!

We appreciate your input.

127.0.0.1:5000/login

FIGURE 8: THANKING PAGE

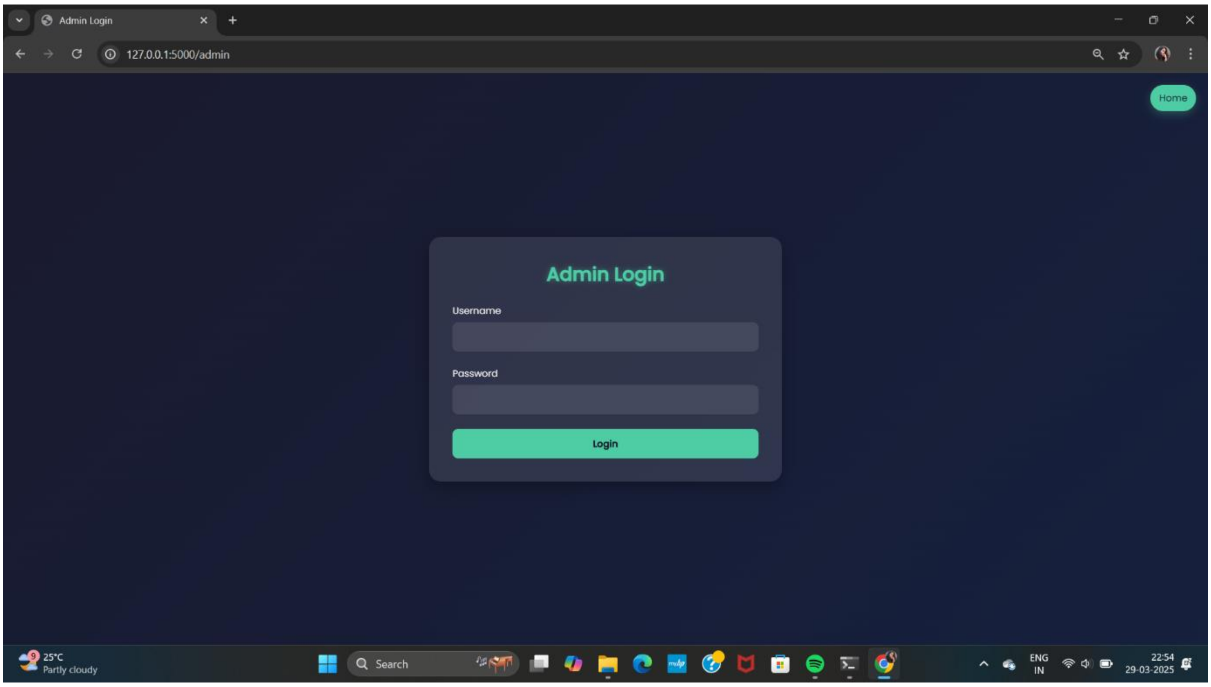


FIGURE 9: ADMIN LOGIN

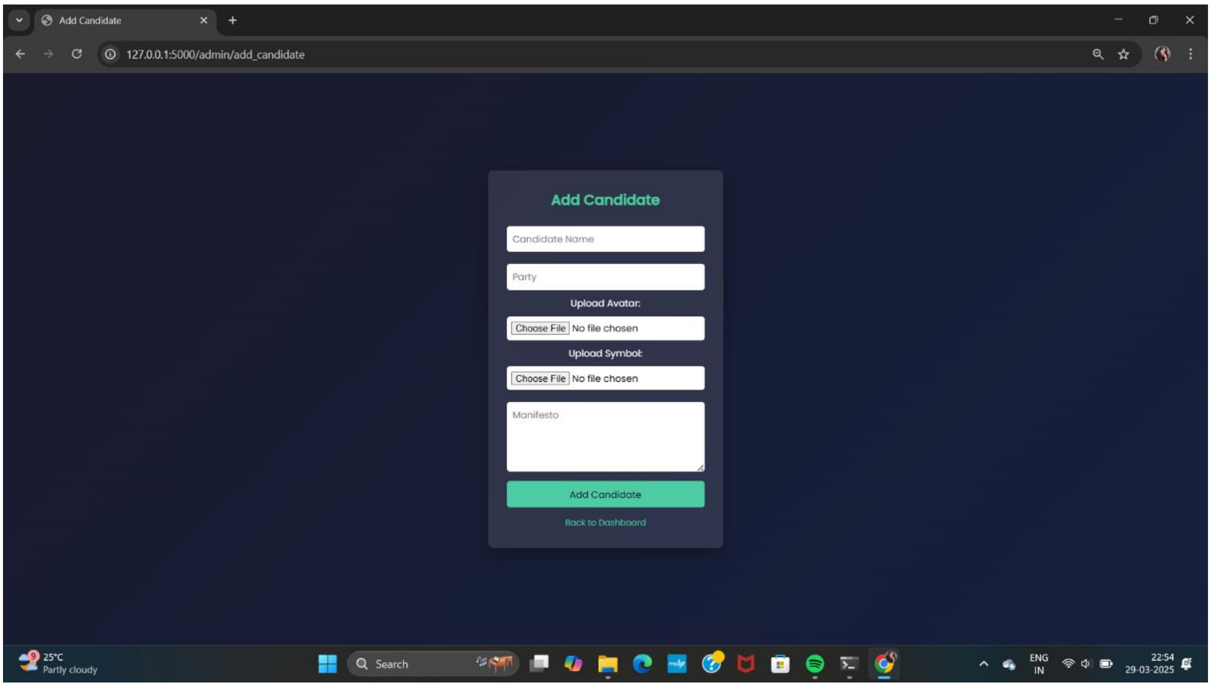
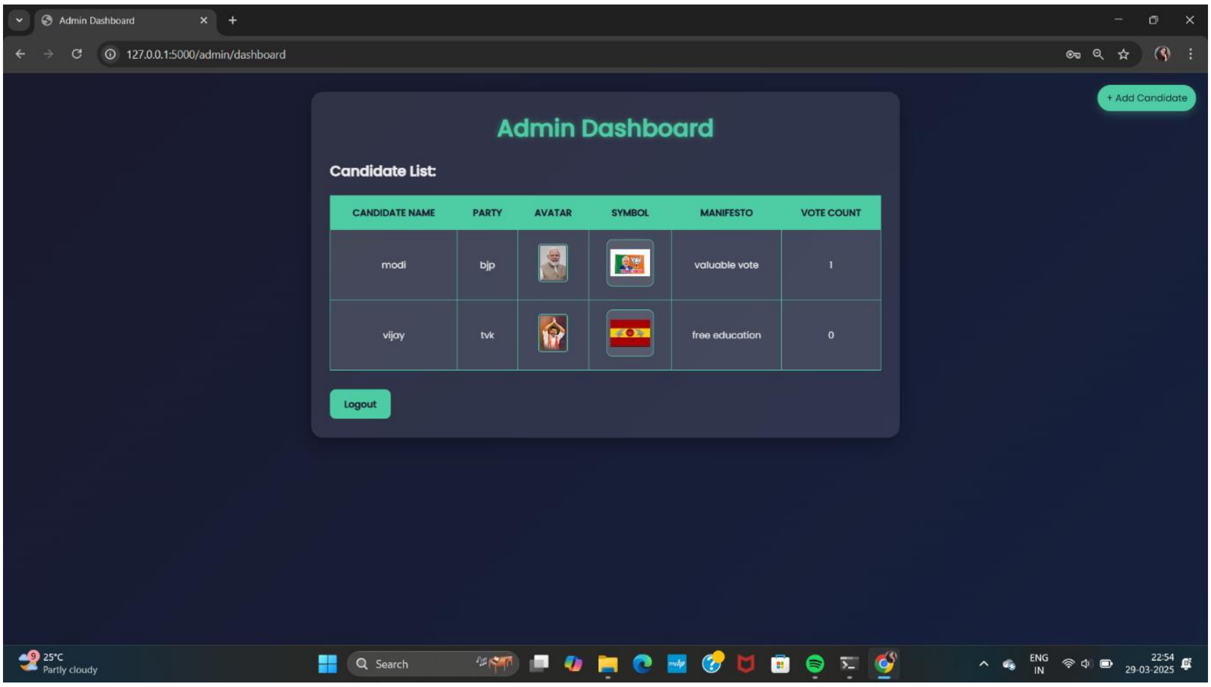


FIGURE 10: ADDING CANDIDATES



Admin Dashboard

Candidate List:

CANDIDATE NAME	PARTY	AVATAR	SYMBOL	MANIFESTO	VOTE COUNT
modi	bjp			valuable vote	1
vijay	tvk			free education	0

FIGURE 11: ADMIN DASHBOARD

CONCLUSION

The proposed Face, Iris, and OTP-based Voting System utilizing Convolutional Neural Networks (CNNs) presents a promising solution for secure and reliable online voting. By integrating facial and iris recognition with OTP verification, the system adds multiple layers of security, reducing the risk of fraud, impersonation, and hacking. The use of CNN algorithms ensures high accuracy in facial and iris recognition, enabling precise voter authentication while minimizing errors. However, the successful implementation of such a system requires careful planning and consideration. Ensuring voter privacy and data security is paramount, necessitating robust encryption and access control mechanisms to protect the database of registered voters and voting records from unauthorized access. Additionally, potential biases in recognition algorithms must be addressed to ensure fairness and impartiality in the voting process, preventing discrimination against individuals based on variations in biometric features. Furthermore, the legal and ethical implications of employing biometric authentication in voting must be thoroughly evaluated. Privacy concerns, data protection regulations, and the ethical use of facial and iris recognition technology must be taken into account to build public trust in the system. By implementing necessary safeguards and regulatory compliance measures, the proposed system can provide a secure, transparent, and efficient method for conducting online elections, ensuring both accessibility and the integrity of the electoral process.

FUTURE SCOPE

The Iris and Face Recognition-based Voting System can be enhanced with several improvements to make it more secure, accessible, and user-friendly. AI-powered chatbots can guide voters through the process, answering questions or resolving issues they may encounter. Accessibility features such as voice commands and screen readers can help people with disabilities. The system can be made compatible with various devices, so voters can cast their votes using smartphones, tablets, or public kiosks. Machine learning can improve the accuracy of biometric recognition over time, ensuring better security. Locationbased restrictions can prevent fraud by ensuring that votes are only cast from authorized regions. Voter privacy can be protected through encrypted data storage, ensuring biometric information is safe. Multiple language options can make the system usable for a broader range of voters, and social media integration can streamline voter verification. An offline mode can be developed for areas with poor internet connectivity, ensuring everyone has access to the system. Regular system updates and security patches will keep the system safe and up-to-date, boosting voter confidence.

REFERENCES

1. P. Lombardi, S. Giordano, H. Farouh, and W. Yousef, ‘‘Modelling the smart city performance,’’ Innov., Eur. J. Social Sci. Res., vol. 25, no. 2, pp. 137–149, Jun. 2012.
2. P. Neirotti, A. De Marco, A. C. Cagliano, G. Mangano, and F. Scorrano, ‘‘Current trends in smart city initiatives: Some stylised facts,’’ Cities, vol. 38, pp. 25–36, Jun. 2014.
3. Y. Mehmood, F. Ahmad, I. Yaqoob, A. Adnane, M. Imran, and S. Guizani, ‘‘Internet-of-Things-based smart cities: Recent advances and challenges,’’ IEEE Commun. Mag., vol. 55, no. 9, pp. 16–24, Sep. 2017.
4. M. E. M. Cayamcela and W. Lim, ‘‘Artificial intelligence in 5G technology: A survey,’’ in Proc. Int. Conf. Inf. Commun. Technol. Converg. (ICTC), Oct. 2018, pp. 860–865.
5. F. Al-Turjman, ‘‘5G-enabled devices and smart-spaces in social-IoT: An overview,’’ Future Gener. Comput. Syst., vol. 92, pp. 732–744, Mar. 2019.
6. R. Molina-Masegosa and J. Gozalvez, ‘‘LTE-V for sidelink 5G V2X vehicular communications: A new 5G technology for short-range vehicle-to-everything communications,’’ IEEE Veh. Technol. Mag., vol. 12, no. 4, pp. 30–39, Dec. 2017.
7. P. Tarasov and H. Tewari, ‘‘The future of E-voting,’’ IADIS Int. J. Comput. Sci. Inf. Syst., vol. 12, no. 2, pp. 1–19, 2017.
8. N. Kshetri and J. Voas, ‘‘Blockchain-enabled E-voting,’’ IEEE Softw., vol. 35, no. 4, pp. 95–99, Jul. 2018.
9. J. Xie, H. Tang, T. Huang, F. R. Yu, R. Xie, J. Liu, and Y. Liu, ‘‘A survey of blockchain technology applied to smart cities: Research issues and challenges,’’ IEEE Commun. Surveys Tuts., vol. 21, no. 3, pp. 2794–2830, 3rd Quart., 2019.
10. A. A. Monrat, O. Schelén, and K. Andersson, ‘‘A survey of blockchain from the perspectives of applications, challenges, and opportunities,’’ IEEE Access, vol. 7, pp. 117134–117151, 2019.
11. K. Curran, ‘‘E-voting on the blockchain,’’ J. Brit. Blockchain Assoc., vol. 1, no. 2, pp. 1–6, Dec. 2018.
12. M. Shafiq, Z. Tian, A. K. Bashir, X. Du, and M. Guizani, ‘‘IoT malicious traffic identification using wrapper-based feature selection mechanisms,’’ Comput. Secur., vol. 94, Jul. 2020, Art. no. 101863.
13. M. A. Khan and K. Salah, ‘‘IoT security: Review, blockchain solutions, and open challenges,’’ Future Gener. Comput. Syst., vol. 82, pp. 395–411, May 2018.
14. U. D. Gandhi, P. M. Kumar, R. Varatharajan, G. Manogaran, R. Sundarasekar, and S. Kadu, ‘‘HIoTPOT: Surveillance on IoT devices against recent threats,’’ Wireless Pers. Commun., vol. 103, no. 2, pp. 1179–1194, Nov. 2018.
15. G. Rathee, A. Sharma, R. Iqbal, M. Aloqaily, N. Jaglan, and R. Kumar, ‘‘A blockchain framework for securing connected and autonomous vehicles,’’ Sensors, vol. 19, no. 14, pp. 1–15, 2019.