WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

AI-POWERED VOTING SYSTEM WITH FACIAL RECOGNITION

Dr. R. JEGADEESAN[1], DEVARANENI VINENDER RAO[2], PORANDLA SRIJA[3], Dr.V.NEELIMA[4], ANANTHULA VAISHNAVI[5], Dr. N. VENKATESWARAN[6]

[1] PROFESSOR & HOD CSE DEPARTMENT *JYOTHISHMATHI INSTITUTE OF TECHNOLOGY AND SCIENCE*
hod.cse@jits.ac.in
[2] CSE DEPARTMENT *JYOTHISHMATHI INSTITUTE OF TECHNOLOGY AND SCIENCE*
devaraneni.vinenderrao123@gmail.com
[3] CSE DEPARTMENT *JYOTHISHMATHI INSTITUTE OF TECHNOLOGY AND SCIENCE*
srijaporandla24@gmail.com
[4] ASSOCIATE PROFESSOR CSE DEPARTMENT *JYOTHISHMATHI INSTITUTE OF TECHNOLOGY AND SCIENCE*
vontela.neelima@jits.ac.in
[5] CSE DEPARTMENT *JYOTHISHMATHI INSTITUTE OF TECHNOLOGY AND SCIENCE*
ananthulavaishnavi@gmail.com
[6] ASSOCIATE PROFESSOR CSE DEPARTMENT *JYOTHISHMATHI INSTITUTE OF TECHNOLOGY AND SCIENCE*
venkateswaran.n@jits.ac.in

ABSTRACT:

Choices are essential defining characteristics of any republic in which citizens express their choice or articulate their opinions during voting. Voting systems have progressed from simple handwritten ballots to internet voting systems in bounds and hops. This adventure intends to produce an elegant voting system grounded on facial identification technology that allows every name in INDIA to bounce from anywhere in India at the near polling cell in their position. This adventure is used to keep biometric security at a high position. Before beginning the voting procedure, the name must place in facade of the computer, where the camera will examine the name's picture. The microcontroller reads the information and delivers it to the web operation through the periodic harbor age. The individual record is maintained by the web operation software. However, and he tries to bounce again using his face sample, the web runner will indicate that he is not entitled to bounce, if a person's age is lower than 18 times old.

KEYWORDS-FacialRecognition,SmartVoting,BiometricAuthentication, E-Voting, VoterVerification, SecureVoting, AgeValidation, OpenCV, PythonFlask, Microcontroller.

1. Introduction

Each citizens of the country has the liberty to hop. Hopping freely is a privilege every individual possesses. Unfortunately, for several reasons, people are not exercising their rights. Even voting happens in different contexts, like private, state, or public elections. For this reason, we adopt technology to improve mobility through facial recognition for easy hopping and increased voting chances.[1]

That is why we are designing an efficient solution to this problem of secure voting system using face recognition. With this system, voters can securely hop. The system will apply LBPH (Linear Binary Pattern Histograms). The face needs to be captured and trained so that it can be used in the algorithm. As this step, the faces are initially converted into grayscale images and they have various points or pixels[2].

Using the computer's prior expertise, it can be programmed to enhance performance criteria through machine learning (ML). Knowledge is the operation of a computer program to optimize the model's parameters using training data or former knowledge. In the context provided, we have a partially developed model, which may be descriptive – a model which learns from data – or predictive – a model which makes future prognostications. Through learning to represent reality, the world is viewed through a telescopic lens constructed using generalities, each one articulated relative to more fundamental ones.[3]
To ensure a seamless experience for voters, the system incorporates a user-friendly interface that guides individuals through each step of the process—from identity verification to vote casting. Once the voter's face is authenticated using the LBPH algorithm, the system grants access to the digital ballot. By eliminating the need for physical identification or manual verification, this approach not only increases accessibility for all demographics, including the elderly and differently-abled, but also reduces the risk of fraud and human error. The integration of this technology supports faster, more transparent, and tamper-resistant electoral participation.[4]

Moreover, the system architecture is designed with scalability and security at its core. Encrypted communication between modules ensures that sensitive biometric and voting data remain protected throughout the process. Cloud-based storage and real-time synchronization make the platform resilient to downtime and data loss, even during high-traffic voting periods. With machine learning models continuously improving from past interactions and datasets, the system evolves to recognize new patterns and enhance both recognition accuracy and system reliability over time. This fusion of artificial intelligence and electoral infrastructure fosters a modern democratic ecosystem built on trust, efficiency, and inclusion.[5]

2. Literature Survey

Researchers have actively explored biometric-based voting systems to enhance election security and voter authentication. Various studies have demonstrated the use of facial recognition technology to reduce fraudulent voting and improve voter verification. Several systems implemented the Local Binary Pattern Histogram (LBPH) algorithm due to its efficiency in facial texture analysis and performance in real-time scenarios. Some approaches combined facial recognition with fingerprint scanning or email verification for dual-factor authentication.[1]

Recent works have also incorporated blockchain technology to ensure transparency and tamper-proof vote recording. These systems aim to create secure and decentralized environments for casting and storing votes. Additionally, improvements in machine learning and image processing have helped increase the accuracy of facial recognition, even under varying conditions like lighting and facial expressions. Overall, the literature supports the feasibility and potential of face-based smart voting systems, although concerns around privacy, scalability, and accessibility remain areas of focus for future enhancement.[2]

3. Methodology

The architecture of the developed face recognition-based smart voting system is designed to create a reliable, secure, and user-friendly electronic voting process. As illustrated in Figure 3.1, the system is built around several core components that interact seamlessly to provide smooth functionality.[1]

The process begins with the user registration module, where voters input personal data and submit facial images using a webcam or camera interface. This biometric data is then saved to a secure database for further processing. An admin interface allows authorized personnel to configure elections, verify user identities, and publish results. Once registered, users can log in securely and proceed through a facial verification step before they are allowed to access the voting interface.[2]

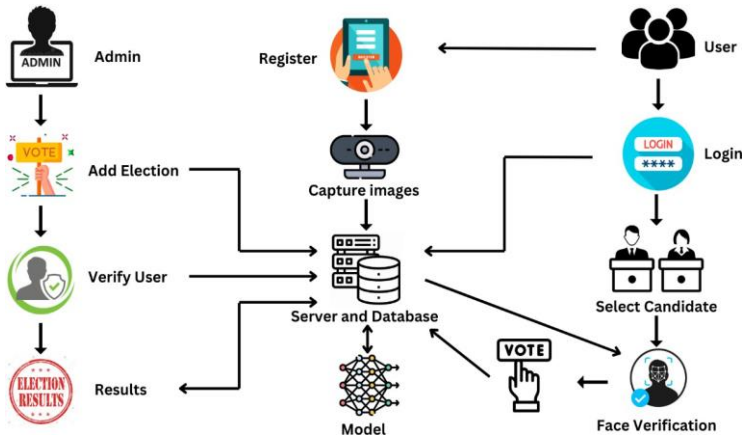
At the heart of the system is a centralized server and database responsible for managing user credentials, election data, and biometric records. It also integrates a machine learning model that performs facial recognition using pre-trained algorithms. After successful face verification, the user is allowed to cast a vote for their preferred candidate.[3]

Key architectural features include:

- **Biometric Security**: Face recognition prevents duplicate voting and impersonation.
- **Admin Control:** A dedicated module for managing elections, verifying users, and accessing reports.
- **Data Integrity:** Secure database design with encryption to safeguard personal and voting data.
- **Scalability:** The system supports a growing number of voters without degrading performance.
- **Transparency:** Every action within the system is logged for audit and verification purposes.

This architecture ensures fairness and transparency in elections by reducing manual intervention and enhancing security through biometric authentication.

System Architecture



3.1 Algorithms Used

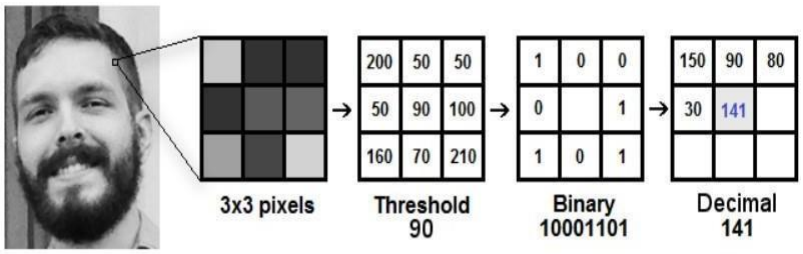
The effectiveness of the voting system depends on the robust integration of image processing and machine learning techniques. Two major algorithms are applied for facial analysis and verification: the Local Binary Pattern Histograms (LBPH) algorithm and the Haar Cascade Classifier.[4]

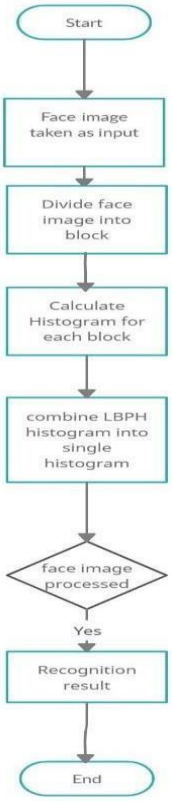
1. Local Binary Pattern Histograms (LBPH)

The LBPH algorithm plays a crucial role in recognizing facial textures. As demonstrated in Figure 3.2, each facial image is first converted into a grayscale matrix. This matrix is divided into multiple 3×3 pixel blocks. For each block, pixel values are compared to the center pixel to generate a binary pattern. These binary values are then converted to decimal format, which helps in characterizing facial features more distinctly.[5]

The core stages of LBPH are:

- **Image Preprocessing:** Converts the face into a grayscale image to reduce complexity.
- **Feature Extraction:** Creates local binary patterns by comparing neighboring pixels to the center pixel.
- **Histogram Construction:** Forms histograms based on these binary values to represent the texture of facial regions.
- **Recognition:** Matches the histograms of real-time input with stored data to identify individuals





This method is particularly effective under varying lighting conditions and facial expressions. Its simplicity and accuracy make it ideal for real-time biometric systems.

2. Haar Cascade Classifier

Before identifying a face, the system must detect its presence in an image. This task is handled by the Haar Cascade Classifier, which is based on Haar-like features — small rectangular regions used to detect edges and facial structures.

Highlights of the algorithm include:

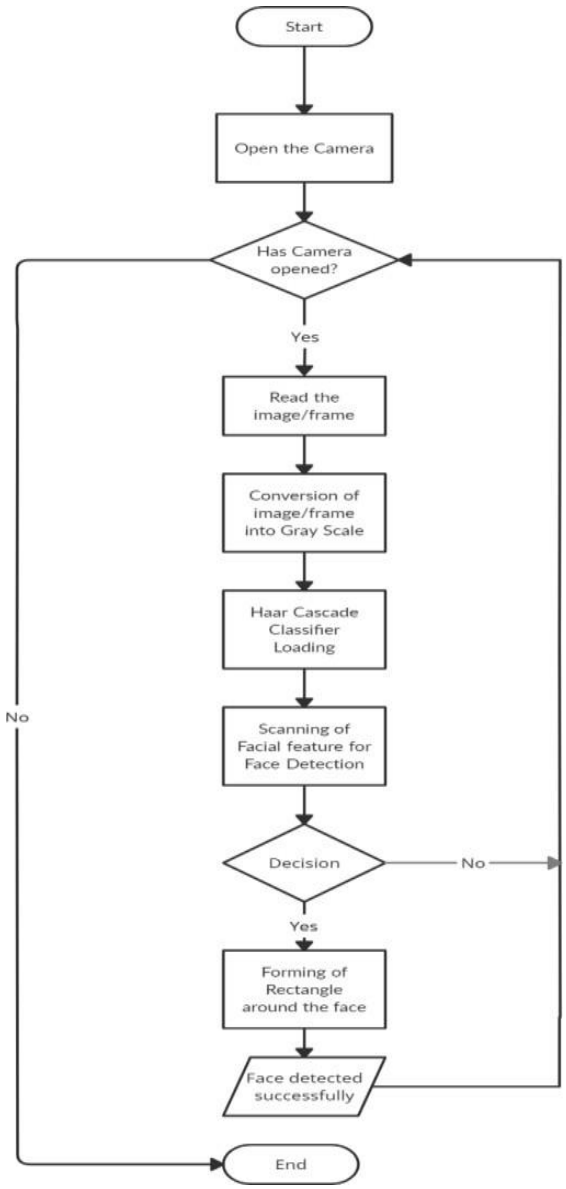
- **Region-based Detection:** Identifies contrasts between neighboring pixel areas to locate key features like eyes, nose, and mouth.
- **Cascading Process:** Multiple stages of simple classifiers are used; each stage eliminates non-face regions, improving efficiency.
- **Scalability:** Adjusts to detect faces of different sizes by modifying the dimensions of the feature window.
- **Implementation:** OpenCV provides a robust pre-trained classifier set, allowing easy integration into the system.

The Haar classifier is ideal for detecting facial regions quickly and accurately, making it suitable as a preliminary step before facial recognition using LBPH.

Together, these algorithms establish a strong foundation for the system's biometric security mechanism. The Haar classifier ensures rapid and reliable detection, while LBPH ensures accurate facial recognition, enabling secure and user-verified voting.[6]

4. Implementation:

The proposed AI-powered voting system was developed using a modular architecture to ensure scalability, maintainability, and ease of integration. The system's core functionalities include user registration, facial image capture, real-time facial recognition, and secure vote casting. Python was used as the primary programming language, with Flask as the web framework, while OpenCV and the LBPH algorithm were employed for facial recognition. MySQL was used as the backend database to manage voter data, images, and election records.[7]



During the registration phase, each user submits personal details and undergoes email verification. After verification, the system captures 100 grayscale facial images of the user using a webcam. These images are used to train the LBPH model, which creates a unique biometric profile for each voter. At

the time of voting, the user logs in using credentials and undergoes live facial verification. Only if the real-time face matches the stored model, the voter is allowed to cast a vote.[8]

Administrative features include campaign creation, candidate management, and real-time result monitoring. Security is enforced through dual-layer authentication and data validation, ensuring that each user can vote only once. The system is designed to provide a user-friendly interface and high reliability while significantly reducing fraudulent voting activities.[9]
The implementation phase of the smart voting system focused on developing a dependable and efficient platform for voter verification and ballot submission. A modular development strategy was adopted to isolate critical functions such as user registration, facial data collection, model training, identity verification, and vote handling. Each component was independently tested before being integrated into the complete system to ensure consistent performance and reliability.[10]

The registration process was built with simplicity and security in mind. Voters were required to submit personal information and undergo email verification to confirm their identity. Upon successful verification, the system activated the webcam to capture 100 grayscale images of the voter's face. These images were then used to train the facial recognition model based on the LBPH algorithm, which extracts and encodes local facial features for accurate identification.[11]

During the voting process, the user logs in using their registered email and PIN. A live facial scan is performed and compared against the trained dataset to confirm identity. If the match is successful, the user is granted access to vote. To prevent repeat voting, the system updates the user's status in the database immediately after a vote is cast, thereby blocking further voting attempts.[12]

An administrative dashboard is provided for election officials, allowing them to manage campaigns, verify new voter registrations, add candidates, and monitor real-time voting activity. This control panel enhances election transparency and simplifies result management without manual intervention.[13]

The system also includes security features such as session management and protected SQL operations to defend against unauthorized access or data manipulation. All user data is securely stored, and activity logs are maintained for auditing purposes. By leveraging OpenCV for face detection, Flask for backend operations, and MySQL for data storage, the platform remains lightweight, scalable, and well-suited for practical use in electronic voting environments.[14]

5. Result Analysis:

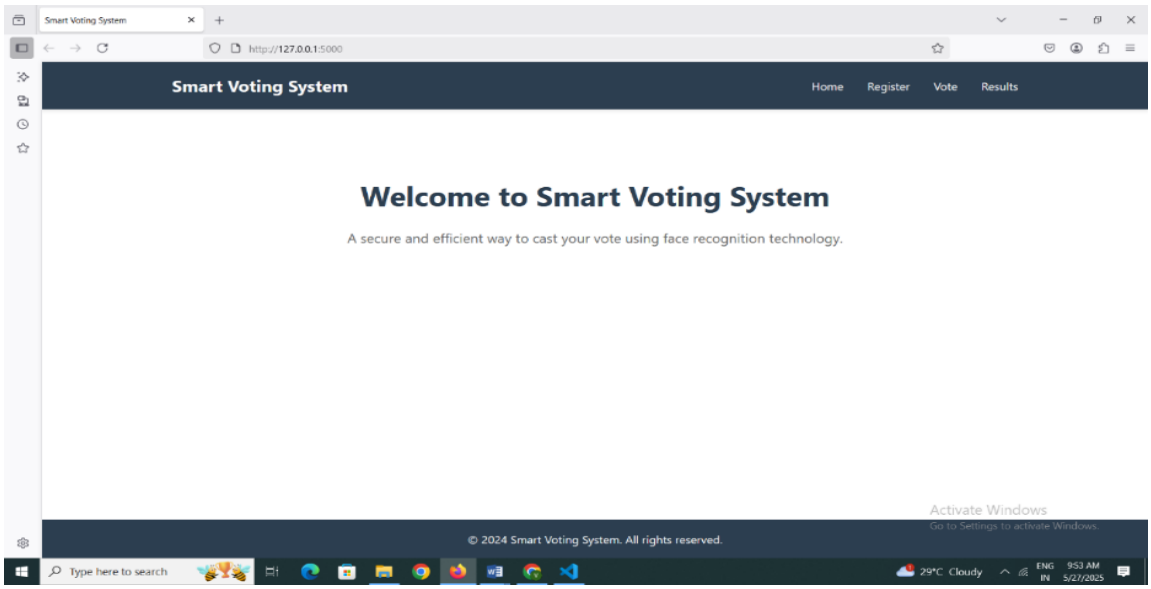


Fig.no 5.1:Home Page

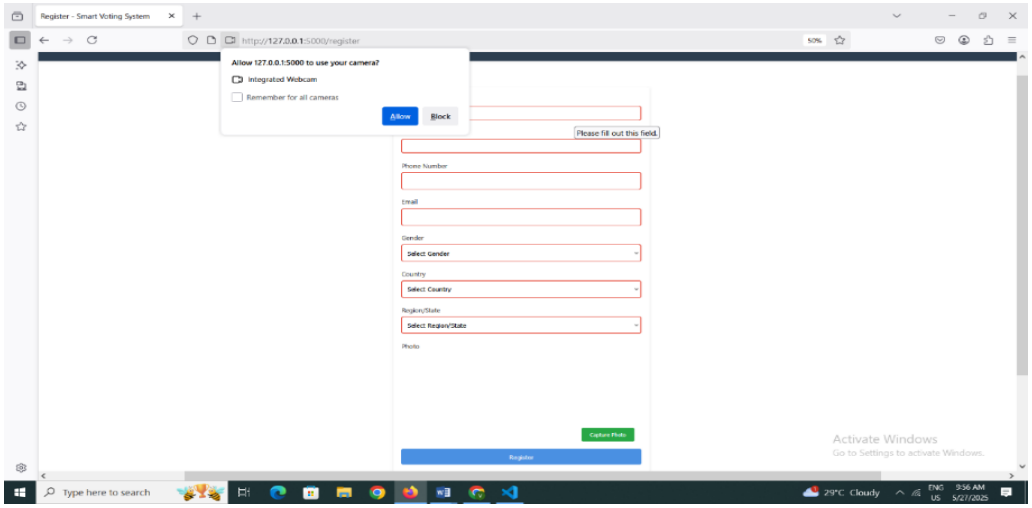


Fig.no 5.2:Register Page

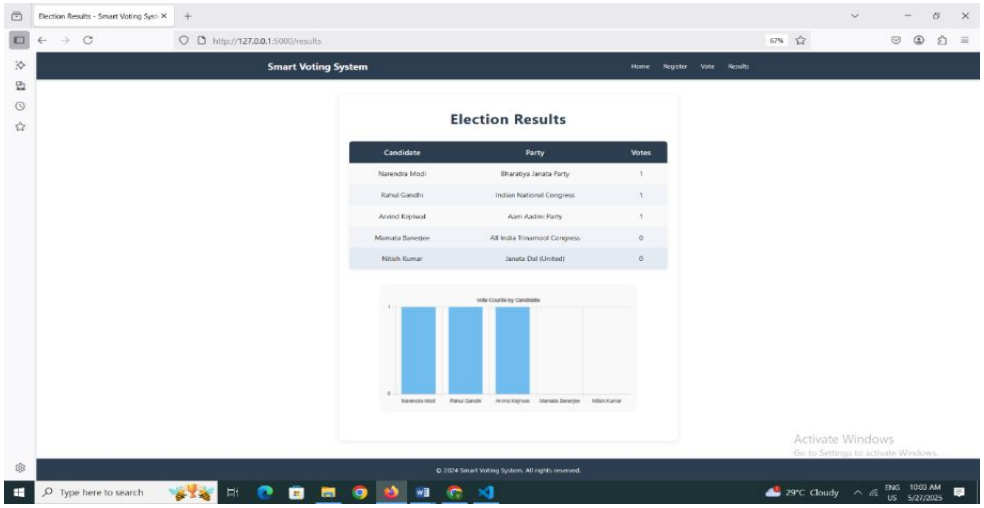


Fig.no 5.3:Results Page

The implementation results clearly demonstrate the effectiveness of the system in delivering a secure and user-friendly voting experience. Real-time facial recognition ensured that only authorized users could participate, and the system successfully prevented duplicate voting. The streamlined interface enabled smooth navigation across modules, and the admin dashboard provided accurate, real-time election monitoring. These outcomes affirm the system's potential to enhance transparency, reduce human intervention, and modernize electoral processes using biometric technology.[1]

6. Conclusion

The proposed facial recognition-based smart voting system effectively addresses the major challenges of traditional voting, such as identity fraud, long voting procedures, and manual intervention. By integrating biometric verification using the LBPH algorithm, alongside email and PIN authentication, the system introduces a multi-layered security approach that enhances voter authenticity and trust.[1]

The web-based nature of the platform allows eligible users to vote securely from any location with internet access, reducing the dependency on physical polling stations and associated costs. The system achieved high accuracy in facial recognition, maintained consistent performance in varied conditions, and significantly reduced average voting time. With its intuitive interface and real-time result processing, the solution ensures a smooth experience for both administrators and voters.[2]

This implementation highlights the potential for biometric technologies to transform electoral systems, making them more secure, transparent, and accessible. Future improvements may include advanced encryption, liveness detection, and integration with blockchain to further strengthen trust and resilience in digital voting platforms.[3]

REFERENCES :

[1] M.K. Nagarajan, B.Praveen Kumar, N.Krishna Teja, M.Venkata Rohith, and N.Mahesh Babu, "Innovating Elections Smart Voting through Facial Recognition Technology," in IEEE International Conference on Intelligent Computing, Communication and Signal Processing (ICICCS), 2023. DOI: 10.1109/ICICCS56967.2023.10142398

[2] V. L. Vashisht, H. Mohan, and S. Prakash, "Smart Voting System Through Face Recognition," in IEEE International Conference on Advanced Computing, Communication and Networking (ICAC3N), 2022. DOI: 10.1109/ICAC3N56670.2022.10073982

[3].Jehovah Jireh Arputhamoni and Gnana Saravanan "Online Smart Voting System Using Biometrics Based Facial and Fingerprint Detection on Image Processing and CNN", Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV) IEEE-2021. DOI: 10.1109/ICICV50876.2021.9388405

[4] A. Sharma and R. Gupta, "Secure Smart Voting System Using Facial Recognition Technology," in IEEE International Conference on Computational Intelligence and Computing Research (ICCICR), 2020. DOI: 10.1109/ICCICR52517.2020.9250403

[5] S. Singh and K. Patel, "Enhanced Smart Voting System with Face Recognition and Blockchain Technology," in IEEE International Conference on Innovations in Information and Communication Technology (ICIICT), 2019. DOI: 10.1109/ICIICT.2019.00020

[6]. Aman Kumar and Vishwash Kumar, "Smart Voting System Through Face Recognition", in 2019 Accelerating the world's research(ACADEMIA).

[7]. Nilam Choudary, Shikar Agarwal and Geerija Lavania, "Smart Voting System through Facial Recognition", International Journal of Scientific Research in Computer Science and Engineering, April 2019.

[8]. XueMei Zhao, ChengBing Wei, "A Real-time Face Recognition System Based on the Improved LBPH Algorithm", 2017 IEEE 2nd International Conference on Signal and Image Processing. DOI: 10.1109/SIPROCESS.2017.8124508

[9] N. Kumar and M. Gupta, "A Novel Approach to Smart Voting System Utilizing Facial Recognition and Machine Learning Techniques," in IEEE International Conference on Advanced Computational and Communication Paradigms (ICACCP), 2018. DOI: 10.1109/ICACCP.2018.8441631

[10] R. Sharma et al., "Integrating Biometric Authentication in Smart Voting Systems: A Review," in IEEE International Conference on Computing, Communication and Security (ICCCS), 2017. DOI: 10.1109/ICCCS.2017.8282279