American Journal of Operations Management and Information Systems
2024, Vol. 9, No. 2, pp. 34-42
https://doi.org/10.11648/j.ajomis.20240902.12

Research Article

Implementing a Three-Step Security Protocol for Advanced Online Election Systems: A Novel Approach

Dia Nandy, Arghyadeep Maiti, Moloy Dhar*, Barna Barman, Anish Aich

Department of Computer Science and Engineering, Guru Nanak Institute of Technology, Kolkata, India

Abstract

Organization of voting is the strength of character of all equalitarianism and system. Our country utilize an offline voting systems that are incompetent and disorganized by cause of the demand for abundant man power, and more refinement time for announcement outcome. Our Online Voting System aims at minimizing the division between traditional voting methods by facilitating and updating them. Our system makes it possible for voters to vote their favorable candidates from home through safe and stable online voting. By integrating India's Aadhaar card system and implementing OTPs (One Time Passwords) for better security, ensure a resilient and trustworthy voting process with full integrity. Once they login, voters are led through a strict authentication rules that checks for the genuineness of their ID cards before allowing them to continue. This comprehensive verification mechanism provides that only individuals who meet the requirements are able to participate thereby considerably decreasing the chance for electoral fraud. In addition to that, we also ensure that the system gives space to vote in secret and the votes are protected using strong cryptography measures. Our platform aims at fulfilling this object by leveraging advanced technologies. In this regard, we work towards a better and more egalitarian and democratic electoral system.

Keywords

Face Recognition System, OpenCV Library, Aadhaar ID based Online Election

1. Introduction

Technology has been a catalyst for enormous change. One area where there are common differences in design is in democracy: robust online voting systems demonstrate that well-designed automatic elections serve not just rulers but also those who are ruled. With an automated approach, users benefit from faster ballot-counting and more convenient electoral procedures. They receive voter-added qualities like increased convenience, better security and especially higher efficiency. The primary task is to increase voter turnout and get more people involved in elections. This system also helps election committees run and supervise all aspectsof elections carefully, whilst minimizing public safety hazards posed by traditional polling stations. Additionally, the system speeds through the vote tabulation procedure allowing for a vote count to finish in one day thanks in part its plain interface and fast result calculations. The setting of the online voting system ensures a quiet, friendly environment for voting: voters feel right at home. Above all, it stops other people from intervening in the progress of voting, thus keeping the elections fair. And there are no geographical restrictions on par-

*Corresponding author: moloy.dhar@gnit.ac.in (Moloy Dhar)

Received: 4 June 2024; **Accepted:** 20 June 2024; **Published:** 6 September 2024

ticipation: citizens can exercise their right to vote from anywhere - no matter across borders within your nation or on foot out of a nursing home. By taking this digital transition to electronic voting, we eliminate the need for people to stand in long lines at traditional election sites. Every measure has been taken in order to guarantee that electronic ballots are safe from tampering or fraud. Our unique thinking is that before voters are able to select their candidate of choice, we prioritize improving reliability of the system through a three-step authentication process. The procedure involves a series of verifications, first checking an Aadhaar card with an OTP linked to the mobile. Then it moves on to verifying the Voter ID and face recognition. By integrating these identification means, not only is the electronic voting system made more secure, but elector's choice entwined with cheating behavior also can hardly be trusted. Moreover, our aim is to provide participates in voting processes at a secure location other than the ballot box for those who cannot get to a polling place.

The content of this paper is organized as follows:

In the second section, we have described some of the Related Works that we have used for our reference. The third section completely explains the Methodology that we have used in our research paper. Further, the fourth section deals with the Result. The next part, which is the fifth section concludes the paper. The sixth section explains the future scope of our research. And lastly, in the seventh section, we have enlisted the references that we have used for our paper.

2. Related Works

This paper [1] "Online Voting System" focusses on switching from stereotypical voting system to digital using PHP and Bootstrap.

Author of this paper [2] "Smart Online Voting System" concentrates on two steps verification which includes facial recognition and OTP verification. It also allows user to vote offline. The paper [3] "Online Voting System using Cloud" approaches online voting system using cloud mechanism. This paper relies [4] "Online Voting System using Blockchain" on online voting system based on Blockchain. The work of this paper [5] "Analysis of an electronic voting system" focusses on eradication of security faults in their voting system. It keeps a paper record for electors to check. The utmost goal of this paper [6] "Multi-purpose Platform Independent Online Voting System" is to make the system of voting versatile and cross-platform for all.

3. Methodology

Table 1. *Comparative Research Analysis.*

Paper Name	Similarities	Differences
Online Voting System by Using Three Step Verification N. Sreenivasa, Gopal Agarwal, Rishab Jain Department of Computer Science and Engineering, Nitte Meenakshi Institute of Technology, Bangalore-560064, Karnataka, India.	Three step verification Haar cascade classifier algorithm Both voting systems are more concise, secure and dependable.	In their paper, they implemented OTP verification using CAPTCHA, whereas we conducted real-time voter verification. They conducted voter card verification using voter IDs, whereas we achieved real-time verification via camera. Our idea prevents multiple voting.
Ms. Kavya Ramesh Naidu, Mr. Ankush Dinesh Ingale, Ms. Pratiksha Sukhadeo Gaikwad, Mr. Hitesh Rajendra Thakare, Mr. Sujal Sunil Chavan Prof. Yogeshk Sharma Department of Computer Engineering Vishwakarma Institute of Information Technology, Pune, India.	Both systems aim to increase voter turnout and provide convenience to voters through online voting. Both systems prioritize secure authentication through various methods such as OTP verification and biometric authentication. Both systems follow a similar structure of phases including registration/authentication, voting, and result declaration.	Our system: tech-driven security like face recognition and Aadhaar integration. Existing: registration, real-time results, cloud voting. Ours: cost reduction, safety, quick results. Existing: accessibility, transparency, fraud elimination. Ours: highlights future enhancements like security, usability. Existing: blockchain, voter confidence.
Online Voting System Voram Bhavan, Laxmi Koli, Lanka Rishi, Marri Sankeerth Reddy Assistant Professor, Dept. of Electronics & Computer Science Engineering, Sreenidhi Institute of Science and Technology, Hyderabad, Telangana, India.	Expanding online voting systems with live result updates, blockchain integration, and global organizational adoption. Highlighting potential benefits such as increased transparency, reliability, and efficiency compared to traditional methods.	Our paper employs Python Django Framework and TensorFlow.js/ Deep Face for implementation, whereas the other paper does not specify these technologies. Our paper emphasizes facial recognition

Paper Name	Similarities	Differences
	Emphasizing security authentication measures to ensure the legitimacy of votes and voters.	for authentication, while the other paper mentions Voter's ID and traditional login methods. Our paper highlights feature like enhanced voter identification via facial recognition, queue-free voting, and integration with blockchain, whereas the other paper focuses on general aims and objectives without specifying detailed features.
Shubham Gupta, Divanshu Jain, Milind Thomas Themalil, "Electronic Voting Mechanism using Microcontroller ATmega328P with Face Recognition, Proceedings of the Fifth International Conference on Computing Methodologies and Communication (ICCMC 2021), pp. 1471-147, 2021.	Multistage verification process (Aadhaar card, face verification). Real time vote count is shown on display. The voting data is continuously uploaded on server. During vote casting user can see their personal details on the screen.	For face verification used algorithms are ensure more accuracy. Additional verification step voter card verification at real time). After successful vote casting e-receipt generation and sending to voter's phone number via SMS Prevents multi time vote casting.
A Study of Vulnerabilities in E-Voting System Xing Shu Li, Hyang ran Lee, Malrey Lee1 and Jae-young Choi, Center for Advanced Image and Information Technology, School of Electronics & Information Engineering, Chon Buk National University, 664-14, 1Ga, Deokjin-Dong, Jeonju, Chon Buk, Korea.	Aims to make the full voting system digitalize. Decrease the vote manipulation. User authentication before vote casting.	It has only one step verification process but our software proposes multistep verification processes. As convolutional voting process we keep users' data encrypted. We have implemented our software such as it is capable to prevent different malware attacks.

In today's Information Age, where technology is integrated into every aspect of our life, the idea of online voting offers great promise [7]. Zeroing in on non-traditional methods: Our proposed approach creates an electoral system that is guaranteed to be foolproof and secure.

Central to our approach is the seamless integration with Aadhaar, India's unique identification system [8]. Whether new store data is published or old store data updated, this involves a crosscheck with Aadhaar to make sure the Aadhaar number has not been faked. On logging in, voters receive a One Time Password on their registered mobile number linked to Aadhaar to increase security and simplify verification while countering voter impersonation.

The following table highlights the similarities and differences of our idea with respect to the referenced papers.

Upon authentication, voters are asked to scan their voter ID cards beginning a rigorous identification process. This not only retrieves and validates the voter ID number from the voter ID database, but is followed by a face verification procedure using advanced facial recognition software [9]. Such rigorous verification can ensure that only qualified persons vote and will cut down substantially on the risk of electoral fraud. To maintain the integrity of the election and prevent duplicated voting, our system has strict controls designed to curb multiple logons, allowing each voter one chance to cast his or her ballot safely and reliably. By preserving the integrity of the election process, our method guarantees that each voter has a fair chance beyond question [10]. Online voting mode is efficient and cost-effective, eliminating the need for physical polling stations. Looking to the future, this innovative method utilizes technology to ensure freedom and fairness in elections. By putting accent on accessibility, transparency/time limits and security, we hope to plant those seeds of trust which will let ordinary people mold the future nation in their homes as well [11]. During software development and use, we carefully select numerous technologies to integrate into a single system to ensure our online voting system is simple yet functional the whole way. All of our software's components are designed and integrated with precision, so that a user can reliably cast their vote from our software even when at a remote location. From the flow chart (Figure 1), we can see that, people first enter into the software the user will encounter Aadhaar verification, where they must input their Aadhaar number. After first validating the Aadhaar number, our system then sends an OTP to the mobile number associated with Aadhaar [12]. This process is achieved through integration with Aadhaar APIs and by means of these interfaces directly into the Aadhaar database to confirm the provided information. To generate and validate OTPs, we use Twilio's messaging service, which com-

municates with backend APIs ensuring secure transmission and verification. The front end is developed with React Native enabling one-time programming of the user interface in which a single interface will serve from desktop to mobile [13]. Navigation service React Navigation is employed for seamless movement within the application; Redux assures that software consistency is maintained at all times - a single sequence of events happens in an entirely predictable manner and handles state management across applications; On the back end, Node.js serves as the run-time environment; Express.js provides a minimal web application framework. With Firebase as a real-time database, it can store data properly and retrieve user-related information instantly [14].

In order to guard the user session and verify the requests, we employ JSON web tokens (JWT). Each time a user logs in, a JWT Token is created and sent up to user device. That token is then passed along in all additional requests as part of the cookie. In this way, token-based authentication enhances security. There are no longer "man-in-the-middle" or "sniffing " attacks on the server that can receive unauthorized access [15].

The second step in verifying a voter is via live video and still images from OpenCV-equipped Android phones. With the idea of edge detection, for example, an OpenCV XML file is employed to automatically detect and enhance the outline of characters one by one. Then comes Optical Character Recognition (hereafter referred to as OCR). We use OCR to extract the non-blurred text of each voter number from the captured images. Regular Expressions (regex) and self-made validation rules are used to verify whether the structure and format of these extracted card numbers are right. Below is the algorithm for implementation of OCR using Python and OpenCV for real-time voter card verification.

Last in the process is face verification, which integrates OpenFace, a neural network-based facial recognition system. OpenFace uses live images or videos taken from a camera to process facial landmarks, then generates facial embeddings. The mobile app side of these embeddings goes through AES encryption before being sent on to the server. On the server end these facial embeddings are decrypted using Node.js and their similarity to stored facial features is compared. If more than a pre-specified number of facial metrics overlap then authentication has been successful, and a new JWT token is either created afresh or updated so as to securely manage the user's verified session.

After users complete those three steps successfully, they can use the application interface to choose a preferred candidate for themselves. Using asymmetric RSA (Rivest, Shamir and Adleman), details of selected candidates and corresponding voter information are encrypted to guarantee their confidentiality and integrity. Encrypted votes are stored securely in a dedicated database, with strict measures to avert tampering and unauthorized access. Upon completion of their vote, users receive a confirmation message which provides both verification and reassurance that they have indeed cast a ballot. Action against double voting is guaranteed by the session management mechanism which introduces fairness into the voting process itself.

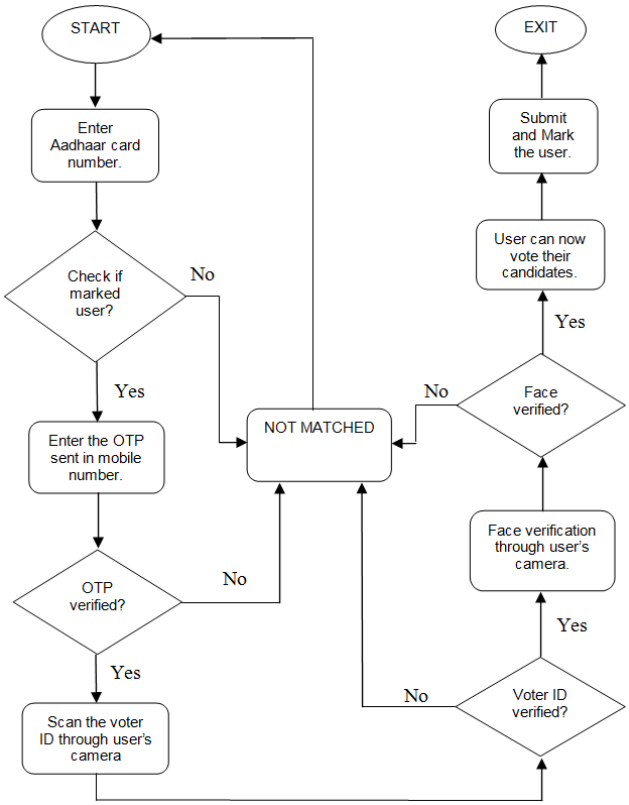

Figure 1. *Flow Chart of Proposed Methodology.*

Algorithm 1. Implementing Optical Character Recognition (OCR) using Python and OpenCV for real-time Voter Card verification.

```
FUNCTION LoadAndEncodeImage(filePath)
  TRY
    image <- LoadImageFile(filePath)
    encodings <- FaceEncodings(image)
    RETURN encodings[0] IF Length(encodings) > 0
ELSE RAISE "No faces found"
  CATCH Exception e
    PRINT "Error: " + e
    RETURN null
  END TRY: END FUNCTION
FUNCTION InitializeWebcam()
  webcam <- OpenWebcam()
  RETURN webcam IF webcam IS NOT null ELSE
PRINT "Error: Could not open webcam"
END FUNCTION
FUNCTION CaptureFrame(webcam)
  RETURN ReadFrameFromWebcam(webcam): END
FUNCTION
FUNCTION ProcessFrame(frame, knownEncoding)
  faceEncodings <- FaceEncodings(frame, FaceLoca-
```

```
tions(frame))
    FOR EACH encoding IN faceEncodings
      RETURN true IF CompareFaces([knownEncoding], encoding)[0]
    END FOR: RETURN false
  END FUNCTION
  FUNCTION Main()
    knownEncoding <- LoadAndEncodeImage("path_to_known_image.jpg")
    IF knownEncoding IS null RETURN
    webcam <- InitializeWebcam()
    IF webcam IS null RETURN
    WHILE true
      frame <- CaptureFrame(webcam)
      IF frame IS null CONTINUE
      match <- ProcessFrame(frame, knownEncoding)
      PRINT "Face match found!" IF match ELSE "No match found"
      DisplayFrame(frame) // Optional
      BREAK IF UserPressedExitKey() // Optional
    END WHILE
    CloseWebcam(webcam)
  END FUNCTION
  CALL Main()
```

A real-time view across the network of WebSocket likewise enhances trust in electoral data as well as encouraging voting. This system is also encrypted with HTTPS to keep the data safe as it travels between users 'devices and the server, thus preventing unauthorized infiltration. Convolutional Neural Networks (CNNs) have been employed to detect and deter false biometric data, thereby enhancing reliability in the authentication process. The voting system has therefore been beefed up with the help of blockchain technology for greater security as well as transparency. Each vote is an individual transaction record on the blockchain ledger, securely linked together with previous transactions. An unchanging and tamper-proof record is formed. This means that once a vote has been cast by the voter, it cannot be changed again at any cost. In this way, the integrity of the voting process itself is reinforced and participants can feel more secure in their actions.

There is continued monitoring of the online voting system and rapid reaction to any security issues or vulnerabilities detected: administrators monitor the system constantly to nip potential security problems in the bud before they start.

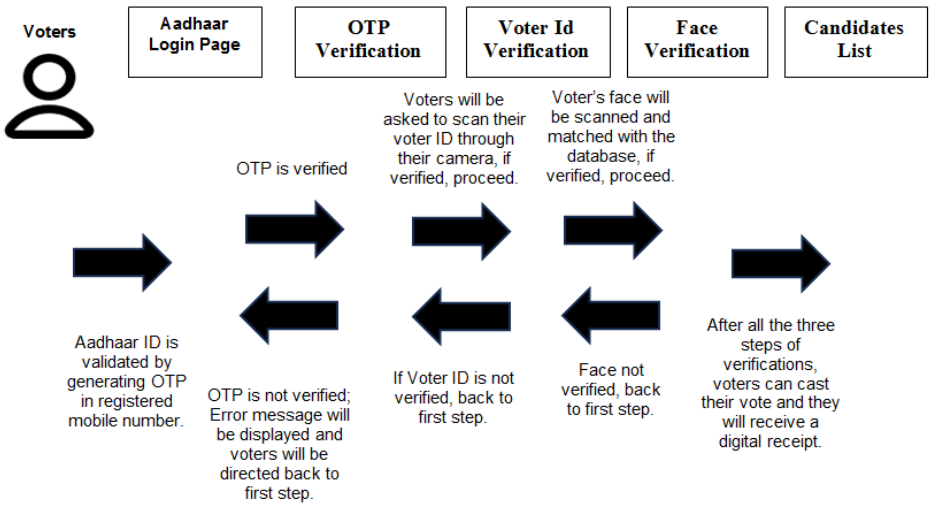

Figure 2. *Sequence Diagram of Proposed Methodology.*

Automated alerts and response tactics optimize the security monitoring procedure, ensuring swift and formidable action if a security event occurs. By linking these technologies together seamlessly the online voting system hopes to offer citizens a secure, transparent platform where they can exercise their voting rights out.

4. Result

The results of the study demonstrate the efficiency and reliability of our multi step verification process.

Through rigorous experiments and analysis, it was found that the OTP-based Aadhaar verification system excels in both accuracy and safety of validating unique identities. The authentication process showed very little false positives or negatives throughout, maintaining the integrity of our verification system. In addition, the OTP-based Aadhaar verification system proved highly scalable. This meant it could successfully process a high number of verification queries and still return them within the time period as specified.

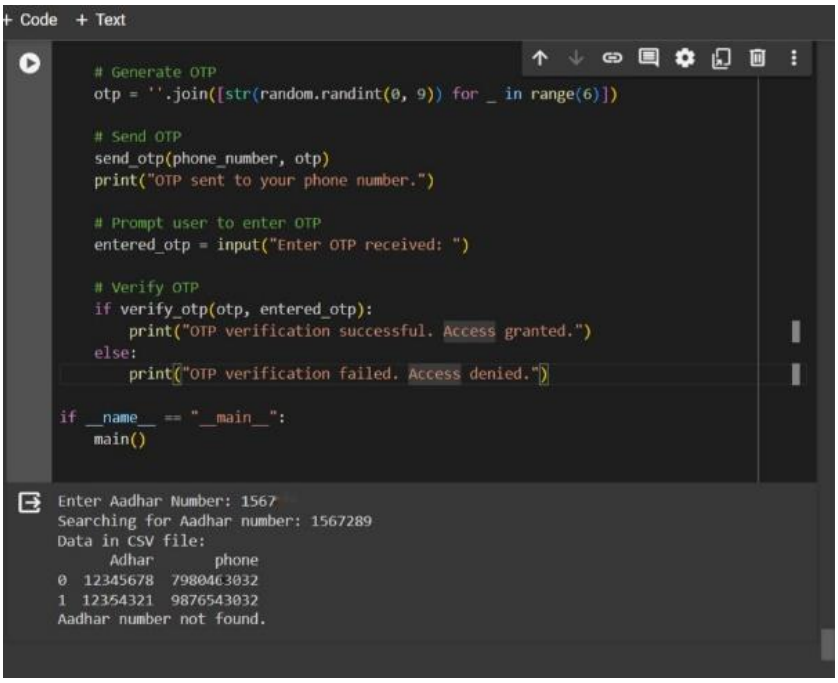

Figure 3. *Measure for Fraudulent Input.*

Furthermore, the security mechanisms contained within the OTP authentication framework were found to be efficient at guarding against potential risks linked to identity theft & unauthorized entry. The employment of dynamic OTPs paired with a rigorous encryption regime rendered the system impregnable against attacks from security threats or unauthorized entry attempts.

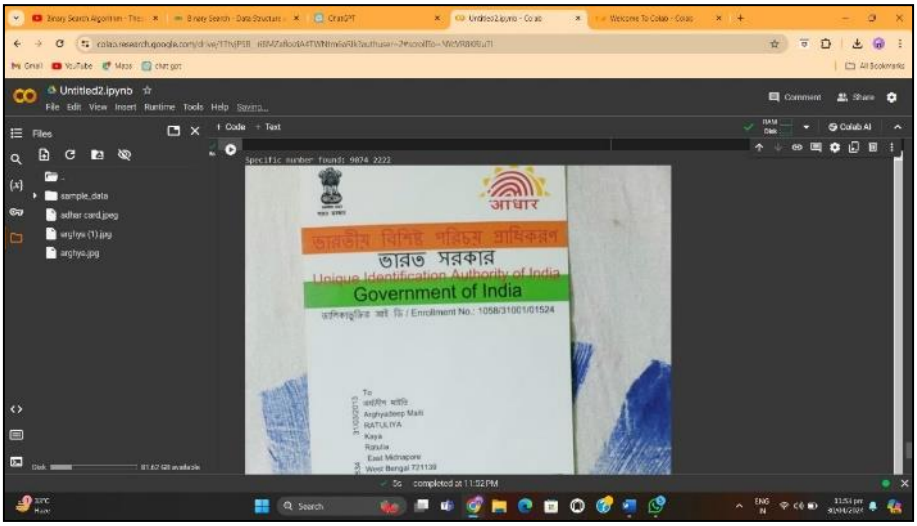

Figure 4. *Real-time Verification.*

Through repeated examination and analysis, it can be seen that the proposed real-time voter identity verification system is effective and viable. The effect was that the Realtime Voter ID System achieved a commendable accuracy rate with only few errors, such as mismanaged data or typos. Overall, the conclusion drawn is that a real time voter card verification system is very promising as legitimate and safe method to guarantee the authenticity of voter's identities during elections. The results reconfirm the system's accuracy, scalability and security, thus verifying that it is suitable for widespread application in electoral engineering which upholds the truth value forwarded by democratic elections themselves.

Haar features are used to detect various objects within an image. There are five kinds of Haar features including: 1.

Edge Features 2. Line Features 3. Four-Rectangle Features 4. Three-Rectangle Features 5. Center-surround Features.

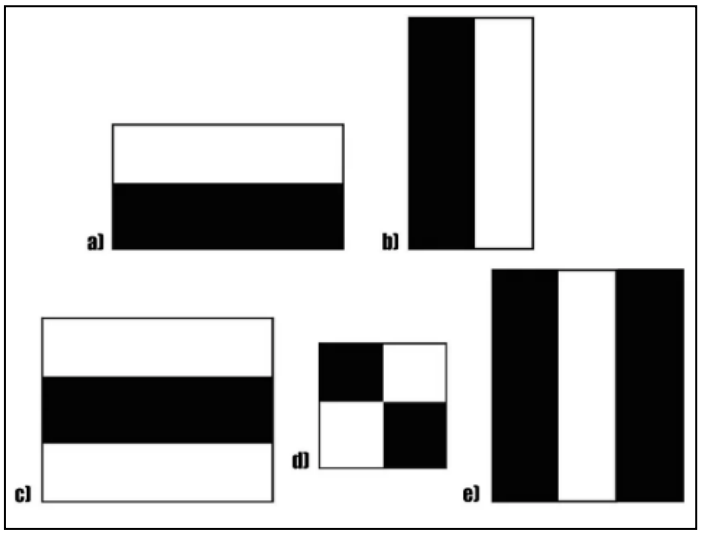

Figure 5. *A sample of Haar features.*

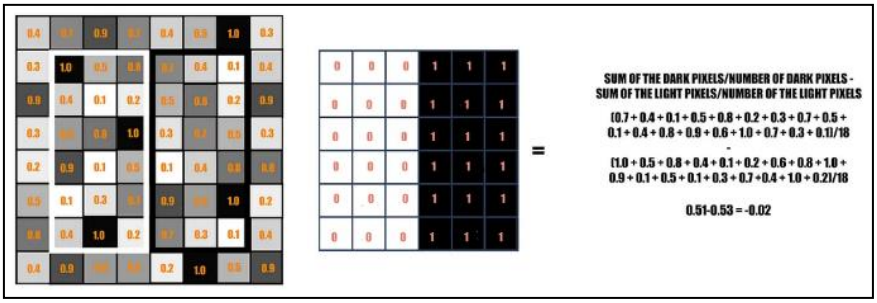

Figure 6. *Edge detected by the Haar feature.*

Calculating the Pixel of the Haar cascade Identification and classification of objects within images is called pixel calculation such things involve breaking an image into smaller regions and applying filters. These features specifically have been quantified by Haar cascade algorithm, according to thedifference in intensity just inside not very-far adjacent rectangular regions (taken from particular points over a strip). This calculation (as shown in Figure 6) is an important part of the whole object detection process, as it helps determine whether a given area contains desired object based on predefined criteria.

In Figure 7, Confusion Matrix of a face recognition model trained on database so as the performance can be seen. Each cell in the matrix represents how many predictions for each class. The class in our case is six different species of Iris flowers. The really rows stand for actual classes, while the columns stand for predicted classes. With visual representation, the distribution of correct and incorrect predictions is most succinctly imparted. Deep shades mean high number-in other words, they may show where acknowledging is or not failing to get an answer about the performance of the model, one meters over this chart encounters biases or misclassifications.

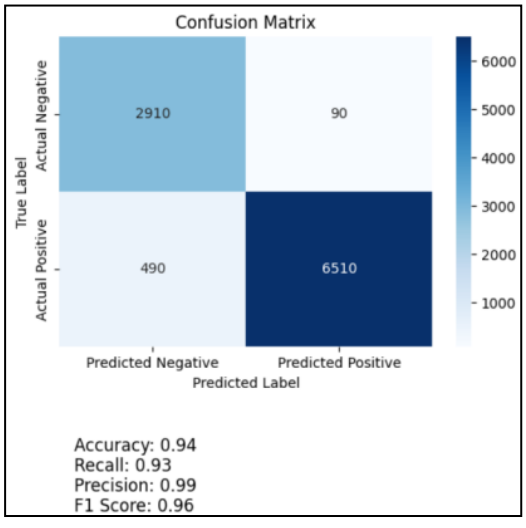

Figure 7. *Confusion Matrix based on Face Verification Algorithm.*

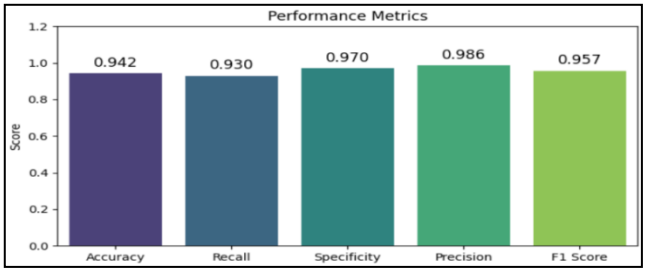

Figure 8. *Bar-chart Presentation of Performance Metrics.*

Through this visualization (Figure 8), we can look at what each class really is and how well it is predicted by the model. In addition, there will be easy comparison between true and predicted classes with this representation. Any tendency toward imbalance in our model's forecasting can be checked.

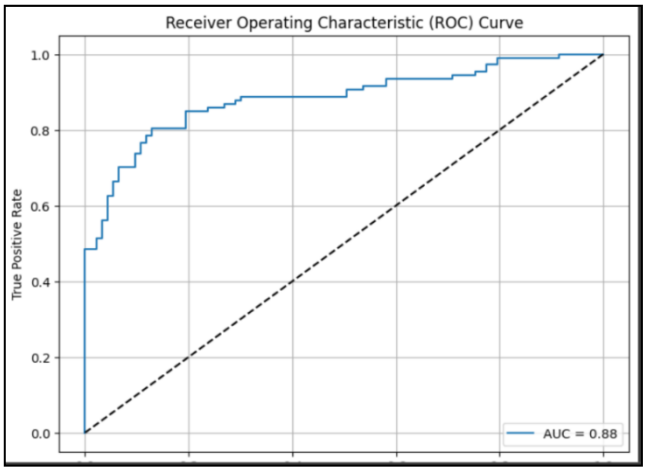

Figure 9. *Receiver Operating Characteristic (ROC) Curve.*

This analysis (Figure 9) is a window into the performance of the face verification model. It reveals how distinct is different classes (e.g., different individuals) for it. The ROC curves illustrate the trade-off between true positive and false positive rates, allowing researchers to judge model effectiveness over a range of thresholds.

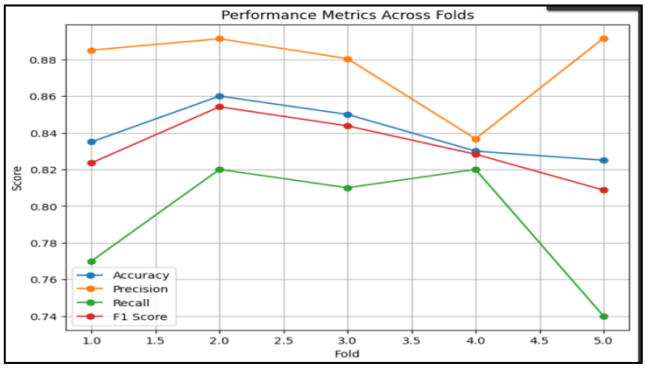

Figure 10. *Performance Metrics across folds.*

In figure 10, we can visualize the changes in performance over iterations or epochs by plotting the changes in performance metrics such as Accuracy, Precision, Recall and F1 Score during training.

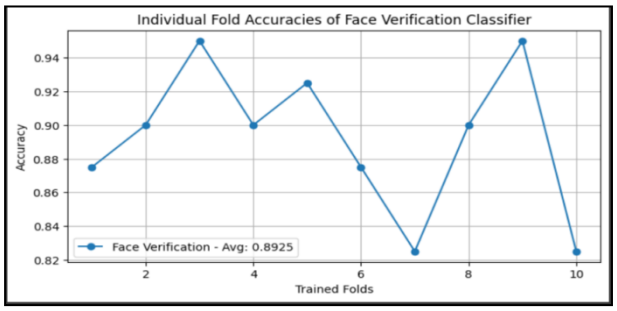

Figure 11. *Cross-Validation result visualization.*

In the plot (Figure 11), every dot represents the accuracy score obtained after every fold of cross-validation. Cross-validation is a technique that helps evaluate how well the algorithm generalizes to new data. It splits the dataset into multiple pieces (or folds), training on one part and then checking its performance against another. The red line marks mean accuracy over all folds; showing an overall measure of how well this algorithm performs averaged across various subsets of the data. Greater mean accuracy means mid-training is more general and robust for face verification. In sum, the results of cross-validation provide a comprehensive assessment of the facial recognition algorithm. The results help confirm its performance and reliability, which is vital for research papers on biometrics and facial recognition techniques.

5. Conclusion

The primary concern of the Online Voting System is to securely manage voter data. An administrator is responsible for a centralized database that has all of the essential details about voters. Users must first input their Aadhaar card number and then, on their linked mobile number, enter the OTP received. This ensures the integrity of the whole voting process because it is done by putting in both pieces yourself. As a result, voting results are processed and securely stored.

Online voting has seen a surge in popularity due to two factors: cost savings and increased operational efficiency. This innovative approach allows people to cast their ballots wherever they may be, due either to work or any other reason. The system has achieved its goal fully and has brought about good results. Indeed, two-factor authentication is expected to offer even greater promise for future improvement, as more people get used to its successful operation.

6. Future Scope

In the future, our research will focus on implementing foolproof security protocols, user-friendly interfaces and in-app chatbots to aid users. These improvements will serve to establish our voting system as a reliable method of choice, which doesn't make the people conform or have anything like which we select presidents, thereby helping equal participation in elections for all.

Moreover, by providing a trial voting scenario before the final certification of elections we can ensure problem-free voting. This would simplify the process and less than the present arrangement for voters.

Abbreviations

OTPs	One Time Passwords
JWT	JSON Web Tokens
OCR	Optical Character Recognition
CNNs	Convolutional Neural Networks
ROC	Receiver Operating Characteristic

Author Contributions

Dia Nandy: Conceptualization, Formal Analysis, Methodology, Resources, Writing - review & editing

Arghyadeep Maiti: Data curation, Funding acquisition, Software, Supervision, Writing - review & editing

Moloy Dhar: Conceptualization, Investigation, Methodology, Supervision

Barna Barman: Formal Analysis, Funding acquisition, Software, Validation, Writing - original draft

Anish Aich: Data curation, Investigation, Project administration, Resources, Visualization

Conflicts of Interest

The authors declare no conflicts of interest.

References

[1] N. Sreenivasa, Gopal Agarwal, Rishab Jain“Online Voting System by Using Three Step Verification” 2023International Conference on Advances in Electrical, Computing, Communications and Sustainable Technologies (ICAECT).

[2] “Online Voting System”, Ms. Kavya Ramesh Naidu, Mr. Ankush Dinesh Ingale, Ms. Pratiksha Sukhadeo Gaikwad, Mr. Hitesh Rajendra Thakare, Mr. Sujal Sunil Chavan, Prof. Yogeshk Sharma“Online Voting System” 2023International Research Journal of Modernization in Engineering Technology and Science (IRJMETS).

[3] Voram Bhavan, Laxmi Koli, Lanka Rishi, Marri Sankeerth Reddy, “Online Voting System” 2022International Journal for Research in Applied Science and Engineering Technology (IJRASET).

[4] Shubham Gupta, Divanshu Jain, Milind Thomas Themalil, “Electronic Voting Mechanism using Microcontroller ATmega328P with Face Recognition”, 2021 5th International Conference on Computing Methodologies and Communication (ICCMC).

[5] T. Kohno, A. Stubblefield, A.D. Rubin, D.S. Wallach "Analysis of an electronic voting system" IEEE Symposium on Security and Privacy, 2004. Proceedings. 2004.

[6] Z.A. Usmani. Kaif Patanwala, Mukesh Panigrahi, Ajay Nair "Multi-purpose Platform Independent Online Voting System" 2017 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS), IEEE.

[7] Shivendra Katiyar, Kullai Reddy Meka, Ferdous A. Barbhuiya, Sukumar Nandi “Online Voting System Powered by Biometric Security” 2011 Second International Conference on Emerging Applications of Information Technology.

[8] Uzma Jafar, Mohd Juzaiddin Ab Aziz, Zarina Shukur. Blockchain for Electronic Voting System—Review and Open Research Challenges.

[9] Dukka Bindu Venkata Raghav, Sunith Kumar Bandi. (2016). Digitalized Electronic Voting System. International Journal of Reconfigurable and Embedded Systems.

[10] Roopak T M, Dr. R Sumathi, “Electronic Voting based on Virtual ID of Aadhar using Blockchain Technology”, Proceedings of the Second International Conference on Innovative Mechanisms for Industry Applications (ICIMIA 2020), pp. 71-75, 2020.

[11] Shubham Gupta, Divanshu Jain, Milind Thomas Themalil, “Electronic Voting Mechanism using Microcontroller ATmega328P withFace Recognition”, Proceedings of the Fifth International Conference on Computing Methodologies and Communication (ICCMC2021), pp. 1471-147, 2021.

[12] Ms. Kavya Ramesh Naidu, Mr. Ankush Dinesh Ingale, Ms. Pratiksha SukhadeoGaikwad, Mr. Hitesh Rajendra Thakare, Mr. Sujal Sunil Chavan, Prof. Yogeshk Sharma, Department Of Computer Engineering Vishwakarma Instituite Of InformationTechnology, Pune, India.

[13] H. Agarwal and G. N. Pandey, "Online voting system for India based on ADHAAR ID," 2013 Eleventh International Conference on ICT and Knowledge Engineering.

[14] V. K. Priya, V. Vimaladevi, B. Pandimeenal and T. Dhivya, "Arduino based smart voting machine," 2017 International Conference on Trends in Electronics and Informatics (ICEI).

[15] S. S. Ramprasad, R. Swathi, K. N. Shireesha and V. S. Gavannawar, "Convenient Voting System," 2018 3rd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT).