Online Voting System Using Face Recognition And Otp (One- Time Password)

Prof.S.S.Shinde[1], Vaijanath Alebale[2], Shreeyash Sabale[3], Tejas Kshetre[4], Yash Rokade[5]
[1, 2, 3, 4, 5] Dept of Computer Engineering
[1, 2, 3, 4, 5] Savitribai Phule Pune University, Sinhgad Intsitute of Technology Lonavala, India

Abstract- *The main purpose of the system is to create an online voting portal. This portal addresses the drawbacks of manual voting and earlier online voting systems using facial recognition and OTP generation. People can vote from anywhere if they are unable to attend their designated voting booths, providing location flexibility. The system ensures security for voters and administrators with several authentication layers. These include facial recognition and OTP authentication using registered user details. A person can use the online system only after their ID is verified against the database of registered voters.*

Keywords: Image Processing, Python, Voting System, Face Recognition, MySQL, OTP

I. INTRODUCTION

As mentioned in The Times of India on January 24, 2009, 11 lakh fraudulent votes were found in Delhi [13]. Additionally, as reported by India News in June 2013, 30,000 voters were found to be unregistered in the Sheila Dikshit constituency [14]. Moreover, according to Ram Vilas Paswan, president of Lok Janshakti Party, about 30% of voter cards used in the Bihar elections were deceitful [15] These facts indicate that there were some issues with conducting an election within a traditional system. Elections can be either public or private, depending on the level of governance, such as local, state, or national elections. In traditional voting systems, people cast their votes by placing them in the ballot boxes located at designated polling stations. After the voting is completed, the ballot boxes are opened to conduct a manual count of the votes. It is a time-consuming and cumbersome process and requires great effort from humans to conduct properly. Thus, in order to address this problem, several electronic voting systems have been introduced [1], [3], [4]. This research work presents a proposal for an online voting system that utilizes facial recognition in conjunction with a one-time password (OTP) authentication system. The biometric system is highly accurate in verifying individuals, especially the face recognition system. OTP-based authentication offers an extra layer of protection [6]. For the system, the person who wants to vote provides their facial image along with an OTP, and the server authenticates it by verifying whether the credentials match those stored in the database. If everything goes well, they are given access to vote. In existing systems, individuals are required to present a voter's ID card, which makes the entire process lengthy.

II. PROBLEM STATEMENT

Despite considerable efforts towards digitization in the country, the current voting system suffers from several shortcomings. First and foremost, the current system requires a voter to be present at a designated polling booth. As voter registration is linked to a particular locality, voters are allowed to vote only at the polling station assigned to them, based on the information in their voter ID cards. This becomes an obstacle for people who have moved in the meantime and are therefore unable to vote [10]. Besides, events like the COVID-19 pandemic have made other problems inherent in the traditional voting system apparent. Namely, physical presence at a polling booth makes voting highly contagious and violates the principle of social distancing [11]. Besides, traditional voting incurs substantial costs and takes a long time due to its manual nature.

1)Electronic Voting Machine with Enhanced Security

The current study proposes an electronic voting machine based on the ATmega32 microcontroller, incorporating a three-level security protocol to enhance system reliability. Conventional paper-based voting methods are time-consuming and entail considerable manual labour. The current method focuses on providing fast, reliable, and efficient elections that can maintain voter anonymity without involving paper ballots [11]. While the Voter Verifiable Paper Audit Trail technology can be used alongside voting machines to ensure the integrity of the election process, its use increases costs. While electronic voting machines offer the advantages of fast result processing and efficiency, they are vulnerable to hardware attacks. To address this challenge, the proposed system includes three additional levels of security [9].

Pros:

- Provides fast vote counting.
- Saves money by reducing manual labour.

Cons: Some security risks cannot be ruled out.

Drawbacks: Compatibility limitations might exist.

2)Decentralized E-Voting Portal Using Blockchain

This document describes the use of blockchain technology for designing an electronic voting system. The suggested solution is most appropriate for use in small-scale election processes. Smart contract technology implemented on the Ethereum blockchain enables decentralized elections [1]. The solution primarily emphasizes the use of blockchain and cryptographic mechanisms, such as homomorphic encryption and secret sharing. Through such mechanisms, it becomes possible to create a more secure electronic voting process that does not necessarily require central authorities. However, there are various challenges associated with this solution, such as scalability issues [4].

Pros:

- Increases transparency in the voting process without violating voter anonymity.
- Provides data protection and privacy, as well as ballot verification.

Cons:

Systems that use blockchain and Internet technologies remain vulnerable to certain attacks.

Drawbacks:

Users require minimal knowledge to use the system.

3)Location-free Voting System with the help of IoT Technology

The proposed solution is an Internet of Things-based voting mechanism that uses mobile phones. The voting system allows users to vote online via mobile applications equipped with biometric sensors. In the initial stage of enrolment, the voter's fingerprints are collected and stored as a digital identifier for use during the verification stage of the voting process [7]. On voting day, the user opens the mobile application and submits their fingerprints through the interface. The application cross-checks the fingerprints against the identifier database to confirm the voter's identity. Access to the voting system is limited to the voting period only. After successful validation of the user's credentials, the voter will be able to submit their vote. Additionally, the voting system allows voters to access the voting platform from any location without being physically present at the polling station. However, the Internet of Things-based voting system might encounter issues related to IoT security risks, dependence on network connectivity, and biometric accuracy [8].

Pros:

- One advantage of this system is that it enables remote voting, allowing users to cast votes from any location using mobile devices.
- It also improves accessibility, especially for people who are unable to visit polling stations.

Cons:

- Highly dependent on stable internet connectivity, which may not be available in rural or remote areas.
- Requires biometric-enabled devices, limiting usability for users without compatible smartphones

Drawbacks:

- IoT security vulnerabilities can expose the system to attacks such as spoofing or data interception.
- Biometric accuracy issues (e.g., fingerprint mismatch due to poor sensor quality or environmental factors)

III. PROPOSED SYSTEM

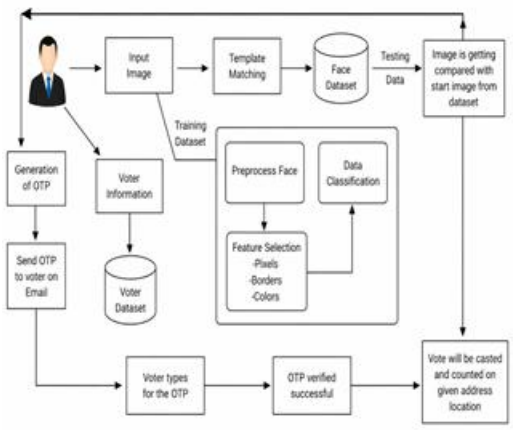

Fig 1: System Architecture

Description

The suggested system will be an online voting system that uses face recognition and OTPs. User registration is the first step towards voting, and here the user needs to provide the required information, including Aadhaar number, phone number, city, age, and password. The entered information is saved in the voter database, while the user's face is captured with a webcam and stored in a face dataset [8]. Voting requires users to log in to the system using Aadhaar and a password. Once the user is authenticated, they need to answer the security question. Then, the user is directed to the voting

page, where they are shown a list of candidates running for various positions. Once the candidate of the user's choice is selected, voting is done by pressing the vote button, which prompts facial recognition. Here, the captured image is checked against the face dataset to authenticate the user. Once recognition is successful, an OTP will be sent to the user's email, and voting is completed upon successful OTP verification [6]. Ultimately, the framework provides an option for the administrator to present the outcome of the voting process. In essence, this strategy guarantees security, efficiency, accessibility, and voter authentication, thus eliminating any form of cheating [3].

Modules

Voter (User):

Voters are one of the key entities in the voting system, selecting the candidates for them. For voters, the individual should be an authorized user whose identity is verified by the system admin during registration. Only those users who are found valid and have their data stored in the database will be allowed to vote.

Machine Learning:

The machine learning process in the system is highly essential since it helps in the process of facial recognition. In the registration phase, images of the faces of the voter are obtained, and then a model is created from the dataset that can recognise any user. In the voting phase, the pre-trained machine learning algorithm will identify whether the person is genuine.

Facial & OTP Verification:

In order to secure the voting process, there are two layers of authentication that take place. First is the facial recognition layer, in which the user is authenticated by comparing their live image with the image present in the stored dataset. Once it is verified, another layer of authentication is initiated by sending an OTP to the email address registered by the user

Algorithm used:

Haar Classifier Algorithm:

Haar-like features make up the basic elements that make up the Haar classifier used in object detection. Different from typical approaches where detection is based on pixel-by-pixel evaluation, the method entails looking for contrast between two adjacent rectangles within an image. It analyses contrasts between light and dark parts of an image by considering the variations in pixel values of two adjacent regions [8]. Usually, Haar-like features involve more than one region that has contrasting intensity relations. Among the most important strengths of such features are their ability to change sizes based on the size of the image. This allows detection of objects across various sizes. Relevant features are extracted using sub-image tests, which facilitate the development of an efficient cascade classifier. Detection rate, false-positive rate, and the number of cascade stages are some of the parameters that can be used to enhance the classifier. performance. This has been demonstrated by the Viola-Jones method that used Haar features to detect faces with very high accuracy, reaching up to 95% in some cases. For the classifier training process, the algorithm of Adaptive Boosting or AdaBoost is used for selecting important features and enhancing the classifier's accuracy. In general, the Haar classifier can be implemented by means of the software library called OpenCV.

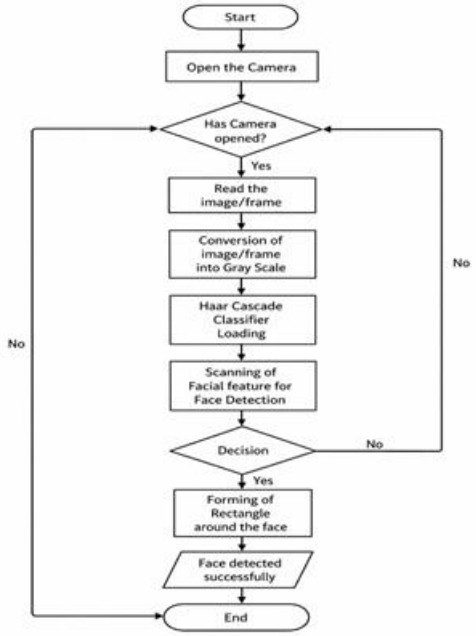

Fig 2: Haar Classifier Flowchart

IV. FUTURE WORK

Potential areas for future research could involve developing the precision, reliability, and scalability of the suggested online election management framework. More advanced face recognition technologies such as Convolutional Neural Networks (CNNs) and biometric identification techniques based on deep learning can be investigated to improve the recognition accuracy regardless of environmental factors, such as changes in light intensity, facial expressions, and occlusions [8].The suggested online election management

system can be optimized by incorporating a live face detection system to prevent possible attacks by spoofing faces using pictures or video footage. Moreover, implementing multiple means of authentication in conjunction with facial recognition, such as fingerprint scanning, OTP verification, and smart ID cards, can increase the security of the proposed system [6]. Future applications of the proposed online election management system may also include its deployment in cloud-based architectures to facilitate wide-scale elections. Finally, using blockchain technology to record the voting information can ensure tamper-proofing, enhanced transparency, and increased voter confidence [1].

V. CONCLUSIONS

The suggested model uses machine learning techniques, as well as face detection, to create a highly secure and reliable voting system. This system allows voters to register and place their votes from anywhere, without being restricted by geographical constraints. This system guarantees that only one vote is counted for each voter, hence preventing any possibility of fraud. Furthermore, the suggested system makes voting easy since it can be done from anywhere without compromising data accuracy. It eliminates unnecessary human involvement, hence saving time and reducing costs.

VI. ACKNOWLEDGEMENT

We wish to express our gratitude to all who have helped us directly or indirectly in making this paper. We are especially thankful to our Guide, Prof. S. S. Shinde, for his valuable guidance on time to time. We are also grateful to the computer department HOD, Dr Shubhangi Patil, for their consistent support and guidance.

REFERENCES

[1] K. M. Khan, J. Arshad, and M. M. Khan, "Investigating performance constraints for blockchain-based secure e-voting system," *Future Generation Computer Systems*, vol. 105, pp. 13–26, 2020.

[2] Z. A. Usmani, Kaif Patanwala, Mukesh Panigrahi, Ajay Nair, "Multipurpose platform-independent online voting system."

[3] M. Kumar, S. Chand, and C. P. Katti, "A secure end-to-end verifiable internet-voting system using identity-based blind signature," *IEEE Systems Journal*, vol. 14, no. 2, pp. 2032–2041, 2020.

[4] X. Yang, X. Yi, S. Nepal, A. Kelarev, and F. Han, "A secure verifiable ranked choice online voting system based on homomorphic encryption," *IEEE Access*, 2018.

[5] P. B. R. and A. R. Pais, "Design and implementation of a secure internet-based voting system with user anonymity using an identity-based encryption system," in *Proc. IEEE Int. Conf. Services Computing*, 2009, pp. 474–481.

[6] H. Parmar, N. Nainan, and S. Thaseen, "Generation of secure one-time password based on image authentication," *CS & IT-CSCP*, pp. 195–206, 2012.

[7] R. K. Chaudhary and S. Agarwal, "Online voting system using biometric authentication," *International Journal of Computer Applications*, vol. 179, no. 7, pp. 20–25, 2018.

[8] A. K. Jain, A. Ross, and S. Prabhakar, "An introduction to biometric recognition," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 14, no. 1, pp. 4–20, 2004.

[9] D. Chaum, "Secret-ballot receipts: True voter-verifiable elections," *IEEE Security & Privacy*, vol. 2, no. 1, pp. 38–47, 2004.

[10] R. M. Alvarez and T. E. Hall, *Electronic elections: The perils and promises of digital democracy*. Princeton University Press, 2008.

[11] S. Wolchok, E. Wustrow, J. A. Halderman, "Security analysis of India's electronic voting machines," in *ACM CCS*, 2010.

[12] A. Juels, D. Catalano, and M. Jakobsson, "Coercion-resistant electronic elections," in *Proc. ACM Workshop on Privacy in Electronic Society*, 2005, pp. 61–70.

[13] The Times of India, "Report on fraudulent votes in Delhi," Jan. 24, 2009.

[14] India News, "Unregistered voters in electoral rolls," June 2013.

[15] R. V. Paswan, "Statement on voter fraud in Bihar elections," 2013.