

Smart Voting System Using Machine Learning

**Mrs.Sk. Rizwana¹, Kadiri Sujana Narayana², Deyyala Geethaprakash³,
Kadali Jeevan Prakash⁴, Kundeti Sujatha⁵, Koppula Prasanna Lakshmi⁶**

¹Associate Professor, CSE Department, VSM College Of Engineering, Ramachandrapuram,
Dr.B.R.Ambhedkar Konaseema Dt, Andhra Pradesh - 533255

^{2,3,4,5,6}Student, CSE Department, VSM College Of Engineering, Ramachandrapuram, Dr.B.R.Ambhedkar
Konaseema Dt, Andhra Pradesh - 533255

ABSTRACT

The election voting process has encountered many difficulties in recent years, especially with regard to voter participation, data security, and voter authentication. Voter turnout has significantly declined as a result of growing urban migration and the inability of many citizens to return to their hometowns on election day. Furthermore, there is a need for a more effective and secure voting method because the conventional paper-based one is prone to fraud and errors. There has never been a more pressing need for a creative, intelligent voting system. By developing an online voting system that guarantees safe and accurate voting for all eligible citizens, regardless of location, this project seeks to address these issues. We use a variety of cutting-edge technologies to create this system, such as machine learning, deep learning algorithms for image processing and authentication, and Python for backend development. The dilb HOG+SVM for effective face detection, Flask for developing the web application interface, and OpenCV for face detection and recognition are some of the key technologies used in this project

Keywords: Smart voting, Voter participation, OpenCV, Dlib HOG+SVM Algorithm, Face recognition, Aadhaar card verification, Machine Learning-Random Forest.

INTRODUCTION

During elections, the voting system is crucial in democracies like India. India's election commission has historically used electronic voting machines, which are less reliable, require more labor, and take longer. Elections, as we all know, are a fundamental democratic process that give people the chance to express their views by choosing a candidate. India is investing a significant amount of money to upgrade our entire voting system in order to give its citizens better governance. For India to have a better democracy, the voting process must be transparent, honest, and completely safe. Because there is a possibility of cheating during the voting process, the current system is less transparent.

The primary issues with voting in the current election are voter authentication, voting process intelligence, and voting data protection. This is due to the fact that an intelligent election voting system must be created. The growing demand for electronic services and their security is brought about by computer technology users' near-complete electronic access to modern communications and the Internet. Elections are naturally improved when new technology is used in the voting process. Following industrialization, a growing number of people relocate to cities in search of employment. However, a large

number of them still have their voter IDs at their home addresses. They are unable to go to their locations on election day, so they do not cast their important ballots.

EXISTING SYSTEM

By calculating the weighted trust of each device, this system isolates the malicious devices and removes the threats that were present during the communication and path formation process. Additionally, a blockchain that incorporates IoT devices is maintained to further develop a secure polling process in order to guarantee transparency in the polling mechanism. Votes are recorded and gathered using IoT devices. Limitations 1) Voting is done through IoT-based hardware 2) IoT devices can be malicious or legitimate 3) malicious devices cannot be added to the blockchain.

PROBLEM STATEMENT

Voter authentication problems, dwindling voter turnout, and an increase in electoral fraud are just a few of the growing problems facing the democratic voting process in recent years. Conventional paper-based voting methods are especially susceptible to manipulation, human error, and inaccuracies. Low participation rates are also a result of many eligible voters being unable to return to their home districts on election day due to urban migration and logistical issues. A safe, scalable, and easily accessible online voting system that guarantees voter identity, preserves vote integrity, and boosts participation is desperately needed. The proposed Smart Voting System seeks to address these issues by developing a web-based platform that makes use of machine learning-based fraud detection, facial recognition and secure data store management to allow safe and effective online voting for all eligible citizens, wherever they may be.

PROPOSED SYSTEM

In order to protect voter integrity and stop fraud, the suggested system is a smart and safe web-based smart voting system that uses biometric authentication in place of conventional voting procedures. HTML, CSS, JavaScript, and Bootstrap are used to create the frontend interface, while Flask is used for the backend. The dlib library is used to implement facial recognition, which uses a Support Vector Machine (SVM) in conjunction with a Histogram of Oriented Gradients (HOG) to detect faces accurately. Key facial features are analyzed using a 68-point facial landmark model. The Eye Aspect Ratio (EAR) is used in conjunction with a blink-based liveness detection technique to verify liveness and stop spoofing attempts using static images or videos. The system strictly enforces a one-person-one-vote policy and uses bcrypt password hashing to securely store user credentials. An extra degree of fraud detection is added by using a pre-trained Random Forest model to spot questionable voting patterns. At the moment, the system stores data in CSV files and allows for the transparent display of vote results in real time. This strategy guarantees a secure, scalable, and dependable solution that can be applied successfully in organizations, institutions, or academic elections.

IMPLEMENTED ALGORITHMS

To guarantee safe and impenetrable voting, the Smart Voting System incorporates a number of clever algorithms. The dlib library, which uses a Support Vector Machine (SVM) classifier in conjunction with the Histogram of Oriented Gradients (HOG) to accurately detect human faces, is used for face detection and facial feature extraction. Important facial features like the mouth and eyes are

located using a pre-trained 68-point facial landmark predictor. The system uses a blink detection algorithm based on the Eye Aspect Ratio (EAR) for liveness detection. This algorithm determines the ratio of distances between particular eye landmarks to identify natural eye blinks, thereby preventing spoofing through photos or videos. A pre-trained Random Forest classification model is also employed to detect fraudulent activity by spotting odd voting attempts or patterns. Bcrypt hashing is used to encrypt passwords in order to protect user authentication. These algorithms combine to create a dependable and impenetrable electronic voting system through a web-based framework driven by Flask.

WORKING OF MACHINE LEARNING ALGORITHMS

Machine learning algorithms form the basis of the Smart Voting System, enabling features like face authentication, fraud detection, and secure data handling. The way these algorithms function in the system is briefly explained below. Based on user activity patterns, a Random Forest Classifier is used in this system to identify fraudulent voting behavior. The artificially created data used to train the model mimics real-world voting characteristics, including the time of the vote, the length of the voting session, and the quantity of prior shady or fraudulent attempts. These characteristics were chosen in order to identify any irregularities that might point to fraud. Being an ensemble of decision trees, the Random Forest algorithm provides high accuracy with little chance of overfitting and works well with both continuous and categorical variables. After training, Joblib is used to save the model, which is then loaded during the voting process to assess user behavior in real time. After a vote is cast, the system gathers pertinent information and applies the model to determine whether the attempt is legitimate or fraudulent. By adding an intelligent layer of security, this machine learning integration improves the system's capacity to uphold the integrity and equity of the voting process.

RESULT ANALYSIS

Smart Voting System Output



Fig:1



Fig:2



Fig:3



Fig:4



Fig:5



Fig:6



Fig:7



Fig:8



Fig:9



Fig:10

CONCLUSION

The bulk of India's cities are largely the result of smart voting. For most of us, it should be regarded as

the primary concern. The current voting procedures require a lot of human labor and manpower to complete by hand, and if voting is to be done online, a secure voting system is required in order to cast a ballot. the method of machine learning. are employed to identify a person's face and verify if a voter is authorized.

REFERENCES

1. “A Secure Verifiable Ranked Choice Online Voting System Based on Homomorphic” Encryption, Author - Xuechao Yang; Xun Yi; Surya Nepal; Andrei Kelarev; Fengling Han, IEEE Access, March 2018
2. “Electronic Voting Using Blockchain And Smart Contracts:” Proof Of Concept, Author - Fáber D. Giraldo; Barbosa Milton C.; Carlos E. Gamboa, IEEE Latin America Transactions 10, October 2020
3. “A Secure End-to-End Verifiable Internet-Voting System Using Identity-Based Blind Signature” Author - Mahender Kumar; Satish Chand; C. P. Katti, IEEE Systems Journal, June 2020
4. “A Smart Contract System for Decentralized Borda Count Voting” Author - Somnath Panja; Samiran Bag; Feng Hao; Bimal Roy, IEEE Transactions on Engineering Management, Nov. 2020.
5. “A Comparative Analysis on E-Voting System Using Blockchain” Authors: Kanika Garg; Pavi Saraswat; Sachin Bisht; Sahil Kr. Aggarwal; Sai Krishna Kothuri; Sahil Gupta, 2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT SIU).
6. “SecEVS : Secure Electronic Voting System Using Blockchain Technology” Authors: Ashish Singh; Kakali Chatterjee, 2018 International Conference on Computing, Power and Communication Technologies (GUCCO)