

E-Voting System with Face Recognition and Aadhar

**Mr. Abhinav Tiwari, Mr. Abhishek Mahajan, Mr. Pushkar Piyush,
Mrs. Lata Lende, Prof. A. S. Shinde**

Department of Information Technology
Sinhgad College of Engineering, Pune, Maharashtra, India

Abstract: *The main goal of this system is to develop an online voting system that will aid in suppressing both the manual voting system's hardware and earlier iterations of online voting that used cameras for Face Recognition and OTP creation. For voters who are unable to travel to the voting location (their hometown), we are also introducing a location-free voting mechanism. Here, we provide a method with many layers of verification, including face and OTP verification with validation data, to guarantee the device's dependability. Each voter can only access the system after being identified and verified against the provided database of registered voters. Once the relevant face has been matched with the data, The voter will be given the opportunity to select the panellist they want*

Keywords: OpenCV, Smart Voting System, Facial Recognition, OTP, VoterID, Winning party, Python.

I. INTRODUCTION

According to TOI records, 11 lakhs of fraudulent votes were discovered in Delhi on January 24, 2009. Then, in June 2013, India News reported that the Sheila Dikshit constituency's election commission discovered 30000 illegal voters.

The use of electronic voting equipment aims to speed up ballot counting, lower the expense of paying people to manually tally ballots, and increase accessibility for voters with disabilities. In the long run, expenses should also go down. Results can be published and communicated more quickly.

The straightforward idea is to combine the name of the game key with the duvet picture on the assumption of the centre photo in the Secure Online Voting System with Multi Security the utilisation of Biometric and Steganography. This method ultimately results in a stego image that closely resembles the duvet image.

For the purpose of performing the voter authentication function, the Stego image is extracted on the server side. 288 bit long mystery message was utilised. Since the actual mystery key is not contained within the stego image, there is no possibility of guessing the mystery key from it.

II. METHODOLOGY

What therefore should the best strategy be to address this problem statement, in our opinion? Well, we reasoned that creating an online system would be better for resolving the majority of the issues we had. We wanted to create a system that is simple to use and can be translated into Hindi and English depending on whatever language the user is most familiar with.

The concept of an electronic voting system with Aadhar authentication provided the solution. Voters will be able to use this program to cast their ballots from any location with an internet connection.

In particular, it has a tremendous chance to lower administrative expenses associated with printing ballots or opening polling places and also boost voter turnout. The concept of block chain can be used to address a number of concerns with electronic voting, making it more secure and cost-effective than previous networks. The primary goal of our approach is to address each of the aforementioned issues, with the presence of less data on websites coming in first

place. By obtaining the user's or voter's information regarding his or her documents, we will be able to solve this issue.

Id, an Aadhar card, face recognition, and cell number verification are all required. The project will provide a one-stop shop for voters who are absent from their home country or whose vote has been cast improperly during an election so that they can cast their ballots legitimately. The project's database will be examined every predetermined amount of time and updated every predetermined amount of time to maintain all the details current.

In today's mobile and technologically sophisticated culture, online voting enables citizens to take part in the democratic process online. The POLYAS online voting system provides the highest levels of election process efficiency, security, and control. Online voting gives voters a convenient and secure way to cast their ballots while also saving election organizers money as they prepare for the next election. Organizers know that arranging a postal or ballot box election will be expensive since they have to identify a suitable location, notify eligible voters, produce postal voting forms, and coordinate the vote count. Give your election planning the most flexibility and effectiveness possible and make it simple to create ballots online.

Email makes it simple to distribute invitations and reminders for elections. Real-time tracking of voter turnout and easy voter interaction. The process of organizing elections is made a great deal simpler by simple ballot construction, customizable election invitations, and automatic vote counting. The POLYAS online voting system makes it simple to sketch out complicated voting processes.

Election fraud was not uncommon in American elections past, and it is also not likely to occur in elections to come. However, electronic voting machines offer more potential for fraud than any previously accessible ones. For instance, malicious code might be concealed in the programs by a crooked insider working for one of the suppliers of commonly used voting equipment. The election results in any state where those machines are utilized may then be tampered with if that vendor unintentionally distributed that malicious malware to thousands of computers across the country. The voluntary testing and certification processes that are now in place for DREs are insufficient to ensure that this kind of tampering will be found. The majority of election officials are not computer security professionals and are unaware of the security flaws with DRE.

The use of electronic voting equipment aims to speed up ballot counting, lower the expense of paying people to manually tally ballots, and increase accessibility for voters with disabilities. In the long run, expenses should also go down. Results can be published and communicated more quickly. By being able to vote independently from their location, voters can save time and money. The overall voting turnout could rise as a result. The voter groups who stand to gain the most from electronic elections include those who reside abroad, those who reside in remote rural areas, and the disabled who have mobility issues.

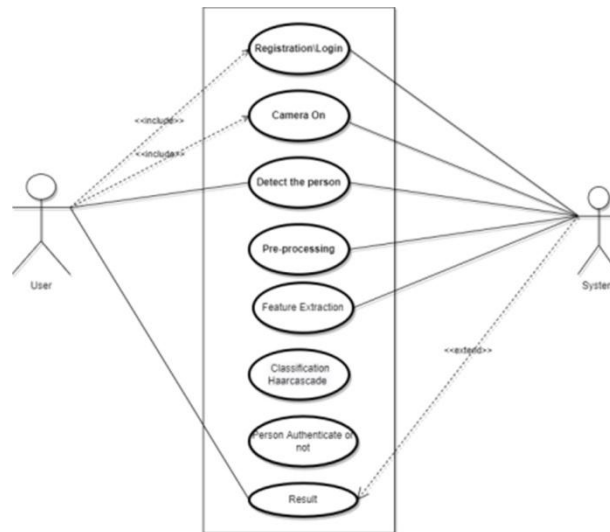
To resolve this issue we have used a algorithm which is-

An object detection algorithm called Haar Cascade is used to find faces in still photos or live videos. The edge or line detection features Viola and Jones suggested in their 2001 study "Rapid Object Detection using a Boosted Cascade of Simple Features" are used by the technique.

Government documents are delicate and easily tampered with if care is not taken, thus adopting a high security strategy and keeping the documents on a secure server will ensure that nothing of the sort occurs.

The problem of secure voting can be solve easily with two factor authentication, which combines the process of facial recognition and otp authentication using the aadhar id of the user, and utilizing the connection between phone number of the user connected with the addhar and voter id.

All the basic features of voting can be easily handled by the windows based application created. It not only allows the voter to vote but also the candidates to register on the platform easily which simplifies the voting process and makes the process transparent and fault proof. The result of the election takes a toll on the working force of the election department. This application eases the process and shows the result using the database. Where the voting results are stored securely. This not only makes the process simple but also maintains security and saves time which can be invested on various tasks to make the voting process more smooth.



The above figure shows the use-case diagram of the e-voting system created.

III. BACKGROUND AND LITERATURE REVIEW

SMART VOTING THROUGH FACE RECOGNITION

(1 Mahalakshmi Mabla Naik, 2 Dr. Preethi N. Patil)[1]

Face recognition is a type of biometric security that synchronizes the features of the face. By using the face recognition technique, it helps with voter verification. The Haar Cascade algorithm, which in this suggested system uses Haar-Like characteristics to coordinate the face, is used for face identification. An object detection algorithm is called Haar Cascade. There are three degrees of confirmation in the suggested system. The first one confirms the user id, and the second one asks for the voter card number. The voter moves on to the next level of checks in the case that they successfully completed the first two levels of confirmation. Utilising face recognition is part of the third degree of verification. This is the essential level of security to verify the voter's eligibility.

ONLINE VOTING SYSTEM USING FACE RECOGNITION AND OTP(ONE TIME PASSWORD)

(1 Ishwari Pawar, Shruti Ragade, 2 Akshada Zaware)[2]

The main goal of this system is to develop an online voting platform that will aid in reducing fraud in manual voting systems and earlier iterations of online voting that used cameras for Face Recognition and OTP generation. For voters who are unable to travel to the voting location (their hometown), we are also introducing a location-free voting mechanism. Here, we provide a system with many layers of verification, including face verification and OTP verification with validation data, to guarantee the device's dependability.

Each voter can only access the system after being identified and verified against the provided database of registered voters. The voter will be able to move forward with selecting their chosen candidate from the panel once the corresponding face is matched with the information provided.

SMART VOTING THROUGH FACE RECOGNITION

(1 Nandan Gowda, 2. Jayam Haresh Tharun,)[3]

Any democracy that is ruled by the people expressing their choices or articulate ideas by voting must have elections as one of its core distinguishing features. The voting process has advanced significantly since the days of straightforward handwritten ballots to include internet voting technologies. This project intends to create a face recognition-based smart voting system that will enable any voter in India to travel to the closest voting location from "ANYWHERE IN INDIA" and cast their ballot. High level biometric security is maintained with this project. The server database contains the voter information. The participant should stand in front of the computer before voting so that the camera can interpret their image.

After reading the information, the microcontroller transfers it over the serial port to the web application. The person database is maintained by the web application software. In the "smart voting system," after someone casts their ballot, the website displays a message confirming that their vote was successfully registered. However, if that person is under 18 years old and tries to cast their ballot again using a face sample, the website will indicate that they are ineligible to vote. After voting is complete, the election commission can log in and review the results. It can also reset the votes and update the candidate results annually.

SMART VOTING SYSTEM USING FACIAL DETECTION

(1.Chandra Keerthi Pothina, 2 Atla Indu Reddy)[4]

The current system requires the physical presence of every voter, which is inconvenient for many people. India is a democracy, that too the largest in the world, but it still conducts its elections using either Secret Ballot Voting or Electronic Voting Machines (EVM), both of which involve high costs, manual labour, and are inefficient. In contrast to the old approach, which requires voters to be physically present, the system discussed in this paper uses faces to unlock the voting system, exactly like it does on your phone. The procedure takes a lot of time. Voters can cast their ballots from any location in the world thanks to the system's solely online nature. The use of face detection technology reduces the possibility of duplicate votes being cast, and individuals who registered prior to the election and are recognised by the system will be permitted to cast a ballot. Every face contains distinctive characteristics, similar to fingerprints, such as the space between the eyebrows and the eyes, which doesn't change as people age, making the system more safe. Therefore, the strategy makes the system the most effective.

SMART DECENTRALISED ONLINE VOTING USING BLOCKCHAIN AND SECRET CONTRACTS

(1.Aaron Fernandes, 2.Karan Garg)[5]

A lot depends on the complicated procedure of voting. It is difficult to create an electronic voting system that can simultaneously guarantee anonymity, verifiability, and openness. To accomplish these properties, ongoing improvements to the voting system are being developed. Blockchain has recently entered the technology scene with a lot of promises, namely the creation of verifiable and transparent decentralised systems. To establish user anonymity while assuring that only authorised voters should be allowed to vote, and that they should only be able to vote once, is a significant difficulty encountered by blockchain-based electronic voting systems. This study suggests a blockchain-based electronic voting system using concealed contracts to overcome these problems.

We have created secret contracts using Enigma, a tool for secure multiparty computation. Most of the features needed to conduct free and fair voting electronically are covered by the proposed system.

APPLICATION FOR ONLINE VOTING SYSTEM USING ANDROID DEVICE

(1. Himanshu Vinod Purandare)[6]

Voting is a critical component of democracies. Elections determine a candidate's suitability and the destiny of a nation; as a result, they should be as transparent as is practical and be held in an environment with a high level of security. However, there are several drawbacks to the current voting method, including a lengthy process that requires voters to wait in lines and a lack of security. As a result, voters' propensity to vote and their participation rate both decline. We are developing an online voting system utilising an Android application to address these problems and enhance the current voting system. This system will increase system security, make voting less time-consuming, and produce better outcomes. Using an android device and the voting app on it, a voter can cast a ballot remotely from anywhere in the nation. Voters cannot cast ballots from a remote location without an internet connection on their Android device. The Android application will work with practically all Android devices, allowing every voter to take use of the online voting system. Due to the two-stage authentication method, which includes facial recognition and one-time passwords (OTP), it offers a better level of security. The database will be used to store voter information such as his voter ID and facial photographs. The server does the verification process itself.

An Android application will retrieve the voter's facial image, which will then be sent to a server for additional verification. The voter will then receive a One Time Password on his registered cell phone for additional vote-casting verification. After a successful face recognition and One Time Password authentication, the voter is able to cast their

ballot. To improve system performance, election results will be shown on each voter's device in the form of notifications, and voters will receive updates regarding the election.

MOBILE BASED FACIAL RECOGNITION USING OTP VERIFICATION

(1. Ms. Ashwini Ashok Mandavkar)[7]

As is well known, the voting process is becoming increasingly difficult in metropolitan areas nowadays due solely to voter identity. The only kind of identity they have is the voting card. So there are many opportunities for voting fraud. To prevent this, we are creating a project that will use facial recognition software on an Android mobile device to store the identification of the voters. Voters' faces will be captured by this technology, and it will compare them to the current faces in the database. The OTP (One-Time Password) is produced and sent to the voters' registered mobile number after the validity of the facial detection is confirmed. Once the voter has been verified, he may cast his ballot.

SMART VOTING WEB BASED APPLICATION USING FACE RECOGNITION

(1. B. Singh, Sh. Ranjan, D. Aggarwal)[8]

India now offers two options for casting a ballot. Although they use electronic voting machines and secret ballots, these two methods have some drawbacks. Additionally, the current system is unsafe. Simply because they must travel to the voting place and stand in queue for several hours, many people lose the chance to vote

SR NO	Paper Name	Author Name	Abstract
1	RSA Implementation for Data Transmission Security in BEM Chairman E-Voting Android Based Application		In terms of leadership, voting is a procedure that should be done. If traditional voting methods are still used, they are less efficient in terms of cost, governance, and labour time. Fraud in the computation procedure and calculation mistakes are also possibilities. The election of the BEM chairman is still being conducted by STMIK Atma Luhur utilising the traditional voting process. We can create an electronic voting system based on Android to address the issues with traditional voting thanks to the advancements in modern technology. E-voting security is now a basic issue that has to be taken into account. The use of RSA cryptographic techniques may be a way to guarantee security. A way to guarantee security can be through phishing techniques. The reason RSA selects it is due to the benefit of its level of difficulty in factoring numbers into prime numbers. Factoring the numbers will make it more challenging to crack the encryption. Another benefit is that the asymmetric algorithm has stronger security. Additionally, this technique is robust to numerous attacks, including brute force. Keywords: - E-Voting; RSA Algorithm; Cryptography; Mobile; Android.
2	Design of a Public Key Infrastructure-based Single Ballot E-Voting System	Irham Mulkan Rodiana; Budi Rahardjo; Aciek Ida W.	Rapid growth in e-voting has made it a contender to displace the paper-based traditional voting method. Because it is simple to disseminate the necessary tools and gather the necessary data, this e-voting approach is more appealing. However, anonymity and verifiability are two crucial elements that must be taken into account when voting. In the suggested system, both



			<p>components will be improved and merged. The voter may always verify the outcome of his or her decision at each level of the electronic voting process without being immediately observed in his or her identity. This article suggests an architecture for such a system based on the hash function and public key infrastructure. Additionally, key management for the electronic voting system will be presented in this article. This system's architecture is taken into account for e-voting applications carried out in a scattered nation like Indonesia.</p> <p>Keywords: - Anonymity, E- voting, Key Management Scheme, Public Key Infrastructure, Verifiability.</p>
3.	On the Design and Implementation of a Blockchain Enabled E-Voting Application Within IoT-Oriented Smart Cities	Geetanjali Rathee; Razi Iqbal; Omer Waqar; Ali Kashif Bashir	<p>A smart city is an intelligent environment created by the coordinated and intelligent deployment of all available resources and cutting-edge technology. When 5G technology and intelligent sensors (Internet of Things (IoT) devices) operate together, consumers' needs are met more efficiently and with greater ease. E-voting, among other IoT use cases, is a significant application that advances IoT to the next stage in the development of smart city technology. In traditional applications, it's common to presumptively trust and cooperate with every single device. In actuality, though, devices could be interfered with by hostile attackers who want to degrade network services. As a result, there is a serious issue with the privacy and security problems in e-voting systems in particular, which allows for the possibility of numerous frauds to be committed by intruders to rig the election. Consequently, the potential difficulty is to separate the trustworthy IoT devices from the dishonest ones by computing their trust values using social optimization in order to create a trustworthy communication environment. Keywords: - Blockchain, trust-based e-voting, blockchain e- voting, smart cities.</p>
4.	E-Voting System In Smart Phone Using Mobile Application	G.Kalaiyarasi; K. Balaji; T. Narmadha; V. Naveen	<p>A new application that would greatly simplify and improve the voting process has grown as a result of advancements in web technology. The E-voting facilitates easy vote capturing and counting during elections. This project describes how to use the Android platform for electronic voting. The planned e-voting system enables users to cast ballots online without going to the polls. In order to prevent voter fraud using the OTP, the programme offers authentication methods. Results of the vote will be made accessible in a matter of seconds once it is complete. To prevent any leaks or disclosure of results</p>

			by anybody other than the administrator, the whole cast vote count is encrypted using the AES256 technique and kept in the database. Keywords:- Aes256, OTP, Biometric
5.	Smart voting through facial recognition	Mahalakshmi Mabla Naik, Dr. Preethi N. Patil	Face recognition is a class of biometric security which works by coordinating the facial features. It assists with making sure about the voter, by utilizing the face recognition strategy. In this proposed system, Haar Cascade algorithm is utilized for face recognition which utilizes Haar- Like features to coordinate the face. Haar Cascade is an object detection algorithm. In this proposed system there are three degrees of confirmations. The first is user id confirmation and second is for the voter card number. In the event if the voter passed the two degrees of confirmation, at that point he/she enters to next degree of checks. The third degree of confirmation incorporates the utilization of face recognition. This is the fundamental security level to confirm the voter is legitimate or not

IV. CONCLUSION

The strategy we suggest combines facial identification with machine learning to enable voters to register and cast ballots from any location, regardless of where they are. This technique offers security and prevents one person from casting multiple votes. This approach, in which we can cast our votes from many locations, is more dependable. Additionally, it reduces work, human needs, and time resources. The great majority of problems with the current electoral system divert attention away from the politics of a country. A transparent voting process is necessary in a democracy to guarantee free and fair elections. The proposed solution overcomes the bulk of the shortcomings of the current system by providing voter privacy, security, and transparency, as well as the capability for users to authenticate their votes. The technique also enables users to vote from nearby areas, increasing the voting percentage. The proposed solution is more cost-effective when compared to traditional electronic voting devices. Our proposed method may be further enhanced so that voter impersonation and election fraud are reduced to a minimum by replacing OTP verification with facial recognition or fingerprint verification in real-time deployment.

REFERENCES

- [1]. Adrià Rodríguez-Pérez, Secret Suffrage in Remote Electronic Voting Systems, Fourth International Conference on eDemocracy & eGovernment (ICEDEG), pp.277 - 278, 2017.
- [2]. Robert Stein ; Gregor Wenda, The Council of Europe and e-voting: history and impact of Rec(2004)11, pp.1-6, 2014.
- [3]. Jens-Matthias Bohli ; Christian Henrich ; Carmen Kempka ; Jörn Muller-Quade ; Stefan Rohrich, Enhancing Electronic Voting Machines on the Example of Bingo Voting, IEEE Transactions on Information Forensics and Security, pp. 745 - 750, 2009
- [4]. Dr. Magdi Amer and Dr. Hazem El-Gendy, "Towards a Fraud Prevention E-Voting System " International Journal of Advanced Computer Science and Applications(IJACSA), 4(4), 2013. <http://dx.doi.org/10.14569/IJACSA.2013.040423>
- [5]. S. Nakamoto, "Bitcoin: a peer-to-peer electronic cash system", Online]. Available: <https://bitcoin.org/bitcoin.pdf>.
- [6]. G. Wood, "Ethereum: a secure decentralised generalised transaction ledger", Ethereum Project Yellow Paper, vol. 151, pp. 1-32, 2014.

- [7]. Olaniyi Olayemi M; Arulogun Oladiran T; Omidiora Elijah O; Okediran Oladotun O, Performance Assessment Of An Imperceptible And Robust Secured E-Voting Model, International journal of scientific & technology research Volume 3 Issue 6, 2014.
- [8]. Prof. Dr. Hala Helmy Zayed Assoc. Prof. Mazen Selim Dr. Ayman M. AlAhwal, Secure E-Voting System, A Proposed Research Plan for M.Sc./PhD Degree, 2011
- [9]. Shalini Shukla ; A N Thasmiya ; D O Shashank ; H R Mamatha, Online voting application using Ethereum blockchain, 2018 International Conference on Advances in Computing, Communications and Informatics (ICACCI), pp. 873 - 880, 2018.
- [10]. R. Skudnov, "Bitcoin Clients," Turku University of Applied Sciences, Turku, 2012.
- [11]. Prof. KritiPatidar, Prof. Swapnil Jain "Decentralized EVoting Portal Using Blockchain.
- [12]. Prof. Shashank S Kadam, Ria N Choudhary, SujayDandekar, DebyeetBard- han, Namdeo B Vaidya "Electronic Voting Machine with Enhanced Security.
- [13]. RahilRezwan, Huzaiifa Ahmed, M. R. N. Biplob, S. M. Shuvo, Md. Abdur- Rahman "Biometrically Secured Electronic Voting Machine".
- [14]. Z.A. Usmani, KaifPatanwala, MukeshPanigrahi, Ajay Nair "Multipurpose plat- form independent online voting system.
- [15]. Ravikumar CV.—Performance analysis of HSRP in provisioning layer-3 Gate- way redundancy for corporate networks ||, Indian Journal of Science Technol- ogy. Vol 9, issue 20, 2016.
- [16]. Ashwini Mandavkar, Prof. Rohini Agwane, "Mobile based facial recognition using OTP verification for voting system", 2015 IEEE, IACC, pp. 644-649.
- [17]. Himika Parmar, Nancy Nainan, Sumaiya Thaseen, "Generation of secure one- time password based on image authentication", CS IT-CSCP 2012, pp. 195- 206
- [18]. Hongyu Zhang., Qianzi You, and Junxing Zhang (2015), 'A lightweight elec- tronic voting scheme based on blind signature and kerberos mechanisms',international conference on advanced networks and telecommunications systems,pp.978- 4799
- [19]. Herb Deutsch (2005), 'Public opinion's influence on voting system technol- ogy', IEEE Standards Association.
- [20]. Anandaraj S., Anish R., and Devakumar P.V. (2015), 'Secured electronic vot- ing machine using biometric', IEEE International conference on innovations in information, embedded and communication systems.