
DEVELOPMENT OF DIGITAL VOTING SYSTEM USING FACE RECOGNITION**Prof. Kalyani Pendke^{*1}, Prashanth Potu^{*2}, Kedar Gorte^{*3},****Mahendra Bhalavi^{*4}, Ashish Samarth^{*5}**

^{*1,2,3,4,5}Department of CSE, Rajiv Gandhi College Of Engineering and Research,
Nagpur, Maharashtra, India.

ABSTRACT

Two types of voting systems are mostly used in India. They are the Secret Ballot Paper and the Electronic Voting Machines (EVM) and both of them have their advantages and disadvantages. Also, the existing voting process is not secure and takes a lot of time. Most individuals skip their chance to vote due to the inconvenience of having to travel to the polling booths, and wait in a long queue. Voters who are not eligible can also use fraudulent methods to cast their ballots, which might cause a lot of issues. Online voting has not yet been adopted in India. Thus, in this paper, we are developing a new online voting system that is beneficial to tackle above issues. We are trying to develop a system that will help to implement facial recognition technology to identify unique voters. We are creating our own dataset where one can manually add registered voters in the database. We are implementing a location-free voting method which will help voters to cast their vote from their own location. Each voter can only access the system after being identified and verified against the provided database of registered voters.

Keywords: Smart Voting System, Dataset, Opencv, Python, Face Recognition, Biometric Security, Password, Voter Id, Winning Party.

I. INTRODUCTION

In a vastly democratic nation like India, where the people choose their leaders, elections are crucial. In a democracy, elections will inevitably happen, and it is the sole responsibility of both the government and the people to ensure that they do so in a secure and orderly manner. Elections keep a true state operating because they provide people the option to choose their own kind of governance. Every citizen of a democratic nation has the right to vote, as democracy is meant to allow for unfettered participation. The outcome of the elections will determine the democratic administration. The voting process has seen multiple significant changes over the past several decades, from traditional paper ballot voting to e-voting and, most recently, internet voting. Every system aims to fill in the gaps that the one before it left. Election loopholes developed with evolution of elections, and resources are also being abused in the name of elections. Other resources are being used for elections like they have no limit, and army personnel are being employed to defend the voting machines since they demand a high level of protection and a lot of money[1].

The flaws, such as falsifying the results, casting a false ballot using a different voter ID, and so forth. All of these issues are present in the current methodology, and we are putting up a new way to address them. The essential fairness, privacy, secrecy, anonymity, and openness of the voting process are limited by the risk of excessive authority and manipulated facts. A problem for a transparent voting process in and of itself is that most procedures are now centralised, licenced by the crucial authority, managed, quantified, and monitored via an electronic voting system. So, the election process should be transparent and free from bias. Every person in a democracy has the right to cast a ballot of their own choosing. One of the major problems with the traditional democratic structure is how much effort and money it consumes. Also, some people could worry about movement that has been published illegally at some time during this election or its preparation. The traditional election voting procedure implemented in our nation has obvious shortcomings, including the possibility of violence, equipment breakdowns, resource and time consumption, spot arrangements, and others. Several people were unable to show up at the polls because voters had to physically travel to the polling places or because they were living too distant from the location of their birth [2].

So, a new system –the online voting system– is proposed to address these limitations. It offers accuracy, security, and flexibility. The primary objective of this paper is to evaluate and contrast the current voting technologies with the conventional voting process. The proposed online voting system is a web-based program for use in the election process. To protect the voting system, we use voter photographs as input and train a facial

recognition algorithm on this dataset. The trained model can recognise the faces of voters, ensuring that they only cast one ballot. The ability to vote in an election depends on whether the taken image matches the voter's image in the database. Since the only level of security in the current system is the voter card, anyone can give another person the right to vote using that card, as you must be aware, the existing system is not significantly more secure. Here, however, we proposed a voting method that is more secure than the current system. At the initial stages, voting was conducted using paper ballots. Later the Electronic Voting Machines appear, they are simple to manage and easy to save the data. They take less time and are more secure than ballots on paper. So, in order to increase voting quality and shorten the voting period, we suggested a system with identity verification. This allows the electorate to help cement their support for their favourite candidate by using their system. We leverage facial recognition and detection technology to determine whether or not a citizen is the right consumer. We provide a number of modules where an administrator may log in and view the tool's many functions. Also, individuals can log in and exercise their right to vote. This innovative technology refers to online electronic voting systems that use a central database to facilitate smooth data transfers and accurate result calculation. When a voter uses the system, it will utilize a web camera to record his or her image and attempt to match it with an image that is registered in the database. The voter may cast a ballot if both photos are identical. The majority of institutions of higher learning regularly hold elections to select an understudy leadership. They suggested using an online system that would make it possible for the registration of voters, the casting of ballots, the verification of those ballots, and the broadcasting of the results.

II. LITERATURE SURVEY

Although there have been several studies on online voting methods, we have chosen ten of the most topical, up-to-date, and important studies to review and to critically examine. It has been noticed that the majority of current publications discuss online voting and the usage of various information technologies.

Yirendra Kumar Yadav presented a concept of an electronic voting system that assures authentication, authorization, and accounting [3]. Approach gathers data from VIDAL and uses it to verify voters and cast votes during the e-voting process. From VIDAL, only data that is absolutely necessary and has some bearing on AAA is gathered. The technology or the platform used were Module (EVRM), EVS, Electorate Information Interface, Member's Information Server.

Ayesha Shaikh presented a paper which emphasises on the significance of thoughtful user-interface design for the use of a diverse group of users with varying degrees of computer proficiency [9]. The technologies used were Detection and Recognition system (FDR), One Time Password (OTP) as an Authentication technique in online voting.

Madhumita Deshpande developed an application that provides remote voting capability, accuracy, increased privacy, a user-friendly interface, and dependability throughout the entire election process are succinctly explained in this paper [8]. The technology and platform used were Android, Face Recognition, Remote Voting, OTP, Template Matching, Two-factor Authentication.

Ashwini Ashok Mandavkar presented an article that clarifies facial recognition technology's use in online voting systems [10]. The technologies and algorithms used were Eigen face, Eigen Vectors, image processing, OTP (One-Time Password), PCA (Principle Component Analysis).

Smita B. Khaimar suggested a method that uses steganography and biometric features to provide authentication for online voting. While registering to vote, the voter is prompted to enter a password. Hashing is used to transform a password into a secret message. Steganography hides this message in images [1]. The algorithms used were SHA256 algorithm, Hash code.

R. Sandhiya developed a system that uses a two-level secure internet voting system. In the first level, a web camera records the voter's face and uploads it to the database. Using Matlab, the person's face is matched in the database for validation. As the second layer of security, a OTP is utilised. After generating mail it is confirmed that they are allowed to vote [7].

Ramya Govindaraj developed an online system in 2020 with features similar to the programmes that a particular party has implemented, based on the programmes that people are going to vote [2]. The languages and databases used were C#, Microsoft SQL server 2012 and Microsoft Azure as a cloud.

Roopak T M developed a scheme which combines biometric information and VIDs (Virtual IDs) of voters

collected from the Aadhar database to cast the vote as well as using the digital signature as the key for the encryption of the votes inside the block, the aforementioned scheme provides a safe e-voting system [4]. The technology used was Blockchain.

Vivek S K developed a safe, open, and decentralised electronic voting system using the Hyperledger Sawtooth blockchain framework. Voters can cast their votes through election polling places with restricted access to the system, and those ballots are stored in an immutable blockchain state [6]. The technology and platform used were Angular 8, Node.js, Amazon RDS, and Sawtooth blockchain, Python with the APIs, Docker technology, Amazon Web Services (AWS).

Ganesh Prabhu S developed a face scanning system that is used to capture images of voters' faces before the election and is helpful when casting a ballot. Instead of voter identification, the offline voting method is improved with the use of RFID tags. Additionally, this technology allows users and citizens to view the results at any moment [5]. The technology used were Arduino Uno, LCD Display, RFID, Push Button.

Table 1: Survey table on Online Voting Systems

Sr.no	Author, Title, Year	Objective	Technologies Used	Advantages	Disadvantages
[1]	Smita B. Khaimar, P. Sanyasi Naidu, Reena Kharat, "Secure Authentication for Online Voting System", 2016	The suggested method uses steganography and biometric features to provide authentication for online voting. While registering to vote, the voter is prompted to enter a password. Hashing is used to transform a password into a secret message. Steganography hides this message in images.	SHA256 algorithm, Hash code.	In this arrangement, a person may also cast a ballot from a location of their choice or from outside of the electorate to which they have been assigned.	Biometric systems may put an undue burden on servers, making them a single point of failure.
[2]	Ramya Govindaraj, Kumaresan P, K. Sreeharshitha, "Online Voting System using Cloud", 2020	The aim behind this particular research is to build an online voting system with features similar to the programmes that a particular party has implemented, based on the programmes we are going to vote.	C# as a programming language, Microsoft SQL server 2012 and Microsoft Azure as a cloud.	The primary reason we need to switch from the traditional voting system to an online voting system is that it allows us to vote from anywhere and does not consume our time.	Using online voting system in cloud is expensive.
[3]	Yirendra Kumar Yadav, Saumya Batham, Mradul Jain, Shivani Sharma, "An Approach to Electronic Voting System using UIDAI", 2014	The concept of an electronic voting system that assures authentication, authorization, and accounting is presented in this paper. Approach gathers data from VIDAI and uses it to verify voters and cast votes during the e-voting process. From VIDAI, only data that is absolutely necessary and has some bearing on AAA is gathered.	Module (EVRM), EVS, Electorate Information Interface, Member's Information Server.	This strategy takes care of problems like voter fraud, accurate and trustworthy voting, time delays, improving participation, giving a user-friendly interface, etc., creating a framework for fair elections.	Some users may find the process a little bit difficult to understand.
[4]	Roopak T M, Dr.	By combining biometric	Blockchain	Vote duplication or	Implementing of

	R Sumathi, "Electronic Voting based on Virtual ID of Aadhar using Blockchain Technology", 2020	information and VIDs (Virtual IDs) of voters collected from the Aadhar database to cast the vote as well as using the digital signature as the key for the encryption of the votes inside the block, the aforementioned scheme provides a safe e-voting system.	Technology	tampering are Prevented via Aadhar integration with the electronic voting system.	such a system can be technically challenging, lack of regulation
[5]	Ganesh Prabhu Set.al., "Smart Online Voting System" 2021	The face scanning system is used to capture images of voters' faces before the election and is helpful when casting a ballot. Instead of voter identification, the offline voting method is improved with the use of RFID tags. Additionally, this technology allows users and citizens to view the results at any moment.	Arduino Uno, LCD Display, RFID, Push Button.	This study focuses on a system that allows users to cast ballots remotely using a computer or a mobile device and eliminates the need for voters to physically travel to the polling place through two-step verification utilising face recognition and an OTP system.	It is challenging to implement in some remote areas due to the high expense of additional hardware.
[6]	Vivek S K, et.al., "EVoting System using Hyperledger Sawtooth", 2020	The Hyperledger Sawtooth blockchain framework is suggested as a foundation for a safe, open, and decentralised electronic voting system. Voters can cast their votes through election polling places with restricted access to the system, and those ballots are stored in an immutable blockchain state.	Angular 8, Node.js, Amazon RDS, and Sawtooth blockchain, Python with the APIs, Docker technology, Amazon Web Services (AWS).	Election process is fair and reliable because there is no chance of vote fraud.	Drawbacks with advanced cryptography approaches could include the requirement for trustworthy hardware or usability and performance restrictions.
[7]	R. Sandhiya , D. Indumathy "Online Voting Using Face Recognition and Password Based Security System", 2017	This essay suggests a two-level secure internet voting system. In the first level, a web camera records the voter's face and uploads it to the database. Using Matlab, the person's face is matched in the database for validation. As the second layer of security, a OTP is utilised. After entering the password generated to their mail, it is confirmed and they are allowed to vote.	MATLAB , OpenCV.	Guarantees security by implementing two-level authentication	The results can be slowly executed and the copy of Matlab is more expensive.

[8]	Madhumita Deshpande,	The design and operation of the application that provides	Android,Face	Enables voter to participate	Less user applicability.
	Deepali Zambre, Prajakta Mandle, Komal Hankare, Kanchan Shelke "E-Voting Systemfor Modern Individual",2015	remote voting capability, accuracy, increased privacy, a user-friendly interface, and dependability throughout the entire election process are succinctly explained in this paper.	Recognition, Remote Voting, OTP, Template Matching, Two- factor Authentic ation.	remotely, increases security, interactive interface.	
[9]	Ayesha Shaikh, Bhavika Oswal, Divya Parekh, B.Y.Jani "E-votingUsing OneTime Password and Face Detection and Recognition", 2014	The paper emphasises on the significance of thoughtful user-interface design for the use of a diverse group of users with varying degrees of computer proficiency	Detection and Recognition system (FDR), One Time Password (OTP) as an Authentic ation technique in onlinevoting.	Increased security because of the use of OTP.	Less user understand ability.
[10]	Ms. Ashwini Ashok Mandavkar, Prof. RohiniVijay Agawane "Webcam Based Facial Recognition Using OTP Verification for Voting System",2015	This article clarifies facial recognition technology's use in online voting systems.	Eigen face, Eigen Vectors, image processing , OTP (One- Time Password) , PCA (Principle Compone nt Analysis).	Face recognition ensures that only voting for a single time is allowed.	It is allowed only once and web cam detects using Eigen face sometimes take more time.

III. PROPOSED WORK

The Admin can Login by the Admin Login ID and Password. The Admin can create the candidates details of elections schedule and Party Symbols of the Candidates and store them in the Database. The Database helps the server to store these and retrieve the details of Voters , Candidates, Generate Elections and Generate Report.

The Project is an online program that aims to provide a secure online voting platform where voters and validity of their votes is ensured by the use of one-time password and face recognition technology. Voters are not required to stand in large queues for hours to cast their ballots; they might do it well by just signing in with their ID. Voters can participate in the elections regardless from where they are physically, by just logging in with the provided Unique ID number and password on the website's first page, using facial recognition to register on the second page, and by using a one-time password that is generated for each voter for each election. Using the symbols of all the parties who are running for office,voters may take their decision. The fake user votes are also counted in the election voting process as security is the number one priority throughout the elections. Face Recognition uses Haar Cascade Algorithm to identify the fake voters using. If the facial features of the user's face match the one from the dataset the user is considered eligible to vote. This makes the whole process secure and

efficient.

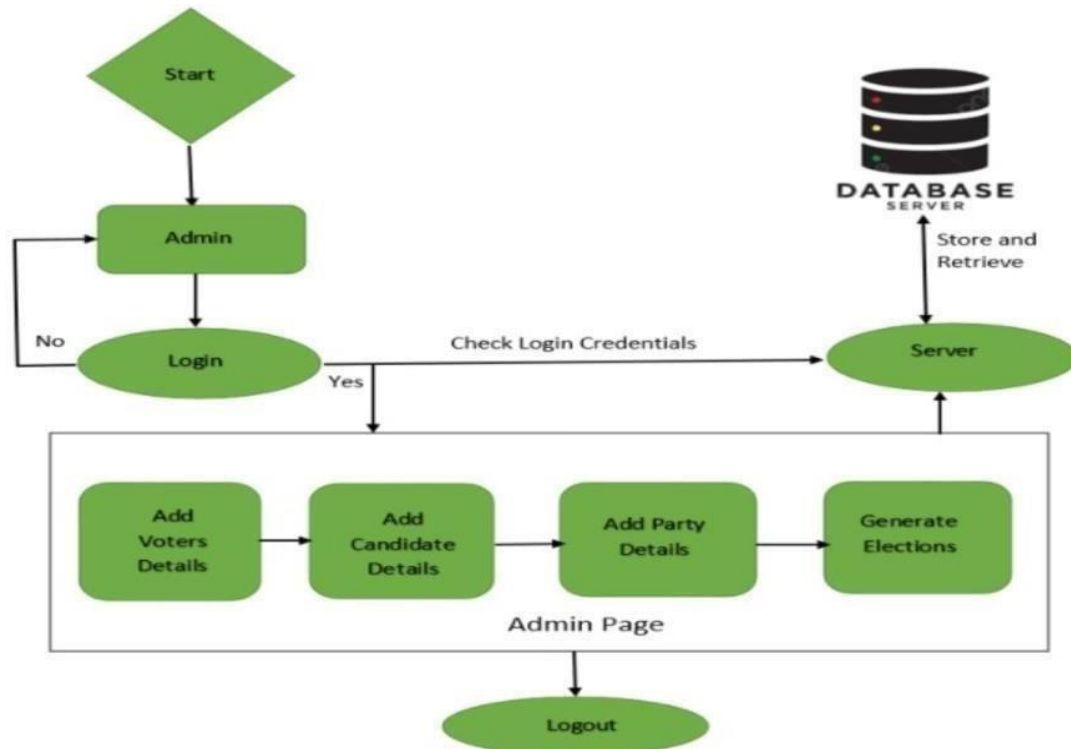


Figure 1: Admin Architecture

Figure 1 shows Admin can login and store the information in the Database server and add details of voters and candidates and generate elections and report.

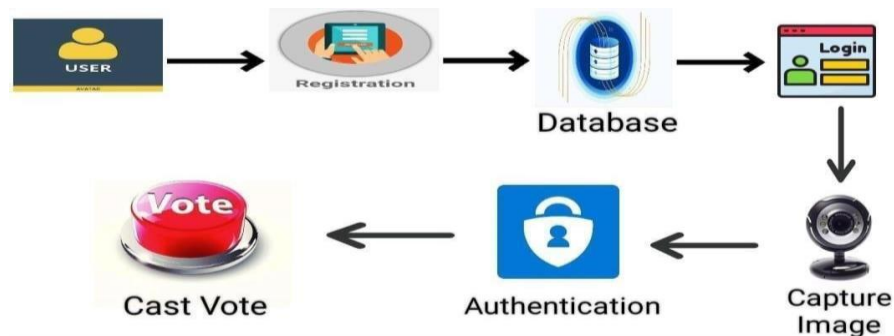


Figure 2: User Architecture

Figure 2 shows Users have to register by entering details which get stored in the database and can login after their face matches the database to verify their identity and finally can cast their vote.

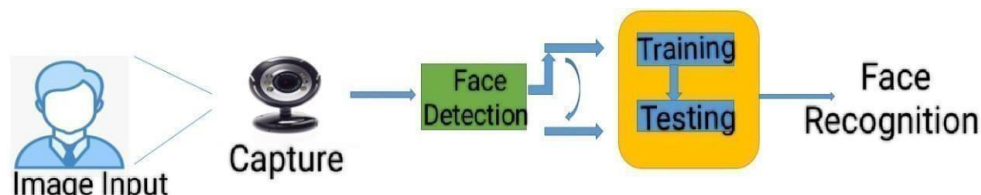


Figure 3: Image Processing

Figure 3 shows The user image is captured and detection works by identifying measuring facial features of a face which is stored in the dataset with the help of training and testing the data face can be recognized.

IV. MODULES

a) Login Page: The login page is a feature of all secure applications and is frequently used online to verify user identity before displaying the secured sections of web apps. Before one may access the application, they must first authenticate themselves on the login page.

Web applications may have application security flaws as a result of an insecure login page. The server-side programme receives user input from the login page and processes it. A server-side application performs the authentication, and the user is shown the authentication results on the website's site login form. The user is directed to the secure area of the website if he/she is authenticated. The first page of our system is a login page where user has to enter his login credentials such as email id and correct password.

b) Registration Page: A registration page enables individuals and groups to sign up and utilise your system independently. When registering for an event, programme, membership, list, etc., a person fills out a registration form with a number of fields and submits it to a company ,person or an organization. The second page of our application is the Registration page where eligible users can register by providing their names, email ids and phonenumber.

c) Face Recognition: The next step is face detection which can be done by using the Haar Cascade Algorithm using which the face can be detected and LBPH algorithm to recognised by Pixels from the given dataset. The face must be normalised using an algorithm in order to be consistent with the faces in the database. Using numerous generic face landmarks is one method to achieve this. Once the faces have been aligned and detected, the next phase is to extract features from the faces, such as the bottom of the chin, the top of the nose, the outside of the eyes, and other places surrounding the eyes and lips. The last step is to match the extracted features with faces in a database.

d) Voting Page: The next step after authentication is voting, where the authorized users can select their parties and vote for their favourite candidates. This page consists of a list of various parties contesting the elections along with their symbols. Voters can select a party from the list and choose to vote for it.

V. EXPERIMENTS AND RESULTS



Figure 4: Login Page

Figure 4. shows the login page for the users/admin where he/she has to enter his/her login credentials first to verify himself/herself by entering a Unique voter Id & correct password.

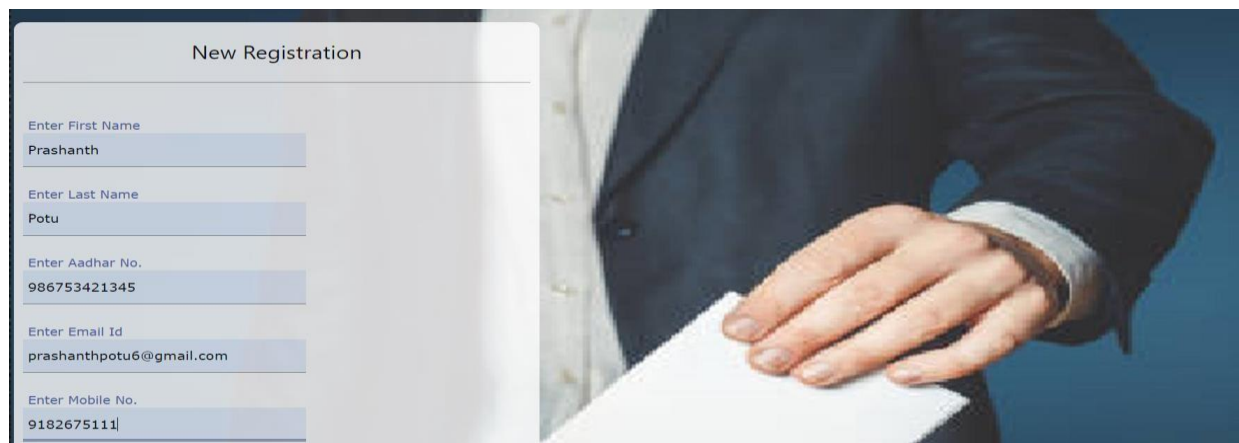


Figure 5: Registration Page

Figure 5 shows the registration page for users , voters , for the digital voting system. Here the voters can

register their name ,email and number by signing up.

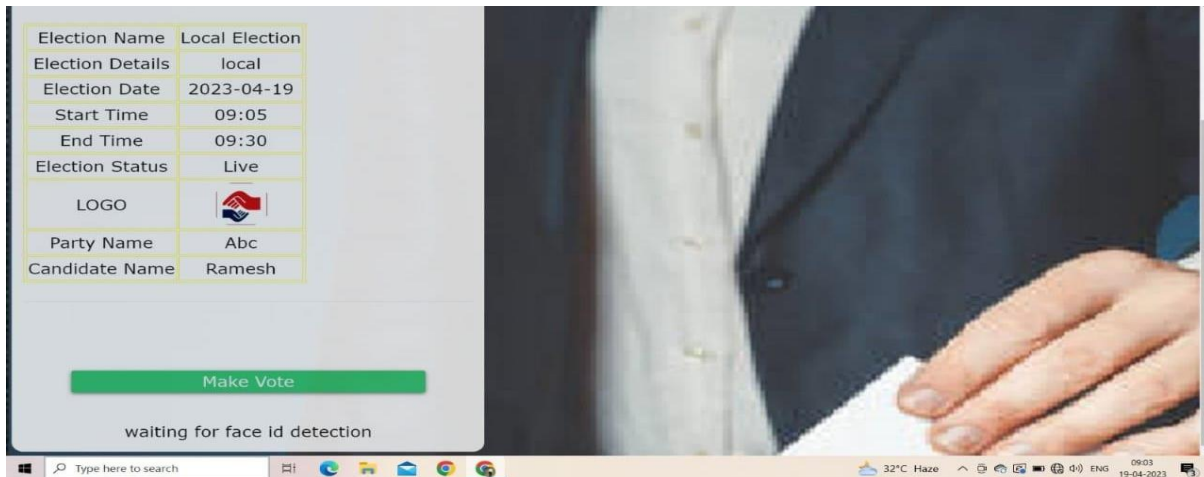


Figure 6: Voting Page

Figure 6. shows that the voters can vote for their Candidate's party through the Voting page which contains a list of all the parties.



Figure 7: Face Recognition

Figure 7. shows that the user is authorised if his or her face matches the face that is stored in the database.

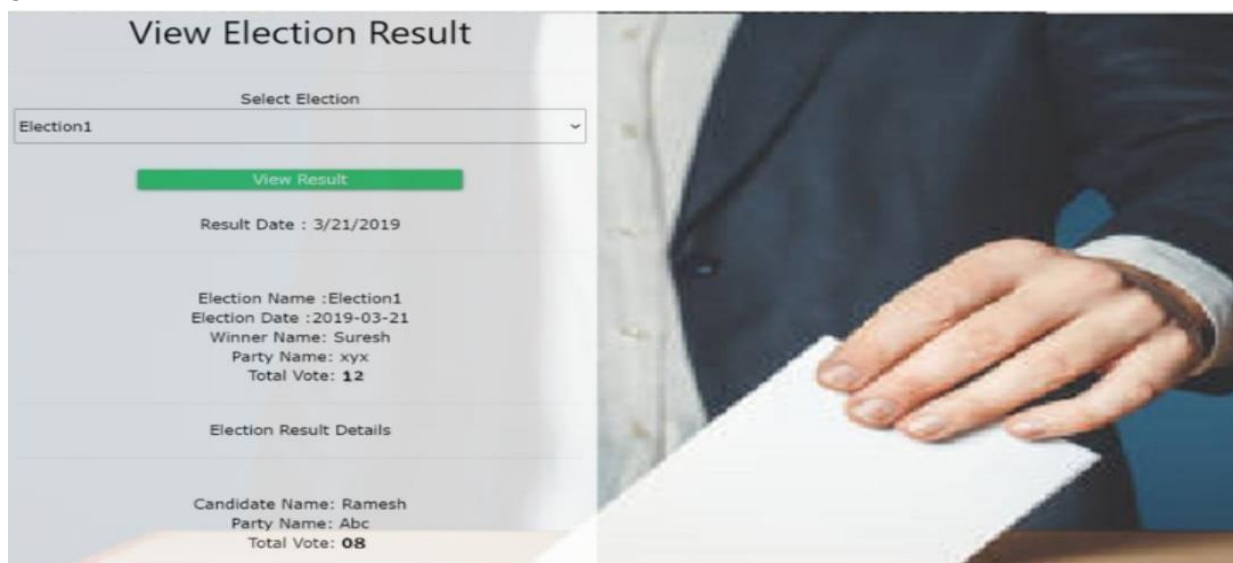


Figure 8: Results

Figure 8. shows the results of the votes of the elected candidates.

VI. CONCLUSION

Currently, existing voting system has many defects such as lengthy process, time consuming, not secure, no security level but now we can say that our approach is more useful and secure from the existing system. The voters can cast their vote from any where by logging in to our proposed smart voting system through internet. Less money and staff are required with this technique. It also offers a lot of powerful characteristics, including verifiability, manageability, accuracy, etc. Every year or just before an election, the database must be updated to include newly registered voters and to delete any deceased voters. Election officials, paper ballots, and electronic voting equipment are not necessary, all that is needed to securely cast a ballot from anywhere is an internet connection, a mobile device for authentication, and a desktop or laptop with a camera for face authentication. The entire world is moving towards digitization. Voting is also digitised in this context as part of digitization. This initiative has the advantage of speeding up the announcement of the election results. Face recognition of voters is added to the system to increase security. Only one vote may be cast per individual under this system. Voting more than once is prohibited. As data is stored in centralized repository so, data is accessible at any time as well as backup of the data is possible.

VII. FUTURE SCOPE

In the future, Admin rights and their utilization of the database and data can be improved. We can also test new algorithms to increase the accuracy of face detection. More efforts can be developed in Real-life in future in moving towards digitization.

VIII. REFERENCES

- [1] Yamini, K., Kumar, S. M., Sonia, S., Yugandhar, P. V., & Bharath, T. Class Attendance Using Face Detection and Recognition with OPENCV. 3822– 3826. (2019).
- [2] Soomro, Z. A., & Ali, A. FPGA based real- time face authorization system for electronic voting system. (2020).
- [3] Pandit, Varad, Prathamesh Majgaonkar, Pratik Meher, Shashank Sapaliga, and Sachin Bojewar. "Intelligent security lock." In Trends in Electronics and Informatics (ICEI), 2017 International Conference on, pp. 713-716. IEEE, 2017
- [4] S. V. Tathe, A. S. Narote, S. P. Narote "Face Detection and Recognition in Videos" Sinhgad College of Engineering 2016 IEEE
- [5] Peter N. Belhumeur, Joao P. Hespanha, and David J. Kriegman "Eigenfaces vs. Fisherfaces: Recognition Using Class Specific Linear Projection" IEEE transactions on pattern analysis and machine intelligence, VOL. 19, NO. 7, JULY 1997
- [6] Patel, C. I., & Patel, R. (2013). Robust Face Recognition Using Distance Matrix. International Journal of Computer and Electrical Engineering, 5(4), 401–404. <https://doi.org/10.7763/ijcee.2013.v5.740>
- [7] Ankit Anand, Pallavi Divya, An Efficient Online Voting System, Vol.2, Issue.4, July-Aug. 2019, pp- 2631-2634. Dinesh Kumar Petal, International Journal of Computer Science and Mobile Computing, Vol.9 Issue.1, January-2020, pg 150-160
- [8] Himanshu Agarwal, G.N. Pandey, Online Voting System for India Based on Aadhaar Id, 2013 Eleventh International Conference on ICT and Knowledge Engineering
- [9] B.Arun, V.K. Gouthaman, A.Nafees Raja, "Online Voting System Using Face Recognition", Faculty of Engineering and Technology, SRM University, April 2007
- [10] Multi-Purpose platform independent online voting System, Dr. Z.A. Usmani, Kaif Patanwala, Mukesh Panigrahi.
- [11] Ajay Nair Computer Engineering Department M.H. Saboo Siddik College of Engineering Mumbai, India. https://www.researchgate.net/publication/355346652_Voting_System_Based_on_Block.
- [12] Electronic Voting System using Biometrics, Raspberry Pi and TFT module Prof. A.M. Jagtap, Miss Vishakha Kesarkar, Miss Anagha Supekar, Computer Science and Engineering Rajarambapu Institute of Technology, Islampur, India. <https://ieeexplore.ieee.org/document/8862671>.
- [13] Matthew A. Turk and Alex P. Pentland. "Eigenfaces for recognition". Journal of cognitive neuroscience,

Volume 3, Number 1, Nov 27, 2002.2

- [14] Secured Smart Voting System using Aadhar Madhuri B. Adarsha M G , Pradhyumna K R, Prajwal B M Information Science and Engineering, Siddaganga Institute of Technology, B H Road, Tumakuru, Karnataka, India 572103 <https://ieeexplore.ieee.org/document>.
- [15] Dimitri PISSARENKO. "Eigenface-based facial recognition". Dec 1, 2002.3.
- [16] Saleh, K., 2003. Specifications of a mobile electronic voting system and a mobile agent platform. Proceedings of IADIS e-Societ. Lisbon, Portugal.
- [17] Elmasri, R. and Navathe, S. B 2004. Fundamentals of Database Systems, Fourth Edition, Pearson/Addison Wesley Publisher.
- [18] Morrison J. and Morrison M. 2003. Guide to Oracle9i, Thomson Course technology Published.
- [19] Abdulhamid, S. M., Adebayo, O. S., Ugiomoh, D. O., & AbdulMalik, M. D. (2013). The Design and Development of Real-Time E-Voting System in Nigeria with Emphasis on Security and Result Veracity. International Journal of Computer Network and Information Security, 5(5), 9–18.
<https://doi.org/10.5815/ijcnis.2013.05.02> Hazzaa, F. I., Kadry, S., & Zein, O. K. (2012). Web- Based Voting System Using Fingerprint: Design and Implementation. II 404–409.
- [20] Nautiyal, J. (2013). An Automated Technique for Criminal Face Identification Using Biometric Approach. 2013(Cac2s), 608–611.
- [21] Ch.sai pratap varma D.sumanth rahul Jithina Jose B Keerthi Samhitha Suja Cherukullapurath Mana, Department of CSE, Sathyabama institute of science and technology.
https://www.researchgate.net/publication/343038732_Aadhar_Card_Verification_BaseOnline_Polling.
- [22] Komminist Weldemariam, Andrea Mattioli, Adolfo Villafiorita eDemocracy Group Center For Information Technology, FBK-IRST Trento, Italy.
https://www.academia.edu/28095568/Managing_Requirements_for_E_Voting_Systems_Issues_andApproaches.
https://www.researchgate.net/publication/220969161_Requirements_design_and_implementation_of_an_e-voting_system. <https://www.e-voting.cc/en/expertise/references/>.