IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)
An International Open Access, Peer-reviewed, Refereed Journal

ONLINE VOTING SYSTEM USING FINGERPRINT SENSOR, FACE RECOGNITION AND QR CODE SCANNER

[1] MS. SHUBHANGI D. DHANE, [2] PROF. S. B. RATHOD

[1] P.G Student, Department of Computer Science & Engineering, Sipna C.O.E.T, Amravati, India,
[2] Assistant Professor, Department of Computer Science & Engineering, Sipna C.O.E.T, Amravati, India.

Abstract: In India, there are two types of voting system: The secret Ballot paper and Electronic Voting Machines (EVM), However, both of the process have some limitation or demerits. The current voting system is not safe and secure too. The voter who is not eligible can also cast its vote by fake means which may leads to many problems. Hence, voter identity authentication is a primary concern. Also, unlike many countries, in India the online voting hasn't been implemented yet.

In this project, a new authentication technique in online voting system is proposed which uses facial recognition of the voter, QR Code and Fingerprint scanner. In our approach we have three modules in the voting process: viz. Super Admin, Admin & User.Super admin has to enroll all the election areas and candidates for the area. Admin have to add the voters via a voter enrollment form along with their photographs, fingerprints and QR code. At the time of elections, the voter can generate their one-time EPP code using face recognition, QR code and fingerprint. This EPP code is used to access the user module. In user module the voter can cast their vote to a particular member. Super admin can release the result at the end of the elections. The results can be viewed in the user panel by the voters. Hence, the voter authentication problem is addressed.

***Index Terms* – Face Recognition, Fingerprint Sensors, Online Voting, QR Code Scanner, Voting Systems**

I. INTRODUCTION

Voting is commonly related to politics and is finished with often exploitation and manual approach where voters stand to vote for his or her decisions. Manual voting may lead to malpractices sometimes.so there is a need to implement online voting system. This is for expand the technology from manual voting system to digital voting system. Electronic voting systems are those which depend on some electronic technology for their correct functionality. Many of them depend on such technology for the communication of election data. Depending on one or more communication channels in order to run elections poses many technical challenges with respect to verifiability, dependability, security, anonymity and trust. Changing the way in which people vote has many social and political implications. The role of election administrators and (independent) observers is fundamentally different when complex communications technology is involved in the process. Electronic voting has been deployed in many different types of election throughout the world for several decades.

Elections form a major part of any democratic society to elect its new government. In earlier times, paper-based elections were conducted. In that, voters cast their votes on the ballot paper and then drop that paper in sealed boxes provided by the election department. When the elections end, the secret ballots are opened and manually counted to proclaim results. The traditional or paper-based polling method served to increase people's confidence in the selection by majority voting. It has helped make the democratic process and the electoral system worthwhile for electing constituencies and governments more democratized. There are 167 nations with democracy in 2018, out of approximately 200, which are either wholly flawed or hybrid [5,6]. The secret voting model has been used to enhance trust in democratic systems since the beginning of the voting system. It is essential to ensure that assurance in voting does not diminish. A recent study revealed that the traditional voting process was not wholly hygienic, posing several questions, including fairness, equality, and people's will, was not adequately [7] quantified and understood in the form of government [2,8]. But in this process sometime there can be manually error or cheating to declare the results. Also, there is lot of wastage of paper and manpower.

Engineers across the globe have created new voting techniques that offer some anticorruption protection while still ensuring that the voting process should be correct. Technology introduced the new electronic voting techniques and methods [9], which are essential and have posed significant challenges to the democratic system. Electronic voting increases election reliability when compared to manual polling. In contrast to the conventional voting method, it has enhanced both the efficiency and the integrity of the process [10]. Because of its flexibility, simplicity of use, and cheap cost compared to general elections, electronic voting is widely utilized in various decisions [11]. Despite this, existing electronic voting methods run the danger of over-authority and manipulated details, limiting fundamental fairness, privacy, secrecy, anonymity, and transparency in the voting process. Most procedures are now centralized, licensed by the critical authority, controlled, measured, and monitored in an electronic voting system, which is a problem for a transparent voting process in and of itself.

The Indian government installed direct record electronics - DRE voting system which are popularly known as E-voting machines – EVMs. The ideation in this work is to redesign electronics voting system to make the system more efficient and reliable. However, the manipulation of voting results still exists. The unreliable nature of the voting system and delays in results of the existing system is the prime motivation to to study for alternative and more secure methods of online voting. Also, the COVID-19 Pandemic have accelerated the use of technologies which includes online shopping, digital payments, telehealth, AI, Remote work, Distance education and online internet. So online voting also seems imminent.

The election processes are primarily held through ballot papers, with eligible voters having to select their candidate/party by marking on the ballot paper. Some countries, like India, utilize a slightly more technological approach to elections, by using Electronic Voting Machines (EVMs), which allow voters to caste their vote by clicking on a button representing the party/candidate of their choice. The election processes currently in place involve a trusted third party, like the election commission or election administration, required to manually tally the votes from ballot papers or EVMs, and aggregate the vote counts from various geographical regions in the country to calculate the final result.

Now, since the entire election process is offline, there is a greater chance of malpractice and unfair means of elections which is a threat to our democracy. However, the existing voting system isn't completely foolproof and reliable. There are a lot of concerns involving tampering of votes, manipulation of results, fake voters, anonymity of the voter, transparency and security. Also, the voters need to go to distributed places like polling booths and stand in a long queue to cast their vote, because of these reasons most of the people misses their chance of voting. The voter who is not eligible can also cast its vote by fake means which may leads to many problems. This motivates us to build a voting system which is online and can address few of the afore-mentioned issues.

II. LITERATURE REVIEW

Although there are many researches works on online voting systems, here we have critically analyzed and summarized twenty research works and projects which are more relevant, recent and pertinent. It is observed that most the recent works addresses the issue of online voting and use of various information technologies.

In the year 2020, Vivek S K, et.al., developed a secure, transparent and decentralized e-voting system is proposed using the Hyperledger Sawtooth blockchain framework [1]. Restricted access of the system through election polling stations allows voters to cast their votes, which are recorded in the immutable blockchain state. Fairness and reliability of the election procedure due to nil possibility of vote manipulation. The issue of fairness and reliability of the election procedure due to nil possibility of vote manipulation was addressed. The technology/platform used were Angular 8, Node.js, Amazon RDS, and Sawtooth blockchain, Python with the APIs, Docker technology, Amazon Web Services (AWS).

In the year 2021, Shubham Gupta, Divanshu Jain, Milind Thomas Themalil developed a system where the voter is registered into the system database well before the time of election [2]. Now at the voting time, In the first step voter must verify his/her government identity such as Aadhar card or voting card with his/her proper picture, once it is verified, he/she moves to the second step. In second step voter has to go under the face reorganization process. Once the corresponding matching or verification is done, the voter will move to next step to cast vote to the candidate from the electronic voter machine. The cast vote is shown on display for the satisfaction of voters. Then the voting data is continuously uploaded on ThingSpeak server. The central office of election department can monitor the data in more reliable way so that no discrepancy/ modification can take place later was addressed. The technology/platform used were PyCharm, JetBrains IDE using Python, IoT, ThingSpeak, Open Source Computer Vision Library OpenCV, Arduino.

In the year 2016 , Mrs. Nilam Kate, Mrs. J.V.Katti developed the technique where a web-based voting system that permits voter to vote independent of location [3]. Security of any information is concerning issue and it very sensitive for online voting system. Mentioned system does not use any biometric application, without using biometric function authentication of the voter is done. In this system votes are encrypted by AES encryption algorithm to provide the security [4]. The issue of saves the time and improves the performance of system was addressed. The mentioned scheme is cost effective and at the same time satisfies the security requirements of an online voting system. The technology/platform used were Visual cryptography and AES algorithm.

In the year 2020, Naseer Abdulkarim Jaber Al-Habeeb, Dr. Nicolae Goga, Haider Abdullah Ali1, Sarmad Monadel Sabree Al-Gayar described an application for m-voting targeting the specific conditions of Iraq in the COVID situation [5]. In the current society, the application of which we are talking about, can also be seen as a significant help for a numerous amount of countries during the pandemic of COVID- 19. The application is based on Mobile technology. Mobile technology is chosen motivated by the fact that although people do not have computers, almost everyone has a mobile phone in Iraq. The technology/platform used were Android Studio, PHP- Restful Services for the BackEnd Component and MySQL database.

In the year 2020, Roopak T M, Dr. R Sumathi developed a scheme which provides the secured e-voting system by using biometric details and VID (Virtual ID) of voters obtained from the Aadhar database to cast the Vote and also using the digital signature as the key for the encryption of the votes inside the block [5]. Aadhar integration to the evoting system overcomes the duplication or tampering of votes.. The technology/platform used were Blockchain Technology

In the year 2005, Claudia Garc´ıa-Zamora, Francisco Rodr´ıguez-Henr´ıquez, and Daniel Ortiz-Arroyo developed A secure electronic voting system for medium scale on-line elections (SELES) [6]. This system efficiently implements a security communication protocol offering protection against double voting and others frauds while avoiding any private voting channel. This system has been tested in a distributed and heterogeneous Internet network comprised by workstations, laptops and PDA nodes interacting through wired and wireless connections. SELES accomplishes all the standard properties of conventional voting systems, namely, accuracy, democracy, privacy, verifiability, simplicity, flexibility and double voting detection. SELES has been designed to deal with communication failures, thus achieving a certain degree of robustness. The technology/platform used were Digital Signature Algorithm (DSA).

In the year 2021, Ganesh Prabhu S, et.al., developed the face scanning system is used to record the voters face prior to the election and is useful at the time of voting [7]. The offline voting system is improvised with the help of RFID tags instead of voter id. This system also enables the user the citizens to see the results anytime which can avoid situations that pave way to vote tampering. This paper focusses on a system where the user can vote remotely from anywhere using his/her computer or mobile phone and doesn't require the voter to got to the polling station through two step authentication of face recognition and OTP system. The technology/platform used were Arduino Uno, LCD Display, RFID, Push Button.

In the year 2003, Robert Kofler, Robert Krimmer, Alexander Prosser developed an algorithm designed to guarantee anonymity of the voter and to avoid the risk of manipulation of votes [8]. The algorithm is based upon the strict separation of voter registration and submission of votes, which implies that certain information has to be stored on a secure media. The issue of security criteria and possible implementation options for secure storage was addressed. The technology/platform used were Electronic Voting, Electronic Democracy, Internet Applications.

In the year 2021, Mohamed Ibrahim, et.al. discussed the design and development of ElectionBlock, a voting system that provides its own blockchain, running on a centralized network of nodes, with the integration of a biometric scanner, to maintain vote integrity and distinguish between registered and unregistered voters [9]. This scheme allows data immutability while providing the user with security and control over their ballot. Experimental results demonstrate the potential for scalability of the system to handle a high volume of votes from multiple servers while maintaining data integrity, performance, and security. This paper address the considerations taken to develop and implement the centralized and independent blockchain network for use as a voting platform with the integration of biometrics for the purpose of enhanced user security. The technology/platform used were Merkle tree, SHA-256 algorithms, ElectionBlock blockchain.

In the year 2021, S. Jehovah Jireh Arputhamoni, Dr. A. Gnana Aravanan discussed that online website has a prevented IP address generated by the government of India for election purpose[10]. People should register the name and address in the website. Election commission will collect the fingerprint and face image from the voters. The database or server will store the images. When the images are obtained on the casting day, it will be compared with database and provides a secured voting on the Election Day. System utilizes faces and fingerprints to unlock the voting system, similar to the mobile phone are used. The current system requires the physical presence of voter, which is inconvenient to many voters. The process consumes less time as well. Using the detection of face and fingerprint images, the number of fake voters can be reduced. The technology/platform used were HTML, Visual Studio, CNNalgorithm,

In the year 2020, Shaikh Mohammad Bilal, Prince Ramesh Maurya developed Voting System utilizing Android Application is progressively effective that the great technique to do a political decision [11]. The task has build up an intuitive GUI board for casting a ballot framework. In addition, Apps Inventor 2 had been utilized to structure the whole task. The database that made additionally does the computation of the information before move the information to the official site. This framework has better exactness contrasted with the conventional strategy for tallying. The technology/platform used were Android applications.

In the year 2021, Awsan A. H. Othman, et.al developed an approach where the IoT and Blockchain have been used with this system to ensure that users' data are protected from theft and prevent eavesdropping or vote tampering to guarantee the integrity of the voting. The blockchain encrypts votes in order to protect every vote from forgery. The system assists the concerned authorities in obtaining results quickly without delay, taking into account the differences in voting process between government and private organizations [12]. Governments can establish referendums or elections, and anyone who has reached the legal age and has a voting card issued by the government will be able to vote, thus we get rid of the traditional methods and dispense with ballot boxes, standing in long queues and delay counting the votes that cost governments a lot of time, effort and money. The technology/platform used were IoT with Ethereum blockchain technology

In the year 2013, Hanady Hussien , Hussien Aboelnaga developed a system where a new EVS is presented. It utilizes Pailier cryptosystem and blind signature based on RSA as security tools [13]. It consists of CTF that communicates with multiple local committee servers that distributed among poll stations. Each server is connected with group of embedded systems acting as voting machines. Pailier cryptosystem provides the secrecy requirement because of its additive homomorphic property, which allows CTF to tally the secret votes without decrypting them. The blind signature based on RSA blinds the votes and voter identity to achieve privacy and accuracy security requirements. The eligibility and uniqueness requirements are accomplished by the data stored in voter's RFID. This paper proposes a new e-voting system that fulfills the security requirements of e-voting. It is based on homomorphic property and blind signature scheme. The system satisfies the vital security requirements. The technology/platform used were Pailier cryptosystem and blind signature based on RSA.

In the year 2017, Dr. Z.A. Usmani, Kaif Patanwala, Mukesh Panigrahi, Ajay Nair, developed the online voting system which is a multi-purpose platform independent system which can be used by any organization and government to conduct the elections [14]. The user just needs to have national identification number such as Aadhaar card number and any operating system smartphone which has a barcode scanning feature implanted in them. As the system is an online based application, the user can vote from their current location. The voter doesn't have to go to a polling booth to cast their vote, thereby encouraging a greater number of people to participate in voting. The mentioned method is platform independent.

In the year 2016, Smita B. Khaimar, P. Sanyasi Naidu, Reena Kharat proposed a new secure authentication for online voting system by using biometrie feature and steganography. Voter is asked to enter a password at the time of registration [15]. Password is converted into secret message using timestamp and hashing. This secret message is stored in image using steganography. In this model, a person can also vote from outside of his/her allocated electorate or from his/her chosen location. The technology/platform used were SHA256 algorithm, Hash code.

In the year 2017, Bhuvanapriya.R, Rozil banu.S, Sivapriya.P, Kalaiselvi. V. K. G developed a system having three phases. First the details of the persons who are above 18years are extracted from aadhar card database [16]. Automatically a new voter id with necessary details will be created and an intimation will be given to the persons through their e-mail. At the time of voting, the user can specify their id and password. To ensure more security, finger prints of the voter is used as the main authentication resource. As soon as they cast their vote, their voter id and other details will be erased automatically and the aadhar card details which they used will be tracked and will be locked to access. This is done to preserve the security. When people cast their vote, the results will be updated automatically and on the same day of election, the results will also be published. Also, our mentioned system supports the online voting too. The technology/platform used were Biometric and steganographic authentication, RSA algorithm

In the year 2010, Cesar R. K, et.al., describes two experiences: The first experiment, called International Direct Digital Election (ID2E), is made for testing the viability for the international voting by mobiles using SMS protocol, using Web 2.0 tools to facilitate discussions about the election main theme [17]. The second experiment is the construction of a voting prototype using Android platform smart phones, with applications and vote collecting databases available on dynamic web pages, trying to simulate de Identical Ballot Boxes strategy described in two papers of Alefragis, Lounis, Triantafillou and Voros. The two experiments are part of a mentioned e-Voting methodology, and were made with the final objective of surveying scenarios about international voting processes, to give some experimental base for future e-Voting projects at international leveI. The technology/platform used were Biometric and steganographic authentication, RSA algorithm Web 2.0 social networks Android smart phones, ID2E,

In the year 2015, Mohammad Hosam Sedky, Essam M. Ramzy Hamed, developed Voting Model System overcomes the issue of security obstacles. Before sending the final result report per polling station automatically to the district's committee, a paper copy of the final result report of each polling station will be audited manually by every candidate' representative and signed it as a proof of his agreement of the final result report [18]. Then, it will be delivered physically to the propagate district's committee Office. Judges in each district's committee office will compare the polling station physically delivered result report with the automatically received report to be sure that the results are accumulated successfully. The same process will be done in all the higher committees till the final results from the Governorates will be submitted automatically and physically signed to the HEC. The proposed e-voting system is designed especially to solve the cost effective, accuracy and transparency problems in a highly secured approach. Security evaluation experiments are performed successfully to the mentioned system proving that it satisfies privacy, accuracy, reusability, eligibility and integrity. The technology/platform used were ID card Reader, Fingerprint Reader, Visual Studio 2010, C# software and SQL Server 2008.

In the year 2020, Ramya Govindaraj, Kumaresan P, K.Sree harshitha developed an online voting system with features like the schemes that the specific party has implemented, based on the features we are going to vote [19]. The main reason we need to shift from normal voting system to online voting system is that we can consume our time and can vote from anywhere through online. The technology/platform used were C# as a programming language, Microsoft SQL server 2012 and Microsoft azure as a cloud.

In the year 2014, Yirendra Kumar Yadav, Saumya Batham, Mradul Jain, Shivani Sharma presented a concept of electronic voting system which ensures authentication, authorization and accounting [20]. Approach collects information from VIDAl and uses this information in validating electorate, casting electorate vote during electronic voting procedure. Only necessary information is collected from VIDAl that has some significance in AAA. The issue of voter frauds, voting accuracy, reliable voting, time delays, increasing electorate participation providing user friendly interface etc., thus providing a framework for fair elections was addressed. The technology/platform used were Module (EVRM), EVS, Electorate Information Interface, Member's Information Server.

The systematic representation of above online voting related work is given in Table 1. The existing approaches are categorized based on the basic concepts involved in the mechanisms. The emphasis is on the concepts used by the concerned authors, the proposed methodology, issues addressed and the technology or platform used. Their claims are also highlighted.

Ref No	Name of Authors, Paper Title, Year	Proposed Methodology	Issue Addressed	Technology/ Platform Used
[1]	Vivek S K, et.al., "E-Voting System using Hyperledger Sawtooth", 2020	A secure, transparent and decentralized e-voting system is proposed using the Hyperledger Sawtooth blockchain framework. Restricted access of the system through election polling stations allows voters to cast their votes, which are recorded in the immutable blockchain state.	Fairness and reliability of the election procedure due to nil possibility of vote manipulation.	Angular 8, Node.js, Amazon RDS, and Sawtooth blockchain, Python with the APIs, Docker technology, Amazon Web Services (AWS)
[2]	Shubham Gupta, Divanshu Jain, Milind Thomas Themalil, "Electronic Voting Mechanism using Microcontroller ATmega328P with Face Recognition", 2021	The voter is registered into the system database well before the time of election. Now at the voting time, In the first step voter must verify his/her government identity such as Aadhar card or voting card with his/her proper picture, once it is verified, he/she moves to the second step. In second step voter has to go under the face reorganization process. Once the corresponding matching or verification is done, the voter will move to next step to cast vote to the	The central office of election department can monitor the data in more reliable way so that no discrepancy/ modification can take place later.	PyCharm, JetBrains IDE using Python, IoT, ThingSpeak, Open Source Computer Vision Library OpenCV, Arduino.

		candidate from the electronic voter machine. The cast vote is shown on display for the satisfaction of voters. Then the voting data is continuously uploaded on ThingSpeak server.		
[3]	Mrs. Nilam Kate, Mrs. J.V.Katti, "Security of Remote Voting System based on Visual Cryptography and SHA" 2016	The mentioned technique is a web-based voting system that permits voter to vote independent of location. Security of any information is concerning issue and it very sensitive for online voting system. Mentioned system does not use any biometric application, without using biometric function authentication of the voter is done. In this system votes are encrypted by AES encryption algorithm to provide the security.	It saves the time and improves the performance of system. The mentioned scheme is cost effective and at the same time satisfies the security requirements of an online voting system.	Visual cryptography and AES algorithm
[4]	Naseer Abdulkarim Jaber Al-Habeeb, Dr. Nicolae Goga, Haider Abdullah Ali1, Sarmad Monadel Sabree Al-Gayar, "A New E-voting System for COVID-19 Special Situation in Iraq", 2020	In this paper, the authors have described an application for m-voting targeting the specific conditions of Iraq in the COVID situation. In the current society, the application of which we are talking about, can also be seen as a significant help for a numerous amount of countries during the pandemic of COVID- 19.	The application is based on Mobile technology. Mobile technology is chosen motivated by the fact that although people do not have computers, almost everyone has a mobile phone in Iraq.	Android Studio, PHP-Restful Services for the BackEnd Component and MySQL database.
[5]	Roopak T M, Dr. R Sumathi, "Electronic Voting based on Virtual ID of Aadhar using Blockchain Technology", 2020	The mentioned scheme provides the secured e-voting system by using biometric details and VID (Virtual ID) of voters obtained from the Aadhar database to cast the Vote and also using the digital signature as the key for the encryption of the votes inside the block.	Aadhar integration to the evoting system overcomes the duplication or tampering of votes.	Blockchain Technology
[6]	Claudia Garc´ıa-Zamora, Francisco Rodr´ıguez-Henr´ıquez, and Daniel Ortiz-Arroyo, "SELES: An e-Voting System for Medium Scale Online Elections" 2005	A secure electronic voting system for medium scale on-line elections (SELES). This system efficiently implements a security communication protocol offering protection against double voting and others frauds while avoiding any private voting channel. This system has been tested in a distributed and heterogeneous Internet network comprised by workstations, laptops and PDA nodes interacting through wired and wireless connections.	SELES accomplishes all the standard properties of conventional voting systems, namely, accuracy, democracy, privacy, verifiability, simplicity, flexibility and double voting detection. SELES has been designed to deal with communication failures, thus achieving a certain degree of robustness.	Digital Signature Algorithm (DSA),
[7]	Ganesh Prabhu S, et.al., "Smart Online Voting System" 2021	The face scanning system is used to record the voters face prior to the election and is useful at the time of voting. The offline voting system is improvised with the help of RFID tags instead of voter id. This system also enables the user the citizens to see the results anytime which can avoid situations that pave way to vote tampering.	This paper focusses on a system where the user can vote remotely from anywhere using his/her computer or mobile phone and doesn't require the voter to got to the polling station through two step authentication of face recognition and OTP system.	Arduino Uno, LCD Display, RFID, Push Button
[8]	Robert Kofler, Robert Krimmer, Alexander Prosser, "Electronic Voting: Algorithmic and Implementation Issues" 2003	The paper develops an algorithm designed to guarantee anonymity of the voter and to avoid the risk of manipulation of votes. The algorithm is based upon the strict separation of voter registration and submission of votes, which implies that certain information has to be stored on a secure media.	The paper discusses the security criteria and possible implementation options for secure storage.	Electronic Voting, Electronic Democracy, Internet Applications
[9]	Mohamed Ibrahim, et.al. "ElectionBlock: An Electronic Voting System using Blockchain and Fingerprint Authentication", 2021	In this paper we discuss the design and development of ElectionBlock, a voting system that provides its own blockchain, running on a centralized network of nodes, with the integration of a biometric scanner, to maintain vote integrity and distinguish between registered and unregistered voters. This scheme allows data immutability while providing the user with security and control over their ballot. Experimental results demonstrate the potential for scalability of the system to handle a high volume of votes from multiple servers while maintaining data integrity, performance, and security.	This paper address the considerations taken to develop and implement the centralized and independent blockchain network for use as a voting platform with the integration of biometrics for the purpose of enhanced user security.	Merkle tree, SHA-256 algorithms, ElectionBlock blockchain
[10]	S. Jehovah Jireh Arputhamoni, Dr. A. Gnana Aravanan, "Online Smart Voting System Using Biometrics Based Facial and Fingerprint Detection on Image Processing and CNN", 2021	Online website has a prevented IP address generated by the government of India for election purpose. People should register the name and address in the website. Election commission will collect the fingerprint and face image from the voters. The database or server will store the images. When the images are obtained on the casting day, it will be compared with database and provides a secured voting on the Election Day. System utilizes faces and fingerprints to unlock the voting system, similar to the mobile phone are used.	The current system requires the physical presence of voter, which is inconvenient to many voters. The process consumes less time as well. Using the detection of face and fingerprint images, the number of fake voters can be reduced.	HTML, Visual Studio, CNNalgorithm,
[11]	Shaikh Mohammad Bilal, Prince Ramesh Maurya, "Online	The Voting System utilizing Android Application is progressively effective that the great technique to do a political decision. The task has build up an intuitive GUI board for casting a ballot framework. In addition,	This framework has better exactness contrasted with the conventional strategy for tallying.	Android application

	Voting System via Smartphone”, 2020	Apps Inventor 2 had been utilized to structure the whole task. The database that made additionally does the computation of the information before move the information to the official site.		
[12]	Awsan A. H. Othman, et.al. “Online Voting System Based on IoT and Ethereum Blockchain” 2021	The IoT and Blockchain have been used with this system to ensure that users’ data are protected from theft and prevent eavesdropping or vote tampering to guarantee the integrity of the voting. The blockchain encrypts votes in order to protect every vote from forgery. The system assists the concerned authorities in obtaining results quickly without delay, taking into account the differences in voting process between government and private organizations.	Governments can establish referendums or elections, and anyone who has reached the legal age and has a voting card issued by the government will be able to vote, thus we get rid of the traditional methods and dispense with ballot boxes, standing in long queues and delay counting the votes that cost governments a lot of time, effort and money.	IoT with Ethereum blockchain technology
[13]	Hanady Hussien , Hussien Aboelnaga, “Design of a Secured E-voting System”, 2013	The mentioned system a new EVS is presented. It utilizes Pailier cryptosystem and blind signature based on RSA as security tools. It consists of CTF that communicates with multiple local committee servers that distributed among poll stations. Each server is connected with group of embedded systems acting as voting machines. Pailier cryptosystem provides the secrecy requirement because of its additive homomorphic property, which allows CTF to tally the secret votes without decrypting them. The blind signature based on RSA blinds the votes and voter identity to achieve privacy and accuracy security requirements. The eligibility and uniqueness requirements are accomplished by the data stored in voter’s RFID.	This paper proposes a new e-voting system that fulfills the security requirements of e-voting. It is based on homomorphic property and blind signature scheme. The system satisfies the vital security requirements.	Pailier cryptosystem and blind signature based on RSA,
[14]	Dr. Z.A. Usmani, Kaif Patanwala, Mukesh Panigrahi, Ajay Nair, “Multi-Purpose Platform Independent Online Voting System”, 2017	In the above paper, the online voting system is a multi-purpose platform independent system which can be used by any organization and government to conduct the elections. The user just needs to have national identification number such as Aadhaar card number and any operating system smartphone which has a barcode scanning feature implanted in them.	As the system is an online based application, the user can vote from their current location. The voter doesn’t have to go to a polling booth to cast their vote, thereby encouraging a greater number of people to participate in voting.	Platform Independent
[15]	Smita B. Khaimar, P. Sanyasi Naidu, Reena Kharat, “Secure Authentication for Online Voting System”, 2016	We propose a new secure authentication for online voting system by using biometrie feature and steganography. Voter is asked to enter a password at the time of registration. Password is converted into secret message using timestamp and hashing. This secret message is stored in image using steganography.	In this model, a person can also vote from outside of his/her allocated electorate or from his/her chosen location.	SHA256 algorithm, Hash code
[16]	Bhuvanapriya.R, Rozil banu.S, Sivapriya.P, Kalaiselvi. V. K. G, “Smart Voting” 2017	The mentioned system has three phases. First the details of the persons who are above 18years are extracted from aadhar card database. Automatically a new voter id with necessary details will be created and an intimation will be given to the persons through their e-mail. At the time of voting, the user can specify their id and password. To ensure more security, finger prints of the voter is used as the main authentication resource. As soon as they cast their vote, their voter id and other details will be erased automatically and the aadhar card details which they used will be tracked and will be locked to access. This is done to preserve the security.	When people cast their vote, the results will be updated automatically and on the same day of election, the results will also be published. Also, our mentioned system supports the online voting too.	Biometric and steganographic authentication, RSA algorithm
[17]	Cesar R. K, et.al., “Web 2.0 E-Voting System Using Android Platform”, 2010	This paper describes two experiences: The first experiment, called International Direct Digital Election (ID2E), is made for testing the viability for the international voting by mobiles using SMS protocol, using Web 2.0 tools to facilitate discussions about the election main theme. The second experiment is the construction of a voting prototype using Android platform smart phones, with applications and vote collecting databases available on dynamic web pages, trying to simulate de Identical Ballot Boxes strategy described in two papers of Alefragis, Lounis, Triantafillou and Voros.	The two experiments are part of a mentioned e-Voting methodology, and were made with the final objective of surveying scenarios about international voting processes, to give some experimental base for future e-Voting projects at international level.	Web 2.0 social networks Android smart phones, ID2E,
[18]	Mohammad Hosam Sedky, Essam M. Ramzy Hamed, “A Secure e-Government's e-Voting System” 2015	The mentioned Voting Model System overcomes the issue of security obstacles. Before sending the final result report per polling station automatically to the district's committee, a paper copy of the final result report of each polling station will be audited manually by every candidate' representative and signed it as a proof of his agreement of the final result report. Then, it will be delivered physically to the propagate district's committee Office. Judges in each district's committee office will compare the polling station	The proposed e-voting system is designed especially to solve the cost effective, accuracy and transparency problems in a highly secured approach. Security evaluation experiments are performed successfully to the mentioned system proving that it satisfies privacy, accuracy,	ID card Reader, Fingerprint Reader, Visual Studio 2010, C# software and SQL Server 2008

		physically delivered result report with the automatically received report to be sure that the results are accumulated successfully. The same process will be done in all the higher committees till the final results from the Governorates will be submitted automatically and physically signed to the HEC.	reusability, eligibility and integrity.	
[19]	Ramya Govindaraj, Kumaresan P, K.Sree harshitha, "Online Voting System using Cloud", 2020	In this specific research mentioned idea is to implement online voting system with features like the schemes that the specific party has implemented, based on the features we are going to vote.	The main reason we need to shift from normal voting system to online voting system is that we can consume our time and can vote from anywhere through online.	C# as a programming language, Microsoft SQL server 2012 and Microsoft azure as a cloud.
[20]	Yirendra Kumar Yadav, Saumya Batham, Mradul Jain, Shivani Sharma, "An Approach to Electronic Voting System using UIDAI", 2014	In this paper we present a concept of electronic voting system which ensures authentication, authorization and accounting. Approach collects information from VIDAI and uses this information in validating electorate, casting electorate vote during electronic voting procedure. Only necessary information is collected from VIDAI that has some significance in AAA.	Our approach addresses issues such as voter frauds, voting accuracy, reliable voting, time delays, increasing electorate participation providing user friendly interface etc., thus providing a framework for fair elections.	Module (EVRM), EVS, Electorate Information Interface, Member's Information Server

III. Problem Statement

Put together, the information technology, big data, AI, blockchain technology, cloud technology, IoT, and smart devices – can make a substantial and positive synergic effect on effectively address the online voting system. Therefore, we hope that the online system convergence will be deployed to facilitate the voters so as to reduce the frauds, increase the voting accuracy, more reliable voting, lesser time delays, increasing electorate participation providing user friendly interface etc., thus providing a framework for fair elections. The development of an overall effective online voting system is anticipated in near future.

After the literature survey, it is found that there are multiple methods tackling various issues of voting systems. However none of them provides the best and optimum solution. Also, a safe, secure & reliable voting system is necessary for a good democracy. This motivates us to do research on this topic.

We have decided to tackle the issue of voter authentication using three methods viz. Face recognition, fingerprint scanning and QR codes, considering their resourcefulness, reliability and utility. In our proposed approach, we have used the fingerprint module, wherein we've used encryption technique using SHA 256 and decryption technique using brute force. It matches the key and select correct one. For face recognition we've used the face recognition library. For QR code we've used one google link. We've used Google Colab for data accessing, CV2 for image, Shutil for crop the image, csv for excel file, PIL for image formation, pandas for RGB format of image.

IV. PROBLEM ANALYSIS

We have analyzed several approaches to implement an online voting system and discusses them with a view to voter anonymity and protection from manipulations. Though, the literature consists of a lot many research contributions, but here we have critically analyzed and summarized twenty significant research works and projects addressing it.

Following are our findings from the literature review:

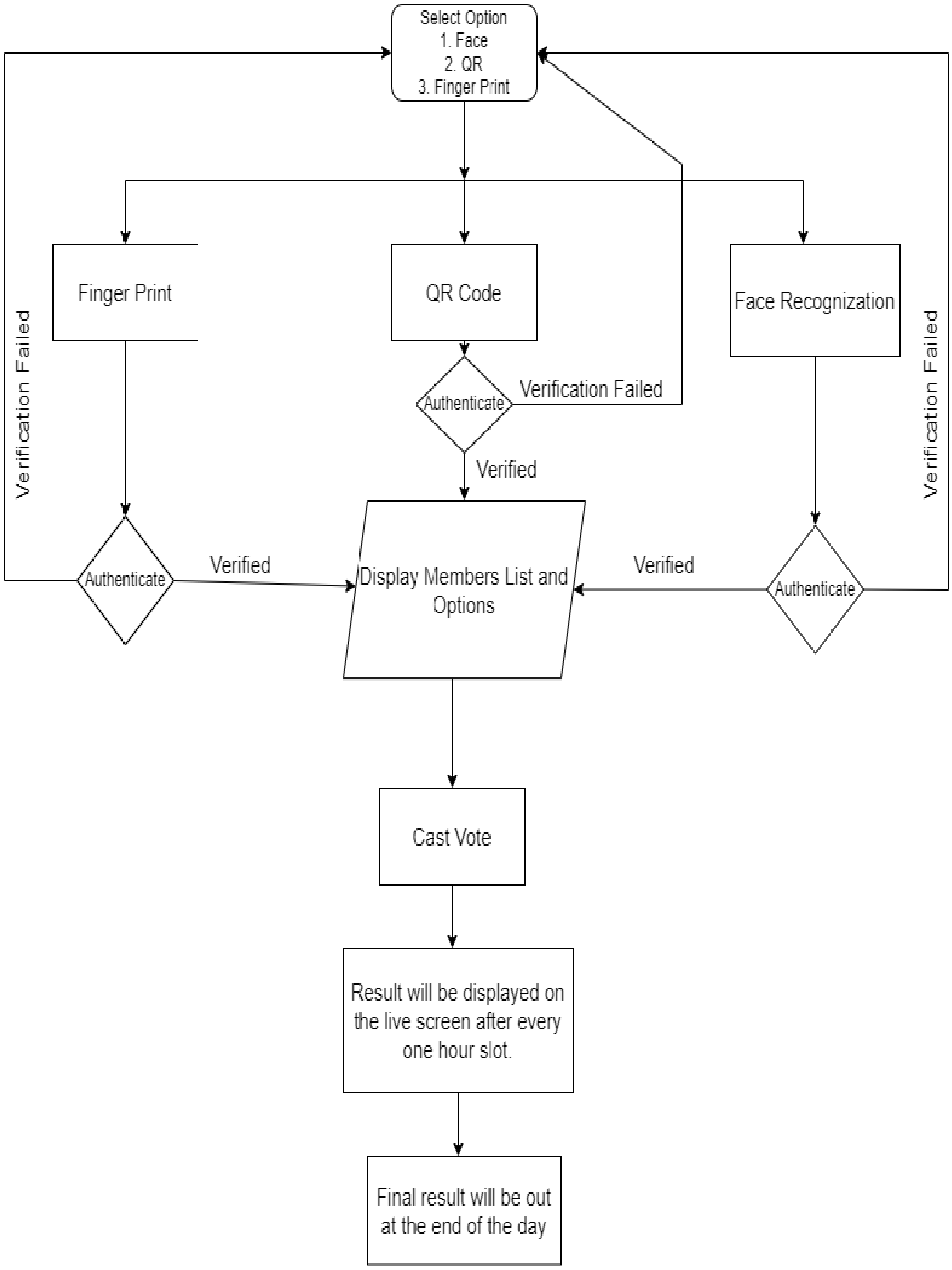
- BlockChain Technology works towards anonymity and decentralization.
- UID, face recognition and fingerprint scanning techniques addresses the issue of voter authentication.
- Web-based voting system that permits voter to vote independent of location
- The face scanning system can be used to record the voters face prior to the election and is useful at the time of voting.
- The offline voting system can be improvised with the help of RFID tags instead of voter id.
- QR code or barcode scanning feature provides multi-purpose platform independent voting system.

V. PROBLEM FORMULATION

After studying the literature, the problem can be formulated as follows

- Biometric fingerprint and camera devices are used in the Electronic Voting machine for voter verification.
- We can design a finger print based voting machine where there is no need for the user to carry his ID which contains his required details.
- The voter had to first enroll himself/herself using his/her fingerprint, photo scanning and QR code
- At the time of voting, the voter needs only to place his finger on the device, thus allowing the acquisition of an on-spot fingerprint from the voter which serves as an identification.
- This finger print reader reads the details from the tag.
- This data is passed onto the controlling unit for the verification.
- The controller fetches the data from the reader and compares this data with the already existing data stored during the registration of the voters.
- For generating QR code we use one google link. For face recognition we use library of algorithm in which we use face algorithm for verification. Data of QR code and face recognition is stored on server on My SQL database
- If the data matches with the pre-stored information of the registered fingerprint, the person is allowed to cast his vote.
- If not, a warning message is displayed on LCD and the person is barred from polling his vote.
- The vote casting mechanism is carried out manually using the push buttons.
- LCD is used to display the related messages, warnings and ensuing results

VI. ALGORITHM FLOWCHART



VII. WORKING OF PROPOSED APPROACH

The software requirements of the server are:

- Operating System: Windows XP/7/8/10
- Coding Language: PHP
- Camera access

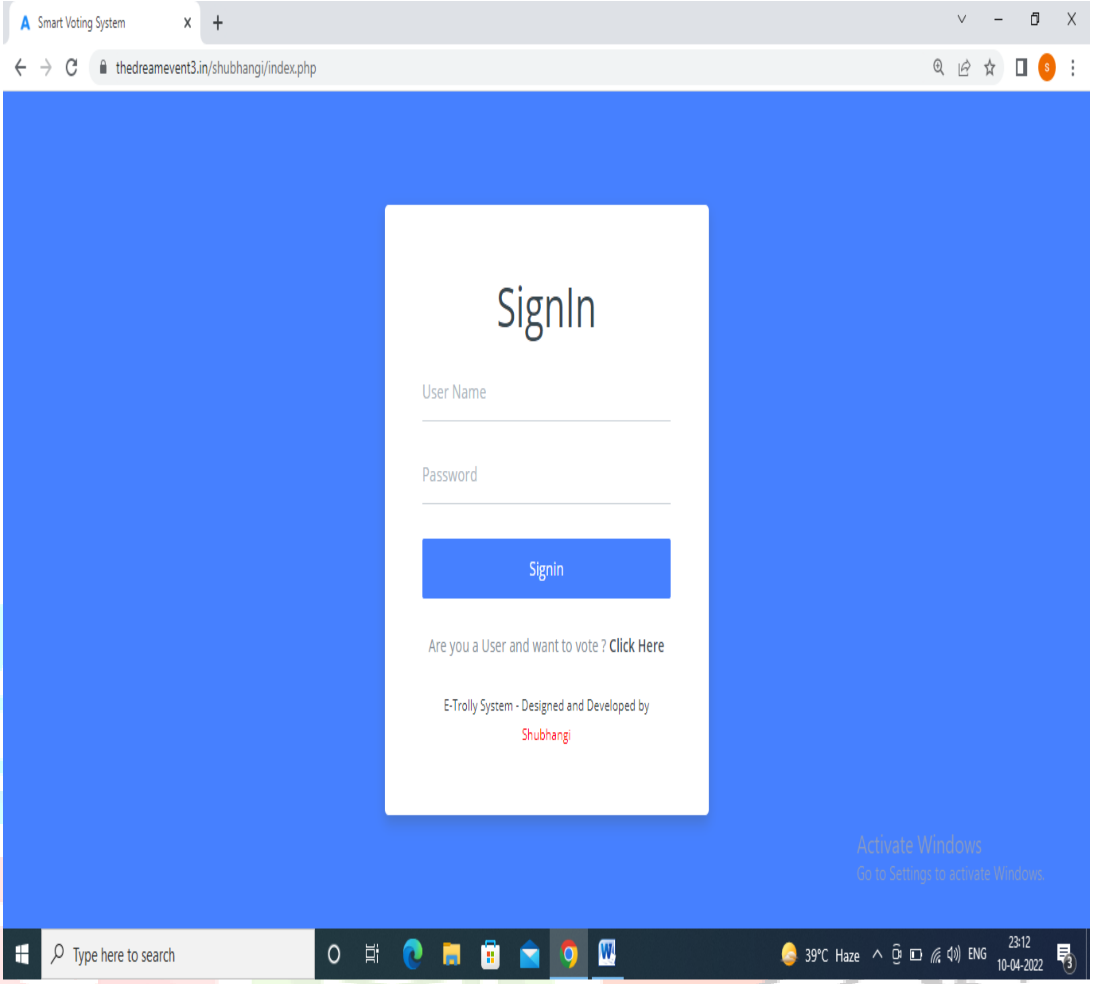
The hardware requirements are:

- Finger print module
- Node MCU
- Microcontroller
- LCD

Working of Software

In our approach we have three modules in the voting process.

- Super Admin
- Admin
- User



Are you a User and want to vote ? Click Here

E-Trolly System - Designed and Developed by Shubhangi

Activate Windows
Go to Settings to activate Windows.

Fig. 1: Login Page for all the 3 modules

Super admin has to enroll all the election areas and candidates for the area

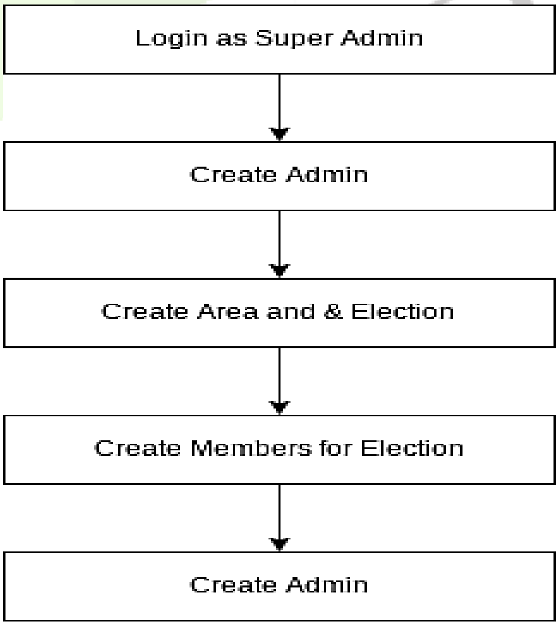
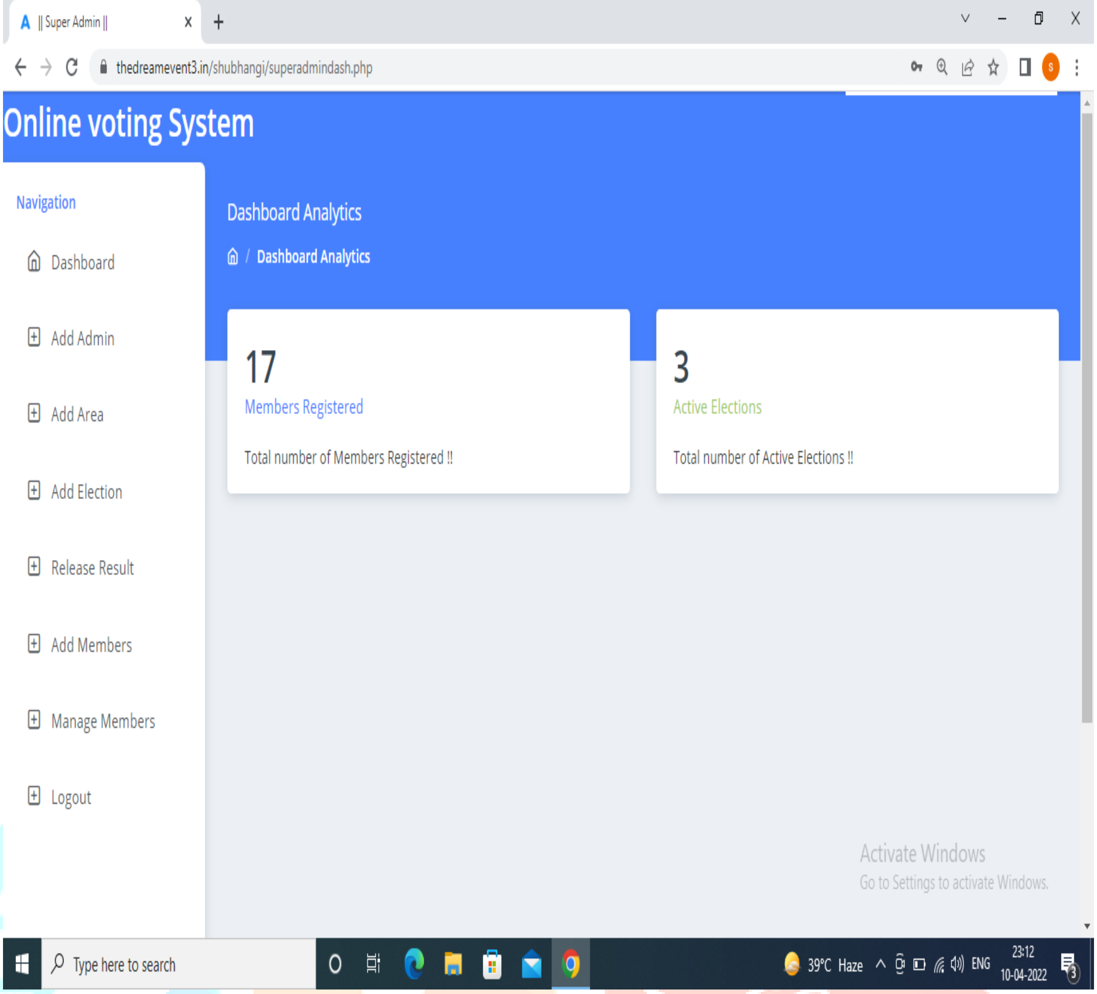


Fig. 2: Super -Admin Flowchart



A || Super Admin ||

thedreamevent3.in/shubhangi/superadmindash.php

Online voting System

Navigation

Dashboard

Add Admin

Add Area

Add Election

Release Result

Add Members

Manage Members

Logout

Dashboard Analytics

Dashboard Analytics

17

Members Registered

Total number of Members Registered !!

3

Active Elections

Total number of Active Elections !!

Activate Windows

Go to Settings to activate Windows.

Type here to search

39°C Haze ENG 23:12 10-04-2022

Fig. 3: Super Admin page

Admin have to add the voters via a voter enrollment form along with their photographs, fingerprints and QR code.

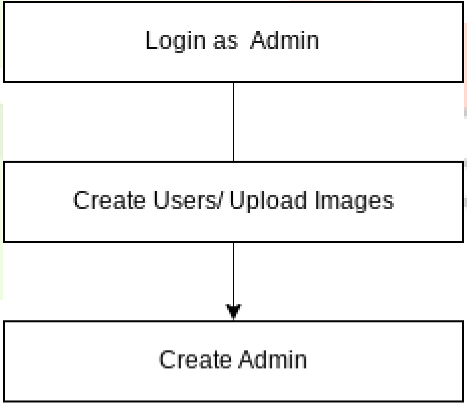
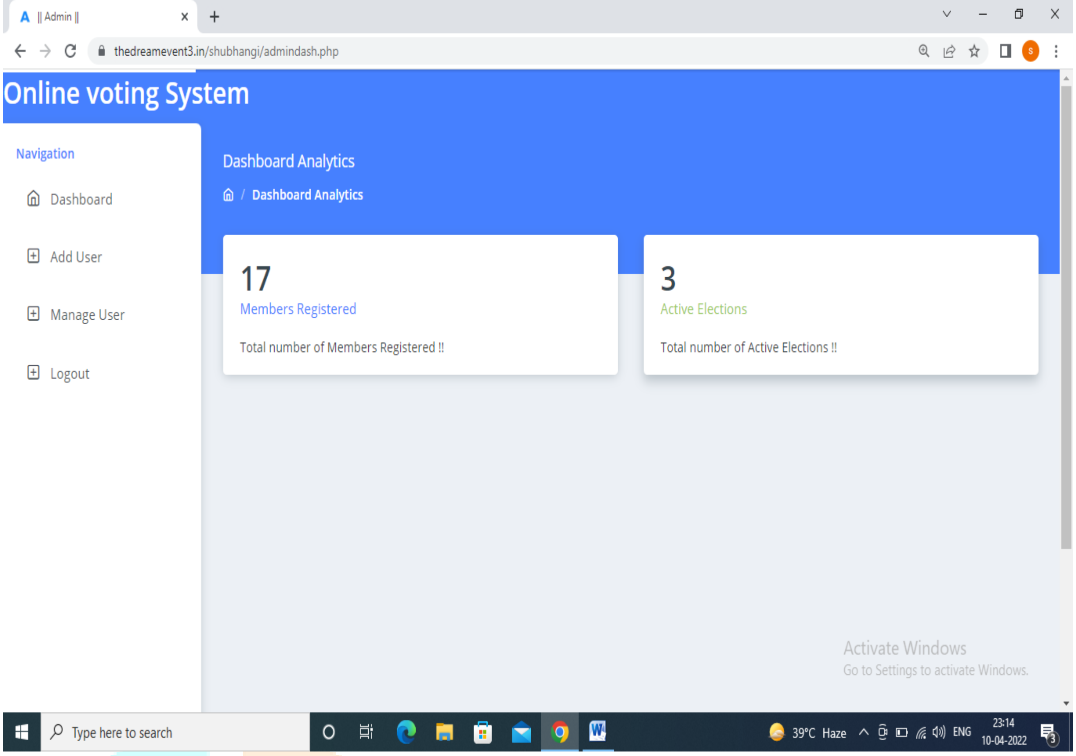


Fig. 4: Admin Flowchart



Online voting System

Dashboard Analytics

Dashboard Analytics

17
Members Registered
Total number of Members Registered !!

3
Active Elections
Total number of Active Elections !!

Activate Windows
Go to Settings to activate Windows.

Fig. 5: Admin Page

At the time of elections, the voter can generate their one time EPP code using face recognition, QR code and fingerprint. This EPP code is used to access the user module.

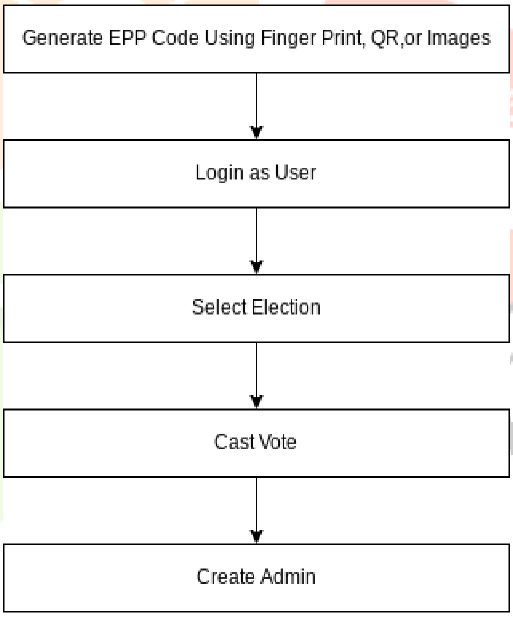


Fig. 6: Voter Flowchart

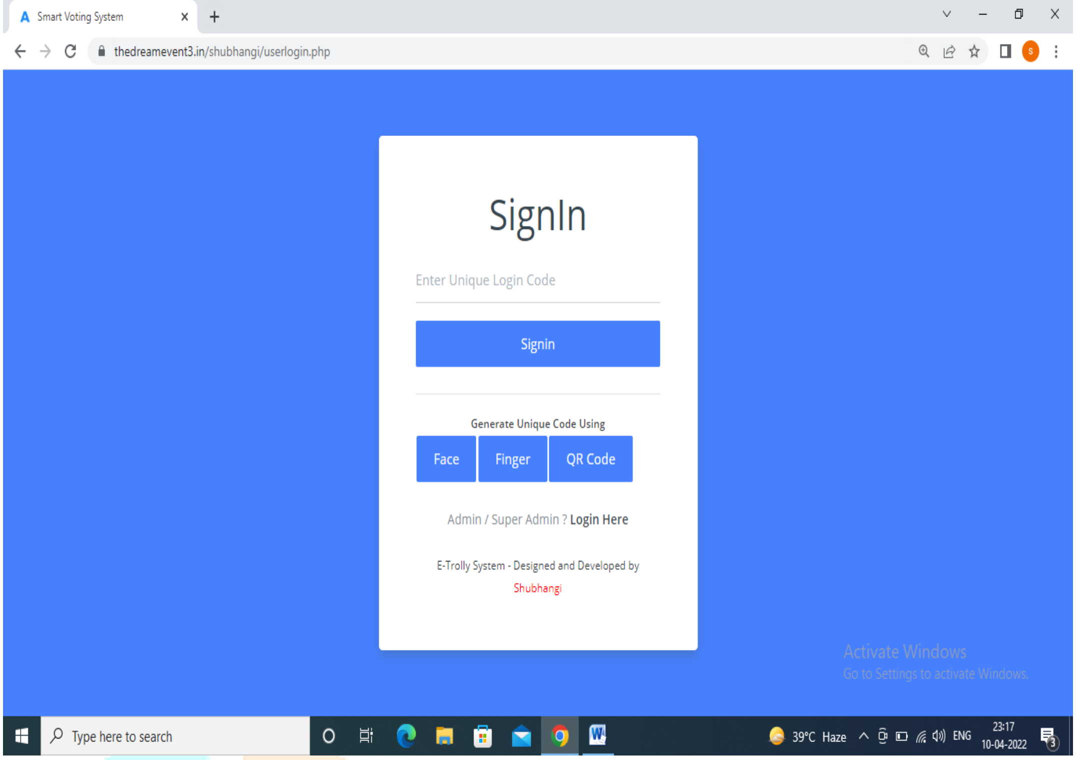

Smart Voting System
thedreamevent3.in/shubhangi/userlogin.php
SignIn
Enter Unique Login Code
Signin
Generate Unique Code Using
Face
Finger
QR Code
Admin / Super Admin ? Login Here
E-Trolly System - Designed and Developed by
Shubhangi
Type here to search

Fig. 7: Login page for voters

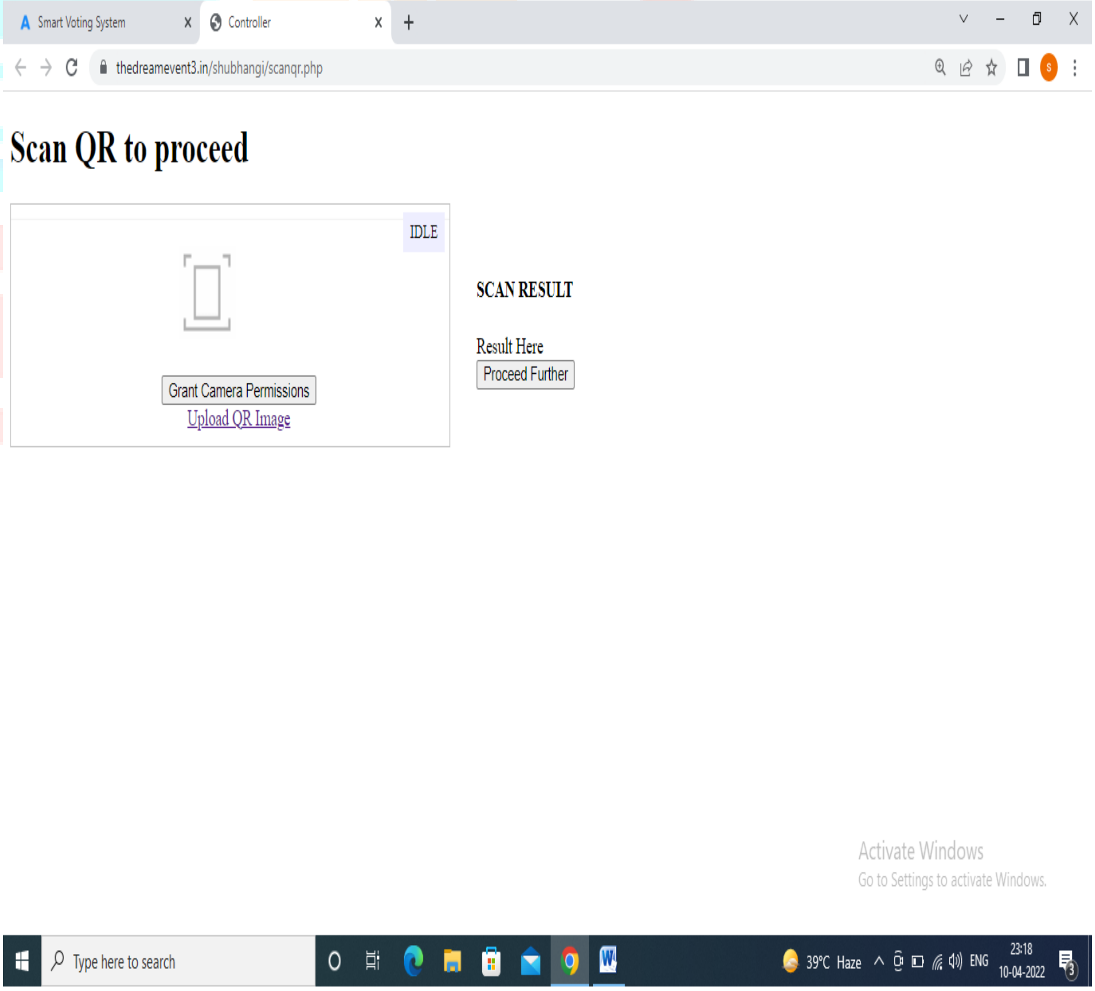
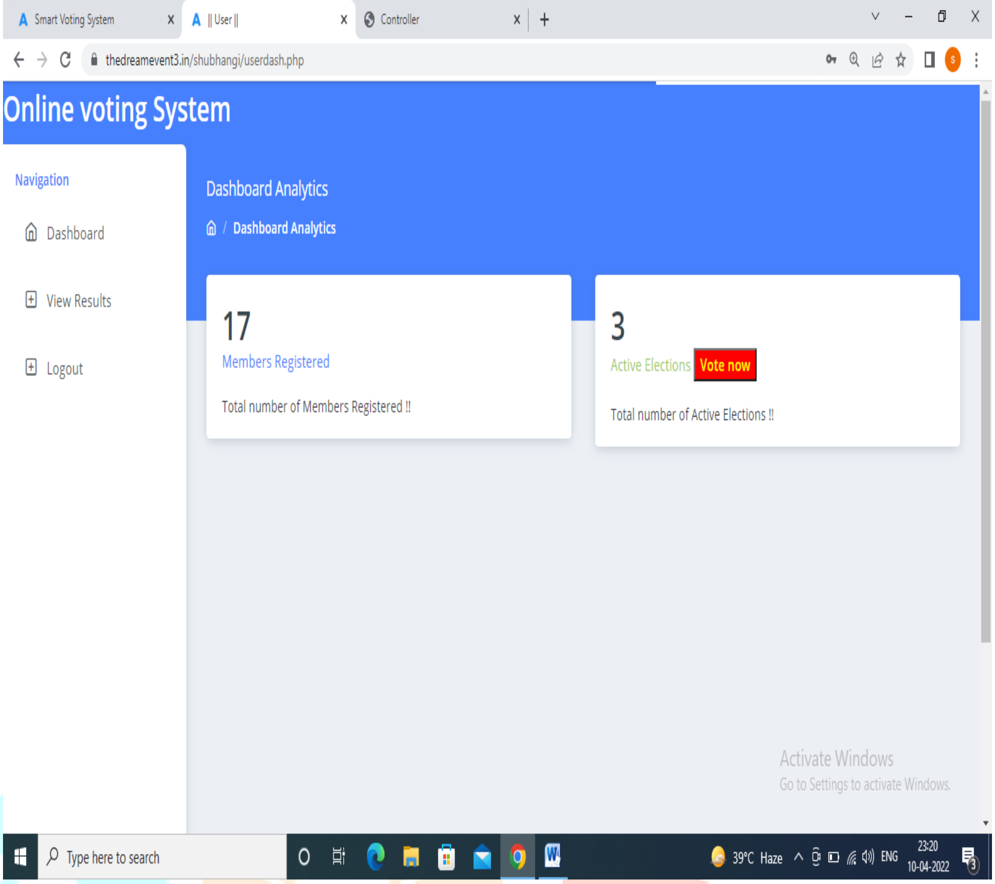


Fig. 8: Add or scan QR code for voter

In user module the voter can cast their vote to a particular member.
Super admin can release the result at the end of the elections. The results can be viewed in the user panel by the voters.



Online voting System

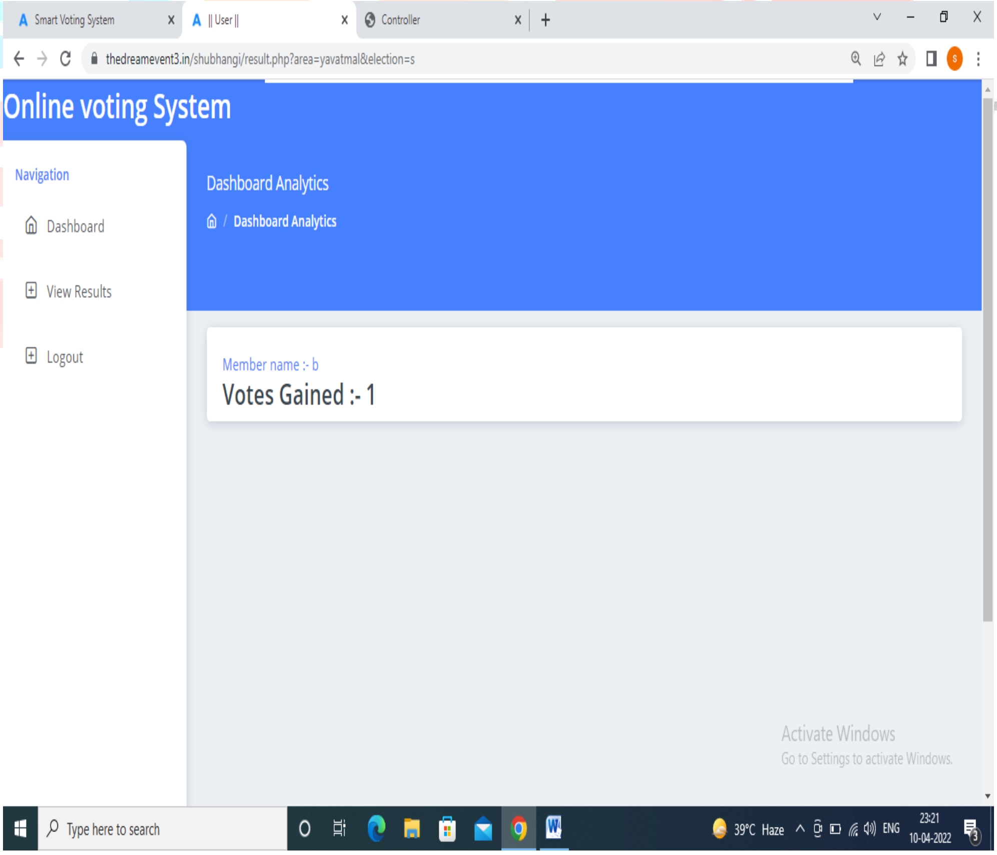
Dashboard Analytics

Dashboard Analytics

17
Members Registered
Total number of Members Registered !!

3
Active Elections
Total number of Active Elections !!

Fig. 9: For voter to cast their vote



Online voting System

Dashboard Analytics

Dashboard Analytics

Member name :- b
Votes Gained :- 1

Fig. 10: Voting Results

Working of Hardware

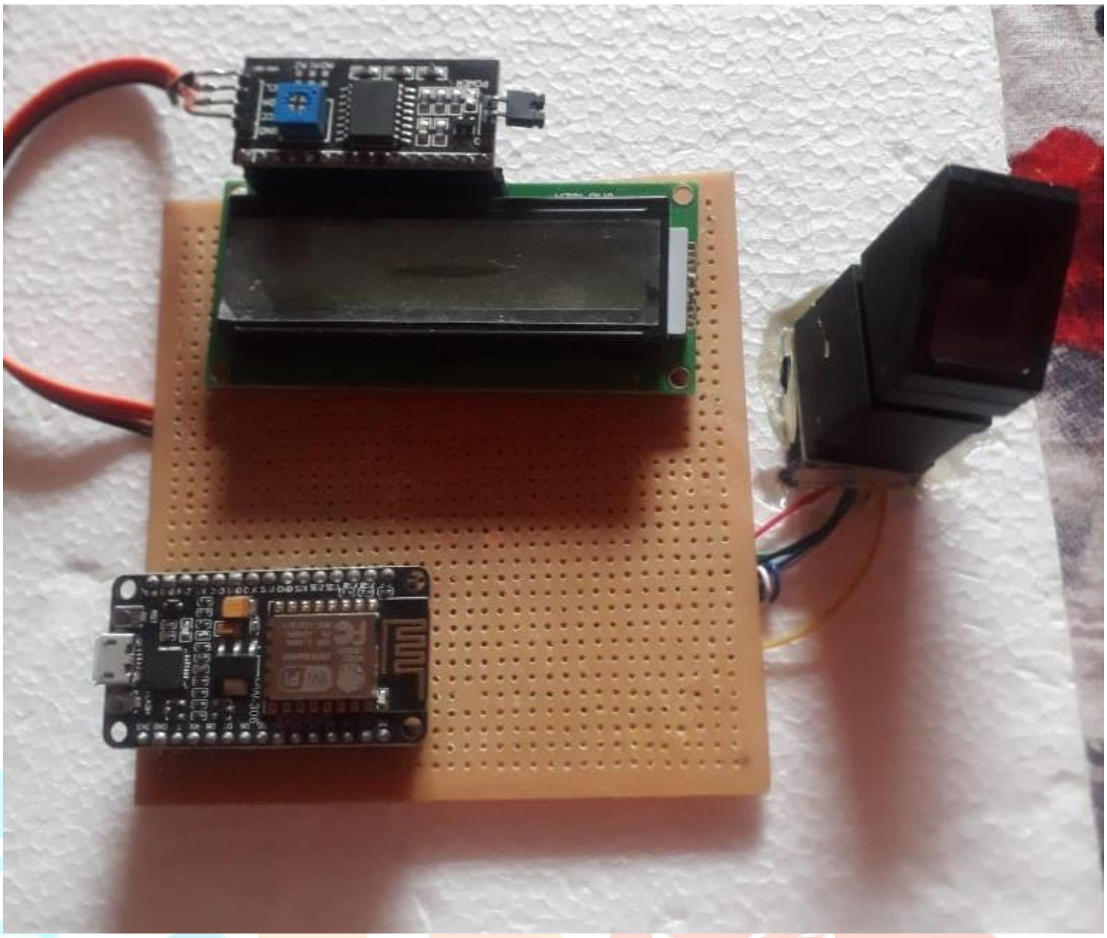


Fig. 11: Fingerprint Scanning System

R305 Fingerprint Sensor Module

Security with biometrics can be done with the help of R305 Fingerprint M odule. This fingerprint sensor module will make adding fingerprint detection and verification super simple. These modules are typically used in safes – there's a high powered DSP chip that does the image rendering, calculation, feature-finding, and searching. Connect to any microcontroller or system with TTL serial, and send packets of data to take photos, detect prints, hash, and search. You can also enroll new fingers directly- up to 162 fingerprints can be stored in the onboard FLASH memory. There's a red LED in the lens that lights up during a photo so you know its working.

Fig. 12: Fingerprint sensor

Fingerprint Sensor Module Working:

Fingerprint processing includes two parts: fingerprint enrollment and fingerprint matching (the matching can be 1:1 or 1: N). When enrolling, a user needs to enter the finger two times. The system will process the two -time finger images, generate a template of the finger based on processing results and store the template. When matching, the user enters the finger through an optical sensor and system will generate a template of the finger and compare it with templates of the finger library. For 1:1 matching, system will compare the live finger with specific template designated in the Module; for 1: N matching, or searching, the system will search the whole finger library for the matching finger. In both circumstances, the system will return the matching result, success or failure.

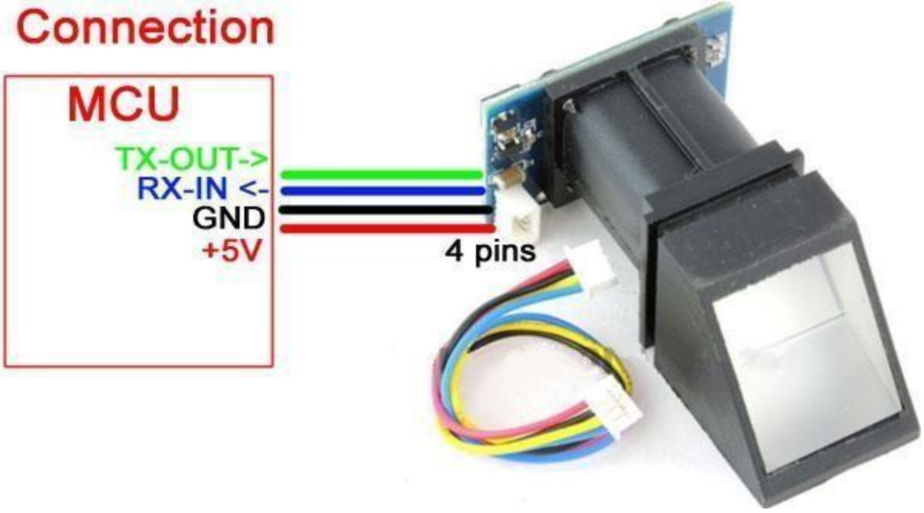


Fig. 13: Fingerprint sensor pinots

Features:

- Supply voltage: 3.6 – 6.0VDC
- Operating current: 120mA max
- Peak current: 150mA max
- Fingerprint imaging time: <1.0 seconds
- Window area: 14mm x 18mm
- Signature file: 256 bytes
- Template file: 512 bytes
- Storage capacity: 162 templates
- Safety ratings (1-5 low to high safety)
- False Acceptance Rate: <0.001% (Security level 3)
- False Reject Rate: <1.0% (Security level 3)
- Interface: TTL serial
- Baud rate: 9600, 19200, 28800, 38400, 57600 (default is 57600)
- Working temperature rating: -20C to +50C
- Working humidy: 40%-85% RH
- Full Dimensions: 56 x 20 x 21.5mm
- Exposed Dimensions (when placed in box): 21mm x 21mm x 21mm triangular
- Weight: 20 grams

NODEMCU ESP8266

NodeMCU is an open-source Lua based firmware and development board specially targeted for IoT based Applications. It includes firmware that runs on the ESP8266 Wi-Fi SoC from Espressif Systems, and hardware which is based on the ESP-12 module.

The NodeMCU ESP8266 development board comes with the ESP-12E module containing ESP8266 chip having Tensilica Xtensa 32-bit LX106 RISC microprocessor. This microprocessor supports RTOS and operates at 80MHz to 160 MHz adjustable clock frequency. NodeMCU has 128 KB RAM and 4MB of Flash memory to store data and programs. Its high processing power with in-built

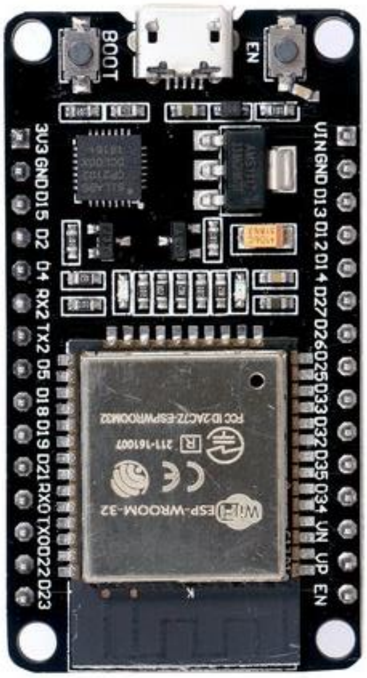

BOOT
EN
ESP-WROOM-32
3V3 GND D15 D2 D4 RX2 TX2 D5 D18 D19 D21 RX0 TX0 D22 D23
VIN GND D13 D12 D14 D27 D26 D25 D33 D32 D35 D34 VN VP EN

Fig. 14: NodeMCU

Wi-Fi / Bluetooth and Deep Sleep Operating features make it ideal for IoT projects.

The NodeMCU Development Board can be easily programmed with Arduino IDE since it is easy to use. NodeMCU can be powered using Micro USB jack and VIN pin (External Supply Pin). It supports UART, SPI, and I2C interface.

Applications of NodeMCU

- Prototyping of IoT devices
- Low power battery operated applications
- Network projects
- Projects requiring multiple I/O interfaces with Wi-Fi and Bluetooth functionalities

ESP8266 NodeMCU Pinout

The ESP8266 NodeMCU has total 30 pins that interface it to the outside world. For the sake of simplicity, we had make groups of pins with similar functionalities. The connections are as follows:

Power Pins: There are four power pins viz. one VIN pin & three 3.3V pins. The VIN pin can be used to directly supply the ESP8266 and its peripherals, if you have a regulated 5V voltage source. The 3.3V pins are the output of an on-board voltage regulator. These pins can be used to supply power to external components. GND is a ground pin of ESP8266 NodeMCU development board.

I2C Pins: These pins are used to hook up all sorts of I2C sensors and peripherals in your project. Both I2C Master and I2C Slave are supported. I2C interface functionality can be realized programmatically, and the clock frequency is 100 kHz at a maximum. It should be noted that I2C clock frequency should be higher than the slowest clock frequency of the slave device.

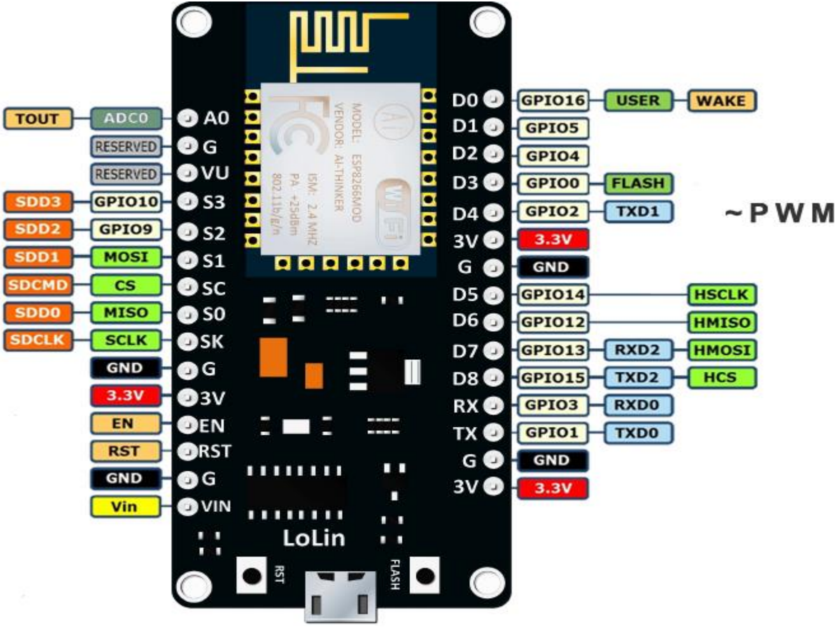


Fig. 15: NodeMCU Pin Diagram

GPIO Pins: ESP8266 NodeMCU has 17 GPIO pins which can be assigned to various functions such as I2C, I2S, UART, PWM, IR Remote Control, LED Light and Button programmatically. Each digital enabled GPIO can be configured to internal pull-up or pull-down, or set to high impedance. When configured as an input, it can also be set to edge-trigger or level-trigger to generate CPU interrupts.

ADC Channel: The NodeMCU is embedded with a 10-bit precision SAR ADC. The two functions can be implemented using ADC viz. Testing power supply voltage of VDD3P3 pin and testing input voltage of TOUT pin. However, they cannot be implemented at the same time.

UART Pins: ESP8266 NodeMCU has 2 UART interfaces, i.e. UART0 and UART1, which provide asynchronous communication (RS232 and RS485), and can communicate at up to 4.5 Mbps. UART0 (TXD0, RXD0, RST0 & CTS0 pins) can be used for communication. It supports fluid control. However, UART1 (TXD1 pin) features only data transmit signal so, it is usually used for printing log.

SPI Pins: ESP8266 features two SPIs (SPI and HSPI) in slave and master modes. These SPIs also support the following general-purpose SPI features:

- 4 timing modes of the SPI format transfer
- Up to 80 MHz and the divided clocks of 80 MHz
- Up to 64-Byte FIFO

SDIO Pins: ESP8266 features Secure Digital Input/Output Interface (SDIO) which is used to directly interface SD cards. 4-bit 25 MHz SDIO v1.1 and 4-bit 50 MHz SDIO v2.0 are supported.

PWM Pins: The board has 4 channels of Pulse Width Modulation (PWM). The PWM output can be implemented programmatically and used for driving digital motors and LEDs. PWM frequency range is adjustable from 1000 μs to 10000 μs, i.e., between 100 Hz and 1 kHz.

Control Pins are used to control ESP8266. These pins include Chip Enable pin (EN), Reset pin (RST) and WAKE pin.

- **EN pin** – The ESP8266 chip is enabled when EN pin is pulled HIGH. When pulled LOW the chip works at minimum power.
- **RST pin** – RST pin is used to reset the ESP8266 chip.
- **WAKE pin** – Wake pin is used to wake the chip from deep-sleep.

ESP8266 Development Platforms

There are a variety of development platforms that can be equipped to program the ESP8266. You can go with Espruino – JavaScript SDK and firmware closely emulating Node.js, or use Mongoose OS – An operating system for IoT devices (recommended platform by Espressif Systems and Google Cloud IoT) or use a software development kit (SDK) provided by Espressif or one of the platforms listed on WiKiPedia. Fortunately, the amazing ESP8266 community took the IDE selection a step further by creating an Arduino add-on. This ESP8266 add-on for Arduino is based on the amazing work by Ivan Grokhotkov and the rest of the ESP8266 community.

Liquid Crystal Display (LCD)

LCD 16×2 Pin Configuration and Its Working

Nowadays, we always use the devices which are made up of LCDs such as CD players, DVD players, digital watches, computers, etc. These are commonly used in the screen industries to replace the utilization of CRTs. Cathode Ray Tubes use huge power when compared with LCDs, and CRTs heavier as well as bigger. These devices are thinner as well power consumption is extremely less. The LCD 16×2 working principle is, it blocks the light rather than dissipate. This article discusses an overview of LCD 16X2, pin configuration and its working.

The term LCD stands for liquid crystal display. It is one kind of electronic display module used in an extensive range of applications like various circuits & devices like mobile phones, calculators, computers, TV sets, etc. These displays are mainly preferred for multi-segment light-emitting diodes and seven segments. The main benefits of using this module are inexpensive; simply programmable, animations, and there are no limitations for displaying custom characters, special and even animations, etc.

The 16×2 LCD pinout is shown below.

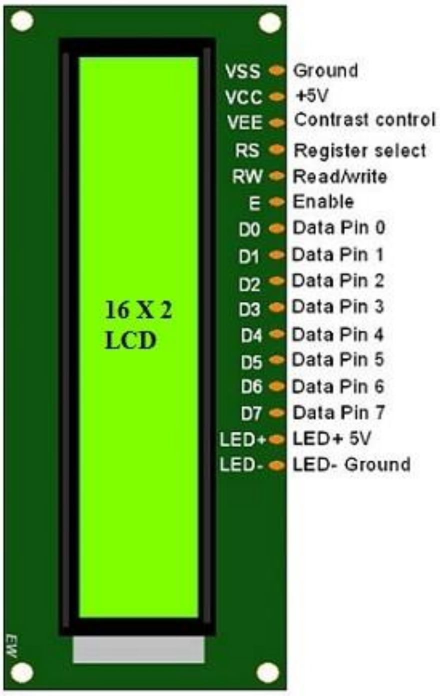


Fig. 16: LCD 16×2 Pin Diagram

- Pin1 (Ground/Source Pin): This is a GND pin of display, used to connect the GND terminal of the microcontroller unit or power source.
- Pin2 (VCC/Source Pin): This is the voltage supply pin of the display, used to connect the supply pin of the power source.
- Pin3 (V0/VEE/Control Pin): This pin regulates the difference of the display, used to connect a changeable POT that can supply 0 to 5V.
- Pin4 (Register Select/Control Pin): This pin toggles among command or data register, used to connect a microcontroller unit pin and obtains either 0 or 1(0 = data mode, and 1 = command mode).
- Pin5 (Read/Write/Control Pin): This pin toggles the display among the read or writes operation, and it is connected to a microcontroller unit pin to get either 0 or 1 (0 = Write Operation, and 1 = Read Operation).
- Pin 6 (Enable/Control Pin): This pin should be held high to execute Read/Write process, and it is connected to the microcontroller unit & constantly held high.
- Pins 7-14 (Data Pins): These pins are used to send data to the display. These pins are connected in two-wire modes like 4-wire mode and 8-wire mode. In 4-wire mode, only four pins are connected to the microcontroller unit like 0 to 3, whereas in 8-wire mode, 8-pins are connected to microcontroller unit like 0 to 7.
- Pin15 (+ve pin of the LED): This pin is connected to +5V Pin 16 (-ve pin of the LED): This pin is connected to GND.

Features of LCD16x2

- The features of this LCD mainly include the following.
- The operating voltage of this LCD is 4.7V-5.3V
- It includes two rows where each row can produce 16-characters. The utilization of current is 1mA with no backlight
- Every character can be built with a 5×8 pixel box The alphanumeric LCDs alphabets & numbers
- Is display can work on two modes like 4-bit & 8-bit These are obtainable in Blue & Green Backlight
- It displays a few custom generated characters

Registers of LCD

A 16×2 LCD has two registers like data register and command register. The RS (register select) is mainly used to change from one register to another. When the register set is ‘0’, then it is known as command register. Similarly, when the register set is ‘1’, then it is known as data register.

1. Command Register

The main function of the command register is to store the instructions of command which are given to the display. So that predefined tasks can be performed such as clearing the display, initializing, set the cursor place, and display control. Here commands processing can occur within the register.

2. Data Register

The main function of the data register is to store the information which is to be exhibited on the LCD screen. Here, the ASCII value of the character is the information which is to be exhibited on the screen of LCD. Whenever we send the information to LCD, it transmits to the data register, and then the process will be starting there. When register set =1, then the data register will be selected.

16×2 LCD Commands

The commands of LCD 16X2 include the following.

For Hex Code-01, the LCD command will be the clear LCD screen For Hex Code-02, the LCD command will be returning home

For Hex Code-04, the LCD command will be decrement cursor For Hex Code-06, the LCD command will be Increment cursor

For Hex Code-05, the LCD command will be Shift display right For Hex Code-07, the LCD command will be Shift display left

For Hex Code-08, the LCD command will be Display off, cursor off For Hex Code-0A, the LCD command will be cursor on and display off For Hex Code-0C, the LCD command will be cursor off, display on

For Hex Code-0E, the LCD command will be cursor blinking, Display on For Hex Code-0F, the LCD command will be cursor blinking, Display on For Hex Code-10, the LCD command will be Shift cursor position to left

For Hex Code-14, the LCD command will be Shift cursor position to the right For Hex Code-18, the LCD command will be Shift the entire display to the left For Hex Code-1C, the LCD command will be Shift the entire display to the right

For Hex Code-80, the LCD command will be Force cursor to the beginning (1st line) For Hex Code-C0, the LCD command will be Force cursor to the beginning (2nd line) For Hex Code-38, the LCD command will be 2 lines and 5×7 matrix

VIII. ADVANTAGES

This system allows only authenticated voting than the existing equipment as the person is identified based on his Fingerprint which is unique to each individual.

Cost effective

Low power consumption

Less manpower required

Time conscious

Avoids invalid voting

Ease of transportation due to its compact size.

Convenient on the part of voter

IX. DISADVANTAGES

Before voting the user has to enroll first.

Sensitivity of face recognition module causes sometimes Combine character error.

X. APPLICATIONS

Before voting the user has to enroll first.

Sensitivity of face recognition module causes sometimes Combine character error.

XI. CONCLUSION

World is becoming completely digitized. As a part of digitization, here voting is also digitized. One of the benefits of this project is that it reduces the time taken to announce the result.

The system is made more secure by introducing face recognition, fingerprint and QR code verification. This system allows one person to vote only once. Multiple voting is not allowed.

References

[1] Vivek S K, et.al., “E-Voting System using Hyperledger Sawtooth”, International Conference on Advances in Computing, Communication & Materials (ICACCM), pp. 29-35, 2020,

[2] 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

[3] Mrs. Nilam Kate, Mrs. J.V.Katti, “Security of Remote Voting System based on Visual Cryptography and SHA”, International Conference on Computing Communication Control and automation (ICCUBEA), 2016

[4] Naseer Abdulkarim Jaber Al-Habeeb, Dr. Nicolae Goga, Haider Abdullah Ali1, Sarmad Monadel Sabree Al-Gayar, “A New E-voting System for COVID-19 Special Situation in Iraq”, The 8th IEEE International Conference on E-Health and Bioengineering – EHB, 2020.

[5] 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

[6] Claudia Garc´ıa-Zamora, Francisco Rodr´ıguez-Henr´ıquez, and Daniel Ortiz-Arroyo, “SELES: An e-Voting System for Medium Scale Online Elections”, Proceedings of the Sixth Mexican International Conference on Computer Science (ENC’05), 2005

[7] Ganesh Prabhu S, et.al., “Smart Online Voting System”, 7th International Conference on Advanced Computing and Communication Systems (ICACCS), pp. 632-634, 2021

[8] Robert Kofler, Robert Krimmer, Alexander Prosser, “Electronic Voting: Algorithmic and Implementation Issues”, Proceedings of the 36th Hawaii International Conference on System Sciences (HICSS’03), 2003

[9] Mohamed Ibrahim, et.al. “ElectionBlock: An Electronic Voting System using Blockchain and Fingerprint Authentication”, IEEE 18th International Conference on Software Architecture Companion (ICSA-C), pp. 123-127, 2021

[10] S. Jehovah Jireh Arputhamoni, Dr. A. Gnana Aravanan, “Online Smart Voting System Using Biometrics Based Facial and Fingerprint Detection on Image Processing and CNN”, Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV), 2021

[11] Shaikh Mohammad Bilal, Prince Ramesh Maurya, “Online Voting System via Smartphone”, Proceedings of the 3rd International Conference on Advances in Science & Technology (ICAST), 2020

[12] Awsan A. H. Othman, et.al. “Online Voting System Based on IoT and Ethereum Blockchain”, International Conference of Technology, Science and Administration (ICTSA), 2021

[13] Hanady Hussien , Hussien Aboelnaga, “Design of a Secured E-voting System”, International Conference on Computer Applications Technology (ICCAT), 2013

[14] Dr. Z.A. Usmani, Kaif Patanwala, Mukesh Panigrahi, Ajay Nair, “Multi-Purpose Platform Independent Online Voting System”, International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS), 2017

[15] Smita B. Khaimar, P. Sanyasi Naidu, Reena Kharat, “Secure Authentication for Online Voting System”, International Conference on Computing Communication Control and automation (ICCUBEA) 2016

[16] Bhuvanapriya.R, Rozil banu.S, Sivapriya.P, Kalaiselvi. V. K. G, “Smart Voting”, 2nd International Conference on Computing and Communications Technologies (ICCCT), pp. 143-147, 2017

[17] Cesar R. K, et.al., “Web 2.0 E-Voting System Using Android Platform”, IEEE International Conference on Progress in Informatics and Computing, pp. 1138-1142, 2010

[18] Mohammad Hosam Sedky, Essam M. Ramzy Hamed, “A Secure e-Government's e-Voting System”, Science and Information Conference, pp. 1365-1373, 2015

[19] Ramya Govindaraj, Kumaresan P, K.Sree harshitha, “Online Voting System using Cloud”, International Conference on Emerging Trends in Information Technology and Engineering (ic-ETITE), pp. 1-4, 2020

[20] Yirendra Kumar Yadav, Saumya Batham, Mradul Jain, Shivani Sharma, “An Approach to Electronic Voting System using UIDAI”, International Conference on Electronics and Communication Systems (ICECS -2014), 2014