Mrs.V.Subitha, 2023, 11:2
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

International Journal of Science, Engineering and Technology

An Open Access Journal

Advanced and Secure Bio-Metric Voting System

Assistant Professor Mrs.V.Subitha, V. Pravinsha, T .Rajitha Roja, T.V. Vibitha, A.S Priya Dharshini
Stella Mary's College of Engieneering

Abstract- This project proposes finger print voting system with Arduino. The main objective of this project is to design and develop biometric based voting machine using Aadhar authentication. The current voting process has safety problems such as authenticity of voters. The main objective is to enhance the security in order to prevent duplication and provide a system which reduces the burden for people on conducting a voting. In this project we used fingerprint for authentication, and for fingerprint authentication we use Aadhar card database. Now a day's everybody has Aadhar card with unique Aadhar number hence it is highly secures compare to current existing system. Fingerprint is one of the unique identities of a human being which is being used in the Aadhar system. Thus, by implementing this system, user can put their vote with fingerprint instead of paper without doubting about their security. Voting Using Fingerprint reduce the polling time, it provides easy and accurate counting without human. In this proposed system, we get the details of voter from AADHAR CARD database. Fingerprint module is automated method of verifying a matching fingerprint and it can provide a security. The voter at the polling booth has to show his Finger and scan his finger on fingerprintmodule. Fingerprint module scan his/her fingerprint and send to controller for matching scan fingerprint with stored AADHAR CARD database. If the fingerprint match with already stored voter AADHAR CARD database, then he/she is valid for polling sections and voter is allowed to pull his/her vote. If not, message is displayed on LCD and the voter is not allowed to poll his/her vote. If any voter comes to vote for the second time the buzzer makes a sound thus avoiding fake voting.

Keywords- Fingerprint voting system, Arduino, Biometric authentication, Aadhar card database, Security enhancement, Voter authentication, Duplicate prevention, Fingerprint module, LCD display, Automated verification

I. INTRODUCTION

N India two types of methods are used for voting. First method is secret ballot paper in which lots of paper are used and second method is electronic voting machine which is used since 2003[1]. In EVM votes gets registered electronically which eliminates the use of ballot paper to vote in election. Today security is major concern and it also needs to ensure that someone can't vote twice. We are presenting a new Voting System with fingerprint scanning that will overcome the drawbacks of current voting methods that are used in India. In current voting system voter has to go pooling booth and show their voter ID then officer check their ID from the list that he has. If it's information is matched then officer allow voter to cast their vote this system is time consuming and there may be possibility of occurring mistake[2] i.e. fake voting, errors in counting of votes or may user can vote twice Hence to avoid such type of problems we designed biometric voting machine using Aadhar

authentication. In this system there is no need to carry voting card simply voter has to press their thumb on fingerprint scanner the system will check whether it matches with Aadhar database and if it's does not match then system will not allow voter to vote and show 'INVALID VOTER' message on LCD screen.

The Biometrics technologies are used to measure and an- alyze personal characteristics. These characteristics include fingerprints, voice patterns, hand measurements, irises and others, all used to identify human characteristics and to verify identity[3]. These biometrics or characteristics are tightly connected to an individual and cannot be forgotten, shared, stolen or easily hacked. These characteristics can uniquely identify a person, replacing or supplementing traditional secu- rity methods by providing two major improvements: personal biometrics cannot be easily stolen and an individual does not need to memorize passwords or codes[4]. Biometrics gives you an alternative and higher security compared to passwords or pin identification due to the fact that passwords and pin can easily be compromised. Authentication by biometric verification is becoming increasingly common in corporate and public security systems and applications. We propose a system where we use biometric Fingerprint Voting system for general public during elections. System records votes based on registered fingerprints[5]. It is interactive GUI for adding efficiency and for automating organization procedures. Fingerprint authentication refers to the automated method of verifying a match between two human fingerprints.

A new Electronic Voting System with Fingerprint scanning that will overcome the drawbacks of the current voting meth- ods. Aadhar card can store all the details about user. If the Aadhar card can be scanned by the scanner and put the thumb print on the fingerprint scanner if it's matched the user can allow the vote or the fingerprint does not match the buzzer will be ringing and passed message to register phone number. The key purpose of this paper is to create a scheme, which requests the voters to provide their fingerprints as personality identification proof. The system reads the fingerprint pattern and it compares with the database stored previously. In case information recorded is available in the database and included in the stored information systems, the voting scheme will permit the users to access the system and cast their votes.

In case the data of the patterns wasn't matching with the stored information, then the schemes will affect the display of authorities and security will take its course.

A biometric defines the technology used to measure science and evaluate the biology information. In the present form of information transfer, which is done electronically, users can access data electronically and hence making services to introduced using electronic devices. As such, this aids in the enhancement of the electronic scheme with the assistance novel technologies in the voting procedure. The information gathered about the election findings is processed, recorded and stored by the above data as digital data. Over the past few years, data security was determined by the ministry of defense who obtained instructions from the federal government. The human body segment like DNA, voice patterns, hand pat- terns and fingerprints are determined using the authentication methods. The electronic services and data privacy ensure that data communication will assure maximum privacy and security to information. The term biometric came from the biological behavior of human being and technology. Some behavior of the biometric voting framework includes the finger printers, hand and face geometry, voice detection and hand- writing detection. The biometric voting scheme, the pattern is determined and might be free and ringing. In this scheme, we have created the thumb impression scheme for voter's authentication and identification for advanced security mea- sures. For further verification process it is connected to the database collected by the government (Aadhar) in our case. Human beings have one and unique thumb impression, which determines the accuracy of enhanced privacy. In a nation, the thump impression database has been created for the users via the Aadhar database. In that case, the

identification of repetition or illegal cases is possible and protected. The voters have no register of their own fingerprints in the election booth. The technology behind fingerprints is utilized to establish the whole scheme. The major purpose of this project is to establish a scheme, which requests users to provide their fingerprint as an identification proof.

The fingerprint-based voting framework encodes the infor- mation pattern thus comparing it to the information that has been stored in the databases. In case the information exists in the database, it can match with the past stored information. The voting framework will permit the voters to compute into the scheme and cast their votes. In that case, the system provides the false users to be caught at the site and the law gets restored, the rights and individuality of a citizen is saved. The Fingerprint optical scanner is the input module used as a controller. Once the users have completed the first stage verification process, they require inputting their thumb in the scanner. In case the fingerprint matches the database of the controllers, the switch of the scheme will only be allowed by the controllers for vote casting. Fingerprint use is convenient and safe for the purposes of ensuring security during the voting process. The systematic procedure for verification, identification and authentication allows fingerprints to act as digitalized passwords and data, which will never be lost, stolen, misused or forgotten. We are using microcontrollers to emancipate the minimal technology outcomes and benefits across the world. Certain countries are still following the ballot sheets for casting the votes. But the scenario here is maximum population and minimum.

II. LITERATURE REVIEW

The focus of this paper is to design and develop a biometric enabled biometric electronic voting machine. The proposed biometric electoral voting system allows the user to scan fingerprint and iris so that his or her credentials can be compared to existing fingerprint and iris images already stored in the system's database. Counting is going on right away, making the voting process more efficient, faster and safer.[6] This system requires the identification of the voter Aadhar card, the voter's thumb impression as well as the iris image. Voter's complete data, including all voters' fingerprint and iris image, is collected and stored in the database. While voting, the voter gives their Aadhar card details and puts eye in front of the iris camera and finger inside a fingerprint scanner, the system looks for the seal already provided in the data base, and then compares the iris image to authenticate the voter's identity. If the data matches, the system commands the voter to vote through the electronic voting machine. If the fingerprints do not match, the voting presiding officer looks for the registration, or the iris image does not match after the fingerprint match, the voter is not allowed to vote, consider it vote rigging.

We propose electronic voting authentication scheme, which is a key management mechanism for electronic voting system intended to limit the number of attacks on a polling station and strengthen the security control. The motivation is to diversify security requirements of messages exchanged between polling stations. There are different types of messages exchanged be- tween polling stations and each type of message has different security needs. A security mechanism developed on the basis of a single key is not enough to ensure the diverse security needs of voting network. In electronic voting authentication scheme, every polling station is responsible to support three different types of keys. These are global key, pairwise key, and individual key. The global keys are public keys shared with all polling stations in the voting network. The pairwise key can be used for communication with polling stations. Individual keys will be used for communication with the server. To ensure authentication of local broadcast, electronic voting authentication scheme uses one-way key chains in a well-organized way. The support of source authentication is a visible advantage of this scheme. We examine the authentication of electronic voting authentication scheme on numerous attack models. The measurement demonstrates that electronic voting authentication scheme is very operative in protecting against numerous elegant attacks such

as wormhole attack, Sybil attack, and HELLO Flood attack. The proposed system is evaluated and the results demonstrate that the proposed system is practical and secure as compared to the direct recording electronic and manual systems.

In almost all democratic countries, voting is practiced regularly. The most common method used in elections is the voting based on paper. The paper ballots are used and the voters cast their vote physically. The counting mechanism in these elections is manual. The voter's intent is estimated from a physical ballot. The results are tabulated manually after the in- terpretation and reading of physical ballots. The project-based voting scheme may be used for recounts. The recounts are applicable where automated or mechanical counting systems are used. While this type of voting systems is dominated by most of the election systems conducted in different countries in terms of problems arose during the election. The reports of fraud or cheat are frequently highlighted in these elections. The reports may be due to voting itself or errors in counting procedure. Many problems were documented in the previous years about the election process. The time required for the election process and the result announcement are other limitations of the manual voting systems.

Conventional security systems used either knowledge based methods (passwords or PIN), and token-based methods (pass- port, driver license, ID card) and were prone to fraud because PIN numbers could be forgotten or hacked and the tokens could be lost, duplicated or stolen. To address the need for robust, reliable, and foolproof personal identification, authentication systems will necessarily require a biometric component. The word "biometrics" comes from the Greek language and is derived from the words bio (life) and metric (to measure). Biometric systems use a person's physical characteristics (like fingerprints, irises or veins), or behavioral characteristics (like voice, handwriting or typing rhythm) to determine their identity or to confirm that they are who they claim to be. Biometric data are highly unique to each individual, easily obtainable non-intrusively, time invariant (no significant changes over a period of time) and distinguishable by humans without much special training. Enrollment and authentication are the two primary processes involved in a biometric security system. During enrollment, biometric measurements are captured from a subject and related information from the raw measurements is gleaned by the feature extractor, and this information is stored on the database. During authentication, biometric information is detected and compared against the database through pattern recognition techniques that involve a feature extractor and a biometric matcher working in cascade A typical automated iometrics-based identification system consists of the six major components depicted.

The data acquisition component acquires the biometric data in digital format by using a sensor. The second and third components of the system are optional, based on the system's storage requirements. The fourth component employs a feature extraction algorithm to produce a feature vector whose components are numerical characterizations of the underlying biometrics. The fifth component of the system is the matcher which compares feature vectors to produce a score which indicates the degree of similarity between the pair of biometrics data under consideration. The sixth component of the system is a decision-maker that can be programmed to accommodate system specifications. Perhaps the most important application of accurate personal identification is securing limited access systems from malicious attacks. Among all the presently employed biometric techniques, fingerprint identification systems have received the most attention due to the long history of fingerprints and their extensive use in forensics. This paper deals with the issue of selection of an optimal algorithm for fingerprint matching in order to design a system that matches required specifications in performance and accuracy. Two competing algorithms were compared against a common database using MATLAB simulations.

Every nation around the world with democratic legislative elects its rulers using their respective voting systems. Different types of mechanisms are

employed for voting ranging from ballots to electronic voting machines. With ever increasing corruption all around us, specifically in the third world countries there is an urgent need to employ secure strategies to make the procedure of voting during elections free from any sort of rigging or other illegal interventions. Many attempts have been made by several people in the academic field to develop systems which promote secure means of voting. Using fingerprint for authenticated entry to enter the voting procedure has been proposed in several articles. Ideas of web-based voting where the voters are allowed to cast their votes using the voting website or e-voting with physical entities (fingerprint, voice recognition) through computer network have been put forward. Several models with GSM alert and updating along with implementing iris recognition and finger vein sensing apart from fingerprint verification for authentication purpose have also been discussed. In some of them, proposals of enrolling the fingerprint to create a database following which during the elections the test fingerprints are matched against the available ones in the pre-created database, which on successful matching allows the voter to continue with voting have been presented. RFID tags have also been used as a valid id to conduct secure voting through the electric voting machines or implemented as a prototype of Aadhar id along with other security measures like finger vein sensing and using alcohol sensors to provide peaceful environment in polling booths. Android mobile OS has also been used to develop an application and fingerprint supported biometric control information to make voting process more secure. Using android smart mobile device makes the system more robust. Using of Aadhar QR code and UID numbers have the ability to provide added security measures to the voting system.

Online e-voting for casting vote online without going to any polling booth has also been proposed. This system claims to be helpful for voters staying away from their home cities but wish to exercise their right to vote. Along with these, proposals for online updating of votes using ZigBee or using the distributed server approach to add for added accuracy and reduced travelling distance have also been doing rounds in the academic circle concerned with developing a secure system of voting for conducting rigging-free elections. Many proposals involve using the Aadhar number for entry to the voting procedure or using the available Aadhar database instead of enrolling the fingerprints separately along with providing the feature of sending confirmation message to voters' mobile number. Another paper incorporates the display of Aadhar card details along with the fingerprint authentication. In order to make the system more secure, the voter is required to fill a registration form through user id and password which gets checked by the database server. If any of the previously stored information is wrong, the voter will not be allowed to participate in polling.

Every citizen or voter of India is allowed to exercise their right to express their choices regarding specific issues, pieces of legislation, citizen initiatives, constitutional amendments, recalls and/or to choose their government and political repre- sentative's through casting their votes. To allow the exercise of this right, almost all voting systems include the follow- ing steps: voter identification and authentication, voting and recording of votes cast, vote counting, publication of election results. Voter identification is required during electoral process. Security is a heart of e-voting process. Therefore, the necessity of designing a secure e-voting process is very important. A secured electronic voting machine using unique identification number i.e. AADHAR number has been developed. To provide additional security along with the AADHAR number biometric identification is used. At the time of voting in the elections, the voter authentication can be done through biometric pattern. If the biometric information of the voter matches the database of the AADHAR then the person is allowed to cast their vote. Transparency is additional advantage for the above system.

From the block diagram we see that there are two levels, Admin and Booth level. In the Admin level the voter registra- tion, scheduling the election date and time are done. This voter details are stored in the data base and are retrieved/fetched whenever

necessary. In the Booth level the election date and time are displayed in the home page, the voter finger print is checked and compared it with the pre stored information in the data base. If the finger print matches, the user is allowed to cast his/her vote. If the finger print does not match with any stored information or the vote has been already casted using the same authentication the screen will display it is invalid. Finger print is considered as one of the most popular biometric method used for human recognition. Every recognition in the globe is or with unique fingerprint and even twins are born with totally different finger print and is naturally unchangeable throughout the life. For that reason, finger print voting system has been made and person ID has been replaced with finger print. This finger print voting system is evaluated and implemented successfully. The evaluation of the system is made using different PC's with different specifications in order to stand on the system strength and weakness. The final result of finger print voting system is significant and compatible with other voting systems.

Biometrics are automated methods of recognizing a person based on a physiological or behavioral characteristic. Exam- ples of physiological characteristics include hand or finger im- ages, facial characteristics, speaker verification, and iris recog- nition. Behavioral characteristics are traits that are learned or acquired. Dynamic signature verification and keystroke dynamics are two examples of behavioral characteristics. The need for highly secure identification and personal verification technologies is now apparent. Biometric technologies are becoming the foundation of an extensive array of highly secure identification and personal verification solutions. The need for utilizing biometrics can be found in Federal, state and local governments, in the military, and in commercial applications. Enterprise-wide network security infrastructures, Government IDS, electronic banking, investing and other financial transac- tions, retail sales, law enforcement, and health and social ser- vices are already benefiting from these technologies. Specific issues related to the application of biometrics in a networked appliance and personal network environments are addressed below.

The Internet of Things (IoT) is a recent technology where electronic devices, software, sensors, vehicles, home appli- ances are interconnected with networks to transfer data without human or computer interaction. The problem in the existing system is, the electronic voting machines do not have any recent security measures by which the voter can verify their identity before casting the vote due to false voters can cast numerous duplicate or fake votes. So, the proposed system is Implemented using RFID and IoT (Internet of Things) to improvise the security mechanisms. Here, an active RFID tag is used in place of voter id where the system can scan the tag and matches with the fingerprints collected in the Aadhar database. The voter has to scan the RFID tag for the identification and further the voter has to confirm the identity with the fingerprints. It includes active reading equipment (reader) for reading data in RFID tag and finger print scanner is used in this voting machine for scanning finger prints. If the prints matched against the database gathered, the individuals can effectively cast their votes, if that's not the case, the buzzer will be alarmed to avoid casting of fake voters. A LCD is applicable in the process of displaying the corresponding information of the voter from the database, thus illegal voting or impersonating can be avoided since the finger prints is not the same for every individual. Due to the fact that the process of voting is connected with the Aadhar database, the system offers maximum security and efficiency. The system also transfers the configured data to the registered phone numbers from the voters' database.

III. EXISTING SYSTEM

EXISTING STYSTEM The Electronic voting system can be operated with the application of controllers, computers, and computerized voting tools in order to enhance the process of casting ballots during an election[7]. Mostly, this is applied in referring to the process that happens through the internet around the globe. The voting frameworks can be utilized to register participants, record votes and the tally ballots. The scheme can further be organized this

way. In part two, various forms of electronic voting system and how they have been implementing have been analyzed. In part three, the evaluation of electronic voting schemes around the world has been done. In part from, a detailed evaluation of advantages and disadvantages of the electronic voting systems in contrast to the traditional paper voting scheme has been given. The concluding section sums up the whole procedure[8]. The Electronic Voting (which is known as the E-Voting) is the microcontroller device designed to aid casting and counting votes that are casted during the elections. 3.1.1 DRAWBACKS The main issue of this scheme in that the checking and identification process of voters is considered manual and there is a big chance of illegalizes voting by the wrong mimic or user. Moreover, there is a high chance to more users casting their vote from one voter. It requires more man power or employing staffs. Unauthorized users can easily acquire passwords through different methods (hacking, guessing and so on.). 24 Retinal Scanner the problem of this device is, it is not user- friendly and the equipment cost is very high.

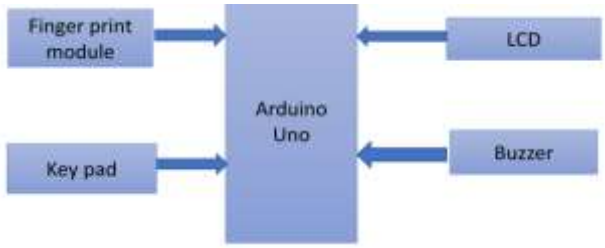

Fig 1 Existing system block diagram

IV. PROPOSED SYSTEM

In this proposed system, we get the details of voters from the AADHAR CARD database. This information is available on the government of India. We will store this voter information in a personal computer.[9] At the time of election, fingerprint accessing is done by using a fingerprint sensing module. The fingerprint module is an automated method of verifying a matching fingerprint and it can provide security. The voter at the polling booth has to show their finger and scan it on the fingerprint module. The fingerprint module scans their fingerprint and sends it to the controller for matching with the stored AADHAAR CARD database. If the fingerprint matches with the already stored voter AADHAAR CARD database, then the voter is valid for polling sections and allowed to cast their vote. If not, a message is displayed on the LCD and the voter is not allowed to poll their vote. If any voter comes to vote for the second time, the buzzer makes a sound, thus avoiding fake voting[10].

Fig.2. LCD Display

The advantages of this system include minimizing the cost of ballot printing and employing more staff. The human errors are reduced in the final voting results as well as minimizing the expenses of the election. There is more participation, faster processing, lower costs, precision placing, better access, and versatility for disabled voters. The system also shows results of casting votes[11].

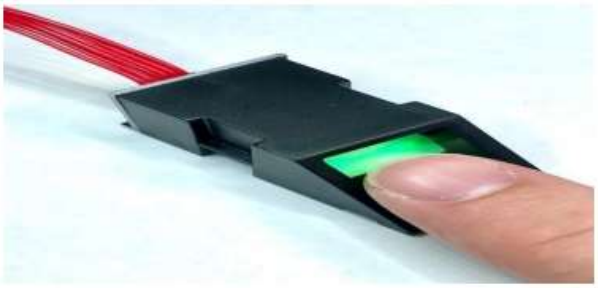

Fig 3. Fingerprint Sensor

The modules of the proposed system include a Fingerprint Sensor, LCD Display, Buzzer, and Push Button. The LCD Display is a flat-panel display or other electronically modu- lated optical device that uses the light-modulating properties of liquid crystals[12]. Liquid crystals do not emit light directly, instead using a backlight or reflector to produce images in color or monochrome. LCDs are available to display arbitrary images or fixed images with low information content, which can be

displayed or hidden.

The Fingerprint based lock system is a reliable and very secure lock that will not only ensure a safer environment but also ease lifestyle[13]. This system can prove very useful in housing buildings, large offices, universities and so on because it offers the flexibility to add more features to the system. Users do not need to implement many systems from scratch. They can simply use the fingerprint lock system because fingerprint scanning is more accurate and cost-effective[14]. It is also secure because fingerprint duplication is virtually impossible.

Push button switches are electrical actuators that close or open an electrical circuit by pressing the switch. These switches control a wide range of electronic circuits and are in the form of a button or a key. They are used to allow voters to vote for their favorite candidate[15].

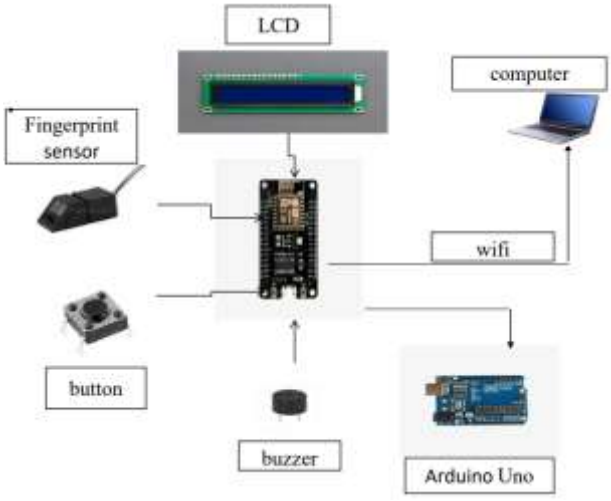

Fig.4. Block Diagram of proposed system

A buzzer is a kind of voice device that converts audio signals into sound. It is mainly used to prompt or alarm. According to different designs and applications, it can produce music sound, flute sound, buzzer, alarm sound, electric bell, and other different sounds[16]. Typical applications include sirens, alarm devices, fire alarms, air defense alarms, burglar alarms, timers, etc. It is widely used in household appliances, alarm systems, automatic production lines, low-voltage electrical equipment, electronic toys, game machines, and other products and industries[17].

An audio signaling device like a beeper or buzzer may be electromechanical, piezoelectric, or mechanical type. The main function is to convert the signal from audio to sound. Generally, it is powered through DC voltage and used in timers, alarm devices, printers, alarms, computers, etc. Based on various designs, it can generate different sounds like alarms, music, bells, and sirens[18].

The pin configuration of the buzzer includes two pins, namely positive and negative. The positive terminal is repre- sented with the '+' symbol or a longer terminal and is powered through 6 Volts, whereas the negative terminal is represented with the '-' symbol or short terminal and is connected to the GND terminal. This buzzer was launched in 1831 by an American Scientist, Joseph Henry, but was used in doorbells until they were eliminated in 1930 in support of musical bells, which had a smooth tone. These buzzers were invented by Japanese manufacturers and fixed into a broad range of devices during the period of 1970s-1980s.
A buzzer is an efficient component to include sound features in a system or project. It is an extremely small and solid two- pin device, thus it can be simply utilized on breadboard or PCB. There are two kinds of buzzers commonly available: simple and readymade. A simple type, when powered, will generate a continuous beep sound. A readymade type looks heavier and generates intermittent beeps due to the internal oscillating circuit within it.

The buzzer uses a DC power supply ranging from 4V-9V. To operate this, a 9V battery is used, but it is suggested to utilize a regulated +5V/+6V DC supply. Generally, it is connected through a switching circuit to switch ON/OFF the buzzer at the necessary time interval.

The advantages of a buzzer include simple compatibility, good frequency response, small size, less energy consumption, a large voltage usage range, and high sound pressure. The dis- advantages include somewhat difficult controlling,

annoying sound generation, and the necessity of training to know how to repair the condition without just turning it off.

The applications of buzzers include communication de- vices, electronics used in automobiles, alarm circuits, portable devices, security systems, timers, household appliances, and electronic metronomes. The proposed system's block diagram connects an Arduino Uno to a fingerprint sensor, LCD, but- tons, buzzer, wifi, and computer.

V. SYSTEM ANALYSIS

The system requirements for this project include both hard- ware and software specifications. For hardware, the system requires an operating system such as Windows or Linux, an Intel i3 processor or higher, RAM of 4 GB or higher, and a hard disk of 250 GB or higher. The software requirements include Windows 7 or higher as the operating system, C++ as the programming language, and Arduino as the IDE.

The Arduino Integrated Development Environment (IDE) contains a text editor for writing code, a message area, a text console, a toolbar with buttons for common functions, and a series of menus. It connects to the Arduino and Genuino hardware to upload programs and communicate with them. Programs written using Arduino Software are called sketches. These sketches are written in the text editor and are saved with the file extension .ino. The editor has features for cutting/pasting and for searching/replacing text. The message area gives feedback while saving and exporting and also displays errors. The console displays text output by the Ar- duino Software, including complete error messages and other information. The bottom right-hand corner of the window displays the configured board and serial port. The toolbar buttons allow you to verify and upload programs, create, open, and save sketches, and open the serial monitor.

When you open the Arduino program, you are opening the IDE. It is intentionally streamlined to keep things as simple and straightforward as possible. When you save a file in Arduino, the file is called a sketch – a sketch is where you save the computer code you have written. The coding language that Arduino uses is very much like C++, which is a common language in the world of computing. The code you learn to write for Arduino will be very similar to the code you write in any other computer language – all the basic concepts remain the same – it is just a matter of learning a new dialect should you pursue other programming languages.

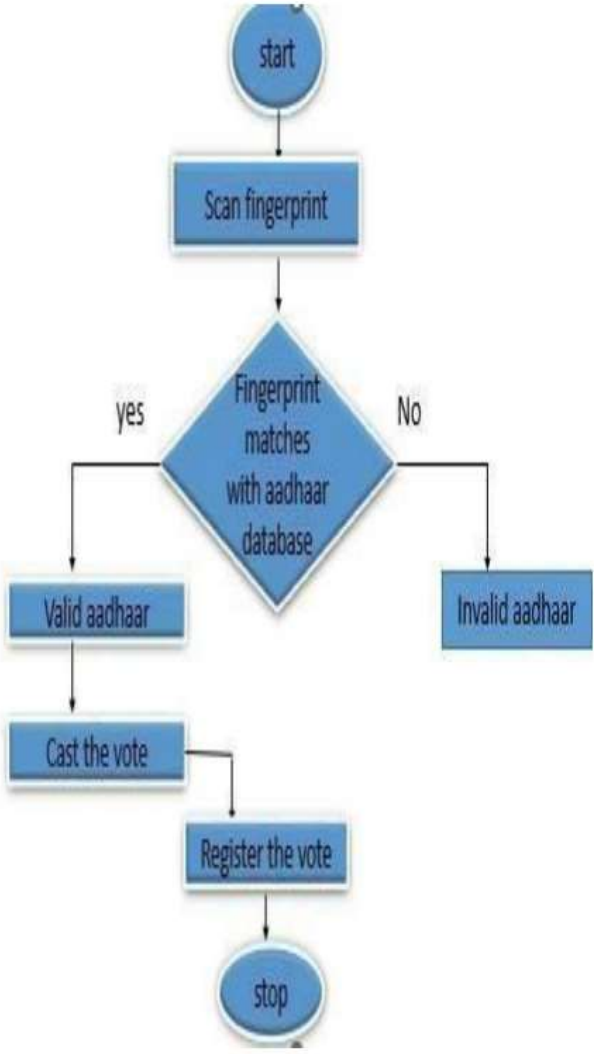

Fig 6. Process Diagram

The code you write is "human readable," that is, it will make sense to you and will be organized for a human to follow. Part of the job of the IDE is to take the human readable code and translate it into machine-readable code to be executed by the Arduino. This process is called compiling. The

process of compiling is seamless to the user. All you have to do is press a button. If you have errors in your computer code, the compiler will display an error message at the bottom of the IDE and highlight the line of code that seems to be the issue.

For software implementation, we first download the Adafruit Fingerprint sensor library from the internet. For enrolling a new finger, we put together a simple sketch and upload it to the Arduino. The fingerprint verification process involves placing a finger against one that was already enrolled. If Arduino recognizes that fingerprint, the door will unlock; otherwise, the door remains locked. To delete any fingerprint, type the IDs in the serial monitor and it will delete that fingerprint.

For hardware implementation, we set the devices and con- nect them according to the block diagram. TX-out and Rx-in of the sensor are connected to pin 2 and pin 3 of the Arduino Uno respectively. The electronic lock is connected with one of the output ports of the Uno. Making a network with the relay allows switching between the 5V and the 12V electrical components. We attach the Arduino Uno to the laptop for registering fingerprints. We require the connection with the computer for assigning the ID to the prints. This can be done through a smartphone with Arduino application as well. We save the ID into the sensor and upload the code to the Uno. We disconnect the Uno from the computer and turn on the power adaptor. Once it gains power, the system boots up the fingerprint IDs saved inside and waits for a print to be matched. If no match is found, the keypad and the switch remain active. Once a match is found, the buzzer will buzz once and the lock will open. If no match is found, the system will not take any action at all.

Arduino is an open-source platform used for building electronics projects. Arduino consists of both a physical programmable circuit board (often referred to as a micro- controller) and a piece of software, or IDE, that runs on your computer, used to write and upload computer code to the physical board. The Arduino platform has become quite popular with people just starting out with electronics, and for good reason. Unlike most previous programmable circuit boards, the Arduino does not need a separate piece of hardware (called a programmer) in order to load new code onto the board – you can simply use a USB cable. Additionally, the Arduino IDE uses a simplified version of C++, making it easier to learn to program.

A typical example of an Arduino board is Arduino Uno. It consists of ATmega428 - a 28-pin microcontroller. Arduino Uno consists of 14 digital input/output pins (of which 6 can be used as PWM outputs), 6 analog inputs, a 16 MHz crystal oscillator, a USB connection, a power jack, an ICSP header, and a reset button. Arduino can be powered either from the PC through a USB or through an external source like an adaptor or a battery. It can operate on an external supply of 7 to 12V. Power can be applied externally through the pin Vin or by giving voltage reference through the IORef pin.

For the power supply, there are many types available. Most are designed to convert the AC Mains electricity to a suitable low voltage supply for electronic circuits and other devices. A power supply can be broken down into a series of blocks, each of which performs a particular function. Here the AC supply main is given to the step-down transformer. The transformer has different voltages. The output from the transformer is given to the rectifier circuit. In this rectifier circuit, the AC voltage is converted to DC voltages. The rectified DC voltage is given to the regulator circuit. The output of the regulator depends upon the regulator IC chosen in the circuit.

A bridge rectifier can be made using four individual diodes, but it is also available in special packages containing the four diodes required. It is called a full-wave rectifier. Smoothing is performed by a large value electrolytic capacitor connected across the DC supply to act as a reservoir, supplying current to the output when the varying DC voltage from the rectifier is falling. Voltage regulator ICs are available with fixed (typically 5, 12, and 15V) or

variable output voltages. They are also rated by the maximum current they can pass. Negative voltage regulators are available, mainly for use in dual supplies.

The ESP8266 Wi-Fi Module is a self-contained SOC with an integrated TCP/IP protocol stack that can give any mi- crocontroller access to your Wi-Fi network. The ESP8266 is capable of either hosting an application or offloading all Wi-Fi networking functions from another application processor. Each ESP8266 module comes pre-programmed with an AT com- mand set firmware. The ESP8266 module is an extremely cost- effective board with a huge, and ever-growing, community. This module has powerful on-board processing and storage capability that allows it to be integrated with sensors and other application-specific devices through its GPIOs with minimal development up-front and minimal loading during runtime. In this system, Wi-Fi is used to transfer the collection of votes to the server so that vote information can be updated to the server.

Software testing is a critical element of software quality assurance and represents the ultimate review of specification, design, and coding. The testing phase involves testing the developed system using various kinds of data. System testing is the stage of implementation aimed at ensuring the system works accurately and efficiently before live operation com- mences. The candidate system is subject to a variety of tests such as recovery, security, and usability tests. A series of testing is performed for the proposed system before the system is ready for user acceptance testing.

Several testing strategies are used for the testing purpose, including unit testing, usability testing, accessibility testing, and reliability testing. Unit testing focuses on the smallest unit of software design of the module. Usability testing is performed to ensure proper ballot selection by any eligible voter. Accessibility testing is utilized to ensure all areas of the voting process have been made accessible to eligible voters with disabilities requiring assistance. Reliability testing involves evaluating the reliability by casting votes on paper-based, direct recording electronic (DRE), and the proposed e-voting system. Test case design involves designing the test cases (inputs and outputs) used to test the system. The goal of test case design is to create a set of tests that are effective in validation and defect testing.

VI. CONCLUSION

The Fingerprint Voting System was developed to allow users to cast their votes using fingerprint authentication, with the primary objective of enhancing security and preventing dupli- cation. This system also aims to reduce the burden associated with conducting traditional voting processes. By replacing paper ballots with biometric verification, the system ensures a secure and user-friendly experience for voters. Fingerprints are recognized as one of the most reliable biometric methods, given that each individual's fingerprint is unique and remains unchanged throughout their life—even identical twins have different fingerprints. The fingerprint system replaces the need for voter ID cards and relies on fingerprint authentication for verification.

The system was successfully evaluated and implemented, with simulations conducted prior to hardware deployment. Tests were carried out on different PCs with varying configu- rations to identify the system's strengths and weaknesses. The final results demonstrated that the fingerprint voting system achieved a high level of accuracy and responded quickly to fin- gerprint scans, ensuring smooth and efficient user interaction. Compared to traditional voting systems, this solution offers stronger security, faster processing, and seamless integration. In the context of our country, where both private and gov- ernment sectors are highly concerned about security, such a biometric-based system holds great potential for real-world application.

Future Work

For future enhancements, the system could incorporate advanced biometric technologies such as face recognition or retinal scan processes. These technologies can further improve the

authentication accuracy, potentially solving existing issues with biometric recognition. Integra- tion with the AADHAAR database plays a vital role in eliminating vote duplication by verifying the voter's identity through a unique national ID. Additionally, by connecting the voting system with multiple security specifications such as AADHAAR ID, biometric authentication, and fingerprint recognition, the possibility of fraudulent activities like vote tampering or position rigging can be minimized. Employing IRIS-based authentication in future versions of the system could offer even more robust security compared to existing biometric methods, making the voting process entirely secure and reliable.

REFERENCES

1. Srivastansridharan "Implementation of Authenticated and Secure Online Voting System" [2013] vol 2.
2. AshokNalluri and B Bhanu Teja "RFID and fingerprint recognition based evoting system for Real time Application" [2014] vol4
3. Rudrappa B Gujanathi "Finger print based Electronic Voting System" [201
4. M Santhosh, S Kavitha and R Keerthan "Electronic voting machine using internet" [2016] vol 4
5. RajashreeRaskar and Bhagyashree Raikar "Literature survey on se- cured mobile based e-voting system" [2015] 6. Ankith Anand and Pallavi Divya "An efficient online voting system" [2012]
6. D. Vinod kumar and M R K Murthy. Fingerprint Based ATM Security by using ARM7. IOSR Journal of Electronics and Communication Engineering (IOSRJECE), Volume 2(5), October 2012, PP 26-28.
7. Raffaele Cappelli, Alessandra Lumini, Dario Maio and Davide Mal- toni. Fingerprint Image Reconstruction from Standard Templates. IEEE Trans. Pattern Analysis and Machine Intelligence, 29(9), pp. 1489-1503. September 2007.
8. Ross J. Anderson. Security Engineering: A Guide to Building De- pendable Distributed Systems, 2nd edition, 2008. John Wiley & Sons, Inc., New York, NY, USA.
9. Fernando L. Podio. Personal authentication through biometric tech- nologies. Proceedings 2002 IEEE 4th International Workshop on Net-worked Appliances 62 (Cat. No.02EX525), Gaithersburg, MD, 2002, pp. 57-66.
10. Yu-Chih Huang. Secure Access Control Scheme of RFID System Application. Fifth International Conference on Information Assurance and Security, China, 2009.
11. D. Maio, D. Maltoni, R. Cappelli, J. L. Wayman, and A. K. Jain. FVC2002: Fingerprint Verification Competition. Proceedings of International Conference on Pattern Recognition (ICPR), pp.744-747, Quebec City, Canada, August 2002.
12. Biometric Recognition. IEEE Transactions on Circuits and Systems for Video Technology, Special Issue on Image and Video Based Biometrics, Vol. 14(1), January, 2004.
13. R. P. Wildes. Iris recognition: an emerging biometric technology. Proceedings of the IEEE, vol. 85, no. 9, pp. 1348-1363, September, 1997.
14. Anil K. Jain, Jianjiang Feng and Karthik Nandakumar. Matching Fingerprints. IEEE Computer, 43(2), pp. 36-44, February, 2010
15. Mary Lourde R and Dushyant Khosla. Fingerprint Identification in Biometric Security Systems. International Journal of Computer and Electrical Engineering, 2(5), October, 2010.
16. Zevdin Pala and Nihat Inanc. Smart Parking Applications Using RFID Technology. 1st Annual RFID Eurasia, Istanbul, 2007, pp. 1-3.
17. Biometric finger print based electronic voting system for rigging free governance using ARM7 TDMI processor based LPC2148 controller,
18. K. Mallikarjuna1, T. Mallikarjuna2, INTERNATIONAL JOURNAL OF ENGINEERING & SCIENCE RESEARCH (IJESR/May 2014/ Vol-4/Issue-5/410- 414) e-ISSNAnil K. Jain, Arun Ross and Salil Prabhakar. An Introduction to 2277-2685, p-ISSN 2320-976