Electronic Voting Using Fingerprint Sensor and Aadhaar Card

D.Satheeswari[1], M.Greeshma[2], Jessila Mohmatha[3], F.Edwin Louis[4]

Assistant Professor, Meenakshi College of Engineering, Chennai, India [1]

UG Students, Meenakshi College of Engineering, Chennai, India [2,3,4]

ABSTRACT: An online voting system is to avoid multiple polling and irregularities at counting location. In this system the voters can vote through the mobile by using application only at the Indian standard time when the election is conducted. A booth will be created for the people who do not have finger print facility in their mobile. After voting, the Aadhaar id will be blocked from the server. In booth section the main concept is to create webpage. Here only two processes are present, first finger print will be scanned; the related data which match with the given finger print will be displayed from the election commission. After verifying the details, the vote can be generated. Next, the ballot list will be displayed according to the address of the voter's data base. After generating the vote it will be sent directly to the election commission and a confirmation message is sent to the voter. First all the information of every candidate should be uploaded in the main database of election commission according to aadhaar identity. An application will be created. In first page, aadhaar id is provided by the voter and it is verified with the main database of election commission. The commission will send a unique password to the mobile number which is stored already in the database. The password must be valid for 2 minutes and if the password is correct then it will ask the finger print authentication. If the finger print match with the data of the server then the ballot list will be displayed according to the address of the voter database. After submitting the vote, the election commission will send the confirmation message to the voter.

KEYWORDS: Finger print sensor, Biometrics, Finger print scanner, E-voting.

I. INTRODUCTION

Voting schemes have evolved from counting hands in early days to systems that include paper, punch card, mechanical lever and optical-scan machines. An electronic voting system which is used nowadays provide some characteristic difference from the traditional voting technique, and also it provides improved features of voting system over traditional voting system such as accuracy, convenience, flexibility, privacy, verifiability and mobility. But Electronic voting systems suffers from various drawbacks such as time consuming, consumes large volume of paper work, no direct role for the higher officials, damage of machines due to lack of attention, mass update doesn't allows users to update and edit many item simultaneously etc. These drawbacks can overcome by Online E- Voting with finger print scanner system. This is a voting system by which any voter can use his/her voting rights from anywhere in the country. Voter can cast their votes from anywhere in the country without visiting to voting Booths, in highly secured way. That makes voting a fearless of violence and that increases the percentage of voting. This project deals with two concepts where one is booth section another one is voting through mobile application. In booth section, webpage is created.

Here only two processes are present, first finger print will be scanned; the related which match with the given finger print will be displayed from the election commission. After verifying the details submit it. Next, ballot list will be displayed according to the address of the voter's database. Finally, the election commission sends confirmation message to the voter.

II.   EXISTING SYSTEM

A. *Expensive and time consuming*

Time and money is spent in printing data capture forms, in preparing registration stations together with human resources, and there after advertising the days set for registration process including sensitizing voters on the need for registration, as well as time spent on entering this data to the database. Electronic voting process involves paper storage which is difficult as papers become bulky with the population size.

B. *An Online Voting System Using Biometric Fingerprint and Aadhaar Card*

This paper deals with the design and development of a web-based voting system using fingerprint and aadhaar card in order to provide a high performance with high security to the voting system. Also the web technology has been used to make the voting system more practical [1]. The proposed Online Voting System allows the voters to scan their fingerprint, which is then matched with an already saved image within a database that is retrieved from aadhaar card database of the government. The voting system is managed in a simpler way as all the users must login by aadhaar card number and password and click on his/her favorable candidates to cast the vote. This will increase the voting percentage in India and reduces the cost of voting process. By using biometric fingerprint it provides enough security which reduces the false votes.

C. *A Secure E-Government's E-Voting System*

This paper proposed a reliable cost effective secure electronic voting system that can be used in cost effectively way in many development countries like Egypt. The important obstacle in any e-voting system across the world is the security issue. Election's results may be modified when delivered to the Higher Elections Committee, unauthorized voter may vote instead of the eligible voter, a vote may not be calculated; also the voter has to ensure that nobody has the possibility to know his ballot data. The proposed Voting Model System overcomes these obstacles [4]. Security evaluation experiments are performed successfully to the proposed system proving that it satisfies privacy, accuracy, reusability, eligibility and integrity.

D. *A Biometric Secure E-Voting For Election Process*

The proposed system warrant well-secured identification and authentication processes for the voter through the use of combined simple biometrics. The design of the system guarantees that no votes in favor of a given candidate are lost, due to improper tallying of the voting counts, with the proper incorporation of system FLAG's. This paper is designed to cater for several essential nonfunctional requirements [3]. Of utmost importance are the requirements for correctness, robustness, coherence, consistency, and security. To verify the robustness and reliability of the proposed system, intensive computer simulations were run under varying voting environments, viz. voter density, voter inter-arrival times, introduced acts of malice, etc.

E. *Design and Build a Secure E-Voting Infrastructure*

We have designed a secure online e-voting system that provides confidentiality, anonymity, integrity, authenticity, auditability and verifiability. Confidentiality prevents anyone else from knowing who has voted for whom except the voters themselves [2]. Anonymity is to prevent the tracking of the voters' real identities. Authenticity is to ensure that voters are eligible with unidentifiable-untraceable signatures of the real votes. Integrity is to ensure that no one else is able to change the ballot, and to detect the change if it occurs. Auditability makes the election auditable with or without tracing back the true identity of the voters. Finally, verifiability enables the system to verify and count the votes, and to detect any missing or fraudulent votes [5].

F. *The Design of an Electronic Voting System*

An electronic voting system based upon the electoral process adopted in Ghana. In recent years, information technology has greatly affected all aspects of life, and to a large extent, this includes politics. The most recent method to be devised is electronic voting (e-voting). It is meant to phase out outdated paper ballot, punched cards and other mechanical voting systems with paperless electronic or online voting systems. E-voting systems endeavor to make elections simple while reducing the total cost of the election. Designing an air-tight and reliable e-voting system is therefore a great task, in that, the system that must be developed must protect the privacy of the voter, be easily understood and used by the entire voting populace - no matter who they are or where they come from. Based on this, OVIS, an On-line Voting System, has been developed.

III.   PROPOSED SYSTEM

This project deals with two concepts where one is booth section and another one is voting through mobile application. In booth section, operations are controlled by Arduino micro controller and finally, information is transmitted to main server. After voting the aadhaar id should be blocked from the server so that vote will be casted by only once.
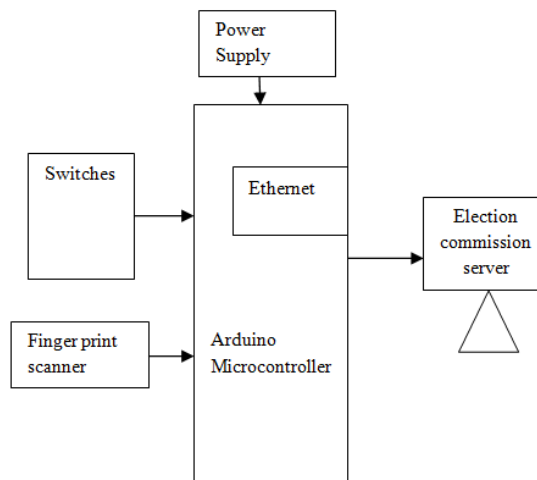

Fig. 1. Block diagram of Booth system

In mobile an application is created. In the first page, Aadhaar id must be entered and the aadhaar id will be verified with the main database of election commission. The commission will send a unique password to the mobile number which is stored already in the database .The password must be valid for 2minutes and if the password is correct then it will ask the finger print authentication. If the finger print matched with the data of the server in next page the ballot list will be displayed according the address of the voter's database. After submitting the vote, the election commission will send the confirmation message to the voter. The vote will be casted only once. If any irregularity happens it will send the message to the control room. The process is highly secured.
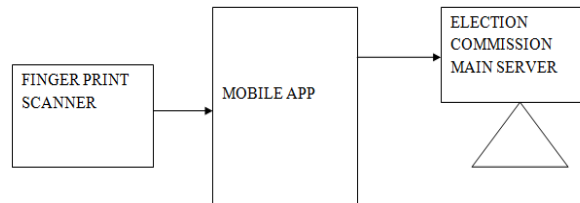
Fig. 2. Block diagram through mobile application

IV. HARDWARE REQUIREMENTS

A. *Arduino Controller*

The features of Arduino controller are high performance, low power. It belongs to Atmel 8 bit microcontroller family. It has 131 powerful instructions. The execution will be in single clock cycle. The operation is fully static. The throughput of the controller is 20MHz. It has non volatile memory segments. It has self programmable flash memory. It has True-Read-While operation. The controller has capactive touch buttons, sliders and wheels for programming lock for software security. There are two 8 bit and one 16 bit timer/counter. It is a programmable serial USART. An On-chip Analog comparator is present. There are six sleep modes. They are Idle, ADC Noise Reduction, Power-save, Power-down, Standby and Extended standby. There are 23 programmable I/O lines.The AVR core combines a rich instruction set with 32 general purpose working registers. All the 32 registers are directly connected to the Arithmetic Logic Unit (ALU), allowing two independent registers to be accessed in one single instruction executed in one clock cycle. The resulting architecture is more code efficient while achieving throughputs up to ten times faster than conventional CISC microcontrollers.

B. *Arduino with ethernet*

The Arduino Ethernet is a microcontroller board based on the ATmega328. It has 14 digital input/output pins, 6 analog inputs, a 16 MHz crystal oscillator, a RJ45 connection, a power jack, an ICSP header, and a reset button. Pins 10, 11, 12 and 13 are reserved for interfacing with the Ethernet module and should not be used otherwise. This reduces the number of available pins to 9, with 4 available as PWM outputs. An optional Power over Ethernet module can be added to the board as well.The Ethernet differs from other boards in that it does not have an onboard USB-to-serial driver chip, but has a Wiznet Ethernet interface. This is the same interface found on the Ethernet shield. An onboard microSD card reader, which can be used to store files for serving over the network, is accessible through the SD Library. Pin 10 is reserved for the Wiznet interface; SS for the SD card is on Pin 4. The 6-pin serial programming header is compatible with the USB Serial adapter and also with the FTDI USB cables or with Sparkfun and Adafruit FTDI-style basic USB-to-serial breakout boards. It features support for automatic reset, allowing sketches to be uploaded without pressing the reset button on the board. When plugged into a USB to Serial adapter, the Arduino Ethernet is powered from the adapter.

C. *Finger print sensor*

Fingerprint processing has three primary functions: enrollment, searching and verification. Among these functions, enrollment which captures fingerprint image from the sensor plays an important role. A reason is that the way people put their fingerprints on a mirror to scan can affect to the result in the searching and verifying process. Regarding to verification function, there are several techniques to match fingerprints such as correlation-based matching, minutiae-based matching, ridge feature-based matching and minutiae-based algorithm. However, the most popular algorithm was minutiae based matching algorithm due to its efficiency and accuracy.

D. *Biometrics*

Biometrics are automated methods of recognizing a person based on a physiological or behavioral characteristic. Among the features measured are face, fingerprints, hand geometry, handwriting, iris, retinal, vein, and voice. Biometric data are separate and distinct from personal information. Biometric templates cannot be reverse-engineered to recreate personal information and they cannot be stolen and used to access personal information. Using a unique, physical attribute of the human body, such as the fingerprint or iris, to effortlessly identify and verify that you are who you claim to be, is the best and easiest solution in the market today. That is the simple truth and power of Biometrics Technology today. Although biometric technology has been around for many years, modern advances in this emerging technology, coupled with big reductions in cost, now make biometrics readily available and affordable to consumers, small business owner, larger corporations and public sector agencies alike. A fingerprint scanner system has two basic jobs, it needs to get an image the finger, and it needs to determine whether the pattern of ridges and valleys in this image matches the pattern of ridges and valleys in pre-scanned images. Only specific characteristics, which are unique to every fingerprint, are filtered and saved as an encrypted biometric key or mathematical representation. No image of a fingerprint is ever saved, only a series of numbers (a binary code), which is used for verification. The algorithm cannot be reconverted to an image, so no one can duplicate the fingerprints. It is important to note that Easy Clocking's biometric time clocks do not actually collect and store fingerprints. Instead, it saves a mathematical representation of the employee's biometric data. When the biometric time clock scans a hand or finger during a supervised enrollment process, only an encrypted mathematical representation of the fingerprint is stored. As a result, it's virtually impossible to duplicate the original image from that mathematical representation. Additionally, if employees question cleanliness, this concern should not be dismissed. Instead, you should assure employees that the time clock's finger zone is not a hot zone for germs. In fact, it will be touched far less frequently than restroom door handles, water cooler spigots, or chairs in the break room.

Conclusion on Biometric & Workforce Management

Biometrics has been used effectively for more than a decade for time and attendance and workforce management. Despite widespread use, confusion and misconceptions about the technology and its capabilities persist. These concerns are easily dispelled when the facts about biometrics are established. Biometrics offers unparalleled ability to quickly and accurately capture real-time, labor data and provide a nonrepudiated audit trail. Biometrics has undergone intense scrutiny and the results are in - when properly deployed, biometrics work well and are safe, secure, and accurate. Biometrics offers organizations a broader range of direct and indirect time, cost, and operational benefits than alternative time and attendance methods. Today over one hundred thousand thriving organizations rely on Easy Clocking's time & attendance systems to automate their employee attendance and as a result they are seeing a significant reduction in direct and indirect labor costs. Workstation, DigitalPersona Pro Kiosk, DigitalPersona Online, DigitalPersona Personal or any of the DigitalPersona SDK packages. Whether you are an enterprise customer, a system integrator or a home user, DigitalPersona's fingerprint authentication solutions provide a natural extension to the security system and applications.

V. SOFTWARE REQUIREMENTS

Embedded c is a set of language extension for the C Programming language by the C Standards committee to address commonality issues that exist between C extensions for different embedded systems. Historically embedded C programming requires nonstandard extensions to the C language in order to support exotic features such as fixed-point arithmetic, multiple distinct memory banks, and basic I/O operations. Embedded C uses most of the syntax and semantics of standard C, e.g., main () function, variable definition, data type declaration, conditional statements (if, switch, case), loops (while, for), functions, arrays and strings, structures and union, bit operations, macros, etc.

VI.   RESULT

Fig. 3. Hardware output for the proposed methodology

VII.   CONCLUSION

Electing a right leader and making India as a developed country is every person's dream. In this aspect voting plays an important role. Citizens who have crossed 18 years must cast the vote in a genuine manner. Electing the wrong person by malfunctioning practices leads to many disasters. In order to avoid this situation, the paper presents an idea conceptually that person who is not a valid user can be easily identified in an accuracy by 97.38% when comparison is made with face and fingerprint traits individually gives 88.87%, 90.21% accurate rates.

REFERENCES

1.   "An Online Voting System Using Biometric Fingerprint and Aadhaar Card", IJCAT International Journal of Computing and Technology, Volume 1, Issue 4, May 2014 ISSN : 2348 – 6090.
2.   "The Design of an Electronic Voting System", Research Journal of Information Technology 3(2): 91-98, 2011 ISSN: 2041-3114.
3.   "A Biometric-Secure e-Voting System for ElectionA Secure e-Government's e-Voting System", Science and Information Conference 2015 July 28-30, 2015.
4.   "The Design and Development of Real-Time E-Voting System in Nigeria with Emphasis on Security and Result Veracity",I. J. Computer Network and Information Security, 2013, 5, 9-18 Published Online April 2013 in MEC.
5.   A. Aviv, P. Cerný, S. Clark, E. Cronin, G. Shah, M. Sherr,and M. Blaze. Security evaluation of ES&S voting machines andelection management system. In Proc. USENIX/ACCURATEElectronic Voting Technology Workshop (EVT), San Jose, CA,July 2008.

BIOGRAPHY

D.Satheeswari received her B.E. degree in Electronics and Communication Engineering from Anna University, Chennai and M.E.degree in Applied Electronics from Sathyabama University, Chennai. She works as Assistant Professor in the Electronics and Communication Engineering Department, Meenakshi College of Engineering, Chennai.

M.Greeshma, Jessila Mohmatha, F.Edwin Louis are doing their final yearin the Electronics and Communication Engineering Department, Meenakshi College of Engineering, Chennai.