IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)
e-ISSN: 2278-2834,p- ISSN: 2278-8735.Volume 10, Issue 1, Ver. II (Jan - Feb. 2015), PP 57-65
www.iosrjournals.org

Biometric System Based Electronic Voting Machine Using Arm9 Microcontroller

[1]M.Sudhakar, [2]B.Divya Soundarya Sai,
[1]Professor in ECE, [2]II Year M.Tech,
Dept of ECE,CMR College of Engineering &Technology,Hyderabad, TS-India.

Abstract:*This paper focuses on simple,low cost fingerprint based electronic voting machine using ARM9 microcontroller. An electronic voting system is a voting system in which the voters' and voting data is recorded,stored and processed digitally. The proposed systemconsistsofcontroller hardware and software. The hardware is implemented with ARM9 microcontroller along with KY-M6 finger-print module. The software code is developed in WINCE6 development environment for interfacing the ARM processor with finger-print module. The proposed system gives the best solution for minimizing the time taken for identifying the voter. The design implemented in the FP-EVM is portable,flexible and with minimum power consumption. The designed system is user-friendly,easily adaptableand cost-effective. Further,the designed system has simple architecture,fast response time and scope for further expansion.*

Index Terms:*KY-M6 Fingerprint sensor,ARM9(mini2440).*

I. Introduction

Fundamental right to vote or voting in elections forms the basis for the democracy. Elections [1] allow the people to choose their representatives and express their preferences for how they are governed. In all earlier elections of India, such as state or central elections, a voter casts his/her vote by marking with stamp against their chosen candidate and then folding the ballot paper as per a prescribed method, before dropping it in the ballot box. This is a time-consuming and very much prone to errors. The same method was continued till the electronic voting machines were introduced in the election process.Because of the EVMs, all the condensed materials like the ballot papers,ballot boxes and stamping are completely replaced into a simple box called ballot unit. EVMs retain all the characteristics of voting by ballot papers, while making polling a lot more expedient.

1.1 Requirements Of E-Voting

The requirement in traditional voting process is also applicable for e-voting and some of them are mentioned below [3]**Fairness**: No person can learn the votingoutcomes before the tally. **Eligibility**: Only eligible voters are allowed to casttheir vote. **Uniqueness**: No voter is allowed to cast the votemore than once**. Privacy**: No person can access the informationabout the voters vote. **Accuracy**: All the valid votes should be countedcorrectly.**Efficiency**: The counting of votes can beperformed within a minimum amount of time.

II. Existing System

An EVM consists of two units namely Control Unit and Balloting Unit

The two units are joined by a five-meter cable. The Control Unit is with the Presiding Officer or a Polling Officer and the Ballot Unit is placed inside the voting compartment. Instead of issuing a ballot paper, the Polling Officer in-charge of the Control Unit will press the Ballot Button. This will enable the voter to cast his/her vote by pressing the blue button on the Ballot Unit against the candidate and symbol of his/her choice.The controller used in EVMs has its operating program etched permanently in silicon at the time of manufacturing by the manufacturer. No one (including the manufacturer) can change the program once the controller is manufactured.EVMs can cater to a maximum of 64 contesting candidates. There is provision for only 16 candidates in a BUif the total number of candidates exceeds 16,then a second BU is to be linked parallel to the first BU.Similarly, if the total number of candidates exceeds 32,then a third BU is to be connected and if the total number ofcandidates exceeds 48,fourth BU is to be connected to cater to a maximum of 64 candidates.As the process is faster and more reliable,the EVMs save considerable amount of time,money, paper and man power.

Actual process of identifying the voter has to be done by the polling officer. For casting of votes with EVMs,the voters have to produce their ElectionPhoto Identity Card(EPIC) issued by the Election Commission. The polling officer needs to verify the EPIC with the official list he has,then he needs to confirm whetherit is an authorized card or not and he allows the voters to cast their votes.Therefore EVMs depend upon manual verification of the EPIC. Consequently,this slows down the voting process. This limitation is overcome with the help of finger-print identification module. The second limitation is the number of contesting candidates

available in the EVM. The EVMs can cater to a maximum of 64 candidates with the use of one CU and four BUs. If the number of contestant candidates exceeds 64,then the polling officer needs to carry one more set of EVM that necessitates more material and additional manpower.

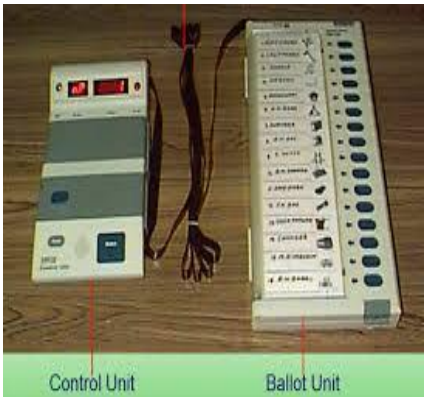


Fig:1: Electronic Voting Machine (EVM)

2.1 Advantages Of Evm

EVMs are powered by an ordinary 6 volt alkaline battery manufactured by Bharat Electronics Ltd., Bangalore and Electronic Corporation of India Ltd., Hyderabad. This design enables the use of EVMs throughout the country without interruptions because several parts of India do not have power supply and/or erratic power supply.It is not possible to vote more than once by pressing the button again and again. As soon as a particular button on the Ballot Unit is pressed, the vote is recorded for that particular candidate and the machine gets locked for next voter. Even if one presses that button further or any other button, no further vote will be recorded. This way the EVMs ensure the principle of "one person, one vote".Bogus voting can be greatly reduced by the use of EVMs. In case of ballot paper system, a bogus voter can stuff thousands of bogus ballot papers inside the ballot box because of manual process. But, an EVM is programmed to record only five votes in a minute.

III. Biometric Systems

Biometrics[5] is a method of recognizing a person based on physical or behavioral characteristics.Examples ofbiometric information used to identify people include fingerprint, voice, face, iris, handwriting, and hand geometry.There are two key functions offered by a biometric system. One method isidentification, a “one-to-many”(1:N)matching process in which a biometric sample is compared sequentially to a set of stored samples to determine theclosest match. The other isverification, a “one-to-one”(1:1)matching process in which the biometric system checkspreviously enrolled datafor a specific user. The verificationmethod provides the best combination of speed and security, especially where multiple users are concerned, andrequires a user ID or other identifier for directmatching. Unprecedented growth in electronictransactions has underlinedthe need for a faster, more secure and more convenient method of user verification thanpasswords can provide. Biometric identifiers offer several advantages over traditional and current methods.This is because only biometric authentication is based on the identification of an intrinsic part of a human being.Tokens such as smart cards, magnetic stripe cards and physical keys, can be lost, stolen, duplicated or left behind.Passwords can be forgotten, shared, hacked or unintentionally observed by athird party. By eliminating thesepotential trouble spots, only biometric technology can provide the security, with convenience needed for today’scomplex electronic landscape.

3.1 Finger-Print Biometric

Human fingerprints are unique to each person and can be regarded as a sort of signature, certifying the person's identity. Fingerprints[6] are the oldest and most widely used form of biometric identification. A fingerprint is formed from an impression of pattern of ridges on a finger. A ridge is defined as a single curved segment,and a valley is the region between two adjacent ridges. The minutaewhich are the local discontinuities in the ridge flow pattern,provide the features that are used for identification.

3.1.1 Finger-Print Recognition[7]

It is an active research area nowadays. An important component in fingerprint recognition systems is the fingerprint matching algorithm. According to the problem domain, fingerprint matching algorithms are classified in two categories: fingerprint verification algorithms and fingerprint identification algorithms. The aim of fingerprint verification algorithms is to determinewhether two fingerprints come from the same finger or

not. On the other hand, the fingerprint identification algorithms search a query fingerprint in a database looking for the fingerprints coming from the same finger. Despite the widespread use of fingerprints, there is little statistical theory on the uniqueness of fingerprint minutiae. A critical step in studying the statistics of fingerprint minutiae is toreliably extract minutiae from the fingerprint images.However, fingerprint images arerarely of perfectquality. They may be degradedand corrupted due to variations in skin and impression conditions.Thus,image enhancement techniques are employed prior to minutiae extraction to obtain a more reliable estimation of minutiae locations.

Straightforward matching[8] of the to-be-identified fingerprint pattern against many already known fingerprint patterns would not serve well, due to the high sensitivity to errors in capturing fingerprints (e.g. due to rough fingers, damaged fingerprint areas or the way a finger is placed on different areas of a fingerprint scanner window that can result in different orientation or deformation of the fingerprint during the scanning procedure). A more advanced solution to this problem is to extract features of so called minutiae points (points where the tiny ridges and capillary lines in a fingerprint have branches or ends) from the fingerprint image and check matching between these sets of very specific fingerprint features.The extraction and comparison of minutiae points requires sophisticated algorithms for reliable processing of the fingerprint image, which includes eliminating visual noise from the image, extracting minutiae and determining rotation and translation of the fingerprint. At the same time, the algorithms must be as fast as possible for comfortable use in applications with a large number of users.

Many of these applications can run on a PC, however some applications require that the system be implemented on low cost, compact and/or mobile embedded devices such as doors, gates, handheld computers, cell phones etc.). For developers who intend to implement the fingerprint recognition algorithm into a microchip, compactness of algorithm and small size of required memory may also be important.

3.2. Related Work

In this section,ARM9,KY-M6 finger-print sensor, MAX 232 for serial communication and Ethernet are described.

A. KY-M6 finger print sensor:

KY-M6 Fingerprint Sensor Module is able to conduct fingerprint image processing, template generation, template matching, fingerprint searching, template storage, etc. Compared with similar products from other suppliers, KY-M6 proudly boasts of following features:

1. **Proprietary Intellectual Property**:Optic fingerprint enrollment device, KY-M6 hardware as well as fingerprint algorithm are all developed by KeyPower Security.
2. **Wide Application Range of Fingerprints with Different Quality:**Self-adaptive parameter adjustment mechanism is used in the course of fingerprint enrollment. This ensures good image quality for even dry or wet fingers, thus it has wider application range**.**
3. **Immense Improved Algorithm**:KY-M6 Fingerprint algorithm is specially written according to optic imaging theory. The algorithm is good for low-quality fingers due to its excellent correction and tolerance features.
4. **Flexible Application**:User can easily set KY-M6 Module to different working modes depending on complexity of application systems. User can conduct secondary development with high efficiency and reliability.
5. **Easy to Use and Expand:**It is not necessary for user to have professional knowledge in the field of fingerprint verification. User can develop powerful fingerprint verification application systems with the command set provided by KY-M6.
6. **Low Power Consumption:**Sleep/awake control interface makes KY-M6 suitable for occasions that require low power consumption.
7. **Different Security Levels:**User can set different security level according to different application environment.
8. **Application:**KY-M6 can be used on all fingerprint verification systems, such as Safety cabinet, door lock, Complicated door-guard system, Fingerprint IC card Identification Terminal, Fingerprint identification and verification system associated with PC.

Fig2:KY-M6 sensor

B. Arm9 Microcontroller:

The S3C2440A is developed with ARM920T core,0.13um CMOS standard cells and a memory compiler. It's low power, simple, elegant and fully static design is particularly suitable for cost- and power-sensitive applications. It adopts a new bus architecture known as"Advanced Microcontroller Bus Architecture". This processor offers outstanding features with it's CPU core. It is a 16/32-bit ARM920 RISC processor designed by Advanced RISC Machines Ltd. The ARM920T implements MMU,AMBA BUS, and Harvard cache architecture with separate 16KB instructions and 16KB data caches,each withan 8-word line-length. By providing acomplete set of common system peripherals, the S3C2440A minimizes overall system costs, and eliminates the need to configure additional components.

Fig3:ARM9 S3C2440Amicrocontroller.

C. Ethernet

Ethernet is a family of computer networking technologies for Local Area Networks. Ethernet was commercially introduced in 1980 and standardized in 1983 as IEEE802.3.It has largely replaced competing wired LAN technologies such as token ring, FDDI and ARCNET.Systems communicating over Ethernet divide a stream of data into shorter pieces called frames .Each frame contains source and destination addresses and error-checking data so that damaged data can be detected and retransmitted. As per the OSI model, ethernet provides services upto and including the data link layer. Ethernet was developed at xerox PARC between 1973 and 1974.Ethernet evolved to include higher bandwidth, improved media access control methods, and different physical media. The coaxial cable was replaced with point to point links connected by Ethernet repeaters or switches to reduce installation costs, increase reliability, and improve management and troubleshooting.

Fig4:Ethernet cable

3.3Proposed System

In the proposed system,finger-print based authentication is used to enhance security to EVM. During enrollment phase,the fingerprints and details of the candidate(photo,name,constituency,voter i.d)are taken and stored in the remote server. During the voting process,the voter places the finger on finger print module. Then the fingerprint is matched with that of the data base and checks its authenticity. A second check is carried out to verify whether the voter has already voted.If the fingerprint is not validated or if the voter has already voted, then he/she is not allowed to vote.Hence,through these authentication checks, unauthorized voters and second time voting is eliminated and thus the security is ensured. If the voter is voting for the first time and has registered,then the list of parties infray is displayed on ARM LCD through which he can cast his vote. The final polling result can be viewed at central server by an authorized person using an IP address and password.

IV. Block Diagram

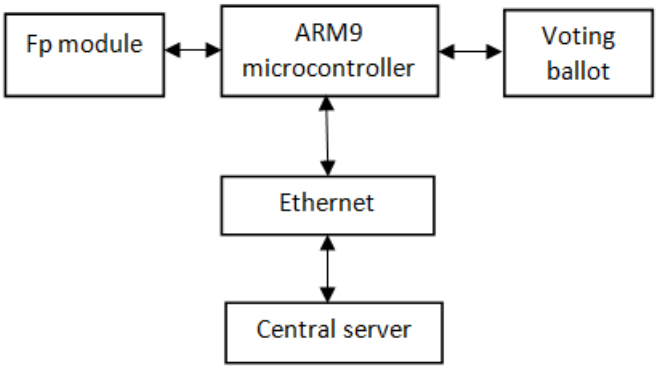


Figure5:Block diagram of proposed system

Interfacing Of Arm9,Finger-Print Module And Pc

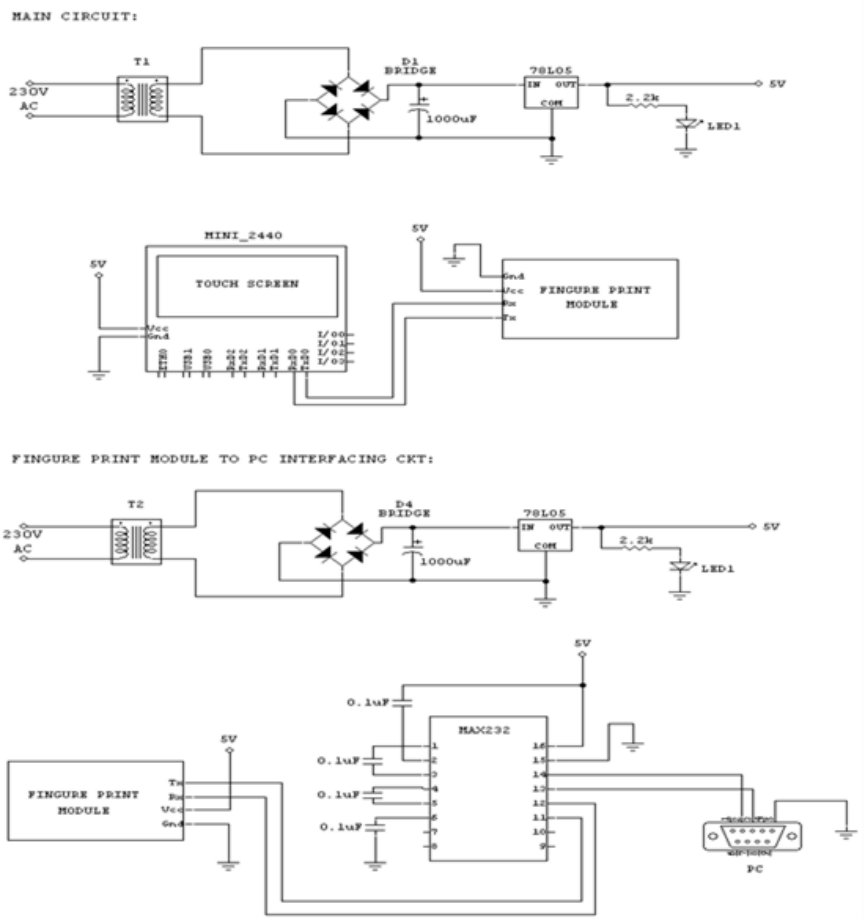


Figure6: Serial communication

The MAX232 is an IC, first created in 1987 by Maxim Integrated Products, that converts signals from an RS-232 serial port to signals suitable for use in TTL compatible digital logic circuits. The MAX232 is a dual driver/receiver and typically converts the RX, TX, CTS and RTS signals.The drivers provide RS-232 voltage level outputs (approx. ± 7.5 V) from a single + 5 V supply via on-chip charge pumps and external capacitors. This makes it useful for implementing RS-232 in devices that otherwise do not need any voltages outside the 0 V to + 5 V range, as power supply design does not need to be made more complicated just for driving the RS-232 in this case.

The receivers reduce RS-232 inputs (which may be as high as ± 25 V), to standard 5 V TTL levels. These receivers have a typical threshold of 1.3 V, and a typical hysteresis of 0.5 V.When a MAX232 IC receives a TTL level to convert, it changes a TTL logic 0 to between +3 and +15 V, and changes TTL logic 1 to between -3 to -15 V, and vice versa for converting from RS232 to TTL.

A. Interfacing Of Dm9000 And S3c2440a

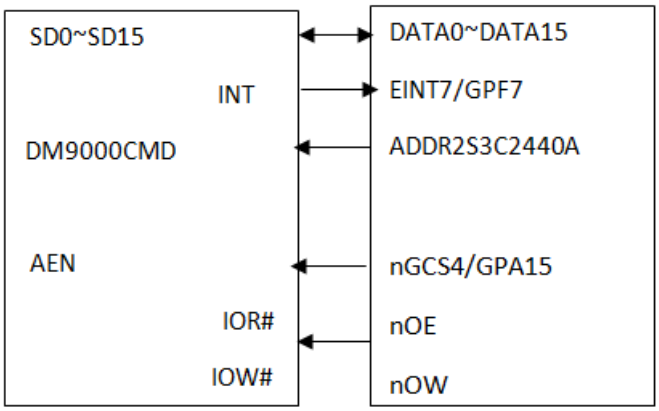


Figure7:Interfacing diagram.

The DM9000 is a fully integrated and cost-effective low pin count,single chip,fast Ethernet controller with a general processor interface,a 10/100M PHY and 4K Dword SRAM It has a very low power consumption mode and compatible with 3.3 and 5.0 tolerant I/O.DM9000 has two ports-address port and data port.Address port is used to input the address of the internal registers and dataport to complete a register read and write.DM9000 CMD pin is used to distinguish between the two ports,CMD pin is 0,the DM9000 data online transmission of register address,when the CMD pin is 1,transmission of read and write data takes place. When A8 and A9 is high,A4 to A7 is kept low and AEN pin receives S3C2440 ADDR2 pin,then two port addresses of DM9000 are defined:#Define DM_ADDR_PORT, #Define DM_DATA_PORT.

V. Functional Flow Chart

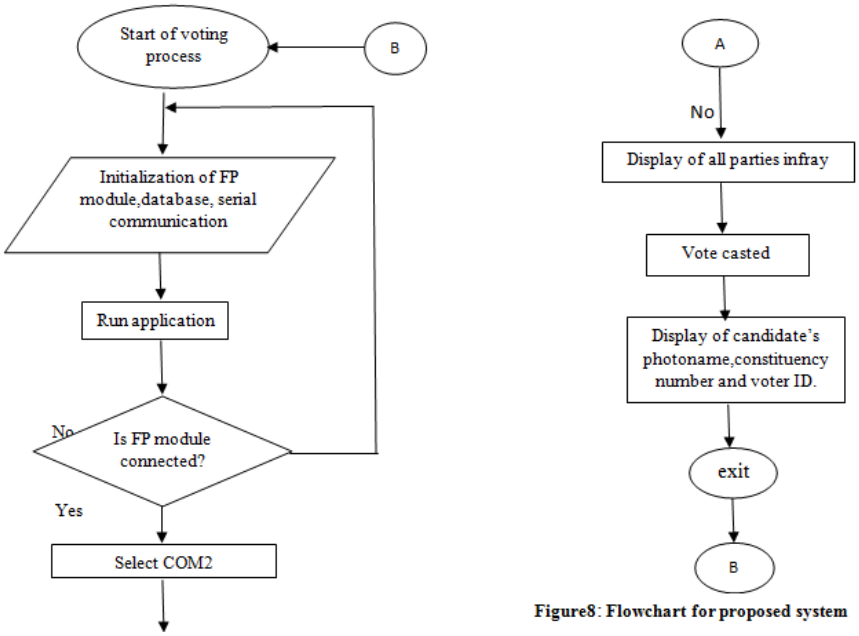


Figure8: Flowchart for proposed system

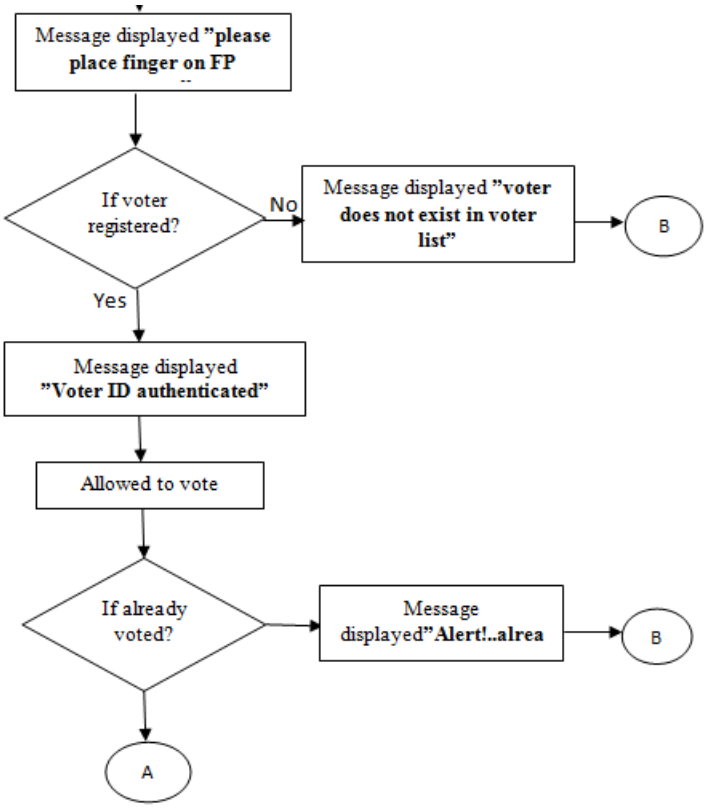


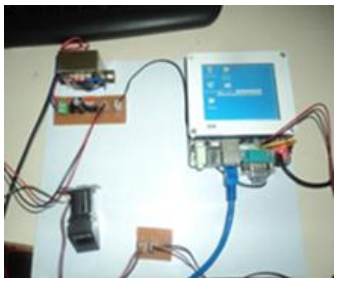
Figure8:**Flowchart for proposed system**

VI. Algorithm Of Proposed System:

Step1: Initialization of process.
Step2: It is assumed that the voters have already registered and their finger-prints and voter details are stored in remote server
Step3: Check if the voter I.D is valid or not i.e whether the candidate has registered or not by comparison of his finger with already stored finger-prints from remote server.
Step4: If the voter has not registered or if the card ID is invalid,then display the message that the user is an unauthorized person.
Step5: Else if the card is valid,then go to next step.
Step6: Check if the candidate has already voted or not.
Step7: If he has already casted his vote,then message is displayed that he has already voted and is prevented from voting for the second time.
Step8: Else, if the candidate is voting for the first time,then he is allowed to vote.
Step9: partiesinfray is displayed on LCD.
Step10: After vote casting,the candidate's photo,name,constituency and voter I.D is displayed on LCD.
Step11: The polling results are sent instantaneously to central server which is accessed by an official using I.P address and password.

VII. Implementation And Results

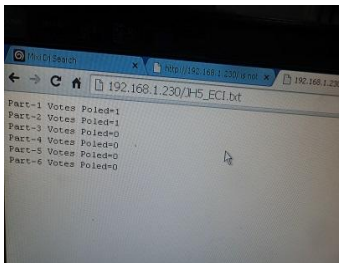
(a) Mini 2440



(b)Interfacing between ARM9 and FP module

(c)Display of voter photo,name,constituency and voter I.D after permitted to vote.

(d).Vote casted by another candidate



(e) Polling results viewed at central server

(f).Alert message for an invalid voter

VIII. Conclusion And Future Scope

This paper is used to enhance security by eliminating bogus voting and vote repetition using finger-print based authentication.As an additional security measure photo and details of the voter are displayed on ARM9 LCD from remote server and results are viewed at central server by an authorized person.In future, security of FP-EVM can still be enhanced if finger-print data can be stored and accessed from central server,

voting ballot unit is separately placed from control unit and photo and details of the voter be displayed on PC rather than on ARM9 LCD as in the present project.

References

[1]. http://www.rspublications.com/ijeted/ijeted_index.htmIssue 2,vol6,september2012 ISSN 2249-6149
[2]. http://en.wikipedia.org/wiki/Indian_voting_machines
[3]. IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 4, No 1, July 2013ISSN (Print): 1694-0814 | ISSN (Online): 1694-0784www.IJCSI.org
[4]. fig:1https://www.google.co.in/search?q=electronic+voting+machine&biw=1366&bih=657&tbm=isch&tbo=u&source=univ&sa=X&ei=r12QVIufDdG7uASWrIK4CA&sqi=2&ved=0CDYQsAQ
[5]. secugen fingerprint reader guide
[6]. FingerprintImageEnhancementandMinutiae Extraction-Raymond Thai
[7]. http://www.codeproject.com/Articles/97590/A-Framework-in-C-for-Fingerprint-Verification
[8]. http://www.neurotechnology.com/fingerprint-biometrics.html

Biographies

Prof. M Sudhakar:He is graduated (B.Tech) from JNTU College of Engineering, Hyderabad in the year 1979, with the specialization of ECE. Later completed his post graduation (M.Tech) from Indian Institute of Technology, Madras in the year 1986 with the specialization of Instrumentation, Control & Guidance. He also did his PG Degree in Aeronautical Engineering (Electronics) from Air Force Technical College, Bangalore in the year 1981. Presently pursuing his research in "Intelligent and Adaptive Control Systems, in JNTU Hyderabad. Completed R&D Project assigned by IAF on "Mathematical Modeling & Simulation of Aero Engine Control System" at Aeronautical Development Establishment, Bangalore and Gas Turbine Research Establishment, Bangalore for a period of 2 years

B.DivyaSoundarya Sai(12H51D5502),received her B.Tech degree in Electronics & Communication Engineering from JCET,Hyderabad,currently perceiving her M.Tech,Embedded Systems in CMR College Of Engineering &Technology,Hyderabad.