

Implementing New Technology in Electronic Voting System

Samiksha Suri

Abstract— Electronic voting systems provide some characteristic different 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.. The very common problem, rigging which can be faced in every electoral procedure. One candidate can cast the vote of all members or of some other members in electoral list illegally. This results in the loss of votes for other contestants. There is some scope of work in EVM, because there is no way of identification by EVM whether the user is authentic or not. To replace this system, a novel approach is introduced i.e., EVM added with a finger print verifier. By this way, a single person can vote only once and also bogus voting is eliminated since it is impossible to replicate the finger print of a person. In this paper, Zig-Bee technology is used for wireless sensor data communication. The results will be updated in Master device i.e. (personal computer) through Zig-Bee. The Master device is operated by election officer.

Index Terms— Zig-bee, Fingerprint, keypad, LCD, ARM7LPC2148

I. INTRODUCTION

The hot discussion at the end of every election is the allegations made by losing parties on the basis of bogus voting. It is true to some extent as ruling parties at the time of election misuse their power to secure power. Also it denies the people of their basic right to select a leader of their choice. So in order to protect the rights of the citizen, a fool proof mechanism of voting is needed. Our research paper aims to fulfill this requirement by adding finger print verification to the EVMs. We chose this technology because finger prints are a unique gift of nature which differs from every single human being. Voting schemes have evolved from counting hands in early days, to systems that include paper, punch card, mechanical lever, and optical-scan machines. The main objective of this research paper is to implement a system that asks the user to show his/her fingerprint as an identity proof. After pressing the identify button of the EVM he has to place his finger on the finger print sensor.

Now the finger print sensor which has optical scanner takes a picture of the finger and compares it with the one already stored in the EVM. When both the finger print matches, then the module will give a signal to the microcontroller. The microcontroller is programmed in such a way that it will give supply to the voting module only if it receives

the signal. The voting module remains off otherwise. Once the voting module gets supply, the voters can register their votes by pressing the appropriate button allotted for each candidate. After the completion of the voting of each & every person the person the results will data will be stored & updated in Zig-Bee. The data also send to Master device through Zig-Bee. The Master device is operated by election officer. After completion of the voting election officer can see the results by entering passwords. Internet census takes precautions to prevent people from stuffing the ballot box; they generally do so at the expense of voter privacy. Recent democratic elections using voting machines have shown that the winning margins could be less than the error margins of the voting systems themselves, making election an error prone task. Electronic voting systems provide some characteristic over traditional voting technique.

In this system ZIG-BEE is wireless sensor network. stealing and copying keys, re-entering PINs and This system assembles the information acquisition, information transmission, information processing units. The Characteristics of this system are low cost, low energy consumption, self-organizing networks. ZIG-BEE wireless sensor network is related to ZIG-BEE technology. This network has high potential.

Finger print biometrics are for physical access control. It can be enhanced security and improved user convenience. It can be used for high security purpose. Finger print technology in the logistics field has been widely adopted; it is recognized as one of the most important industry in this century. The function of finger print is enrolling, verifying, and store that particular finger image. It has mainly two functions as “Enroll” and “verification”. faking swipe cards. For environments requiring an extra level of security is the fingerprint biometrics can be deployed inexpensively and in tandem with existing security measures such as swipe cards and tokens for multi-factor authentication.

Enrollment:

To enroll yourself, swipe or place finger on the sensor. When using optical sensor, full finger print image is captured at one time. When captured the image to create a template using unique features. A master template is created from templates. The master template is stored securely when finger print image is not stored.

II. RELATED WORK

Authentication:

ZIG-BEE, FINGER PRINT TECHNOLOGY AND THEIR CHARACTERISTICS

To authenticate, just swipe or place finger. When using optical sensor, full fingerprint image is captured at one. The template is compared in this authentication.

A. Zig-bee technology :

Zig-Bee technology for short-range wireless communication technology. This protocol stack is formed by the physical layer, medium access control layer, network layer, security layer and application layer. Physical layer and medium access control layer are IEEE802.15.4 format. Network layer and security layers are developed by Zig-Bee purpose, application layer for user’s need. The system of Zig-Bee module of block diagram shown Figure1.

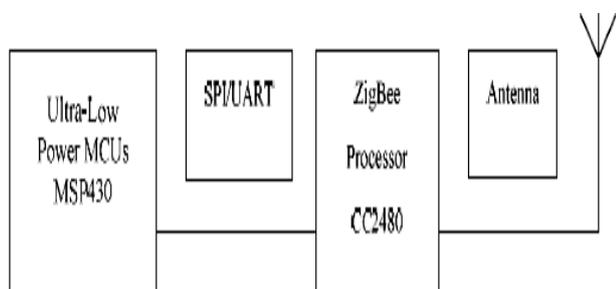


Figure 1. ZigBee module block diagram of the system

B. Finger Print Technology:

Finger print for physical access control is becoming increasingly clear enhanced security and improved user convenience. It reduces threats to traditional physical access controls such as picking locks, **Security:**

The function of physical access control is security. For biometric finger print technology, security is determined by the sensors, it can be captured high quality images.

III. HARDWARE PLATFORMS OVERVIEW

An evaluating hardware was developed with Maxstream, Zig-bee pro Zig-bee module, it consumes only 2mW and 1.25 mW power at active and sleep mode. It is compatible to transfer data up to 400 Meter range at 250Kbps. Zig-bee pro communicate based on DSSS (Direct Sequence Spread Spectrum) and it’s very suitable to Mesh, point-to-point and point-to-multipoint networks. it also gives 3V CMOS UART option to interface External devices like,microcontroller,sensors and etc. Zig-bee pro manufacturer provide XTU software package to programmed the Zig-bee module. Here LPC2148microcontroller is used to process individual systems and personal computer is used in monitoring and control station. Both of the

microcontrollers and personal computer are interfaced with Zig-bee module through UART port.

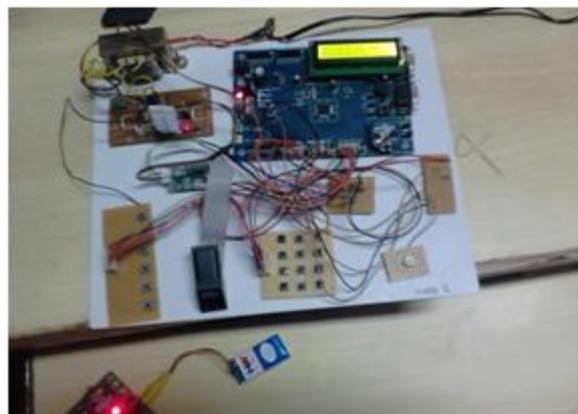


Fig2: Snap Shot of nodel (slave)

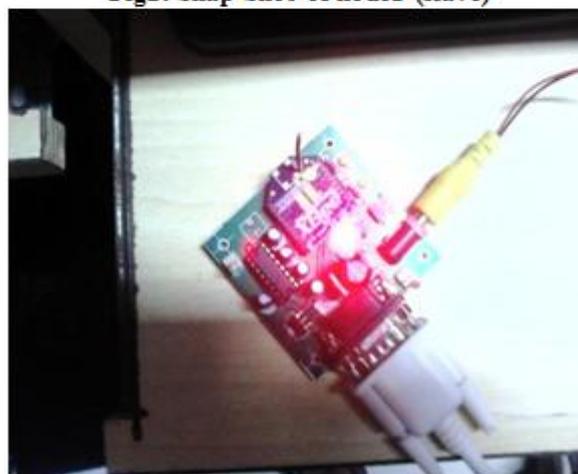


Fig3: Snap shot for master device

IV. SYSTEM IMPLEMENTATION

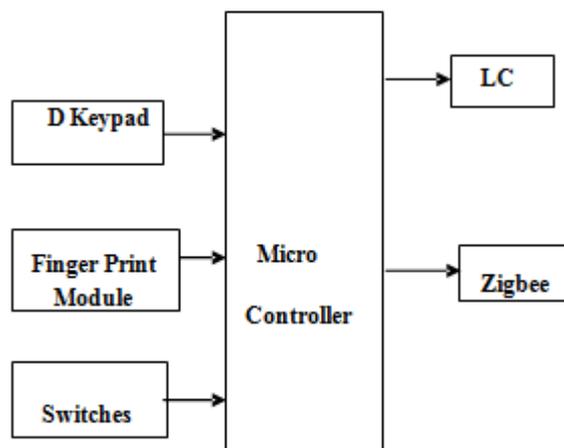


Fig4: Nodel (slave)

Here NODE2 contains fingerprint module, Zig-bee, LCD. Initially user has to enroll his finger print before the voting. Enrollment can be done with the help of finger print module. The enrolled fingerprint will be stored in database. When the person is coming to poll his vote again his

to enter his fingerprint that will be read with the help of finger print module. This fingerprints are going to compare with the already fingerprints stored in database. if it matched then microcontroller gives the supply to voting module. Then user can poll his vote by selecting party, Otherwise user cannot poll his vote. After completion of the voting of each & every person the data will be stored and updated with the help of Zig-bee.

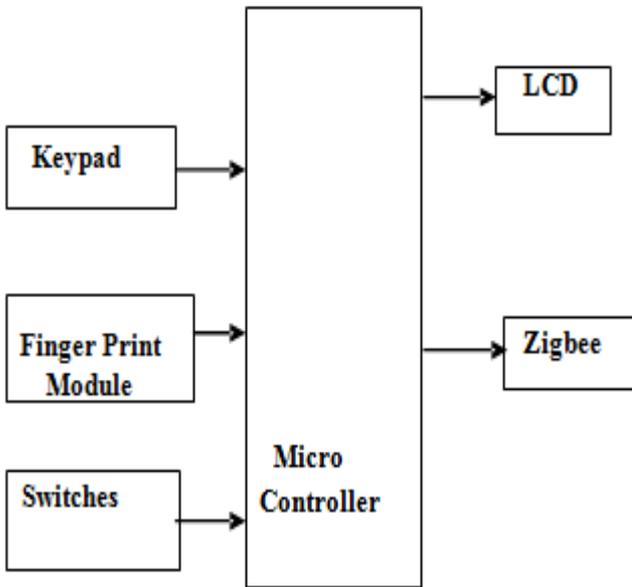


Fig5: Node2 (slave)

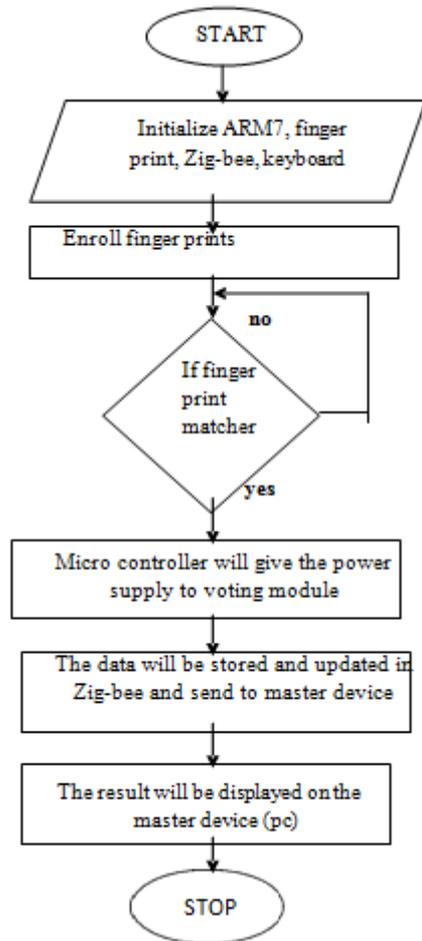


Fig7: Flow Chart

Here NODE1 contains fingerprint module, Zig-bee, LCD. Initially user has to enroll his finger print before the voting. Enrollment can be done with the help of finger print module. The enrolled fingerprint will be stored in database. When the person is coming to poll his vote again he has to enter his fingerprint that will be readable with the help of finger print module. This fingerprints are going to compare with the already fingerprints stored in database. if it matched then microcontroller gives the supply to voting module. Then user can poll his vote by selecting party, Otherwise user cannot poll his vote. After completion of the voting of each & every person the data will be stored & updated with the help of Zig-bee. Here node1 and node2 will send the data that will be stored in master Zig-bee. Master Zig-bee is connected to personal computer through max232. The master device is operated by election officer. The results will be displayed on personal computer by entering passwords.

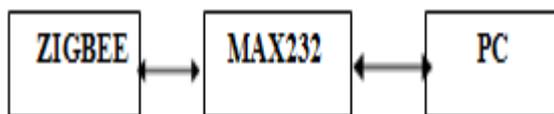


Fig6: Master device

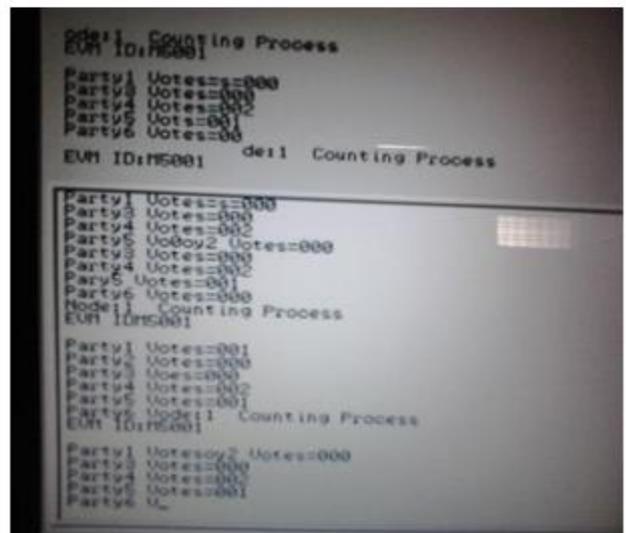


Fig8: Snap shot of result

V. CONCLUSION

In this paper, the combination of Finger print and Zig-Bee is used to achieve a secured electronic voting machine. Finger print technology is used to avoid the bogus voting. Zig-Bee wireless transmission module using a star network topology is used to store and update results and then will be sent to master device i.e., personal computer so there is no chance to change the results.

VI. FUTURE SCOPE

When the current EVM technology is innovated with networking capabilities, one can vote from anywhere in the world from any internet center provided with thumb impression/Iris device on the same day. The using of electronic voting has the potential to reduce or remove unwanted human errors. In addition to its reliability, e-voting can handle multiple modalities, and provide better scalability for large elections. E-Voting is also an excellent mechanism that does not require geographical proximity of the voters. For example, soldiers abroad can participate in elections by voting online.

The EVM software developed with minor modifications will favor the conduct of elections for both assembly and the parliament at the same time and it can also use for local body elections.

The EVM has to be designed for addressing larger population so that we can conduct election for entire country without any day intervals.

REFERENCES

- [1] Abishek matching Rawat., A Hierarchial Fingerprint system, indian institute of technology, kanpur, july 2009
- [2] Ashok kumar D., Ummal saiba Begum T., "A Novel design of Electornic voting system using Fingerprint, International journal of Innovative Technology
- [3] California Internet Voting Task Force. "A Report on the Feasibility of Internet Voting", Jan. 2000.
- [4] Chaum D., "Secret-ballot receipts: True voter-verifiable elections", IEEE Security and Privacy, 2(1):38-47, 2004.
- [5] Grizzlies D., [Editor], "Secure Electronic Voting", Springer-Verlag, Berlin Germany, 2003.
- [6] Harris B., "Black Box Voting: Vote Tampering in the 21st Century",
- [7] Zig-Bee Alliance. Zig-Bee Specification V1.0. <http://www.ZigBee.org>, 2005.
- [8] IEEE 802 Std 802.15.4. Wireless Medium Access Control (MAC) and Physical Layer (PHY). Specifications for Low Rate Wireless Personal Area Network. <http://standards.ieee.org>, 2003
- [9] JIN Shyan Lee, YANG- Chih Huang. ITRI ZB node: A Zig-Bee/IEEE 802.15.4 platform for wireless sensor networks. 2006 IEEE Conference on Systems, Man, and Cybernetics, 2006
- [10] Gritzalis D., [Editor], "Secure Electronic Voting", Springer-Verlag, Berlin Germany, 2003.
- [11] Electronic Voting Machine- A Review, Proceedings of the International Conference on Pattern Recognition, Informatics and Medical Engineering, March 21-23, 2012, D. Ashok, computer science engineering Trichy-22. Tamil Nadu, India.