Secure Voting using Aadhaar Database and Wireless Technology

Mariyat.P.A.[1], Ramya.L[2], Sumathi.R[3], Ms.Preethi Vinnarasi[4]

ECE Department, DMI College of Engineering, Chennai, Tamil Nadu, India

Abstract— *This paper proposes a secured voting gadget which uses Aadhaar database to keep away misconceptions which might be taking place in elections. The gadget ensures authentication of a person by identifying and evaluating the photograph taken and which is available in the Aadhaar database. It ensures accuracy, transparency and produces the overall vote casted for a specific candidate. If a person, who has already casted vote, enters into booth along with his Aadhaar card for the second time balloting, then the information of that person will be displayed. This technique is used to keep away from bogus votes.*

Keywords*— *RFID , Ballot , Weigand technology.

I. INTRODUCTION

India, being the second largest country in population-voting is compulsory and also a human right. We need to increase superior and fool evidence automation mechanism for secured and cheaper balloting. In India, so far no communicable balloting happened. We are able to use devices like RFID, finger print scanner, and eyeball sensors for authentified security along with automated face reading. in the proposed system ,no storage will be allowed at the vote casting region. Using Embedded and RF technology, we can transfer the voted data's on line to the master server unit. Properly crafted software will be developed with foolproof mechanism. In final, when the final voter cast the vote, the total will be declared immediately.

II. EXISTING SYSTEM

E-voting is an election system that permits a voter to file their ballots in an electrically secured method. In paper based election, Casted votes will be sealed in a box and counted manually when the election period ends. Fingerprints are certainly one of many kinds of biometrics used to perceive individuals and confirm their identity in election process. The problem present in fingerprint verification technique is, the person's identity might be mismatched with another person who's fingerprint pattern is close to the actual pattern. Other methods such as eyeball sensing technique can be implemented for identity verification. But the similar problem arises here such as mismatching.

III. PROPOSED SYSTEM DESIGN

✓ **PIC-Microcontroller and personal computer:**

Peripheral Interface Controller (PIC) is an embedded controller. PIC Micro controller has the several advantages such as Fast Data acquisition, Compactness, Accuracy. Here PIC used to Inter-Connect the ALS kit and personal computer. Output of the ALS kit will be given as input to the personal computer and output of personal computer will be given as input to the ALS kit through PIC. Personal computer here used for monitor the data, which are all, acquired from ALS kit by PIC.

✓ **RS-232 Converter:**

This is a serial port connector and voltage regulator. RS-232 converter used to make connection between PC and PIC and make voltage regulation between them. (PIC: 5 volts, PC: 10 volts).

✓ **26 BIT weigand converter:**

The composition of the open de facto 26 Bit Weigand industry standard has 8 bits for the facility code and 16 bits for the identity number field. Mathematically, these eight facility codes allows for a total of 256 (0 to 255) facility codes, while the sixteen id number bits permit for a total of 65,536 (0 to sixty five, 536) individuals within each facility code.

- ✓ **RFID Reader**

An RFID reader accomplishes following tasks – it gets commands from the application software; and it communicates with tags. Readers can be stationary, hand held or set up on mobile objects. The reader transmits radio waves via an antenna. The important attributes for a reader are study range, read fee and handle tag or reader sign collisions. These attributes are dependent on the frequency of the radio waves – generally used frequencies are 125~134 kHz, 13.5MHz, 415MHz, 868-925MHz, and 2.4GHz.

- ✓ **RFID Tags:**

A RFID tag consists of a silicon chip that stores data and an antenna that receives instructions from reader and also transmits data to the reader. These RFID tags can be active or passive, read-only or read-write. Based on the application requirements, the relevant tag type can be selected.

3.1 Requirements for secure voting

- ✓ **Authentication:** Only the authorized and certified voters can cast their vote.
- ✓ **Confidentiality:** Nobody can determine the details of vote casted by an individual voter.
- ✓ **Simplicity:** The system is designed to be extremely simple
- ✓ **Accuracy:** The system shall collect the votes and display the number of votes accurately.
- ✓ **Uniqueness:** No voter is able to cast their vote more than once

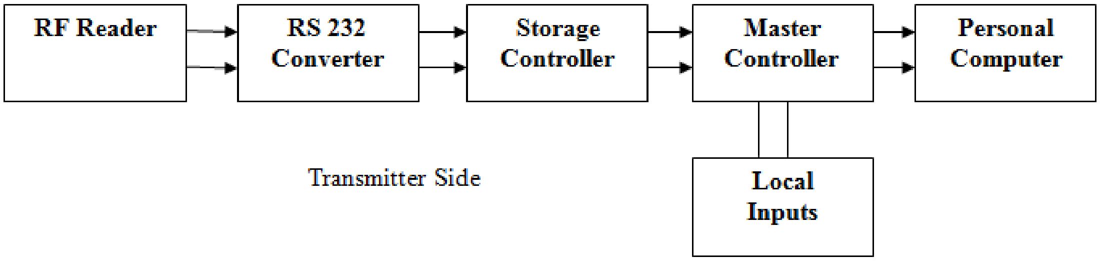

FIG.1. BLOCK DIAGRAM OF PROPOSED SYSTEM

IV. IMPLEMENTATION

In this proposed system, polling process is made secured and simple using Aadhaar RFID. RFID stands for radio frequency identification. The Aadhaar card contains all the personal details of the voter including his photograph. When a voter comes to cast vote, the first phase of identification will be done by storage controller. Storage controller checks whether the ID is valid or not. The person will undergo second phase of identity checking if the Aadhaar ID is valid. In this phase, a system consists of a database that has complete details of the voter is provided and the master controller will be used to identify the image by comparison. The person's face is manually compared with the image displayed in the system from aadhaar database. If the images compared are valid, then the time at which the person entered will be saved and voting pad will be enabled by the polling booth officer.

If the images are not valid, then it displays that the data is invalid. This voting pad will be active only for 30 seconds and after the allowed time, voting pad will be disabled. The voter should cast the vote within the certain time limit. If the voter is unable to cast vote within given time limit, then the election officer must enable the voting pad again. Once a vote is casted, the system will be disabled automatically. Whenever the vote is casted, they will be directly sent to the election commission server using wireless technology. Then the overall votes for a particular candidate are calculated. In this process there is no possibility for bogus votes. No person will be able to determine the details of the voter. This method ensures has high security, accuracy and simplicity

V. CONCLUSION

In this paper, we have proposed a vote casting gadget which is better and faster than existing systems. The new system ensures transparency, maintains integrity of the balloting technique and prevents fraudulent voting. This system checks eligibility of voter and avoids multiple votes from the same person by disabling the voting pad.

REFERENCES

[1] Fingerprint Based e-Voting System using Aadhar Database. International Journal For Research In Emerging Science And Technology, Volume-2, Issue-3, March-2015. Rohan Patel, Vaibhav Ghorpade, Vinay Jain and Mansi Kambli.

[2] Design of Secure Electronic Voting System Using Fingerprint Biometrics and Crypto-Watermarking Approach.I.J. Information Engineering and Electronic Business, 2016, 5, 9-17.Olayemi M. Olaniyi, Olugbenga Joseph.

[3] Fingerprint and RFID Based Electronic Voting System Linked With AADHAAR for Rigging Free Elections. International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering. B.Mary Havilah Haque, G.M. Owais Ahmed, D. Sukruthi, K. Venu Gopal Achary, C. Mahendra Naidu.

[4] Design of secure electronic voting system using fingerprint technique. IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 4, No 1, July 2013. Sanjay Kumar, Manpreet Singh.

[5] A Fingerprint Identification Algorithm for Integration into an Electronic Voting Machine using a Microcontroller. The Pacific Journal of Science and Technology .Volume 13. Number 1. May 2012. Jonathan A. Enokela, Ph.D.