AADHAR CARD BASED ELECTRONIC VOTING SYSTEM

[#1] R. Sri Ganesh, [#2] S. Shivashankar, [#3] N.U.Sanjay Krishna, [#4] N. Vidhyalakshmi.

[1,2,3,4] *Department of Electronics and Communication Engineering, Easwari Engineering College, Ramapuram, Chennai.*

---***---

Abstract- *This paper introduces a new method of secured voting system. The conventional voting mechanism follows the issue of voter id and other details which is generated manually. So, there are chances of parallax errors. To avoid this, automation had been developed. The details of the voters are extracted from aadhar card database. OTP (One Time Password) will be sent to the persons through their mobile phones to enter in the keypad. At the time of voting fingerprint authentication and OTP is required for the voter. When people cast their vote the results will be updated automatically in IOT (Internet of Things). As soon as they cast their vote, their voter id and other details will be erased automatically and the aadhar card details which they used will be tracked and will be locked to access again. Results will also be published on the same day of election.*

Keywords- **IOT, Fingerprint, OTP, Aadhar card, keypad.**

1. INTRODUCTION

Voting is the freedom of the people in a democratic country. The current voting system is called as Electronic voting system. It uses electronic ballot to store votes. Sometimes fake display units can be installed in order to show manipulated numbers but fake votes will be generated in the backend. Such fake display units are commonly available in the market so there will not be a need for hacker to hack the device. The people who are in powerful government position can do this within overnight with their money and powers they possess. Then what about democracy? What about people's who vote? The Democracy principles depend upon the people's decision. So, to have great vision we need to take correct decision. This can be made by "voting". The conventional voting mechanism follows the issue of voter id and other details which is generated manually. It leads to many manual errors. Moreover the electronic voting machine may be devised in a such a way that people whomever they vote, will be converted into some other's party or candidates. It may be misused in many ways. Electronic voting is the usual way of voting. E-voting (Electronic Voting) is one in which a representative supervises when the person castes his/her vote. I-voting (Internet Voting) is one in which the voter votes from home with the help of the internet.

2. OVERVIEW

The details of the persons who are above 18 years are extracted from aadhar card database.OTP will be sent to the persons mobile phones. At the time of voting, the user can give their fingerprint authentication and specify OTP in keypad. Once the voter casts the vote, the vote gets stored in the server which is made possible using the IOT. By this way we can avoid fake votes and multiple votes casted by the same voter. The server gets update automatically after each vote is casted. So by the end of the voting process we can directly get the results from the server and announce the results on the same day.

2.1. Hardware architecture

In our proposed model we make use of the PIC controller for processing data and fingerprint sensor to detect the fingerprints for authentication and security. It takes the fingerprint access from the voter to allow the person to cast the vote. It also consists of a power supply, LCD display, Buzzer, Keypad, UART and mobile phone as the receiver unit.

2.2. IOT technology

For this voting system we use the IOT technology to store the votes. A server is created and the votes are stored and updated automatically. By doing this the results of the election can be announced on the same day which is much easier than the counting process.

2.3 Working

The power supply acts as the source for the kit. The buzzer is used to acknowledge once the voter has casted the vote successfully and also to alert when a user has voted multiple times. The keypad is used to enter the OTP which has been sent to the mobile unit which is registered already in the aadhar card. The voting unit is used to cast the vote to the preferred party and the LCD display is used to display the name of the party for which the voter has voted. All the information and details are stored and updated into IOT. So at the end of the voting, results can be published immediately by retrieving the data from cloud server.

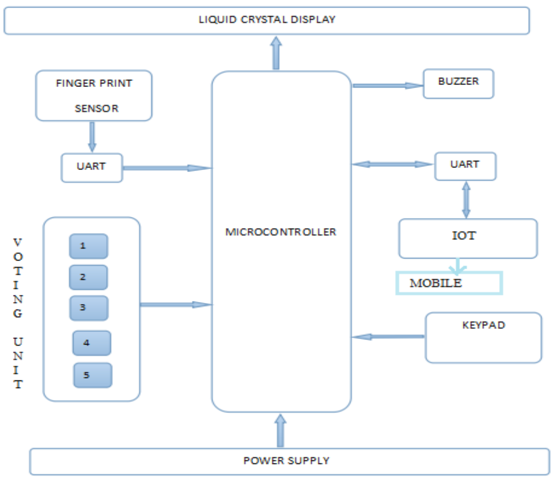


Fig -1: Block diagram.

2.4 Implementation

Initially the power supply is switched on to start the process. A step down transformer is used to convert AC high to AC low voltage and current. The bridge rectifier is used to convert the AC to DC. In order to reduce the noise present in the DC signal the capacitor is used to filter it. The circuit requires only 1A and 12v supply. The PIC microcontroller has 40 pins out of which 32 pins are used for I/O operations (Input and output). Port A is connected to the fingerprint sensor, Port B is connected to the keypad, Port C is connected to the Buzzer and the Port D is connected to the LCD display respectively. Then sim card is inserted in the IOT. Now the fingerprints are registered using the sensor and once the fingerprint is verified with the aadhar card database, an OTP is sent to the receiver unit. This OTP is entered in the keypad. If the entered OTP is correct the vote can be casted by selecting the party else the LCD display shows wrong OTP and the buzzer also notifies the wrong OTP entered. The votes casted by the candidates are stored in the server through IOT cloud.

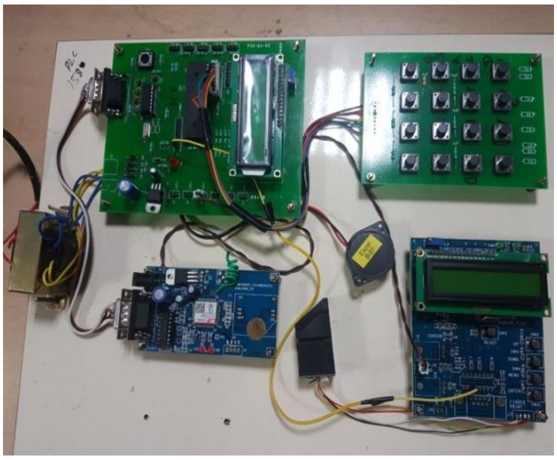
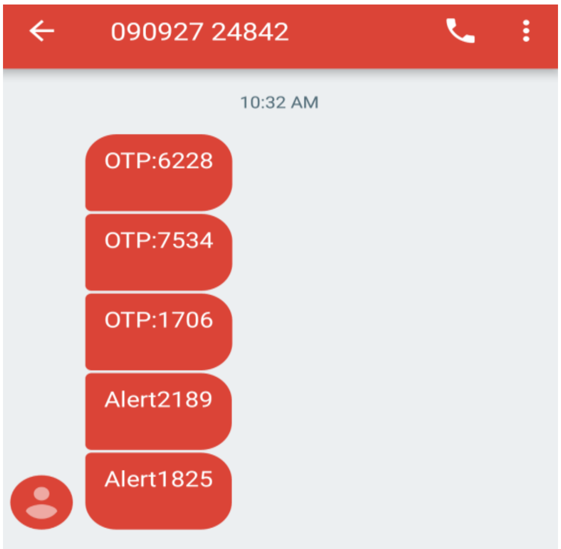


Fig -2: Electronic voting system kit



090927 24842

10:32 AM

OTP:6228

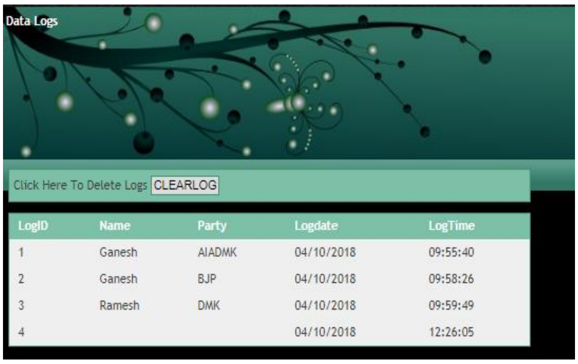
OTP:7534

OTP:1706

Alert2189

Alert1825

Fig -3: OTP Notification



Data Logs

Click Here To Delete Logs CLEARLOG

LogID	Name	Party	Logdate	LogTime
1	Ganesh	AIADMK	04/10/2018	09:55:40
2	Ganesh	BJP	04/10/2018	09:58:26
3	Ramesh	DMK	04/10/2018	09:59:49
4			04/10/2018	12:26:05

Fig -4: IOT Cloud for results

3. Conclusion

The proposed system consists of a few additional components in order to improve the security and also to provide authentication. This paper tells about the new way of voting system. This kit can be further minimized to small size with more advanced technologies. This eliminates difficulties faced due to the fake voting and reduces the vote counting time since IOT technology is used. In future, I-Voting can also be changed with these security measures where face recognition can be used instead of fingerprint biometric. It reduces the queue standing for voting since everyone can vote from their house itself.

REFERENCES:

[1] Cetinkaya, O. &Cetinkaya, D. (2007) “Towards Secure E-Elections in Turkey: Requirements and Principles”.

[2] Brennock, M. (2004) Cabinet to press ahead on E-voting in EU and local polls. *The Irish Times*.

[3] Jefferson, D.R., Rubin, A.D., Simons, B., and Wagner, D. (2004) *A "Security Analysis of* the Secure Electronic Registration and Voting Experiment (SERVE)".

[4] Gritzalis D, editor. (2002) Secure electronic voting. Advances in information security.

[5] Chaum, David (2000) Secret-Ballot Receipts and Transparent Integrity.

[6] Cranor, L. &Cytron, R. (1997) "Sensus: A Security-Conscious Electronic Polling System for the Internet".

[7] Benaloh, J.& Tuinstra, D. (1994) "Receipt-free Secret-Ballot Elections", *In Proceedings of the 26th ACM Symposium on Theory of Computing (STOC'94)*, Montreal, Canada.

[8] Chaum, D. (1982) "Blind Signatures for Untraceable Payments".

[9] Chaum, D. (1981) "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonym.

[10] California Secretary of State Ad Hoc Touch screen Voting Task Force Report.