Design and implementation of convenient and compulsory voting system using finger print sensor and GSM technologies

Abstract: **India is a developing country, where still the electronic voting system is under threat due to the rigging in elections. The future of country is decided mainly by the elections, so the electronic voting machine must be trustworthy. The existing voting system, doesn't have person identification, so that there are chances to misuse the others' rights. Fingerprint based authentication for voting is proposed in this paper, which eliminates the misuse in voting. GSM module is incorporated with finger print sensor to collect the data before election. The proposed model is implemented in Arduino for effective authentication and quick process with more flexibility. GSM module is used to transfer the collected information to nearby taluk office or district office so that the authorized persons will access the information.**

***Keywords*—Fingerprint sensor module, GSM, Arduino, voting machine**.

I. INTRODUCTION

India is a world's largest democratic country and the democracy principles are based on people's decision. For the great future of country, the elections need to be conducted without any rigging. Elections allow the people to choose their leaders according to how they wish to be governed. The conventional voting mechanism uses the voter id or any other documents as identity proof to pole the vote manually. At present the voting system is moved into Electronic Voting Machine (EVM) to reduce the human burdens and improve the security. Due to its reusable nature, it reduces the election conduction cost and supports large scale election operations. However, EVM system has few security flaws and is more vulnerable than traditional process. The security system must provide more authentication, confidentiality, voter privacy etc. There were many negative opinions by experts on e-voting due to its authentication process. To improve authentication and confidentiality, a finger print based system is designed and implemented in the proposed model. Every human being has their unique fingerprints. The fingerprint sensor module captures fingerprint image and is stored in the Arduino processor in its equivalent form. The votes in traditional system is counted manually, in this system that count is also done automatically performed by the processor so that the duplicate or false counting can be avoided. The fingerprint scanning system demands the voter to enroll before the voting sessions. The main objective of the proposed system uses the fingerprint for authentication of the desired person. The peoples need to enroll a few days before the voting process starts using fingerprint sensor. To authorize a person the essential details are enrolled by seeing their voter id. The details are shared with server located in the district / Taluk office and details are centralized. On the day of voting, the voter can choose any of the voting station for the voting. The voter needs to authenticate themselves and if the fingerprint matches with server data, then candidate could able to pole their vote. The total count of that voting station is sent to taluk or district office at end of the day. Rest of the paper is organized as follows: Section II describes about the existing technologies and current voting systems. Section III describes about the proposed system. Section IV describes the result analysis of the system. Section V presents the conclusion and future scope of the proposed system.

II. RELATED WORK

The voting system is changing since many years. Jhani et al designed a system by with RFID tag on voter id. When the voter comes for voting to polling booth then RFID needs to be swiped to decide whether voter id belongs to particular booth. If it matches the voter can vote. In order to avoid duplicate of votes, Md. Mohiuddin proposed the system using smart card and iris recognition. The voter ID card is replaced by smart card. The authorized person with the smart card is allowed for voting, if gets matched with iris pattern. Ishani et al. proposed a system for scanning facial image through deep learning algorithms. The face recognition scanner verifies with pre-captured images in the database during the voting. Srivatsa Sridham implemented an online voting system. The most of Indian population is illiterate; this system can't be utilized all over the country. Soma Bhattacharya. proposed a system with wireless based voting system using iris pattern for the authentication. Dr. Usmani explained about different types of voting system on online with their advantages and disadvantages. Our country existing voting system is by seeing the Govt. Ids and permitting the person to vote. There are chances of fraud or fake voting in this process. So, to avoid chances, a design is proposed using fingerprint for voting.

Table 1: Different voting types with its disadvantages

Sl. No	Voting type	Hardware	Disadvantages
1	Voting by ballot paper	Ballot box and paper	Papers are collected and counting is done, then results are announced.
2	EVM	Ballot and control units	The difficult task is the complexity of system
3	Remotely voting using internet	Software, internet and website	The internet is must for the system with high speed
4	Biometric voting	Fingerprint scanner and Arduino	Suitable for small scale

Table 1 describes about the hardware and disadvantages of different voting types.

III.PROPOSED SYSTEM

The flow chart of proposed system is shown below.

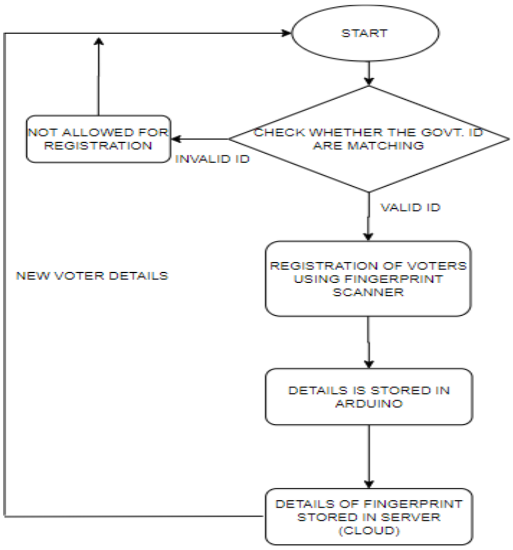

START
NOT ALLOWED FOR REGISTRATION
CHECK WHETHER THE GOVT. ID ARE MATCHING
INVALID ID
VALID ID
NEW VOTER DETAILS
REGISTRATION OF VOTERS USING FINGERPRINT SCANNER
DETAILS IS STORED IN ARDUINO
DETAILS OF FINGERPRINT STORED IN SERVER (CLOUD)

Fig 1: Registration of voters

Figure 1 describes about the registration process of voters. The voter is checked with the any Government ID like Aadhar, PAN card, voter id etc. If it valid and matches then, the registration of voter is done by using fingerprint scanner. The people are told to place the fingerprint onto fingerprint sensor module. This data of fingerprint is stored in the Arduino for authentication when they come for voting. This data is transferred to server and stored as database which can be accessed by any voting station from authorized person only. The advantage is that the voter has flexibility to vote from any nearby voting station. If the Govt. Id's won't match with their face, the address and other parameters, then that person is not allowed for voter registration. The data from Arduino is stored and is transferred to the server using GSM module. Once the data is stored in server and its security to server is provided by server seeding.

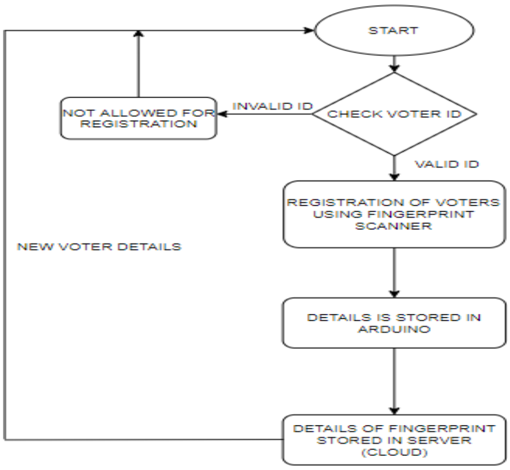

START
NOT ALLOWED FOR REGISTRATION
INVALID ID
CHECK VOTER ID
VALID ID
NEW VOTER DETAILS
REGISTRATION OF VOTERS USING FINGERPRINT SCANNER
DETAILS IS STORED IN ARDUINO
DETAILS OF FINGERPRINT STORED IN SERVER (CLOUD)

Fig 2: On the day of voting

Figure 3 describes the voting day process. On the day of voting, the voters are informed to place their fingers on the fingerprint reader. The finger print reader senses the ID and sends this information to the Arduino. After receiving the ID, the Arduino checks for authorization, if its fingerprint is valid then this person is allowed to vote. Keypad or switches is used for selecting the voting preferences. After selecting voting preference, the LED will be turned on for the particular key or switch pressed. After the voting done for the day, the controller calculates the total votes for that day. The total count of vote's information is sent to the taluk office or district office data base. If the voter id fingerprint vote match, then thatperson is not allowed to vote.

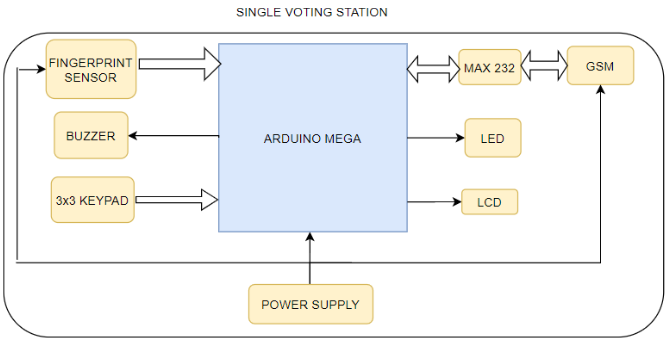


fig3: Proposed system blocks of voting station

The figure 3 describes about the basic block diagram of the voting station. In the propose system, the disadvantage of existing system can be eradicated. The system consists of Arduino mega2560, GSM module, 16x2 LCD, Max 232, buzzer, 3x3 keypad and fingerprint scanner.

The main hardware tools required for the system are:

1) *Arduino mega2560*: Arduino is [13] open-source prototyping platform. It has an Integrated Development Environment (IDE) where the uploading of the program can be done on the physical board. The Arduino mega2560 is four times faster than the Arduino Uno.
2) *Fingerprint sensor (R307)*: This fingerprint sensor can be connected to personal computer. The sensor makes the loading, detecting and verification very simple. It can store up to 162 fingerprints on its flash memory. Firstly, the enrolling of fingerprints is done with specific IDs. After enrolling, the verification can also be done based on the IDs.
3) *GSM (Global System for Mobile communication) module:* It's a modulator-demodulator (modem) module. It can be operated by inserting the SIM card [15] and operated over the mobile operator subscription. This module communicates over mobile network for sending and receiving messages.

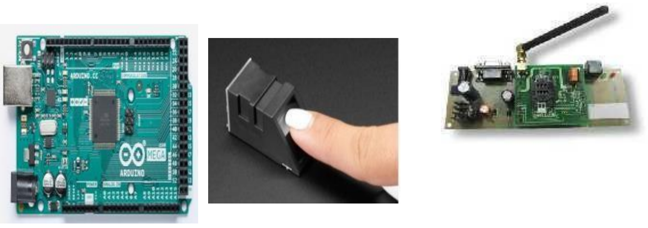


Fig 4: Main hardware components for the proposed system

The figure 4 shows the main components for implementation of proposed system. The sequence contains Arduino, fingerprint sensor and GSM module

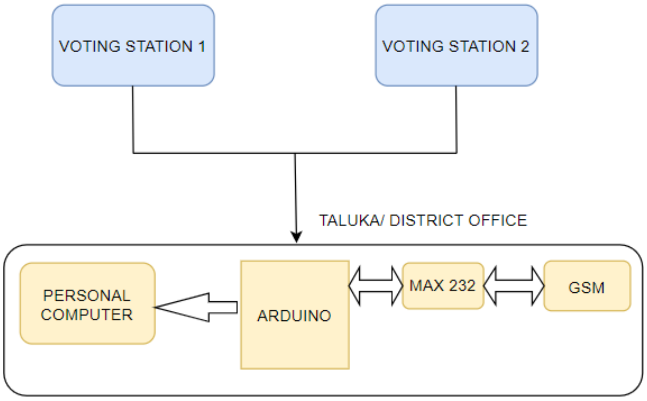


Fig 5: Interconnection of voting stations with Talk/ district office

Figure 5 describes about how the total count of number of votes received by the voting stations. For the implementation, two voting stations with a Taluk/ district office interface are addressed. The voter can vote from any of the two stations for voting. In the existing technology, the voter can vote in the particular voting station decided by government based on the voter id. If voter goes to some other voting stations, the voter is not permitted to vote. The proposed system can enable the voters to vote in any voting stations. The number of votes casted in voting station is counted and this detail is sent to central office through GSM. Central office receives these details via GSM and is displayed in PC placed in central station. The total votes in all the voting stations can be counted.

V. RESULT ANALYSIS

The proposed system hardware model of two voting stations is shown in figure 6.

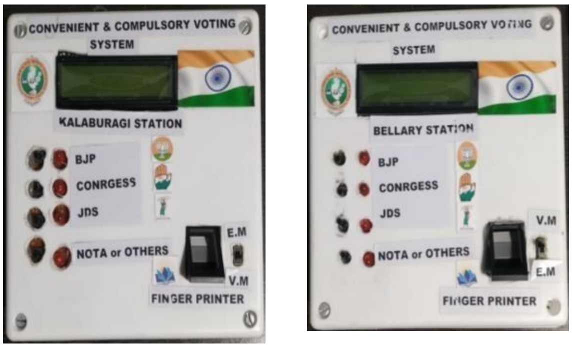
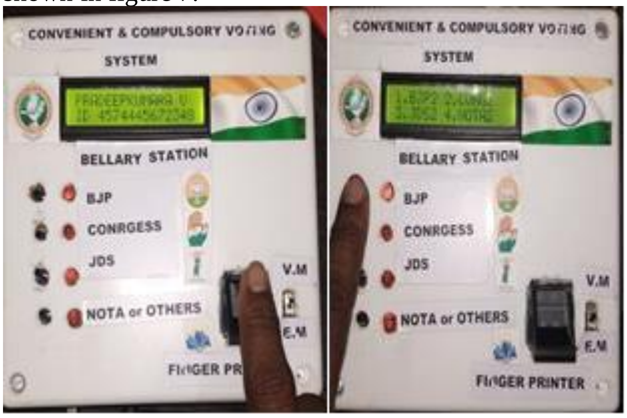
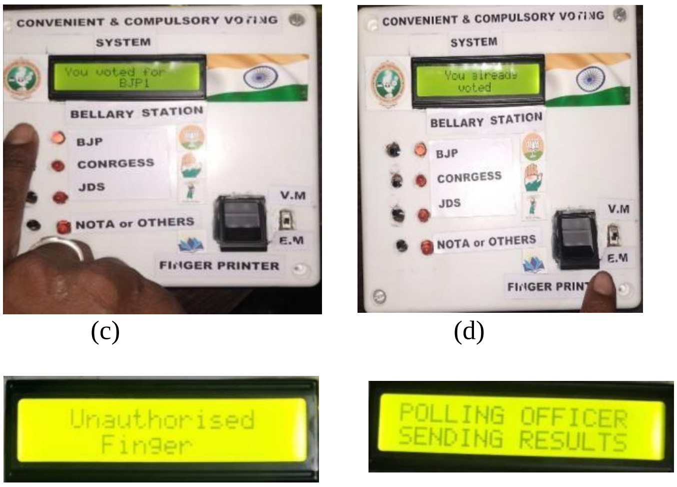


Fig 6: The two different voting stations voting machines

In the prototype the stations are named as Kalaburagi and Bellary station. It has 3 parties' switches in front of their names and NOTA (none of above). The voter is allowed to vote after authentication. The voter places the finger; the LCD displaces the name of voter and its unique ID for confirmation. The voter can vote by pressing the switches of any of the 4 options. If authentication is invalid which does not match with Arduino Mega2560 microcontroller database then LCD displays as "unauthorized finger" with the buzzer sound as shown in figure 7.



(a) (b)

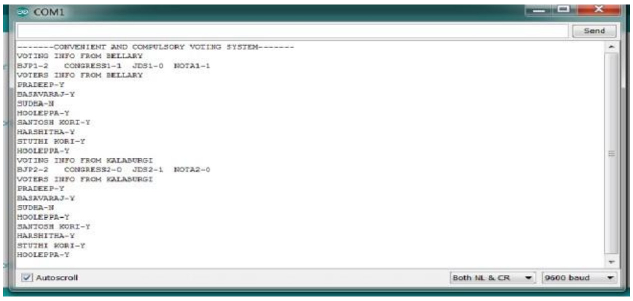


(c) (d)

€ (f)

Fig 7: sequence of steps in voting system. A) placing the finger on fingerprint scanner b) voting for the desired party c) LCD displays which party the voter has voted d) already voted e) invalid fingerprint f) polling officers sending thevoting information.

If the same voter comes for voting again then after authentication, the voter when places finger the fingerprint scanner matches and displays as “You already voted”. If the voter tries to vote again, the system rejects the vote. If the voter has registered in any voting station cam vote from any other voting station also. After all the votes have been casted at the particular station, polling officials must Place the finger. If the officials’ fingers valid it will communicate with sever or central station as shown in Fig 7. The voting information on that particular day are sent to district/ taluk office through GSM module and its displayed-on PC using sketch Arduino
1.8.5 software for serial monitor as shown the total final count of votes and the total count of each party will be must match while verification. The figure 8 shows the display on the PC of the voting information.



```
-------CONVENIENT AND COMPULSORY VOTING SYSTEM-------
VOTING INFO FROM BELLARY
BJP1-2    CONGRESS1-1   JDS1-0   NOTA1-1
VOTERS INFO FROM BELLARY
PRADEEP-Y
BASAVARAJ-Y
SUDHA-N
HOOLEPPA-Y
SANTOSH KORI-Y
HARSHITHA-Y
STUTHI KORI-Y
HOOLEPPA-Y
VOTING INFO FROM KALABURGI
BJP2-2    CONGRESS2-0   JDS2-1   NOTA2-0
VOTERS INFO FROM KALABURGI
PRADEEP-Y
BASAVARAJ-Y
SUDHA-N
HOOLEPPA-Y
SANTOSH KORI-Y
HARSHITHA-Y
STUTHI KORI-Y
HOOLEPPA-Y
```

Figure 8: voting information display in district / taluk office

V. CONCLUSION AND FUTURE WORK

Finger print-based authentication for secure voting is presented in this research work. The security issues in electronic voting machine are reduced by introducing finger print based authentication and GSM based data sharing for effective and transparent election process. The proposed model attains better results and provides more advantages to the candidates to pole their vote at any location. It reduces the human interference and issues in voting count process. To improve the security of the system, the information must be encrypted and stored. This helps to avoid data leakage and provides more privacy to users. The collected votes are sent to main server which is in taluk/ district office as centralized process. This proposed system avoids fake voting. The limitation of this prototype is present in its fingerprint acquisition process. Since the finger print gets tampered due to age, work and other factors such as skin problems, wet hands. so that the system may lags to recognize them. The future scope of the research could be implementation of iris scanner along with the fingerprint for more secure and reliable operation. It may reduce the limitations in finger print based operations. The proposed system can also be made online in future for e-voting. The system can be done automatic without any human interference during voting. Only single person should be allowed in the room, the single person identity can be checked with the help of lasers. The co-relation between fingerprints can be obtained in order to reduce the storage place in the server and to enhance the performance of system.

REFERENCES

[1] R. Bhuvanapriya, S. Rozil Banu, P. Sivapriya, and V. K. G. Kalaiselvi, “Smart voting,” *Proc. 2017 2nd Int. Conf. Comput. Commun. Technol. ICCCT 2017*, pp. 143–147, 2017, doi: 10.1109/ICCCT2.2017.7972261.

[2] K. M. R. Alam and S. Tamura, “Electronic voting using confirmation numbers,” *Conf. Proc. - IEEE Int. Conf. Syst. Man Cybern.*, no. October, pp. 4535–4540, 2009, doi: 10.1109/ICSMC.2009.5346787.

[3] M. J. Moayed, A. A. A. Ghani, and R. Mahmod, “A survey on cryptography algorithms in security of voting system approaches,” *Proc. - Int. Conf. Comput. Sci. its Appl. ICCSA 2008*, pp. 190–200, 2008, doi: 10.1109/ICCSA.2008.42.

[4] B. Ondrisek, “E-voting system security optimization,” *Proc. 42nd Annu. Hawaii Int. Conf. Syst. Sci. HICSS*, pp. 1–8, 2009, doi: 10.1109/HICSS.2009.173.

[5] M. Charitha and K. U. Raju, “Electronic Voting System using Finger Print Based on Aadhar,” vol. 6495, no. 4, pp. 96–99, 2017, doi: 10.22161/ijaers/nctet.2017.ece.26.

[6] J. B. Shaik and M. H. Shaik, “Voter Identification and Detection System using RFID and GSM to stop rigging in the elections,” vol. 2, no. 6, pp. 1544–1546, 2014.

[7] M. Mahiuddin, “Design a Secure Voting System Using Smart Card and Iris Recognition,” *2nd Int. Conf. Electr. Comput. Commun. Eng. ECCE 2019*, pp. 1–6, 2019, doi: 10.1109/ECACE.2019.8679118.

[8] I. Mondal and S. Chatterjee, “Secure and Hassle-Free EVM Through Deep Learning Based Face Recognition,” *Proc. Int. Conf. Mach. Learn. Big Data, Cloud Parallel Comput. Trends, Prespectives Prospect.Com.2019.*