Digital Voting System as Internet of Things Application

Rajashree S, Sheetal V A, Soman K S, Bhuvankumar P

Abstract*: *The objective for the efficient functioning of the Indian democracy is purely dependent on the decisions made by the citizens of our country. To avoid duplicate or illegal votes we need a secure system which uniquely identifies our citizen. In India AADHAR uniquely identifies the citizens of INDIA by their thumb impression and also provides the other details like Date of birth, address, gender, father's name, Spouse details etc. The election process is carried out in 3 steps Creation of voter list, actual voting process, and counting of votes. Creation of voter list can be done by database which is efficient to store big data with the person's name and his AADHAR number. In actual voting process verification can be done by using fingerprint recognition and votes should be stored depending on ward numbers. Counting is the last process which can be done very easily if previous steps are digitized. In the world of Internet of things a voter should be able to cast his vote from anywhere by validating his credentials. This paper describes a voting system with 3 possible ways for voter to cast his vote.

***Keywords* :Digital election system, Aadhar card, voter list, IoT Application..**

I. INTRODUCTION

Election commission is an independent body constituted under Indian constitution. It is assigned with the work of electoral commission management team. Election to legislative assembly and parliament are undertaken by this commission with the help of state and central administrative officer. The commission makes out a list of all eligible voters and publishes it after proper scrutiny in major news papers and gazette.

After making a list of eligible voters the commission with the help of survey department fixes the geographical area for each Member of Parliament (MP) and Member of Legislative Assembly (MLA) constituency. After this the commission in consultation with government of India or State government fixes the date for election and dates will be made available in all available media sources. The election process starts with such notification. The notification signifies the date for submission of application, date of withdrawal, date of verification and voting date. It also fixes date for declaring the results. Once the results are announced each winning member with a certificate for having elected under seal and signature of returning officer. They are required to take an oath in their respective legislative or parliament, which completes the process of election.

In the current voting system, the citizen who comes to vote will be authenticated by his valid identity proof with the voters list provided form the election commission to the corresponding polling station. If the ID proof matches with the voter list the person is allowed to vote. The voting system has the following units i.e. Control unit, Ballot unit, and Voter verifiable paper audit trail (VVPAT). The permission is given from control unit, the person can select the candidate and the same will be displayed on the VVPAT as proof that the person has selected the candidate of his choice and the corresponding slip will be printed and gets stored in the place provided in VVPAT.

Internet of Things refers to interconnection of machine to achieve a task[1] anywhere anytime along with or without human interactions. In the IoT digital voting system voter need not have visit the polling station but can cast his vote remotely through biometric finger print scanner using internet facility. All the data needs to be stored in a database which will be very big database[2].

II. RELATED WORKS:

[3] Proposes the smart voting by using Aadhar card for verification process where finger print of a person is matched with Aadhar, if matched his face and retina is scanned and verified. If both matches the person is allowed to vote. [4] In this thevoting takes place with the help of web so called web voting with cognitive radio technology and adhoc network. The voting process uses Aadhar ID and facial as biometric where the voters face is captured and send to Unique Identification Authority of India (UIDAI) database where after confirmation the voter is allowed to vote. This system of voting proposes two copies of casted votes. One copy is stored in the cloud and the other is the duplicate copy in local storage that guarantees correctness. More space and time required as two copies are maintained. [5] Uses Finger print, Face and Iris as biometric Verification. This system uses matrix laboratory (MATLAB) to train the data. Since the population of India is very large, training and preparing the initial eligible dataset itself is complex.[6]Uses Aadhar ID and finger print as biometric for voting purpose and also uses local database which are used in the specified region and contains data with respect to that region and central database where the complete eligible population is maintained. Maintaining databases and duplicating to several local databases andupdating are an issue. [7] Uses Aadhar for verification and finger print as biometric authentication, and proposes a Mobile App using Android for casting the vote. The drawback is that not all citizens will have android phone.

Revised Manuscript Received on January 27, 2020.

***** Correspondence Author

S Rajashree*, Assistant Professor, Departmant of Computer Science, PES University Bangalore, rajashrees@pes.edu .

Sheetal V A, Assistant Professor, Department of Computer Science, BMS College of Engineering, sheetal.cse@bmsce.ac.in, Bangalore

Soman K S, Software Consultant, Bangalore Somanks@gmail.com .

Bhuvankumar P, Student, Department of Electronics and electrical, KSSEM, Bangalore bhuvankumar1717@gmail.com .

Most of the people in rural areas may not have and are not aware of its features and its usage. Aadhar for verification and finger print as biometric authentication for non smart phone users and OTP for citizens with smart phones is proposed in [8] It may be difficult to differentiate citizens between the two authentication process i.e. Citizens with smart phone and Citizens without smart phones.

III. PROPOSED VOTING SYSTEM

This system requires a person willing to vote to send his finger print image to UADAI first where the details of the person is verified and Aadhar number is sent to the polling station which is the password for the voter. The person enters his/her 12 digit Aadhar number to enter to the voting screen. The Aadhar number entered by user and that received Aadhar number from UIDAI are matched. If match is not found invalid message is displayed. The age of voter is verified if age is greater than 18 the person is allowed to vote and the vote is stored according to ward (constituency) number and the party.

Creation of lists

This process has following steps.

1. Generation of voter list with each ward or constituency.

For generating voter list Aadhar number should be used. This ensures that no duplicate voting is done.

2. Candidate list for each constituency along with party details.

Each of the wards needs to prepare one candidate list along with party details and with address and other required parameters that should be register before election process.

3. Election date list with time slot and date for each ward.

Election date for each ward with time should be announced in all essential website and media for effective voting system.

4. Mapping of political party name to a unique ID used internally.
5. Database containing party ID and the count of votes received should be maintained with each ward. Party ID is the unique value generated by SHA 256[9] algorithm using Party name and candidate name.

After a voter casts his vote depending on his voter list the vote can be counted for party candidate in that particular ward. Here the information about voter for whom he has voted need not be stored just vote can be counted against the candidate. But if a voter has not voted than his Aadhar number can be stored for further action. If government wants they can take action against the voter who has not voted as it is duty of every responsible citizen.

Voting process:

Voting by citizen can be done in three ways to achieve full digital voting.

1. Through polling station where each ward can be given one system consisting of microprocessor (like Raspberry Pi) with a finger print scanner.
2. Through website that is with any computer or laptop with a finger print scanner where a candidate can enter his Aadhar number to enter voting system followed by finger print impression to cast his vote.
3. An android application running on a mobile with built in finger print scanner.

Through polling station:

In this each polling system needs to have a computer or a microprocessor with a display unit to display the options to the user. Providing computer to each polling station leads to huge finance as more number of polling stations is involved. Using a microprocessor along with display unit reduces the cost per polling station. Since every citizen will not be having biometric (finger print scanner[10]) polling stations are one of the main requirement in conducting elections. Each voter first scans his thumb impression to the scanner which is sent to UADAI for verification. If the voter is valid then the system displays the list of candidates who are contesting the elections from a particular constituency. The voter then can select among the list and can cast his vote or can select NOTA (None of the above) option. Once the vote is casted by voter the Aadhar ID of the voter and the unique ID of the party to which the candidate belongs will be sent in secured way to the constituency database depending on the ward number.

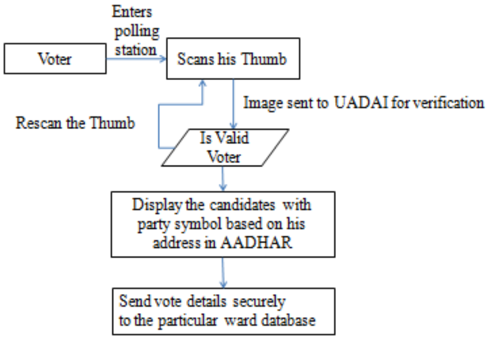

Voter
Enters polling station
Scans his Thumb
Image sent to UADAI for verification
Rescan the Thumb
Is Valid Voter
Display the candidates with party symbol based on his address in AADHAR
Send vote details securely to the particular ward database

Fig 1: Dataflow for polling station voting process

Through website:

Any voter who has the fingerprint scanner should be able to connect his biometric machine easily with the website with just a few instructions and cast his vote using the website[11]. As a voter login to the website the thumb impression is scanned and it should be sent across the internet in a secured way to verify the validity of the voter. If the scanning process indicates valid voter then the website will display the list of candidates and voter can select the desired candidate. If the scanning process does not indicate the valid voter then the voter should be given finite number of attempts to reenter his bio-metric image. If the number of attempts exceeds maximum limit then voter is invalidated to ensure fake voters do not vote and provision should be provided for face recognition for further analysis and actions.

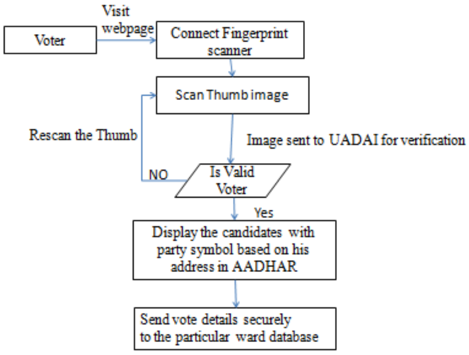

Voter
Visit webpage
Connect Fingerprint scanner
Scan Thumb image
Rescan the Thumb
Image sent to UADAI for verification
NO
Is Valid Voter
Yes
Display the candidates with party symbol based on his address in AADHAR
Send vote details securely to the particular ward database

Fig 2: Dataflow for voting through website

Through mobile:

Many of the android set come with the feature of finger print scanner built internally to provide security to access the mobile phone. This can be used by the voter to cast his vote. An android application[12] must be built which needs to be downloaded by the voter who have finger print scanner with the mobile set. The application must get the biometric of the voter and send it securely along the network to validate the voter. If a valid voter enters the application then display the options for voter to cast his vote.

In all these above scenarios if the voter is valid and candidate option is selected the Aadhar ID along with the unique party ID will be securely sent to the constituency database where the results will be processed.

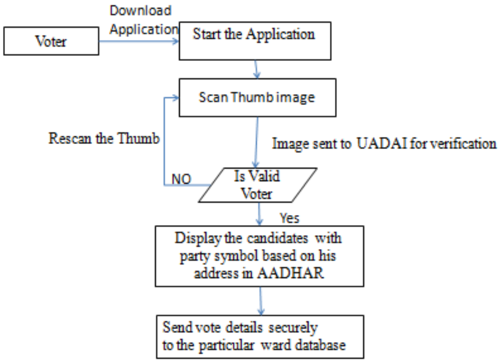

Voter
Download Application
Start the Application
Scan Thumb image
Rescan the Thumb
Image sent to UADAI for verification
NO
Is Valid Voter
Yes
Display the candidates with party symbol based on his address in AADHAR
Send vote details securely to the particular ward database

Fig 3: Data flow for Android application

Sending data securely to remote database:

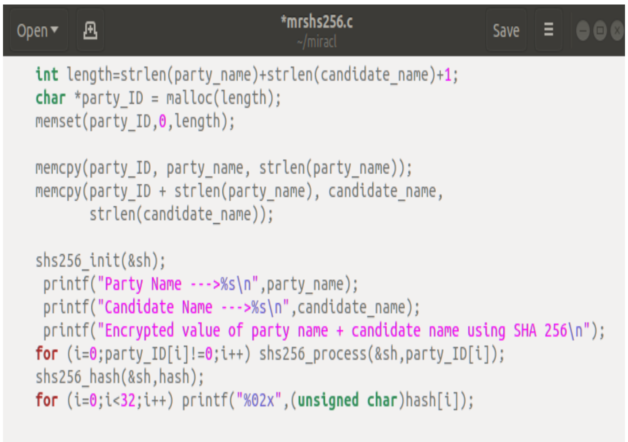
Constituency database will contain the following:
Aadhar number, Ward number and list of candidates contesting from that constituency and their party names. When the voter ID is validated the list of candidates and party is displayed from this database for voter to select candidates of their choice. When the voter selects the candidate the aadhar number the ward number and party ID is encrypted using some secured algorithm and sent to the server where the data will be stored.

Aadhar ID	Party ID

Aadhar ID = 12 digits = 48 bits
Party ID = SHA 256 (Party name + candidate name) = 256 bits

Fig 4: Data to be sent for server

SHA256 algorithm which is provided in mrshs256.c from MIRACL crypto library is edited to produce Party ID as shown in figure 5 and the output generated is shown in figure 6. The data that is sent is the output of figure 6 concatenated with Aadhar ID of the voter.

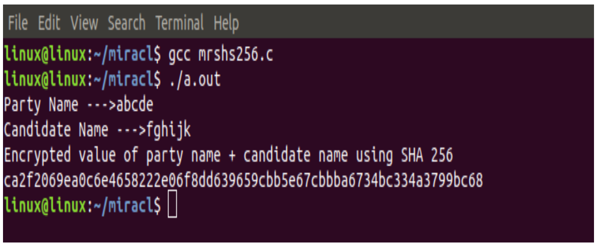


```
int length=strlen(party_name)+strlen(candidate_name)+1;
char *party_ID = malloc(length);
memset(party_ID,0,length);

memcpy(party_ID, party_name, strlen(party_name));
memcpy(party_ID + strlen(party_name), candidate_name,
       strlen(candidate_name));

shs256_init(&sh);
 printf("Party Name --->%s\n",party_name);
 printf("Candidate Name --->%s\n",candidate_name);
 printf("Encrypted value of party name + candidate name using SHA 256\n");
for (i=0;party_ID[i]!=0;i++) shs256_process(&sh,party_ID[i]);
shs256_hash(&sh,hash);
for (i=0;i<32;i++) printf("%02x",(unsigned char)hash[i]);
```

Fig5: Screenshot of edited mrshs256.c



```
linux@linux:~/miracl$ gcc mrshs256.c
linux@linux:~/miracl$ ./a.out
Party Name --->abcde
Candidate Name --->fghijk
Encrypted value of party name + candidate name using SHA 256
ca2f2069ea0c6e4658222e06f8dd639659cbb5e67cbbba6734bc334a3799bc68
linux@linux:~/miracl$
```

Fig6: Screenshot of Party ID generated by SHA 256

IV. CONCLUSION:

This paper proposes the election system as internet of things application where the citizen can cast the vote using any of the three methods. The Aadhar number along with the secured unique id generated which is the combination of candidate name and party name is sent to the database. The all possible combinations of unique values containing the combinations of candidate name and party name will be maintained in a central database which will be matched when the person casts the vote and will be counted later. This also helps to avoid manipulation if the data is locally stored thereby preventing issues present in the current system where the data is stored in the local EVM (electronic voting machine).

REFERENCES:

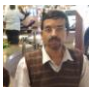
1. Shah, P.M.a.D.P., Machine to Machine Metamorphosis to the IOT. Ausjournal,. **vol. 1,** (no. 1, pp. 31-34
): p. pp. 31-34
2. Manjunath, P., M. Prakruthi, and P.G. Shah. IoT Driven with Big Data Analytics and Block Chain Application Scenarios. in 2018 Second International Conference on Green Computing and Internet of Things (ICGCIoT). 2018.

3. Bhuvanapriya, R., et al. Smart voting. in 2017 2nd International Conference on Computing and Communications Technologies (ICCCT). 2017.
4. Awathankar, R.V., R.D. Raut, and S. Rukmini. Ad-hoc network based smart I-voting system: An application to cognitive radio technology. in 2016 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC). 2016.
5. N. Kavitha, S., K. Shahila, and S.C. Prasanna Kumar, Biometrics Secured Voting System with Finger Print, Face and Iris Verification. 2018. 743-746.
6. Lakshmi, C.J. and S. Kalpana. Secured and transparent voting system using biometrics. in 2018 2nd International Conference on Inventive Systems and Control (ICISC). 2018.
7. Madhuri, B., et al., Secured Smart Voting System using Aadhar. 2017. 1-3.
8. Patil, P.S., et al. E-Smart Voting System with Secure Data Identification Using Cryptography. in 2018 3rd International Conference for Convergence in Technology (I2CT). 2018.
9. [cited 2019; Available from: https://github.com/miracl/MIRACL/blob/master/source/mrshs256.c.
10. ; Available from: https://en.wikipedia.org/wiki/Electronic_fingerprint_recognition.
11. Technology, M.S.B.O.B.; Available from: http://www.m2sys.com/blog/fingerprint-scanner/how-to-integrate-fingerprint-scanner-with-web-application/.
12. NewGenApps. Available from: https://www.newgenapps.com/blog/bid/219838/10-steps-to-create-a-successful-mobile-application.

AUTHORS PROFILE

Rajashree Soman, received the Bachelor of Engineering degree from Visvesvaraya Technological University, Belagavi, India, in 2003. She is pursuing Ph.D. degree from the Jain University, Bangalore, India, from 2017; currently she is working as Assistant Professor in PES University Bangalore, India. Her current research interests include Internet of Things, Cryptography, and IP security. Rajashree has coauthored 4 papers in peer reviewed conferences.

Sheetal V A, received the Bachelor of Engineering degree from Visvesvaraya Technological University, Belagavi, India, in 2005 currently working as assistant professor in the computer science department BMS College of Engineering Bangalore.



Soman K S, received the Bachelor of Engineering degree from Bangalore University India, in 1994. He has worked in many areas including IP Protocols, IP Forwarding ATM Signaling (UNI 3.1, UNI 4.0, PNNI), Fault Tolerance and ATM Traffic Management.

Bhuvan Kumar Panduranga, he is studying in Bachelor of Engineering degree in the department of Electrical and Electronics Engineering at K S School of Engineering and Management, Bangalore from Visvesvaraya Technological University, Belagavi, India. Domain areas of research are Internet of Things, Android application Development.

DOI: 10.35940/ijrte.E1009.0285S20