International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 04 | Apr 2019 www.irjet.net p-ISSN: 2395-0072

Smart and Secured Voting System using Magnetic Stripe Voter ID Card and Cloud Storage: A Client-Server Paradigm

Avinash Pratap Budaragade[1], Vajrashri R. Biradar[2]

[1,2]*Department of Computer Network Engineering, Visveswaraya Technological University, Belagavi, Karnataka, India*

Abstract - *Election play a vital role in the development of a country. These elections must be transparent and corrupt free. An appropriate action must be taken to authenticate every vote and voter. In country like India election is challenging task because of its huge population. In this context election requires more manpower for authentication of every voter and for results announcement. In this paper an efficient method is proposed for the authentication of every voter using magnetic stripe voter ID card and cloud storage. Double authentication can be done by using fingerprint of voter. Details of voter are stored in cloud storage. At the time voting using magnetic stripe voter ID card and fingerprint of voter can be authenticated using client-server prototype. Casted votes from all Electronic Voting Machine (EVM) are stored in another database in cloud storage, so that results can be declared as early as possible compared to traditional methods.*

Keywords—EVM, Cloud storage, biometric, magnetic stripe voter ID card, client server model

1. INTRODUCTION

Elections in the Republic of India include Parliament, Rajya Sabha, Lok Sabha, Legislative Assemblies and numerous other Councils and local bodies. According to the Constitution of India, elections should take place to the Parliament and State Legislative Assemblies every five years, unless an emergency is under operation. Further, any vacancy caused by death or resignation must be filled through an election within six months of occurrence of such vacancy. All these elections at the central and state level are conducted by the Election Commission of India while local body elections are conducted by state election commissions. In first general elections in India held in 1951-52, the voters were to place the ballot papers in the box assigned to a particular candidate, and ballot was secret. Over 224,000 polling booths, one for almost every 1000 voters, were constructed and equipped with over 21 million steel ballot-boxes, one box for every candidate. Nearly 620,000,000 ballot papers were printed. About a million officials supervised the conduct of the polls.

As the technology evolved these ballot papers were replaced by electronic voting machines (EVM). In 1980, M. B. Haneefa invented the first Indian voting machine, which was called as electronically operated vote counting machine. An EVM consists of two units, control unit and balloting unit. The two units are joined by a five-meter cable. Balloting unit facilitates voting by voter via labeled buttons while control unit controls the ballot units, stores voting counts and displays the results on 7 segment LED displays. The controller used in EVMs has its operating program etched permanently in silicon at the time of manufacturing by the manufacturer. No one can change the program once the controller is manufactured.

EVMs are powered by an ordinary 6 volt alkaline battery manufactured by Bharat Electronics Limited, Bangalore and Electronics Corporation of India Limited, Hyderabad. This design enables the use of EVMs throughout the country without interruptions because several parts of India do not have power supply and/or erratic power supply. An EVM can record a maximum of 3840 votes and can cater to a maximum of 64 candidates.

In general election 2014, at the time of counting votes following are the facts that shows how much expense made by the election commission of India [5].

i. 1,000,000 was the number of counting personnel.
ii. 550,000 was the number of security personnel.
iii. 989 counting centers were set up.

As per the report given by Election Commission government spent around Rs.3,426 crores on Lok Sabha elections which was held in 2014 in which these EVM machines were used. Most of expenses were spent for electoral officers, security of EVM [5].

This problem can be overcome by using smart and secure voting system. Initially all the data and biometric details of voter are stored in a cloud storage. For every voter a card with magnetic stripe is given. At the time of voting using client server model double authentication can be performed. If authentication is successful EVM is automatically activated and voter can cast his/her vote. These votes are directly stored in another database in cloud storage.

2. RELATED WORK

In [1] authors proposed a method in which details of the persons who are above 18years are extracted from aadhar card database since it had became mandatory in present

scenario. Automatically a new voter id with necessary details will be created and intimation will be given to the persons through their e-mail or by SMS. At the time of voting, the user can use their id. To ensure more security, finger prints of the voter is used as the main authentication resource. Since the finger pattern of each human being is different, the voter can be easily authenticated.

In [2] authors proposed system that uses Arduino and Finger Print Scanner that can identify each voter, count votes and can prevent fake votes. Authors have also confirmed that the proposed system is more digital, technology-based and secured system.

In [3] In this paper they proposes a new state-of-the-art Electronic Voting Machine design in quest for election legitimacy, to provide an inexpensive solution which is based on pragmatic biometric system using fingerprint detection along with inclusion of Near- Far Communication technology.

Technology for local ATM is currently being offered in a number of devices, such as routers, switches, and switching hubs. These devices provide the capability for an ATM switched internetwork. In general, a switched internetwork consists of an ATM backbone and a number of hubs. The hubs, by providing ATM adaptation functionality, serve as access points to the ATM backbone for servers and clients. A simulation model is developed to study the performance of the different configurations. Simulation results for end-to-end delay and loss are presented for each alternative configuration [4]

3. PROPOSED WORK

In this paper an efficient method is proposed which is cost efficient and eliminates fraud votes. Initially data of voter like name, age, magnetic stripe voter ID card number, address, name of the constituency, biometric (fingerprint), etc is stored in cloud storage. For every voter a magnetic stripe voter ID card is provided which contains information of voter in encoded form. At polling booth a machine is installed with magnetic card reader device, fingerprint scanner, voter interface machine and EVM. While voting voter must insert his/her magnetic stripe voter ID card into magnetic stripe voter ID card reader. It checks the voter authenticity from database using client-server model.

Once card and is verified voter has to go for biometric authentication which also uses client-server model. Once authentication of voter is confirmed EVM is automatically activated. Once voter casts his/her vote that vote details is directly stored in another database in cloud storage. Here only to which party vote casted is stored in cloud storage. Time and other details of voter are not stored in the database after casting his/her vote. As casted votes are stored in database results can declared immediately after completion of elections.

4. SYSTEM ARCHITECTURE

This subsection describes the system architecture of proposed system. Schematic diagram of proposed (Smart and secured voting system) is shown in figure 1.

Each user will have a magnetic stripe voter id card which consists of the tag; all the baseline information like name, age, gender, location will be stored. The magnetic stripe voter ID cards come with a unique number for the identification purpose of each voter. The information is kept discrete by encapsulation process and the information can be manipulated at the starting set up procedure. The magnetic stripe voter ID cards are blank at the initial stage and have to be initialized to be entered into the back end system. Once the card id is held within the vicinity of the controller, through the use of serial monitor, the data or the baseline information contained becomes valid. When the user inserts card into magnetic stripe reader machine, it retrieves the data from the tag and passes the information to the server over the internet. If the user is genuine, the id matches with the stored data in the database, he/she will be allowed to move to the next level of authentication, otherwise a message will be shown in the display that the person is not an authorized user. Only registered users may process further to cast vote. Once they have places their card within the vicinity the magnetic stripe reader, then the card is acknowledged by the reader, it checks for the unique identification number is present in the database, when this is done the voter is signaled to move to the next stage.

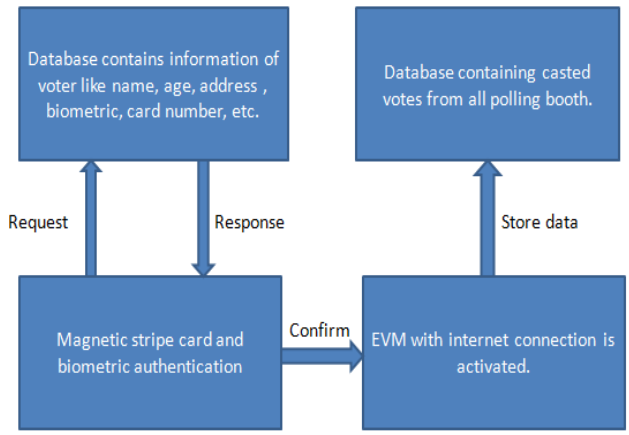

Figure 1. Schematic diagram of smart and secured voting system

Once the voter cast his vote, he won't be allowed to vote again and if multiple votes are tried by the same person this will be reported to the screen. The fingerprint of the voter will be taken by the scanner and is being sent to the server for verification. The processed image of the fingerprint is transferred to match with the sample templates in the database. If the person's identity matches, he/she can cast his vote in real time only once, choosing the candidate as per choice and if invalid user, then the buzzer will be raised and a message will be displayed as unauthorized user.

The option which is entered by the voter is being sent to server which keeps on updating through internet every instant. Once voted, it automatically gets incremented with respect to the voting. The server retrieves the data and starts the validation process. Finally, the in-charge of election commission or the authorized admin has the complete control on the application and is fully-responsible for governing important functionalities. The admin can ensure that the elections are conducted in an unprejudiced and fair manner. He/she can search the database to verify a person has not voted under two different names. And also the voting details of a person is available, he can also track down a vote in case of any irregularities. Finally after the vote submission phase is over, the results can be displayed through internet within fraction of time.

5. HARDWARE REQUIREMENTS

This subsection gives the brief details of hardware requirements for proposed smart and secure voting system using magnetic stripe voter ID card and cloud storage.

A. Magnetic stripe voter ID card

A magnetic stripe card is a type of card capable of storing data by modifying the magnetism of tiny iron-based magnetic particles on a band of magnetic material on the card. The magnetic stripe, sometimes called swipe card or magstripe, is read by swiping past a magnetic reading head. Figure 2 is the sample magnetic stripe card.

Figure 2. Sample magnetic stripe card

B. Magnetic stripe reader

A magnetic stripe reader, also called a magstripe reader, is a hardware device that reads the information encoded in the magnetic stripe located on the back of a plastic badge. Magnetic stripe readers can be read by a computer program through a serial port , USB connection, or keyboard wedge , and are generally categorized by the way they read a badge. For instance, insertion readers require that the badge be inserted into the reader and then pulled out. Swipe readers require that the badge pass completely through the reader.

Figure 3. Magnetic stripe card reader

C. Cloud storage

Cloud storage is defined as "*the storage of data online in the* cloud," wherein a voter's data is stored in and accessible from multiple distributed and connected EVM that comprise a cloud. Cloud storage can provide the benefits of greater accessibility and reliability; rapid deployment; strong protection for data backup, archival and disaster recovery purposes; and lower overall storage costs as a result of not having to purchase, manage and maintain expensive hardware. In this work for testing we used a wamp server for local storage of data.

D. Voter interaction machine

For testing purpose we used windows operating system computer. For interaction with user, GUI (Graphical Interface Unit) is designed using HTMl,CSS and PHP.

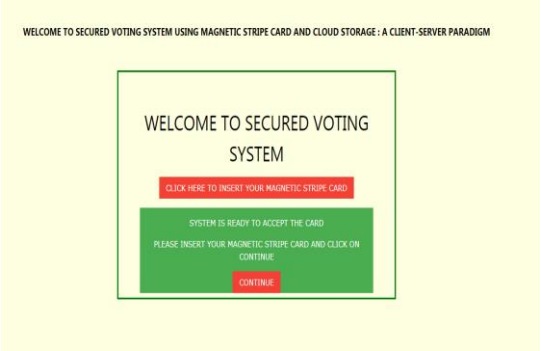

Figure 4. GUI system

E. Biometric sensor (SM 630)

Fingerprint recognition, the electronic process of recording, storing, searching, matching and recognizing an individual fingerprint has advanced substantially due to introduction of modules like SM360. Now-a-days, identification can be achieved within fraction of seconds with great accuracy. SM630 consist of optic fingerprint sensor, high performance DSP processor and flash. It possesses features like self-proprietary intellectual features,

self –adaptive a adjustment to fingerprints high imaging quality, can be applied to a wider range of people. It has excellent tolerance and correction to deformed and poor quality fingerprints and also low power consumptions.

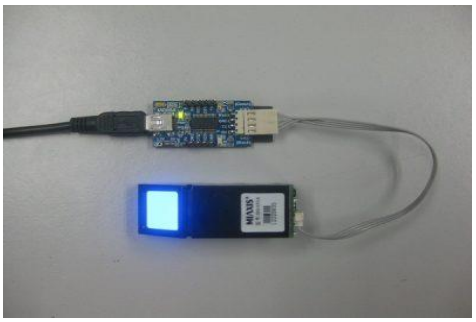

Figure 5. Biometric sensor (SM 630)

F. EVM with internet connection

Electronic voting (also known as e-voting) is voting that uses electronic means to either aid or take care of casting and counting votes. EVMs or electronic voting machines provide the voter with a button for each choice which is connected by a cable to an electronic ballot box. For this we need to provide internet connection.

6. IMPLEMENTATION AND RESULTS

This subsection describes the implementation process of proposed work and also implemented results. Figure 6 gives the flow chart of proposed work.

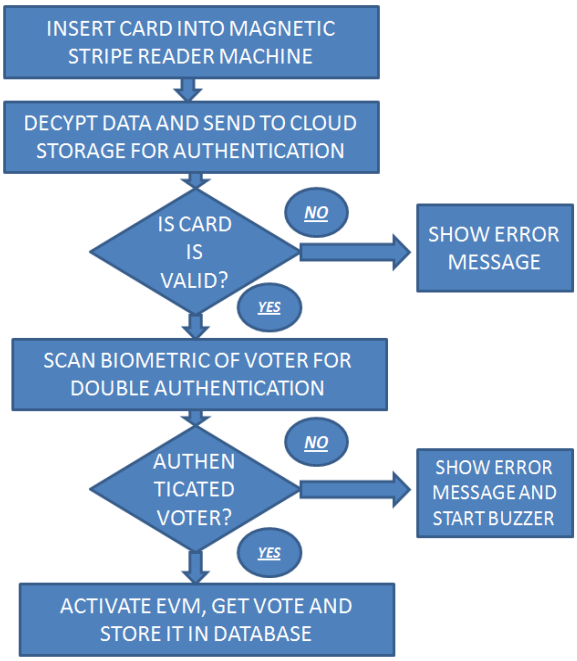

Figure 6. Flow chat for proposed work.

1. When voter enters into polling booth he/she needs interact with the system as shown in figure 7. System is asking for voter to enter his/her card into machine. After inserting need to select continue.

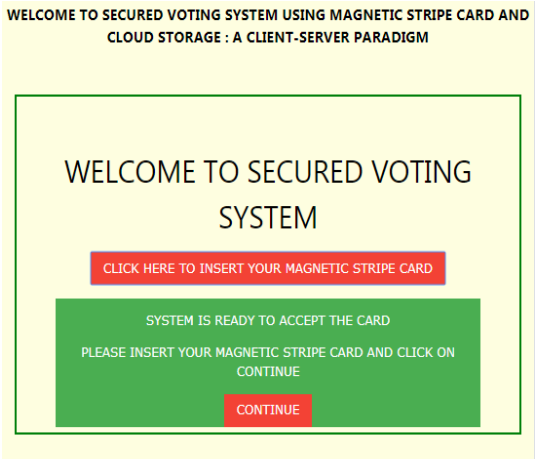

Figure 7. Main page of voter interface

2. Once voter inserts card into machine, it is authenticated if data found correct. After successful authentication details of that card holder is displayed on screen as shown in figure 8. Voter need to cross verify that information, if found correct need to select confirm otherwise abort.

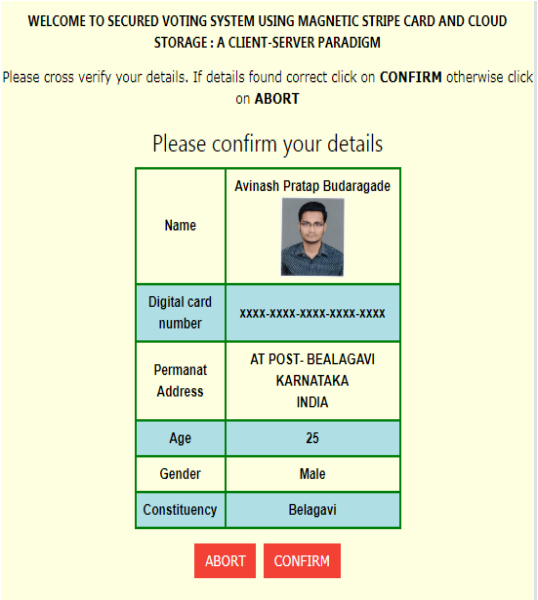

Figure 8. Cross verification by voter

3. After voter selecting confirm, next windows opens, that shows fingerprint authentication. Voter must give thumb impression on fingerprint scanner. If fingerprint authenticated EVM will be activated automatically. Figure 9 shows that system asking for voter to give his/her biometric input.

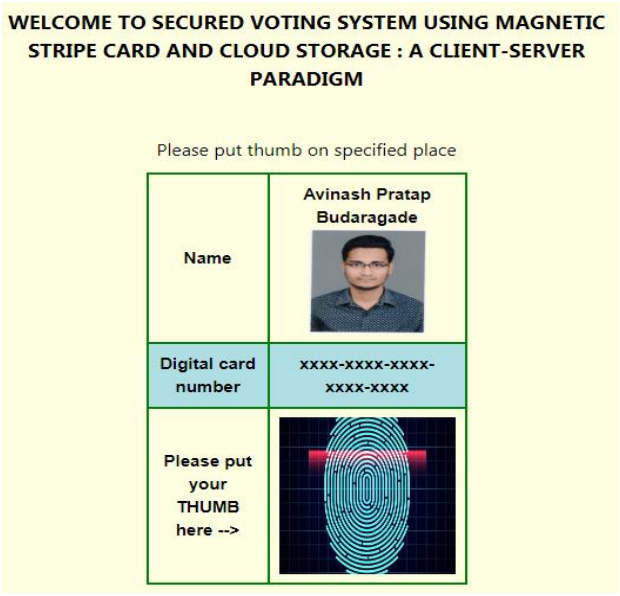

Figure 9. System asking biometric input

4. After fingerprint of voter is verified, authentication successful window will be popped as shown in figure 10.

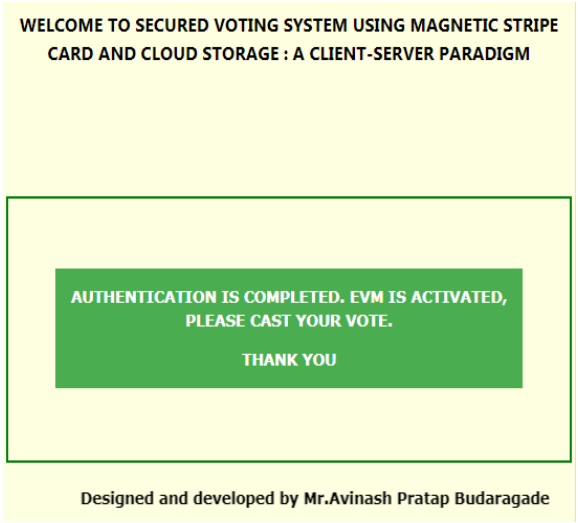

Figure 10. Result showing authentication successful.

7. CONCLUSION

In the democratic country, the word election means the government's formative and direct involvement of the people of the country. These elections represent the common will of the people, expressed in their votes. Corruption should be free for better government elections. A system that requires voting enhancement and a secure polling system is required. In this model for every voter magnetic strip voter ID cards provided. At the polling center these cards are used for authentication. Once they are verified another level of security is created by using biometric fingerprint as an authentication of voter. At every instance these data are stored in the server through internet. Results are also obtained very fast compared to the traditional methods.

REFERENCES

[1] Rishab Garg, Poonam Yadav, Vishal, Vibhu Chinmay, "Online voting system linked with Aadhar", IEEE *international conference on computing for sustainable global development 2016.*

[2] Anooshmita Das, Manas Pratim Dutta, Subhasis Banergee, "VOT-EL: Three Tier Secured State-Of-The-Art EVM Design Using Pragmatic Fingerprint Detection Annexed With NFC Enabled Voter -ID Card", *IEEE, National Institute of Technology 2016*

[3] Rahil Rezwan, Huzaifa Ahmed, M. R. N. Biplob, S. M. Shuvo, Md. Abdur Rahman," Biometrically Secured Electronic Voting Machine", 2017 IEEE *Region 10 Humanitarian Technology Conference (R10-HTC)*

[4] Friesen, V.J. & Wong, J.W.. (1995). A case study in local area migration to ATM. 442-450. 10.1109/ICCCN.1995.540157.

[5] Election Commission Of India, "India Votes*", The General Elections* 2014