ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 4, April 2017

Aadhaar and Server based Electoral system

[1]Yugansh Garg [2]Sakshi Mishra
[1] [2]B.Tech Computer Science 2nd Year
[1] [2]IBM-ICE Program, People's University, Bhopal

Abstract- This paper describes an advance Aadhaar and server based electoral system for Indian elections. The voting systems in an easier way that all voter can cast votes via biometric Aadhaar based authentication .It provides a higher security pre-casting which could reduce the chances of temperance as a simultaneous backup is created at State/Central level servers. In this system we renounce the use of traditional voter ID cards and election voter verification list. This method would help us to eliminate invalid votes, ends booth capturing and makes counting easier, faster and accurate.

I. INTRODUCTION

This paper prescribes a new methodology towards a digital Aadhaar and centrally server based electronic vote- casting systems.
In current election verification system police personnel or election booth personnel are to authenticate voter ID cards through a provided list of voters but in this new method the fingerprints are used to authenticate verify and determine the malicious activities. It could prevent repetition and automatically creates a simultaneous backup in centralized server in encrypted form that is hard to temper.

1.1 Verification and authentication

First the voter has to provide its thumb impression on biometric machine which is linked with the central UIDAI server, from where the voter`s identity and eligibility to vote is verified and voter is authenticated to vote.
1. Filtration of eligible voter.
2. Maintaining the records of eligible voter.
3. Allow to vote only if belongs to concerned constituency.
4. Providing access to the voter only once.
Through this mechanism we can ensure that each voter can cast vote only once and if violated the standards, the malicious activity can be determined.
5. After verification the voter can cast the vote.
6. After casting vote, the vote of voter is recorded both in EVM machine and centralized server.
The biometric verification machine is attached to the EVM as well as UIDAI server.

II. LITERATURE SURVEY

2.1 BIOMETRIC

Biometric is the measurement and statistical analysis of people's physical and behavioral characteristics. The technology is mainly used for identification and access control, or for identifying individuals that are under surveillance. The basic premise of biometric authentication is that everyone is unique and an individual can be identified by his or her intrinsic physical or behavioral traits. There are two types of biometric identifiers:
1. Physiological Characteristics: The shape or composition of body.

2. Behavioral Characteristics: The behavior of a person

Examples of physiological characteristics used for biometric authentication include fingerprint, DNA, face, hand, retina or ear feature and odor. Behavioral characteristics are related to the pattern of the behavior of a person, such as typing rhythm, gait, gestures and voice.
Authentication of biometric verification is becoming increasingly common in corporate and public security systems, consumer electronics, and point-of-sale application. In addition to security, the driving force behind biometric verification has been convenience, as there are no passwords to remember or security token to carry.
Biometric devises such as fingerprint readers consist of a reader or scanning device, software that converts the scanned information into digital form and compares match points, a database that store the biometric data for comparison.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 4, April 2017

2.2 UIDAI

The Unique Identification Authority of India (UIAID) is a statutory authority established under the provision of the Aadhaar (Target Delivery of financial and other subsides, benefits and services) Act, 2016("Aadhaar Act2016") on 12 July 2016 by the government of India, under the Ministry of Electronics and Information Technology (MeitY).

UIAID was created with the objective to issue Unique Identification numbers (UID), named as "Aadhaar" to all residents of India that is robust enough to eliminate duplicate and fake identities and can be verified and authenticated in an easy, cost effective way. The first UID number was issued on 29 September 2010 to the resident of Nandurbar, Maharashtra. The Authority so far issued more than 111 crore Aadhaar numbers to the residents of India.

Under the Aadhaar Act 2006,UIAID is responsible for Aadhaar enrolment and authentication, including operations and management of all stages of Aadhaar life cycle, developing the policy, procedure and system for issuing Aadhaar number to individuals and perform authentication and also required to ensure the security of identity information and authentication records of individuals.

2.3 EVM

EVM stands for Electronic Voting Machine. These machines have been used in the election since 1999 paving the way for electronic voting. EVMs are used in both the General and State election of India. For first time users, starting at an EVM can be daunting if you don't know what to do.

EVM is designed with two units: the control unit and the balloting unit. These units are joined together by a cable. The control unit of the EVM is kept with presiding officer or the polling officer. The balloting unit is kept within the voting compartment for electors to cast their votes. This is done to ensure that the polling officer verifies your identity. With the EVM, instead of issuing a ballot paper, the polling officer will press the Ballot Button which enables the voter to cast their vote. A list of candidates and names and/or symbols will be available on the machine with a blue button next to it. The voter can press the button next to candidate's name they wish to vote for.

In order to cast your vote, you must present your Voter ID and your name should appear in the Electoral Rolls. The officer in charge will then press a button that enables you to vote. You can then enter the polling booth and cast your vote. Once you have pressed a button to vote, your vote is recorded. Pressing the button again, how many times you want, will not record another vote. The machine will be locked till the officer in charge sends in the next voter and enables him to vote. This ensures one person equals one vote. Once the last voter has cast their vote, the officer in charge will press a button labelled "Close". The EVM will not accept any votes after this. The Balloting unit will be disconnected from the Controlling unit and both units will be kept separately. After the polls are closed, the presiding officer will give each polling agent the accounts of the recorded votes. After counting votes, the account of voters registered will be tallied against the votes counted. Any discrepancies can be pointed out by the counting agents. After the counting, the Results button can be pressed to display the result. There is also a safety measure provided to prevent the result button from being pressed before the counting of votes begins. The button cannot be pressed till the "Close" button is pressed. The button is also sealed and hidden inside. This can be accessed only at the counting center in the presence of an officer designated to this task. With these measures and features, the EVMs can be sealed and the votes can be counted on a later date even weeks or months after collecting the polls. EVMs also have added security such as CCTV coverage, storage in strong rooms, transport under armed guards, and 24/7 armed police guard.

2.4 Centralized Server

A server is a computer designed to process requests and deliver data to other (client) computers over a local network or the internet. Although any computer running special software can function as a server.

In a centralized server the votes read on EVM is simultaneously store in both EVM memory as well as the central server which holds all the records of votes. The special feature of this central server is that some restrictions will be provided. The network established between EVM and the central server allows only the write operation from EVM to central server. The write operation keeps the record of the vote casted. Through this mechanism even if somehow the EVM machine gets hacked the record remains safe. Another feature of central server would be that it only allows the read operations to be performed on central server. In that ways one is not able to manipulate the vote records stored on central server.

III. PROBLEM IDENTIFICATION

The heart of democracy is voting. The heart of voting is TRUST that each vote is recorded and counted with accuracy and impartiality. The purpose of an election is not to name the winner, but it is to convince the losers that they lost. Despite elaborate safeguard, India's EVM are vulnerable to serious attack. In current electoral system, Voter ID is used as a unique identification of any person identity. This system by far provides the unique identification as all the things are recorded on paper which can be tempered easily. For example the person who is somehow not available at voting center but someone else

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 4, April 2017

has casted the vote on behalf of him. This brings biasing in electoral system. Following are the problem faced in current EVM machine:

1. Dishonest insiders or other criminals with physical access to the machines at any time before ballots are counted can insert malicious hardware that can steal votes for the lifetime of the machines. Attackers with physical access between voting and counting can arbitrarily change vote totals and can learn which candidate each voter selected.

2. The EVM has no means for the voter to verify that his/her votes have been tallied properly.

3. The EVM has no means outside of the memories of the voting machines themselves to audit or recount the votes.

4. Susceptibility to fraud: Although some may believe that tampering with an electronic voting machine is extremely hard to do, computer scientists have tampered with machines to prove that it is quite easily done. If people have access to the machines, and know how to work them, they can take the memory card out of the machine, which stores the votes, and in place they put their own memory card with a virus that can tamper with the votes

5. Secure storage of cast votes: The votes that are cast using the electronic voting machines, are stored in a safe storage or space in the computer machine memory. The time gap between election and the counting of votes is a risk to possible hacking and manipulation. The chance of tampering increases as the time gap increases.

IV. IMPLEMENTATION AND METHODOLOGY

4.1. Verification

In this process, instead of traditional approach as practiced the voter did not had to provide its voter id cards, but just have to give his thumb impression for verification.

In order to verify, firstly the identity of the voter will be fetched from UIDAI (Unique identification authority of India) server. After the identification of the voter his eligibility to vote through a constituency, polling center will be verified through EIC server (election commission of India) data such that details will be fetched to check whether he/she is eligible or not.

In the third step it will be checked whether he/she has already casted the vote or not.

After the three steps the voter will be given only one time access to EVM, and only a single vote can be casted.

4.2. Voting

After the three steps of verification of the voter, he can cast a single nontransferable vote. As usual the votes will be stored in voting machine.

4.3. Backup

After casting the vote, every new entry will be stored in both machine as well as server. Both the data in machine as well as server can be stored in encrypted formats. A simultaneous encryption can be used to store data, in machine. In currently used machine the data is not stored in encrypted form, neither any backup of data is taken. The

Concept of cloud computing and virtualization can be used if required to provide each EVM a separate access to server. Through this mechanism each machine will have two copies of votes casted, one is in local machine and other at the centralized server. In the case of tempering of data in machine, the data at central server can be used to generate election results.

Memory required to store votes of election

Let us consider 1 vote of size 1 byte

In 2014 general elections, India has 814 million voters,

So,

Kilo bytes required = 814000000/1024

Megabytes required = 814000000/ (1024*1024)

= 776 MB

That is less than one Gigabyte,

Means an ordinary machine can store the data of all the EVMs

4.4. Security

The data stored at the centralized server or backup server will be saved in encrypted formats. Thus cannot be easily access or tempered by cyber threats. The algorithms such as RSA, AES, two-fish, DES can be used, which are open source and unbreakable.

4.5. Connectivity

Each of the machine used in this paper can be connected to other through intern machine connectivity. .Biometric machine fitted with an Ethernet cable can be used to connect the machine with other machines such as EVM, and servers. The biometric machine can be connected to internet can fetch data from ECI and UIDAI servers, and if provided with a verification mechanism can be used to verify the voter and act as access check point. At present IoT is used by many commercial giants to verify the details of their users. For example Amazon is using IOT technology to aide billing system in America. IoT can be used to connect different types of machines easily, if provided with dedicated Internet connection.

5. Conclusion

As the recent, litigation applied in Honorable Supreme court, created question on election system, traditional EVMs and verification systems. As the world is moving towards digitalization it is need of the hour to bring drastic change in the field of electoral systems to provide fair and unbiased machinery with trusted verification system, which is hard to temper. To maintain the spirit of Republican Democracy.

VI. FUTURE SCOPE

The implementation provided in this paper can be used to transform electoral system in India and can bring a revolution in election system. This would also remove chances of biased voting system. Beside this it would prevent invalid means of voting. This suggests a simultaneous backup system, which can make the result generation easier and faster. By implementing such methodology we can almost prevent tempering and hacking of EVMs.

VII. REFERENCES

- http://www.uidai.gov.in
- http://www.eci.nic.in
- http://www.dhs.gov/biometrics
- https://www.hypr.com/iot-security/
- IBM IT Infrastructure Booklet (for server technologies)
- Daily journals :The Hindu, Dainik Bhaskar, The Hitavada
- Books: - Indian polity. By M lakshmikanth (for electoral system and electoral reforms)