International Journal of Students' Research in Technology & Management
eISSN: 2321-2543, Vol 6, No 1, 2018, pp 40-44
https://doi.org/10.18510/ijsrtm.2018.616

PROPOSITION OF A SECURE SYSTEM OF VOTING USING UIDAI DATA VIA IOT

[1*]Shakya Chakrabarti, [2]Neelanjan Acharya
[1 2]Department of Electronics and Communication Engineering, Kolkata, India
*shakyachakrabarti@gmail.com, neelanjanacharya@gmail.com

Article History: Received on 13th May, Revised on 2nd June, Published on 19th June 2018

Abstract

Purpose of the study: The paper proposes a secure system of voting using UIDAI Data and implementing IoT to save a copy of the voting statistics via VMAC encryption.

Methodology: The paper proposes a secure system which will utilize the Aadhar database along with the Electronic Voting Machine units, to authenticate voters by bio-metric means which will be synchronized by Internet of Things. After successful casting of vote, two sets of voting statistics will be stored in the local polling station as well as a centralized register respectively; through a cascade of servers. These will be secured from virtual third-party vulnerability by VMAC encryption. Finally, an impenetrable system of voting can be established by the above method.

Applications of this study: If the proposed system of voting is practically implemented, then a proper consensus can be obtained by avoiding poll-day violence. Furthermore, if UIDAI data is used then the voter's authenticity is also verified.

Novelty/Originality of this study: The use of biometric data, as well as storage of a second set of data using VMAC encryption to a secondary storage site.

Keywords: EVM; UIDAI Number; Bio-metric Authentication; VMAC Encryption; Data Server

INTRODUCTION

The backbone of a democracy is a secure and fool-proof election system. India and her elections, being the largest democracy in the world, have always been a leviathanic affair with a huge expense of tax-payer's money going into the process of conducting a secure and peaceful election. However, as much as it is a challenge; even 70years post-independence, large parts of rural India still face hurdles while conducting a peaceful election. Many of the booths see violence marring the election days, while booths are 'rigged' and in the whole process Ballot Units, EVMs are destroyed and thus public consensus is hampered.

Even after the implementation of all these systems, one thing which the current voting system lacks is a proper "One Man, One Vote" mechanism.

BRIEF DESCRIPTION OF THE PROPOSED PROCEDURE

In this paper, we have proposed a system which will put to use the EVMs along with implementation of IoT on UIDAI (i.e. Aadhar Data). Along with that, a biometric verification system will also be introduced which will work as the trigger of the self-automated control unit. The next stage will be the voter casting his/her vote on the basis of his/her UIDAI authentication. After cast of successful vote, the same will be registered in two locations-a local register and a centralized register.

The local register will be the control unit, which will save the voting data at the site of voting.

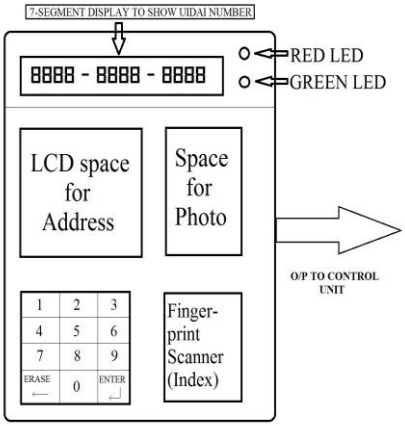
The centralized register would comprise of dedicated constituency specific mini-servers of the ECI which will be stationed at a secure location under the guard of ECI far away from the physical voting sites. This centralized register via its mini-servers would obtain the details of each successful vote cast via an encrypted VMAC system through a secure internet channel.

DIFFERENT COMPONENTS OF THE IOT EVMs

The EVMs will comprise of different components, each interlinked to the other with a main Control Unit synced to the Internet. The Biometric Unit (Fig 1), The Control Unit (Fig 2), The Ballot Unit (Fig 3) and VVPAT Unit. This would be directly connected to the Ballot Unit which would contain a paper trail. It will send out a slip after successful acceptance of a vote. The slip would show the UIDAI No. and the Symbol of the political party to whom the respect vote was given to.

International Journal of Students' Research in Technology & Management
eISSN: 2321-2543, Vol 6, No 1, 2018, pp 40-44
https://doi.org/10.18510/ijsrtm.2018.616

Fig 1. Components of the Biometric Unit



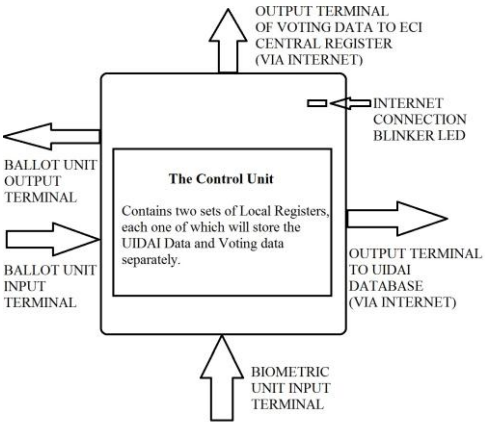
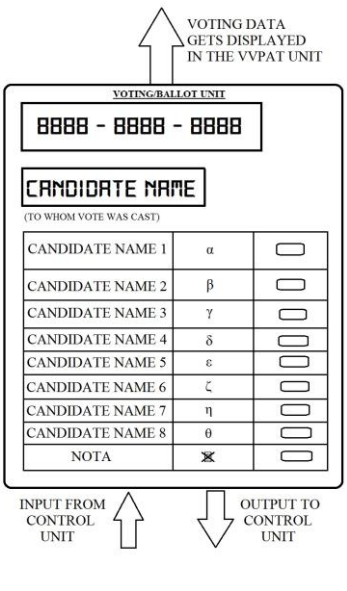


Fig 2. Components of the Control Unit

Fig 3. Components of the Ballot Unit



IMPLEMENTATION OF THE PROPOSED METHOD

A huge part of the proposed method depends upon the UIDAI or Aadhar database of the Govt. of India and to use it via IoT to improvise a tamper-proof Voting mechanism.

The procedure for the whole Voting mechanism is as follows.

A. Authentication of UIDAI Number by Biometric means:

When the Voter enters to cast the vote, it should be mandatory for the former to carry the Aadhar Card along with the EPIC Card.

i. The Voter will first proceed towards the Biometric unit.
ii. Voter enters the 12 Digit UIDAI No. in the Numeric Keypad on the Biometric unit. If the voter is unable to do so, the presiding officer would help the voter to do the same.
iii. The Biometric unit via its 7-segment display would show the 12 Digit No. so that the Voter can verify if the input is correct or erroneous.
iv. If the input is correct then the Voter will press the 'ENTER' Button.
v. If the input is incorrect Voter will press the 'ERASE'button to re-enter number.
vi. After pressing enter key, the Green LED will glow prompting the Voter to insert the Index finger onto the fingerprint scanner. (It should be noted here that Aadhar database contains all the 10 finger scans of an individual. However, the Index finger input is chosen as it is unique for any individual thus avoiding vulnerability of information mismatch).
vii. After inserting the Index finger the UIDAI No. and the Fingerprint data will get transmitted through the Control Unit to the Aadhar Database via secure Internet connection. After obtaining the Aadhar information it will return back through the Control Unit to the Biometric Unit, at the same time the Ballot unit will also be unlocked for casting of a single vote.
viii. If the data matches the Green LED will glow first, followed by the LCD displays showing the Image of the Voter as it is on the Aadhar Card along with the address. The presiding officer will then authenticate the candidate so that he can proceed to vote in the Ballot Unit.
ix. If the UIDAI data does not match the Red LED will glow, prompting the Voter to re-enter and again follow the previous steps.

B. Voting in the Ballot Unit:

After the authentication, the voter approaches the Ballot Unit which is available only to accept a single vote to be assigned to the respective UIDAI No.

i. The voter casts the vote to the candidate of his choice by pressing the button.
ii. After casting of the vote the Ballot Unit displays the UIDAI No in the top column followed by candidate name in the next column.
iii. Subsequently, the VVPAT produces the paper slip which shows the candidate details, UIDAI No. and the symbol of the respective candidate to whom the vote was cast. After some time the slip retraces into the machine itself.
iv. At the same time the Ballot Unit transmits the UIDAI No. and the voting data via the Control units to the ECI Mini-Servers via a secure 64-bit VMAC system.

C. Data Compartmentalization and Data Security:

The cast vote information will contain the voting information (to which political party the vote was cast) along with the respective UIDAI No. to which the vote was given to. The cast vote information will be separated into two copies.

It should be noted that there will be no mapping of the UIDAI No. of the voter and the cast vote information, i.e., the two sets of data will be stored separately in two different data registers in the Control memory.

i. Local Register: The first copy will be stored in the Control Unit storage memory. While counting of votes will take place the information will be taken from the local register if there is no report of discrepancies in the process of voting for the respective EVM Control Unit.
ii. Centralized Register: This will be present in the secure mini-servers of the ECI, which will be far away from the physical polling station locations. Now the architecture of the Centralized registers comprise of a chain of Mini-Servers and data collectors which will integrate the information from the lower to the upper strata finally giving the total votes cast in the election.

The chain will integrate as follows:

i. Constituency based Mini-Servers: These are the integral data collection units which will collect cast voting information from each constituency.

ii. District based Data-collector: All the constituency servers will then be redirected to the respective district data collectors which will collect information of all the constituencies of the respective district.

iii. State based Mega-Server: This will collect the information of the votes cast in all the district of a particular state and would send the information to the ECI Mainframe.

Fig 4. Process flow of server data

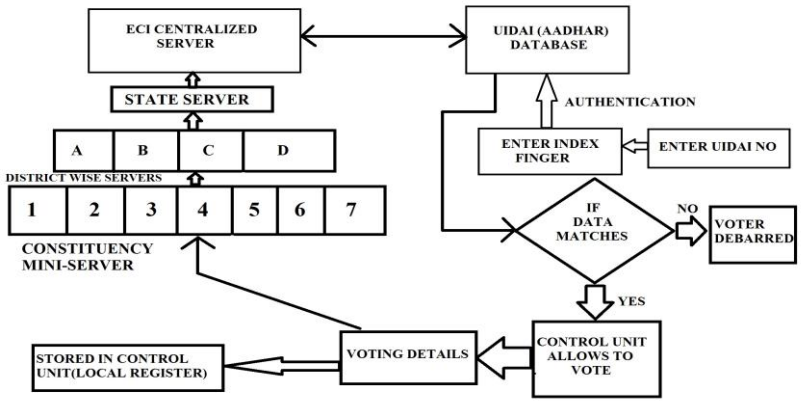
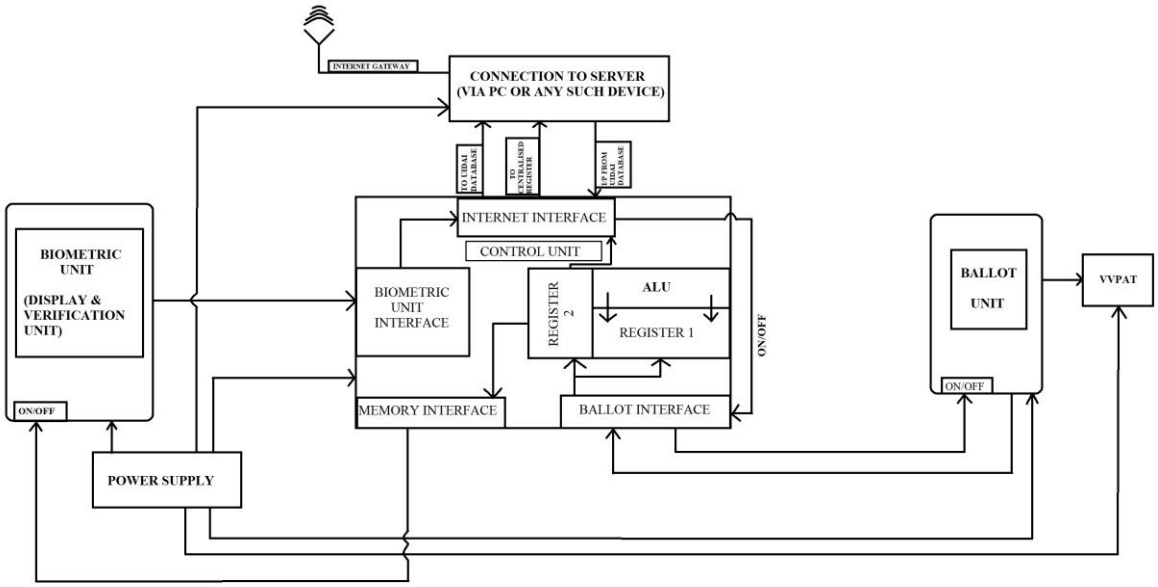


Fig 5. Architecture of the whole system



SYNOPSIS OF THE TOTAL PROCEDURE

From the above description, we can conclude a cynosure of the total process, as follows:

i. At first the voter would proceed to the Biometric unit, enter the 12 digit UIDAI and then after successful prompt from the unit would insert the Index finger on the scanner.

ii. The Biometric unit after scanning the image would transmit the UIDAI along with the index fingerprint through the Control Unit to the Aadhar Database to search for a data match.

iii. After getting a successful match the Aadhar Image and address of the voter would then be transmitted through Internet to the Control unit in the physical poll station and via control unit would get displayed in the Biometric Unit.

iv. The presiding officer would thus verify the credentials of the Voter and thus authenticate them. The presiding officer would then allow the person to proceed towards the Ballot unit.

v. The voter would then cast the vote to the candidate of choice. After successful acceptance of Vote, the UIDAI No. and the candidate name to whom the vote would be given to would be displayed.

vi. Immediately the VVPAT unit would produce a slip showing the party to whom the vote was given to along with the UIDAI No. of the voter.
vii. At the same time the UIDAI No. and the voting data would get stored inside the Control unit and another copy would be transmitted through the Control Unit to the ECI-Mini Server.

RESULTS AND ADVANTAGES

The first and foremost advantage of the whole system is that it is biometrically authenticated and the total proposed implementation happens using IoT. There can be no human intervention in the whole procedure and thus any type of vulnerability to the system is avoided.

The second factor is the storage of 2 copies of data. Often, the Control Unit of the EVMs get damaged either by jeopardising the voting by miscreants and sometimes even manual error leads to damage of the same. Thus a public consensus cannot be taken and sometimes even a re-poll is ordered. The later again incurs more loss of public money and man power. However, as the proposed mechanism uses 2 copies of the data, even if the Local register data is lost from the Control Unit, ECI could easily access the same from its constituency based Mini-Servers.

Usage of a VMAC encryption is another step to secure the voter's identity. During the transmission of the voting data and the UIDAI No of the voter, the VMAC encryption would create an impregnable barrier (by creating a secure hash cipher of the transmitted data) to any third-party trying to access the data. Thus, the procedure keeps in mind both the physical and virtual vulnerabilities of security and implements an impenetrable system.

Measurement of the idle time between two consecutive casting of vote should be as minimum as possible with a accurate precision in the order of seconds. The time delay between the transmission of request and receival of the UIDAI data set is in the order of milli-second subjected to change with the speed of internet, but the correspondence should be maintained for correct pick up from UIDAI data pool. A secure unique and non-overlapping data link should be established between strata of the concerned meta-servers. The centralized register should be having enough gateways for accessing different local registers.

The final vote count of each candidate is given as a sum total of all the votes received by the same in that particular polling booth. There is no information of the individuality of the cast votes to the respective UIDAI holder. After every 2 hours the Control Unit will send a brief statistic of percentage of vote cast in the physical polling station. It is the duty of the ECI to ensure the from their statistical data, the number of voter should not exceed the stack length of the local register.

CONCLUSION

The proposed method introduces a unique approach towards the whole process of election conduct. The introduction of using UIDAI/ Aadhar Database to conduct the election is an approach anew. A double data copy prevents the vulnerability of data loss. On the other hand the introduction of VMAC hash cipher to transmit the second copy of data to the ECI mini-servers thus protects the privacy of the voter.

The complexities which the whole implementation faces is that it would require computational devices like a PC or a Laptop at the site of voting along with a un-interrupted Internet connection. Considering the fact, the violence in elections take place remote villages in the rural parts of India, getting an uninterrupted internet connection would certainly be a challenge.

Moreover, the Biometric verification would require proper know-how and literacy of the voter so that he/she may enter the UIDAI No. at one go. Finally, it should be mentioned that the focus of the paper is mainly on the architecture of the system, more emphasis has been laid on the detailed working procedure of the system rather than the success rate of the encryptions used in the system. However, the authors did emulate a simple brute force attack on the MAC tags generated after voting. But the attack failed to retrieve the tags. So it can be concluded that the system is not vulnerable to a simple brute force attack.

BIBLIOGRAPHY

1. "Biometric Voting Machine (BVM) using IOT"-K.Dinesh, G.SaiNadha.
2. "Advanced Secure Voting System with IoT"-Ms.Nithya.S, Mr,Ashwin.C, Mr.Karthikeyan.C, Mr. Ajith Kumar.M (IJECS)
3. "Design and development of voting data security for electronic voting (E-Voting)"-SupenoDjanali; Baskoro Adi Pratomo; KarsonoPuguhNindyoCipto; AstandroKoesriputranto; HudanStudiawan, IEEE ICoICT(2016)
4. " Secured electronic voting machine using biometric"-Anandaraj S; Anish R; Devakumar P. V, IEEE 2015 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS)
5. "An electronic voting system based on homomorphic encryption and prime numbers"-Ali Azougaghe; Mustapha Hedabou; Mostafa Belkasmi, IEEE 2015 11th International Conference on Information Assurance and Security (IAS)

