E-Voting System Using Homomorphic Encryption Technique

Dr. A.C. Santha Sheela [1], Ramya. G. Franklin[2]

[1][2] Assistant Professors, Dept. of Computer Science and Engineering, Sathyabama Institute of Science and Technology, Chennai, India

[1] shantha.jasmine@gmail.com [2] mikella.prabu@gmail.com

Abstract. The main objective of this project is to develop a safe Electronic voting System Software using Fingerprint Authentication method. i.e., e-voting system. Initially, fingerprints are collected and stored in a large database which will be created by the admins. During the elections, a valid authentication can be done through finger vein sensing. This authentication system is highly reliable and will facilitate casting of votes by the voters. In many democratic countries, elections have become a huge matter of concern. An election is seen as a system that basically creates the formal structure of a nation. It is an opportunity to elect the right leader and contribute towards the development of the nation. In addition, security and authenticity of these elections have become a major concern for the authorities. Although we use advanced electronic voting machines, the problem of rigging often arises. This e-voting software provides solution to rigging and also facilitates high authenticity and reliability. Depending on the particular implementation, e-voting may use standalone electronic voting machines (also called EVM) or computers connected to the Internet. It may encompass a range of Internet services, from basic transmission of tabulated results to full-function online voting through common connectable household devices. The data collected from the election will directly be transferred to the nearest database centers on real time basis using Zigbee systems and applications of cryptography

Keywords: Visual Studio, Sql Server, Devices, Fingerprint Authentication, Voting.

1. Introduction

In India there are two types of voting procedure which are used to be followed during an election. The first one is Ballot Paper System and the second one is Electronic Voting System (EVM). In the Ballot Paper system people need to cast their votes on a piece of paper issued by Election Commission of India. After casting the vote, they need to drop that paper in the Ballot Box. The Electronic Voting Machine consists of two units, Control Unit and Ballot Unit. In the Electronic Voting Machine system people need to cast their vote by pressing a button against the candidate and the political party in the Ballot Unit. The vote will automatically be updated against the candidate in the Control Unit of that machine because they are interlinked with a cable. This control Unit is operated by the presiding officer. But both the systems cannot achieve and attain proper security and authenticity. Antisocial activists can easily cast false votes by threatening people and creating terror in the locality. They sometime force genuine voters to cast their votes to a specific party by threatening them. As there is lack of security and authenticity in
both systems so election procedure is not becoming transparent too much. To get rid of this serious problem, Biometric voting system can be used for any election procedure. It will achieve and attain the highest possible privacy and security while casting the vote by a voter because, the machine uses biometrics. Every single person in the world has unique fingerprint. The BVS unlocks with identifying the voter by his/her fingerprint and when the voting process is over, the machine can automatically count the number of votes that a candidate has acquired. As the system unlocks the voter to cast his/her vote by identifying his/her fingerprint, so there is very less possibility that antisocial activists cast false votes.

The main theme of voting is to allow voters(people) to practice their right to express their choices regarding specific issues, pieces of legislation, citizen initiatives, constitutional amendments, recalls and/or to pick their government and political representatives. Technology is being used more and more as a tool to help voters to cast their votes. To allow the exercise of this right, almost all voting systems around the globe include the following steps: voter identification and authentication, voting and recording of votes cast, vote counting, publication of election results.

Voter identification is required during two phases of the process. First for voter registration in order to establish the right to vote and afterwards, at voting time, to allow a citizen to exercise their right to vote by checking if the person satisfies all the obligations needed to vote. Security plays a major role in e-voting process. Therefore, the necessity of designing a secure and safe e-voting system is very important. Usually, mechanisms that ensure the safety and security and privacy of an election can be time consuming, cost for election administrators, and inconvenient for voters.

There are different steps of e-voting security. Therefore, serious actions must be taken to keep it out of Public domain. Also, safety and security must be applied to hide votes from publicity. There is no scale for acceptable security level, because the level depends on type of the information. An acceptable security level is always a compromise between usability and power of security method.

![Fig. 1 (a), (b) Matching Encrypted and Decrypted Fingerprints](image)

**2. Securities of the E-Voting Systems**

The main objective of a secure e-voting is to ensure the privacy of the voters and of the votes. A secure e-voting system are satisfying the following requirements,(1) Eligibility: only votes of appropriate voters shall be taken into account;(2) Un Reusability: each voter is allowed to cast one vote;(3) Anonymity: votes are set secret; Accuracy: cast ballot cannot be altered. Therefore, it must not be possible to delete
poll nor to add poll, once the election has been closed; (4) Fairness: partial summery is impossible; (5) Vote and go: once a voter has casted their vote, no further action previous to the end of the election; (6) Public verifiability: anyone should be able to readily analyse the validity of the whole voting process.

It based elections voters cast their votes by simply depositing their polls in sealed boxes distributed across the electoral circuits around a given country. When the election period ends, all these boxes are opened and votes are tally manually in presence of the certified officials. In this process there can be error in tallying of votes or in some cases voters find ways to vote more than once. Sometimes votes are even manipulated to alter the results of an election in favour of certain candidates. In order to avoid these shortcomings, the government of India came up with Direct-recording electronic (DRE) voting system which are usually specify as Electronic Voting Machines or EVMs. These devices have been praised for their subtle design, ease of use and reliability. However, it has been found that EVMs are not tinker proof and are easily hack able. Moreover, this harm, hardware as well as software, go without any detection but are quite simple to implement. This made us to bring forth a system that is safe and secure, transparent, reliable as well as easy to use for the citizens. Biometric e-voting systems are not a circumstance anymore they are being mostly used in countries like Ghana and Ireland and are spreading to many other developing nations. We propose an alliance of the CIDR with that of e-voting mechanism to make e-voting in India a reality.

3. Related Works

3.1. Aadhar Based Electronic Voting Machine Using Arduino [1], this paper describes an online electoral system for Indian election is proposed for the first time. The voting system is managed in an easier way as all the users should login by Aadhar card number and password and click on his/her favorable candidates to cast the vote. This features a larger security in the sense that voter high security password is confirmed before the vote is accepted in the main database of ECI. The extra feature of the model is that the voter will ensure if his/her vote has gone to correct candidate/party. The votes are going to be done automatically, therefore saving an enormous time and facultative ECI to announce the result at intervals a very short period.
3.2. Security Analysis of India’s Electronic Voting Machines [2], Elections in India are conducted almost exclusively using electronic voting machines developed over the past two decades by a pair of government-owned companies. These devices, known in India as EVMs, have been praised for their simple design, ease of use, and reliability, but recently they have also been criticized following widespread reports of election irregularities. Despite this criticism, many details of the machines’ design have never been publicly disclosed, and they have not been subjected to a rigorous, independent security evaluation. In this paper, we present a security analysis of a real Indian EVM obtained from anonymous source. We describe the machine’s design and operation in detail, and we evaluate its security in light of relevant election procedures. We conclude that in spite of the machines’ simplicity and minimal software trusted computing base, they are vulnerable to serious attacks that can alter election results and violate the secrecy of the ballot. We demonstrate two attacks, implemented using custom hardware, which could be carried out by dishonest election insiders or other criminals with only brief physical access to the machines. This case study carries important lessons for Indian elections and for electronic voting security more generally.

3.3. Online Voting System with Reliable Voter Authentication Protocols [3], A detailed and critical analysis was done on manual and e-voting systems implemented. These systems exhibited weaknesses of unreliable protocols, denial of service attacks hence the need to implement the public-key encryption e-voting system. Using Makerere University as a case study, the major aim of the public-key encryption e-voting system is to assure reliability and security of the protocol hence guaranteeing voting convenience. Interviews and document review were used to determine inputs, processes and outputs. As a result of the requirements specification, the system was summarized into three processes: access control process which involves identification and authentication phases for eligible voters. Secondly, the voting process was done by encrypting voter’s electronic ballot before submitting to the server. Finally, the final result was sorted through deciphering the received encrypted information. The System is more efficient than other E-Voting systems since voters can vote from their devices without extra cost and effort, and encryption ensures the security.
3.4. An Online Voting System for Colleges And Universities [4], This paper describes an online voting system that was designed to meet the electoral needs of universities and colleges. Design/Methodology: The prototyping model was adopted as the methodology for designing the application. In designing the Online Voting System, Flowcharts, Use Case Diagrams and Data Flow Diagrams (DFD) were also employed. Results: The system generated a more convenient voter and candidate registration interface, an efficient voting interface, vote storage and count plus immediate result compilation etc. Outputs from the application include a page showing a list of all the registered voters, a list of all qualified candidates, and the results of the total vote count for each candidate in the Faculty of Science. A functionality test was also carried out on the developed system where 20 registered students appraised the system by filling out an electronic questionnaire. Originality: Several e-voting systems have been developed for varying uses. This system however was specifically developed for use in tertiary institutions and had security capabilities inbuilt into its design. This originality though peculiar to the adopted case study can be used for developing other kinds of applications. The system was also designed for faculty level voting but can be easily adapted for smaller or larger scenarios. Practical Implications: It can be concluded that the Online Voting System incorporates all the features of a regular Voting system but offers an alternative method of conducting elections that is less stressful, easier and faster through the use of a network. It eliminates the moribund activities associated with the manual system and reduces drastically the duration of elections, thus, resulting in huge financial savings. It is thus recommended for use in any election if well adjusted.

3.5. Biometric Voting System [7], The paper will give an overview of a Biometric Voting System (BVS) which will access the data stored in the database of Aadhaar card, a Government Id card for each citizen in India, while casting their votes. While issuing the Aadhaar card a citizen of India needs to give his/her unique biometric data i.e. the fingerprint image and iris image of both eyes to the government. The BVS is integrated with a biometric fingerprint machine for the authentication of a genuine voter on the Election Day by comparing the given image with the already stored fingerprint image of that voter in
the Aadhaar card database. This system has been developed in Microsoft Visual Studio 2015 with the help of ASP.NET, c# and SQL Server 2014. To eradicate the evil of vote rigging now-a-days in several elections in India, this proposed system can be implemented to get a transparent election in future.

4. Proposed System

In this method, the details of the voter(people) will get from the Aadhar card database and it was a newly developed database which is having all the information about the people (Voters). By using this data, we took the voter’s information will be stored in the Personal Computer. At the time of elections, for finger print insinuate we use finger sensing module. Fingerprint recognition or fingerprint authentication refers to the automated method of authenticating a match between two human fingerprints. Fingerprint are one of many kinds of biometrics used to identify individuals and verify their identity.

A fingerprint looks like the patterns found on the fingertips. There are a variety of ways to fingerprint verification. Some emulate the traditional police method of matching pattern, others use straight minutiae equal devices; and still others are a bit more different, including things like moiré fringe patterns and ultrasonic features. A greater variety of fingerprint devices are available than for any other bio metric.

Advantages:

- Everyone file their vote.
- Low cost.
4.1 Proposed Architecture For E-Voting System

An EVS-Electronic Voting System is a set of guidelines that determine how elections and referendums are conducted and how their results are determined. So let us know the process of a safe and secured e-voting system. The first thing we need to take is the Aadhaar card number of the particular voter and then check whether the given number is correct or not from the Aadhaar card detail database. Then verify the fingerprint and check if everything matches then the voter is a valid person if not reject the person from voting as the person is not valid for voting. And now in the further step we have to check the person is eligible person if eligible then verify if the person has voted already or need to vote, if the person already voted then declare the person as duplicate voter and take the required charges to be taken, if the person has not yet casted his/her vote then allow the person for voting. Your vote is a representation of your voice and opens the door for other ways for you to be engaged and create a relationship with your lawmakers. So this method provides us the best and secure way to citizens to elect their leaders.

Fig. 7 Detail Architecture of Online e-voting System
5. Conclusion

This voting system helps everyone to cast their votes without any difficulty. Online voting will increase the percentage of voting, Manual tallying is not required. So, by this we will get the very clear and fast result. By using this newly developed system we can overcome many issues of existing system. This proposed system is more efficient than the existing one.

References

[1] Murali R Prasad, Polaiah Bojja and Madhu Nakirekanti, “AADHAR based Electronic Voting Machine using Arduino, International Journal of Computer Applications “Vol. 145(12), pp.39-42, July 2016.

[2] Hari K. Prasad et.al., “Security Analysis of India’s Electronic Voting Machines, International Journal of Engineering Science”, October 4th 2010.

[3] Julius Mutebi, Emily Bagarukayo, Ivan Ssempebwa, Michael Kalanda, “Online Voting System with Reliable Voter Authentication Protocols”, 2018 IST-Africa Week Conference (IST-Africa).

[4] Idongesit Efaemiode Eteng, paul umoren, “An Online Voting System for Colleges and Universities”, publication/326059800 May 2018.

[5] Saurabh Yadav and Ajay Kr. Singh, “A Biometric Traits based Authentication System for Indian Voting System, International Journal of Computer Applications”. (0975 – 8887) Volume 65, pp.15, March 2013.

[6] Prof. R.L. Gaike, Vishnu P. Lokhande, Shubham T. Jadhav and Prasad N. Paulbudhe, “Aadhar Based Electronic Voting System”, Vol. 1, Issue 2 May 2016, ISSN (Online) 2456-0774 international journal of advance scientific research and engineering trends.

[7] Soumyajit Chakraborty1, Siddhartha Mukherjee1, Bhaswati Sadhukhan1 and Kazi Tanvi Yasmin1, “Biometric Voting System”, Vol. 4, Issue 4, April 2016.

[8] Firas Hazzaa, Seifedine Kadry, “New System of E-voting Using Fingerprint, International Journal of Emerging. Technology and Advanced Engineering”, Vol. 2, pp 355-363, 2012.

[9] Sobia Baig, Ummer Ishtiaq, Ayesha Kanwal, Usman Ishtiaq, and M. Hassan Javed, “Electronic Voting System Using Fingerprint Matching with Gabor Filter, Proceedings of International BhurbanConference on Applied Sciences & technology Islamabad, Pakistan”, pp 130-135, 2011.

[10] Santha Sheela A.C,“Efficient Data Linkage Using One Class Decision Tree”, Research Journal of Pharmaceutical, Biological and Chemical Sciences(RJPBCS),6(5), pp 655-660.

[11] Kashif Hussain Memon, Dileep Kumar and Syed Muhammad Usman, “Next Generation A Secure E-Voting System Based on Biometric Fingerprint Method", 2011 International Conference on Information and Intelligent Computing IPCSIT Vol.18 (2011).

[12] Davide Balzarotti, Greg Banks, Marco Cova, Viktoria Felmetsger, Richard A. Kemmerer, William Robertson, Fredrik Valour, And Giovanni Vigna, “An Experience in Testing the Security of Real-World Electronic Voting Systems”, IEEE Transactions on Software Engineering, Vol. 36, No. 4, July/August 2010.
[13] Abdalla Al-Ameen and Samani Talab, “The Technical Feasibility and Security of E-Voting”, The International Arab Mayur Patil, Vijay Pimplodkar, Anuja R. Zade, Vinit Vibhute, Ratnakar of Advanced Research in Computer Science and Software Engineering, Vol. 3, Issue. 1, Jan 2013, p.no. 114-117.

[14] Sreena. M, Sukumar. P, Naganarasaia Goud.K, P. Sivakalyani & V.P.ani Kumar, “GSM based electronic voting machine using our screen”, SR Journal of Electronics and Communication Engineering, June 2014.

[15] Steng Li and Alex C. Kot "Fingerprint Combination for Privacy Protection", IEEE Transactions on Information Forensics and Security, February 2013. Journal of Information Technology, Vol.10, No.4, July 2013, p.no.397-404.

[16] Rosario Gil, Mohamed Tawfik, Alberto Pesquera Martin & Sergio Martin, "Fingerprint Verification System in Tests in Moodle", IEEE Journal of Latin-American Learning Technologies, February 2013.