ISSN: 0975-766X
CODEN: IJPTFI
Available Online through ***Review Article***
www.ijptonline.com

SURVEY ON SECURE ELECTRONIC VOTING SYSTEM

K.Ramya Devi[a] and J.V.Vidhya[b]
[a]M.Tech. , Department of Computer Science and Engineering, SRM University, Kattankulathur, India.
[b]Assistant Professor (O.G), Department of Computer Science and Engineering,
SRM University, Kattankulathur, India.
Email: ramyakottidi@gmail.com

Received on 09-01-2017 *Accepted on: 20-02-2017*

Abstract:

Voting system has a set of laws to be followed for voting which is considered to be a valid and set how the votes are counted to get final result of an election. Face recognition, Iris recognition, finger print recognition are used to define the identification and authorisation for a voter. Different voting systems have different ways of allowing individuals to express their votes. But, the achievement of this new generation of machines depends on our ability to capitalize from the lessons we examine the systems currently deployed. The work we present in this paper is one way in which we can get a better understanding of the strengths and the weaknesses of existing systems which leads for the development of more secure technologies for polling stations.

Keywords: Face recognition, IRIS, finger print recognition, Authorisation

1. Introduction

Electronic voting:

An electronic voting (e-voting) system is a process in which the election data is recorded, stored and proceeded primarily as digital information. It uses an electronic means of casting and counting votes. E- Voting systems have been in use since 1960 when the punched card system appeared and was used on seven different counties in US for the presidential election of 1964 and nowadays it had become a very practical way of voting. Electronic voting has many advantages. They are lesser cost, faster results, greater accuracy, and lower risk of human and mechanical errors. It offers improved availability for the people with disabilities, and it provides multiple-language support for the ballots. Electronic voting has tremendous increase in popularity around the world. It has become well-established and deployed in many European countries. Electronic voting is a term that may encompass various types of voting, embracing both counting and casting a vote and votes. Electronic voting systems were first debuted when punched card systems were introduced for the 1964 US Presidential Elections. Then, optical scan voting systems emerged that permit computer systems to enumerate marks on direct-recording electronic (DRE) voting machine. There are two types of Electronic voting which can be outlined as: e-voting which is manage physically by independent electoral authorities or representatives. Like the machines at polling stations, Remote electronic voting is where the vote is not manually monitored by government or independent officers like voting from a personal computer, mobile phone or television via the internet also known as i-voting. A Voting machine is the collaboration of mechanical, electromechanical or electronic equipment which includes its software, firmware and the necessary documentation to program control and endorse equipment which is used to count and cast votes, defined ballots, to show or report election outcomes and to produce and handle audit trail information. This machine is able to give the voter a immediate response such possible problem as overvoting or undervoting which will result in a spoiled ballot. It has various levels of security, usability, accuracy and efficiency. Currently, the most common machine use is electronic .Certain machines may be more or less accessible for voters.

1.1 Advantages of E-voting:

- Secure ,Auditable, transparent and accurate

For some nations, automated elections mean that people can trust the outcomes because it allows for a process that is so transparent and secure. Human errors can be reduced with the help of electronic voting .

- Faster results and make trust

For other countries, particularly large ones like India, electronic counting and electronic voting means that people can get official election results within hours, instead of weeks which builds trust.

- Increases approachability

It’s also important that everyone who is qualified to part in elections can do so and electronic voting make the process eath for disable people and provides facility for them to vote independently .The Electronic voting makes voting process more accessible.

- Electronic voting that is completely inspectable

One reason our electronic voting framework has been commended so exceptionally is that it's composed around the possibility that all gatherings, natives and race commissions can review the constituent procedure at each stage, including before a decision has even started. The way to our prosperity is what's known as the voter-confirmed paper review trail (VVPAT). Our voting machines print a paper receipt each time a vote is enrolled electronically. This makes it simple to perform describes and reviews since you can contrast the electronic number and the paper tally.

- Electronic voting that is visibly secure

The VVPAT assists people see that our electronic voting framework is totally secure. In the event that anybody could hack into our framework, there would be a disparity between the electronic check and the paper tally. In more than 2.5 billion votes, there never has been. Obviously, our framework likewise ensures the Concealment of the vote.

- What makes our electronic voting so safe?

Voting machines highlight information data storage and transmission ensured with 256-piece encryption and superfluous, a term given to as framework where information is held in a wide range of areas, to make it clear if anybody somehow managed to change it in one.

2. Methods of Secure E-voting:

Electronic voting machines:

The System is a set of two devices. Voter uses a device called Voting Unit, and another device is called Control Unit which is operated by the Electoral Officer. Both units are connected by a cable. The Voting unit has a Blue Button for individual candidate. The Control Units consist of three buttons. One button to vote, one to see the number of votes casted , and one to close the election process. The outcomes are concealed and sealed.

Internet voting:

Internet voting can be done even from remote areas (any Internet enabled computer can be used) or can use traditional polling locations with voting booths composed of Internet connected voting systems. To elect officers and Board members, Business enterprises and organizations make use of Internet voting and for the other proxy elections. Privately Internet voting systems have been used in many modern nations.

Finger print recognition:

Fingerprint recognition has been using in many applications such as forensic,civilian applications etc. fingerprint-based biometrics is the most used technique when compared to other recognitions.it is used to define uniqueness. It operates in affirmation mode or in empathy mode.

Iris recognition:

Iris recognition is the method of identifying people based on individual patterns within the ring shaped region around the pupil of the eye. The process of capturing an iris into a biometric frame is made up of 3 steps: 1. Encapsulate the image 2. Discover the location of the iris and modify the image 3. Storing and comparing the image..Because it makes use of biological characteristic, it is considered as a form of biometric verification.

3. Approaches for secure E-voting:

Title: Security Analysis of India's Electronic Voting Machines

The processes of voter registration, vote counting, vote casting and ballot generation are becoming machine controlled. Numerous cases of allegedly accidental errors have been reported, along with suspicions of fraud. However, the borderline between accident and fraud is delibaretly unclear. Serious security exposures are common place in most voting systems, furnish distributed opportunities for computer-system misuse, particularly by insiders Indeed, incentives for graft and fraud are likely to be intensified by the stakes involved in winning or losing an election. There is no generally accepted standard set of criteria that voting systems are required to satisfy.

Clip-on Memory Manipulator Attack

An attack device that attaches straightly to the memory chips that depot the votes in the control unit the device fits in a shirt pocket and can be used to steal votes or to infract ballot secrecy. The display board can only see votes as they are displayed by the control unit CPU, must display each vote right away and enhance the display to the total after a particular time interval. As a result, it has to declare to a vote total for each candidate before it sees the votes left for the remaining candidates. In other words, vote-stealing algorithm should be online. Despite this added complication, an online proportional boost vote-stealing algorithm is implemented which ensures no candidate's votes falls below a certain threshold, maintains some consistency properties of the generated results, and gives additional votes to its favored candidate.

Title: **Design of Secure Electronic Voting System Using Multifactor Authentication and Cryptographic Hash Functions**

The goal of a voting system is to ensure that the vote counts therefore, electronic democratic governance that provides a obvious and trusted election is needed. The usual method of voting involves the use of paper ballot to casts vote. This is susceptible to time waste, ballot abduct, lack of voter privacy and question the integrity of fair electoral process. To improve the authentication and integrity of evoting system, multifactor authentication and cryptographic hash function methods are used. This meets two of the key security issues in secured e-voting system: The threat of erring voter's authentication and identification of vote transmitted over wireless medium. The results obtained from the evaluation of secured electronic voting system defines an avenue to ensure the unity of the electoral process to have beleif in the election, through the detection of altered votes in wireless medium and voter authentication through OTP.

Hash functions: Hashes are mathematical functions or equations that read in a piece of information and output a set of letters that are unique to the input. This process is used to identify malicious modifications to the software or when a software is corrupted or when incorrect versions are about being installed.

Title: A Secure Blind Signature Application in E Voting

Voting is an important social activity in democratic society. The democracy is based on the security of electronic voting scheme. It is essential to use the cryptographic technique for election. Current electronic voting schemes protect the voter's identity from the vote. A technique called blind signatures is defined to a voter's ballot so that it is difficult for anyone to trace the ballot back to voter. E-voting employs cryptographic technique to handle the security issues in the election process. This fully conforms to the requirement of privacy, fairness, unreusability.

Digital signatures:

Digital signatures are numerical functions that work in a corresponding manner to cryptographic hashes and also help to identify who sent a message or a file. Digital signatures are not analogous to physical hand written signatures as they provide stronger identity of who signed a message in elections, impressions are used to sign the contents of a voters ballot selections to ensure that ballot box or vote was not altered.

Title: Voting Mix-Net

The basic decryption mix-net works as a series of proxy servers, each with its own public and private key. The proxy server will be called as a mix-server. The client encrypts its input once using each of the proxy servers' public key in a certain order.

The mix-servers then decrypts the input in that same order. Each mix-server takes a list of encrypted texts. It decrypts them using its private key, shuffles the order and then sends it to the next mix-server.

Mix-Nets:

A mix net takes cipher text, stored data and then re encrypts it and shuffles the order in which it is stored.only then are the data encrypted and the values of votes were revealed. It is unendurable to decrypted vote values can be linked back to the original data received or identity of the voters.

Title: Secure E-voting Using Homomorphic Technology

The e-voting is based on Homomorphic Technology and guarantees eligibility, un reusability, privacy, verifiability and also receipt-freeness, no vote selling and un coercibility. This can be implemented in a practical environment, since it does not use voting booth or un tappable channel, only anonymous channels are applied.

Homomorphic encryption: It is an cipher technique that allows for computations to be done on an encrypted data without requiring access to a decryption key as individual votes are never decrypted, there is no possibility of associating voters to the way they voted.

Literature survey:

Table 1: Overall Survey on Existing Algorithms.

S.NO	Title	Algorithm/Formulation	Drawbacks	Achivements
1	an effective algorithm for fingerprint matching	error propagation based matching algorithm	The image itself changes much when large deformation is observed Reducing the similarity of images is difficult	concept of error propagation is applied to track nonlinear deformation adaptively. Meets the response time and accuracy
2	Model based algorithm for singular point detection from finger print images	AFIS(Automatic Finger Print Identification System)	Points are difficult to extract	-
3	Secure biometric systems,2006	Cryptography algorithms	illegal sharing of keys (i.e. key management problem) is a big problem	data based alignment scheme is performed well will not leak critical information outside the vault

4	Filterbank-Based Fingerprint Matching algorithm	Filterbank-Based Fingerprint Matching algorithm	handling nonlinear distortion and refinements of initial strategies for feature extraction	Computationallyattractive matching/indexing capability the identification of finger print effectively involves a “bit” comparison.
5	A comparative study on finger print matching algorithm for evm	Direct matching algorithm	not suitable for large databases	secure way in terms of time and memory
6	New algorithm biometric based IRIS pattern recognition system: basis of authentication and verification	Pattern recognition algorithm	Accuracy is not defined	IER feature extraction used for pattern matching was compared with the stored patterns within the database to ensure high quality result in authentication.
7	Security analysis of India’s Electronic Voting machine	Clip-on Memory Manipulator Attack	Stealing votes,violating ballot secrecy	-
8	E-voting protocol based on public-key cryptography	RSA public key encryption algorithm	Prevention of brute force attack, the choice of the key size becomes crucial.	The protocol is more efficient than the other E-Voting protocol. It allows the voter to vote from his/her own personal computer (PC) without any extra cost and effort.
9	An e-voting system for medium scale online election	Communication protocol	They tend to produce high communication overhead in vote counting phase	SELES is able to obtain a final exact tally of up to five thousand votes in less than 140 Seconds.
10	Online hand written signature identification	Hidden marcov model	Only basic feature set is done by using some derived features.	It captures live signature data from some sensor and compares it against templates stored in the database to find the best match.
11	Handwritten signature identification using basic concepts of graph theory	Graph theory	Image pixels are not clear	a good tool for some biometric systems that use other biometric characteristics (e.g. face recognition) suitable for implementation even in the off-line handwritten identification systems

References:

1. Olayemi Mikail Olaniyi "Design of Secure Electronic Voting System Using Multifactor Authentication and Cryptographic Hash Functions" International Journal of Computer and Information Technology (ISSN: 2279 – 0764) Volume 02– Issue 06, November 2013
2. Satish Chhokar "A Secure Blind Signature Application in E Voting" Proceedings of the 5th National Conference; INDIACom-2011 Computing For Nation Development, March 10 – 11, 2011
3. Joakim uddholm hjalmarsson "voting Mix nets" KTH Computer Science and Education 2011
4. "An identity-Authentication Systems using Fingerprints". proceedings of the IEEE,vol 5,no:9,sep 1997.
5. S.Prabhakr, S.Pankati and A.K.Jain, "Biometric recognition; security and privacy concerns", IEEE security privacy/Mag.,vol.1,pp 33-42,2003
6. Majid Javid Moayed Abdul Azim Abdul Ghani Ramlan Mahmod "A survey on Cryptography Algorithms in Security of Voting System Approaches" IEEE 2008.
7. Ann cavoukian and Alex Stoianaov" Biometric encryption chapter" from the encyclopedia of biometrics.
8. W.stallings, cryptography and network security: Principles and Practice, Prentice Hall College, 2006.
9. Jain A.K., Hong L., Pankanti S. and Bolle R., "An identity authentication system using fingerprints," Proc. IEEE,vol.85, pp. 1365-1388, Sept.1997.
10. Ann Cavoukian and Alex Stoianov Biometric Encryption Chapter from the Encyclopedia of Biometrics
11. F Chafia ,C Salim and B Fraid ," Biometric crypto system for authentication" International Conference on Machine and Web Intelligence ,Pp434 -438,2010
12. Anil K. Jain Michigan State University, USA Patrick Flynn University of Notre Dame, USA Arun A. Ross West Virginia University, USA , Handbook of Biometrics.
13. U. Uludag, "Secure biometric systems," PHD thesis, Michigan state university,2006.
14. Uludag.U, Pankanti.S. Prabhakar.S, Jain.A.K"Biometric cryptosystems: issues and challenges " Proceedings of IEEE ,Vol 92,No.6,Pp948-960 ,2004
15. V Prasathkumar, V.Evelyn Brindha "Personal Authentication using Fingerprint Biometric System",IJIRCE,2014

16. R. Mukesh, A. Damodaram and V. Subbiah Bharathi, "A robust finger print based two-server authentication and key exchange system," *Communication Systems Software* .

17. B. Miroslav, K. Petra and F. Tomislav, "Basic on-line handwritten signature features for personal biometric authentication," *MIPRO, 2011 Proceedings of the 34th International Convention*, Opatija, 2011, pp. 1458-1463.

18. Bodo, "Method for producing a digital signature with aid of a biometric feature," Germany: German patent DE 42 43 908 A1, 1994

19. F.Ayoub and K Singh ," Cryptographic techniques and network security" IEEE proceedings of communications, Radar and Signal Processing,Vol 131,No.7 Pp 684-694 , 1984

20. F Chafia ,C Salim and B Fraid ," Biometric crypto system for authentication" International Conference on Machine and Web Intelligence ,Pp434 -438,2010

21. Russel Ang, Rei Safavi-Naini and Luke McAven "Cancellable key based fingerprint templates" Australasian Conference on Information Security and Privacy Pp 242-252,2005.

22. Uludag.U, Pankanti. S.Prabhakar.S, Jain.A.K"Biometric cryptosystems: issues and challenges " Proceedings of IEEE , Vol 92,No.6,Pp948-960 ,2004

23. Rajlaxmi Chouhan, Agya Mishra, Pritee Khanna" Fingerprint Authentication by Wavelet-based Digital signature",Vol4,IJECE,2012

24. V Prasathkumar, V.Evelyn Brindha "Personal Authentication using Fingerprint Biometric System", IJIRCE,2014

25. B. Miroslav, K. Petra and F. Tomislav, "Basic on-line handwritten signature features for personal biometric authentication," *MIPRO, 2011 Proceedings of the 34th International Convention*, Opatija, 2011, pp. 1458-1463.