Receipt-free Multi-Authority Voting with (2,2) Secret Sharing Based Authentication-Review

Ms. Ashwini Walake
Student-Mtech(CSE),
B.D.C.O.E., Sewagram.
Pin Code-442001

Prof. Ms. Pallavi Chavan
Assistant Pofessor(Sr. Gr.)
B.D.C.O.E., Sewagram
Pin Code-442001.

Abstract

This paper describe the survey among the schemes used for the voting system. Each of them is having unique features while overcoming the limitations of existing schemes. Security is an important issue for the voting system. This paper also describes a secured authentication mechanism for the voting system with the help of secret sharing.

Keywords- Threshold secret sharing ,shares, authentication.

1.Introduction

Election is an efficient mechanism for democracy. It is a way to collect public opinion to form government. Voting is a mechanism through which public can select their representative but because of the inconvenient traditional voting system and fraud in voting system there has been decrease in number of voters. To overcome the drawback of traditional voting system online voting system is introduced. Online voting system is a effective mechanism for election because of the expansion of the internet, communication network and advances in cryptographic techniques. There is no restriction of physical location in online voting. Voter can participate in election no matter where they physically are at the time of voting process. Online voting system has many advantages over traditional voting system. Some of the advantages are greater accuracy, lesser cost of establishment, faster tabulation of result, and it lowers the risk of human error. Online voting improves the voter confidence. Online voting scheme must work securely and effectively in insecure environment. Following are certain requirement that every voting system must satisfy to work effectively.

Privacy: A system is private if voters identity is not linked with the vote casted by the voter so that voters safety is considered.

Universal Verifiability: Universal Verifiability provides ability to voter or any one in the system to check whether all the votes are counted correctly or not.

Eligibility: Only authenticated and eligible voters are allow to vote. Voter must satisfy all the eligibility test.

Robustness: The system is robust if can detect the faulty behavior of voter or any authority. And it must recover from it.

Efficiency: The system must compute the result in reasonable amount of time and computational load must be light.

Uncoercibility: The voter should not be forced to vote. And voter should not be able to prove to whom he has voted.

Receipt freeness: Voter should not be able to prove his vote.

Some conditions may occurs in which voter register but may decide not to vote. In such condition if the voting process is controlled by single authority then the authority may misuse his power. And may add extra ballot as he wishes. To overcome this problem we introduce the concept of multiple authority in which the complete voting process will be handled by multiple authorities to provide the fairness in the system. Also security is an important part of the online voting system. Security is provided through the authentication process. User authentication is a tool to provide security to any system. The primary goal of user authentication is to prevent any adversary from impersonating other user. Mutual authentication is useful in preventing fraud. Secret sharing schemes are very useful technique used for authentication. Secret sharing is the way of hiding the secret information. It is a technique used to hide a piece of information called the secret by splitting this secret into several parts called shares and spreading them among participants. Secret sharing concept can be apply in hierarchy of user to provide the confidentiality. In a way the secret can be recovered from certain subsets of the shares. The same concept of secret sharing is used in online voting system. Here we are applying the concept of secret sharing to provide security so that the system will be more secure .

2. LITERATURE SURVEY

Based on the cryptographic technique used the voting systems are classified as
Homomorphic encryption based voting system
Mixnet based voting system
Blind signature based voting system

Homomorphic encryption based voting system: An encryption function E(k,x) is said to be homomorphic if encrypted forms of two messages m1 and m2 that is E(k,m1) and E(k,m2) satisfy the additive homomorphic or multiplicative homomorphic property. It apply certain property of probabilistic cryptosystem where correspondence between plaintext and ciphertext exist between certain group. It provides mechanism to directly combine the encrypted tally. This is useful in tallying phase, since only few decryption operations are necessary to obtain the result.

Blind signature based voting system: Blind signature were first introduce by Chaum in 1982. It is the form of digital signature. It is employed in many privacy related protocol. It allows an entity to get the signature on message without revealing the content of message.

Mixnet based voting system: Mixnet based schemes consist of multiple mix servers and it takes set of encrypted messages as an input and same message is represented in new form as a output. It provides channel shuffling. Each server in system receive the votes permutes their order transform the votes and send the votes to next server.

In 2008, Mohammed Khasawneh, Mohammad Malkawi, Omar Al-Jarrah, and Thaier S. Hayajneh [1] proposed a secure e-voting system using biometric. This scheme can handle electronic ballot with multiple scopes at the same time. This system guarantees that during the tallying phase no vote in favor of candidate will lost. Transparency of voting system follows in all phases of an election process to provide assurance to the voter that his/her vote went in favor of his/her candidate of choice. It provides correctness, robustness, coherence, consistency, and security. It uses client/server web enabled e-Voting software architecture. A global database is maintained for all registered voters and candidates on the server side. client side maintains local database to reduce the traffic rate on the network links. As compare to global database at server side the size of local database at the client side is small. It uses an identification followed by an authentication process. In identification it reads the official ID card of a voter and get the voter record from the local DB , if data is not found it loads the record from the central DB. The voter record includes a biometric description of the voter. This scheme uses the fingerprint authentication.

In 2008, Sanjay Saini and Dr. Joydip Dhar [2] gives an framework for online voting system. This framework enable voter to vote in public environment and the neighbor or third party will not know to whom voter has vote. This framework provides security using cryptographic schemes and zero knowledge proof. This framework has certain assumptions like
1) line through which communication is carried out are assumed to be secure.
2) It assumes minimal delay in the data transfer with minimal error rate.
3) The servers used in election process are computationally fast enough to handle large number of clients and it performs necessary encryption- decryption and hashing without delay.

In 2010, Cesar R. K. Stradiotto, Angela I. Zotti, Claudia O. Bueno, Sonali P. M. Bedin, Hugo C. Hoeschl and Tania C. D. Bueno, Thiago P. S. Oliveira[3] describes two experiments. The first experiment test the viability for the international voting through SMS protocol by using mobile. Author uses Web 2.0 tools. In second experiment it construct the voting prototype using Android platform smart phones. It also uses different applications and vote collecting databases which are available on dynamic web pages.

In 2011, Shivendra Katiyar, Kullai Reddy Meka, Ferdous A. Babhuiya and Sukumar Nandi [4] proposed a scheme for online voting system using biometric security. This scheme uses ryptography as well as stegnography. The basic idea of this scheme is to merge the secret key with the cover image on the basis of key image. This key image is the biometric measure like fingerprint image. For casting the vote user log into the system by entering the unique identification number and secret key. User also have to produce thumb impression on fingerprint sensor. For the thumb impression system will generate cover image and embed secret key into the cover image and finally stego image will get generated. Server will authenticate the user using this stego image. The server uses Optical character Recognition technique to identify the unique identification number embedded in image. Security is more in this scheme as it combines both cryptography and stegnography.

In March 2011, Chinniah Parkodi, Ramalingam Arumuganathan and Krishnasamy Vidya, [5] proposed a new voting system based on the elliptic curve technique. It involves multiple authorities in election. This scheme uses trusted center which is responsible to distribute the share among multiple authorities. It uses Shamirs (t,n)secret sharing scheme. Hence it uses n number of authorities at the tallying phase. This scheme assumes the vote casted by the voter as a point on the curve. This scheme requires addition of few points for the computation of ballots. Hence this scheme is computationally efficient. It gives two way multiauthority. In first one it select vote Vi from [-1,1]. In second one it selects vote Vi from V1,V2...........Vr. This scheme meets the essential requirements of online voting.

In 2012,Haijun Pan, Edwin Hou, and Nirwan Ansari [6] proposed a scheme for E-voting. It is an improvement over their previous work NOTE. The proposed scheme is referred as E-NOTE. This scheme uses hardware device watchdog. Watchdog ensures voters confidentiality also provides voting accuracy. This scheme consist of Election Committee (EC), Vote counting committee (VCC), and Ballot Distribution center (BDC). BDC handles the responsibility of ballot distribution. EC, BDC, VCC are independent from each other. Watchdog is used to prevent the voter fraud. It records all voting transactions. This scheme provide voters confidentiality and solves the problem of voter fraud using watchdog device.

Anida Sarajlic, Narcis Behlilovic,Irma Sokolovic [7] present a modular concept in online voting. This ensures that the registered voters can vote only once. This scheme also provides privacy to the voter. This is done through the random password distribution and there will not be any trace of password used by the user. This system consist of modules voting consol VC, module for password distribution MPD, voting management module VMM, module for vote storage and result storage MSRM. Module for password distribution is important it maintains two list one for voter id and second for access password. This system provides privacy to the voter but single voter get the number of password that degrades the performance of the system.

In 2013, Hoda Ghavamipoor and Maryan Shahapasand [8] proposed a scheme for secure and efficient electronic voting scheme based on the blind signature in which voters do not need a set of public/private keys. The participants involve in this scheme are voters, central authority (CA) , a voting authority (VA) and set of scrutineers (s1,s2......sn). scrutineers are responsible for preventing VA and CA from dishonest handling of the voting process. Two databases are used in Hoda Ghavamipoor and Maryan Shahapasand scheme. These are VDB1and VDB2 .VDB1 and VDB2 are installed in VA. It is used to record the identification number of the registered voters. VDB2 is another database which is also installed in VA. And it is used to record the ballot cast by voter. After completion of election, the VDB2 will made publish. In this scheme CAn > VAn to prevent the problem of reblocking. This scheme is efficient because user do not need a set of public/private keys. But this scheme does not satisfy the problem of coersability.

In 2013, Honady Hussien and Hussien Aboelnager [9] proposed a scheme based on homomorphic property and blind signature. This system uses RFID which is prepared by government before election to store all conditions to check voters eligibility. This scheme uses Central Tabulation Facility (CTF), it collects all secret ballots from all servers at poll station. RFID contains all information related to voter to check
the voters eligibility.

In 2011, Prabir Kr. Naskar, Ayan Chaudhuri, Debarati Basu, and Atal Chaudhuri [17] proposed a secret sharing scheme in which shares are generated by performing graphical masking by simple AND operation. The secret can be reconstructed by simply ORing the qualified set of shares. This scheme provides confidentiality and integrity because it produce compressed shares. This scheme uses Shamirs (t,n) secret sharing scheme.

In 1979, Adi Shamir [10] proposed a way to share a secret data D into a group of n users. The secret data D is shared among n users in such a way so the reconstruction of shares will be easy using any (k + 1) or more shares. No information about the secret data D can rebuilt using k or less shares. This Adi Shamir’s secret sharing scheme is called (k +1,n) threshold secret sharing scheme. In this scheme n is the number of users holding the secret data D and (k + 1) is the threshold value. Threshold is the least number of users needed to rebuilt the secret data. Thus in 1979 Adi Shamir proposed the (k + 1,n) threshold secret sharing scheme. The goal of Shamir's [1] a (k + 1; n)-threshold secret sharing scheme is:

Divide the secret data D into n no. of pieces in such a way that:

1.D easily computable using any k+1 or more Di pieces;

2.The calculation of secret data D is impossible using k or lesser Di pieces .

In a two-dimensional plane each of the n users will have one point represented as, (x1; y1),...,(xn; yn). Each xi is different and yi = q(xi) for all the users i where, q(xi) is a random k degree polynomial of the form q(xi) = a0 + a1xi + :::akxik I where a0 = D and a1:::ak are random integers in polynomial. For ith user the secret share is computed using Di = q(xi). It is sufficient to find a0:::ak is easily computable using knowledge of any k + 1 of those secret shares, by interpolation, where a0 is the original secret. By Adi Shamir's [1] scheme, if a secret is shared among a group of n users, there is no need to cooperate with all the users. Therefore this scheme is convenient to use. On the other hand, if a number of members are less than the threshold value (k + 1), then they can never rebuilt the secret. To reconstruct the secret, at least a number of users must be greater than the threshold value. This improves the reliability of the scheme. The disadvantage of Adi Shamir's [10] hierarchical secret sharing scheme is the storage problem as larger number of shares have to be store by higher level users .

3. COMPARISON

Research in voting process is still in progress. Many authors proposed different schemes for the voting system. From survey of current literatures about various voting system, it is possible to compare them as follows:

Year	Author	Title	Technique used
2008	Mohammad Khasawaneh, Mohammad Malkawi, Omar Al-Jarrah,Thaier S. Hajajneh	A Biometric-Secure e-Voting System for Election Processes	It uses biometric features for authentication. It uses client/server web enabled architecture.
2008	Sanjay Saini Dr. Joydip Dhar	An eavesdropping proof secure online voting mode	Uses cryptographic scheme zero knowledge proof to provide security.
2010	Cesar Stradiotto, Angela Zotti, Claudia Bueno, Sonali Bedin, Hugo Hoeschl, Hania Bueno, Thiago olivera.	Web 2.0 E-Voting System Using Aandroid Platform	Uses web 2.0 tools and SMS protocol. Also uses Android platform.
2011	Shivendra Katiyar, Kullai Reddy Meka, Ferdous Babhuiya, Sukumar Nandi.	Online Voting System Powered By Biometric Security Using Steganography	It uses both cryptography as well as stegnographic scheme.
2011	Chinniah Prkodi, Ramalingam Arumuganathan, Krishnasamy Vidya.	Multi-authority Electronic Voting Scheme Based on Elliptic Curves	It uses elliptic curve technique. Uses Shamir's (t,n) secret sharing scheme.
2011	Haijun Pan, Edwin Hou, Nirwan Ansari	E-NOTE: An E-voting System That Ensures Confidentiality and Voting Accuracy	It uses watchdog hardware device for confidentiality.
2011	Anida Sarajlic, Nargis Behlilovic	A Modular Concept of E-voting System	Complete system is divided into modules.

		that Protects User Privacy Using Password Distribution	
2013	Hoda Ghavamipoor, Maryan Shahapasand.	An Anonymous and Efficient E-voting Scheme	It uses blind signature property.
2013	Honady Hussien, Hussien Aboelnager.	Design of a Secured E-voting System	It uses blind signature and Homomorphic property.
1979	Adi Shamir	How to Share a Secret	Proposed (k+1,n) secret sharing scheme. It uses langrangeous interpolation.

Table 1. Comparative study

4. CONCLUSION

This review paper explain various methods for the voting system. This paper also explains the methods based on the secret sharing schemes. Security is an important issue in voting system. Authentication is the way to provide the security to the system. Authentication is provided through the secret sharing schems.

5.REFERENCES

[1] Mohammed Khasawne, Mohammad Malkawi, Omar Al-Jarrah, Thaier S Hayajneh, “A Biometric-Secure e-Voting System for Election Processes” proceeding of *IEEE Transaction, 5 International Symposium on Mechatronics and its Applications (ISMA08)*, Amman, Jordan, May 27-29, 2008

[2] Sanjay Saini and Dr. Joydip Dhar, “An eavesdropping proof secure online voting model”proceeding of *IEEE Transaction, International Conference on Computer Science and Software Engineering*, 2008, pp. 704-708.

[3] Cesar R. K. Stradiotto, Angela I. Zotti, Claudia O. Bueno, Sonali P. M. Bedin, Hugo C. Hoeschl and Tania C. D. Bueno, Thiago P. S. Oliveira, “Web 2.0 E-Voting System Using Aandroid Platform”, proceeding of *IEEE Transaction*, 2010,pp. 1138-1142.

[4] Shivendra Katiyar, Kullai Reddy Meka, Ferdous A. Babhuiya and Sukumar Nandi, “Online Voting System Powered By Biometric Security Using Steganography”, proceeding of *IEEE Transaction, Second International Conference on Emerging Applications of Information Technology*, 2011,pp. 288-291.

[5] Chinniah Parkodi, Ramalingam Arumuganathan and Krishnasamy Vidya, “Multi-authority Electronic Voting Scheme Based on Elliptic Curves”, proceeding of *IEEE Transaction, International Journal of Network Security*, Vol.12, No.2, Mar. 2011, pp. 84-91.

[6] Haijun Pan, Edwin Hou, and Nirwan Ansari, “E-NOTE: An E-voting System That Ensures Confidentiality and Voting Accuracy”, in *IEEE, ICC ,Communication and Information System Security Symposium*, 2012, pp. 825-829.

[7] Anida Sarajlic, Narcis Behlilovic,Irma Sokolovic, “A Modular Concept of E-voting System that Protects User Privacy Using Password Distribution” proceeding of *IEEE Transaction, 18th International Conference on System, Signal and Image Processing, IWSSIP*, June 2011.

[8] Hoda Ghavamipoor and Maryan Shahapasand, “An Anonymous and Efficient E-voting Scheme”, proceeding of *IEEE Transaction, 18th International Conference on e-Commerce in Developing Countries with focus on e-Security*. April 2013.

[9] Honady Hussien and Hussien Aboelnager, “Design of a Secured E-voting System”, proceeding of *IEEE Transaction*, 2013.

[10] Adi Shamir, “How to Share a Secret”, in *Communications of ACM*, Vol.22, no.11.