ISSN:0975-9646

Efficient Voting system with (2,2) Secret Sharing Based Authentication

Ms. Ashwini Walake
Student-M.Tech.(CSE)
B.D.C.O.E. Sewagram
Pin code-442001

Prof. Ms. Pallavi Chavan
Assistant Professor(Sr.Gr.)
B.D.C.O.E. Sewagram
Pin code-442001

Abstract- This paper describes the online voting system with secure authentication. This is a web based voting system which allow voter to vote irrespective of location. Providing security to any data or information is an important issue and it becomes sensitive for online voting system. The proposed system provides secured authentication through the Shamir's secret sharing scheme.

Keywords- Secret Sharing, Shares, Authentication.

1. INTRODUCTION

Trustworthy election is an efficient mechanism to democracy. It is a process in which people choose their representative to form a government. The key requirement for effective election process are correctness, robustness, and security. There are variety of voting schemes which are based on the traditional method. But because of the inconvenient traditional voting system there is tremendous decrease in number of voters. Hence online voting system is introduced to overcome the drawback of traditional voting system. Online voting system has the facility to complete voting process faster than the paper ballot voting procedure.

This system itself should be intelligent to earn the trust and confidence of the user by providing enhanced security and reliability. The security is an important factor in any voting system. Here security is provided through the authentication. Authentication is a secured way to check the voters identity. The principal objective of authentication is to prevent any adversary from copying other user. Secret sharing schemes are the powerful mechanism used for the authentication. Secret sharing schemes are ideal for storing information that is highly sensitive and highly important. Secret sharing is also termed as secret splitting. Secret sharing is a method for allocating a secret among a group of participants. Each of whom is allocated a share of the secret. For reconstruction it uses t shares out of n no of shares. The system uses the idea to fit a unique polynomial of degree (t-1) to any set of t points that lie on the polynomial. For straight line it takes two points, three points to define a quadratic, and to define cubic curve it takes four points , and so on. It means to form the polynomial of degree t-1 it takes t points. The method is to generate a polynomial of degree t-1 with the secret as the first coefficient and the remaining coefficients picked at random. It finds n points on the curve and give one to each of the participants. When at least t out of the n participants expose their points, there is sufficient information to fit a (t-1)th degree polynomial to them, and the first coefficient being the secret.

2. RELATED WORK

There are different techniques used for the voting system.

In 1982 the concept of blind signature were introduced by the Chaum. Many privacy related protocol uses the blind signature as a form of digital signature. It do not reveal the content of message and get the signature. It is a cryptographic protocol which involves two parties.

Some of the voting schemes are based on the Homomorphic encryption where specific algebraic operations are performed on the plain text and different operation on the cipher text. Homomorphic function E(k,x) is used. E(k,m1)is the encrypted form of message m1. E(k,m2) is the encrypted form of message m2. If the encrypted form satisfy the multiplicative homomorphic or additive homomorphic property then E(k,x) is called as the homomorphic function. This correlate the plain text with the cipher text. This property is useful for combining the encrypted tally. Homomorphic encryption based system do not support write-in vote.

The first mixnet based system were introduced by the David Chaum. It composed of the several servers which are linked with each other. Each server takes input as encrypted vote randomize it and then output the batch of permuted vote so that the input and output are disagreeable.

In 1979, Adi Shamir[1], proposed a scheme to share the secret among the group of users to provide the better security. If the secret D is distributed into n shares then it can be rebuilt from any (k+1) or more shares. Secret can not be reconstructed using k or less shares.

In 2011 Prabir Naskar, Ayan Chaudhari, Debarati Basu, Atal Chaudhari[2] use the secret sharing concept for the image. In their paper they recommend the scheme which uses simple graphical masking. In graphical masking for generating the share they uses the ANDing operation. To reconstruct the original secret uses ORing operation of qualified set of shares. It provides the strong protection to secret image.

In 2012, Yi-Hui Chen and Ci-Wei Lan [3] proposed a self authentication mechanism for (3,3) threshold secret sharing scheme. This scheme uses authentication image along with the secret image to provide the better security.

Pallavi chavan , Dr. Mohammad Atique and Dr. A. R. Mahajan[4] proposed an intelligent system for secured authentication using hierarchical visual cryptography. In their scheme they provide the secured authentication mechanism using visual cryptography.

In January 2012, Che-Wei Lee and Wen- Hsiang Tsai[5] gives a new method for authentication of grayscale document. In this scheme authentication signal is generated

from grayscale document and transformed into shares using shamir's secret sharing scheme. These shares gets implanted into alpha channel plane and then combine with the original gray scale document to form PNG image. It also provide data repairing capability.

In October 2013, Mundalik Vijay, Sable Suvarna, Khandave Dipali and S. K. Patil[6] proposed a scheme for online voting system which uses face detection and recognition system as an authentication mechanism. It uses the concept of stegnography.

Chetana Hegde, Manu S, P Deepa Shenoy, Venugopal and L M Patnaik[7] proposed a scheme to provide a secured authentication in banking area. This scheme is based on visual cryptography. It uses secret sharing scheme for the authentication. To produce the shares signature of customer is used.

In 2008, Sanjay Saini and Dr. Joydip Dhar[8] proposed a framework for online voting. The proposed framework gives capability to voter to vote in public environment. To provide the security it uses cryptographic technique and zero knowledge proof.

Cramer et al[9] gives a new model for election. This model uses some properties of homomorphic encryption technique. It uses homomorphic operation $\oplus$ for the message space and an operation $\otimes$ for the cipher space. If the encryption of any two votes is E(v1) and E(v2) then product of E(v1) $\otimes$ E(v2) is nothing but E(v1$\oplus$ v2) encryption of two votes.

J. Benaloh and D. Tuinstra[10] proposed scheme for receipt free secret ballot election. This scheme uses the concept of homomorphic secret sharing. In this scheme voter share their vote among the authorities of election. Using the public key of distinct authority the share gets encrypted and display on the bulletin board. At the time of tally each authority produce third share and combine to get the final tally.

Shivendra Katiyar, Kullai Reddy Meka, Ferdous A. Babhuiya[11] gives online voting system using biometric features. It uses the cryptography and the concept of stegnography.

3. PROPOSED METHODOLOGY

The proposed system involves several steps. It can be accessible from two sides Election Commission Officer i.e. administrator and the voter. Following figure shows the detail architecture of the proposed system.

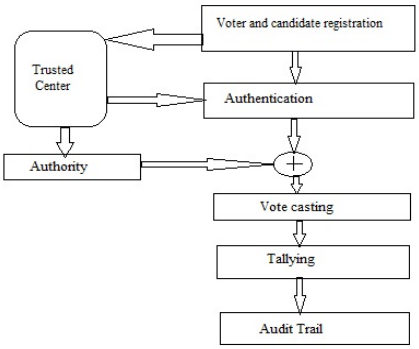

Fig1. Phases of voting system.

Registration Phase

In registration phase voter as well as candidate have to register first. After registration password will get generated by the system. Trusted centre play an important role in registration phase. Trusted centre divide the generated password into shares. One share is held by voter and another by central authority. For share generation it uses Shamir's (2,2) threshold secret sharing scheme.

Algorithm to form shares

Input: d is secret in the form of an integer, n is number of participants, and k is threshold .

Output: shares for the n participants to keep.

Step 1. Choose randomly a prime number p that is larger than d.

Step 2. Select (k-1) integer values c1,c2….c_{k-1} within the range of 0 to p-1 .

Step 3. Select n distinct real values x1,x2….xn.

Step 4. Use the following (k-1)-degree polynomial to compute n function values ,F(xi) called *partial shares for i=1,2…n.*

$F(x_i)=(d+c_1x_i+c2x_i^2….+c_{k-1}x_i^{k-1})$ mod p

Step 5. Deliver the two-tuple (xi,F(xi))as a *share to the ith* participant where i=1,2…n.

Authentication Phase

Authentication is an important mechanism to provide security to the system. Secret sharing is an efficient technique used for secured authentication. For authentication it requires both the shares. At the time of authentication voter will produce his share and authority will produce his share both the shares are necessary to reconstruct the original secret. Using authentication only valid voters will be capable to cast the vote.

Algorithm for reconstruction

Input: k shares collected from the n participants and the prime number p .

Output: secret d hidden in the shares.

Step1. Use k shares (x1,F(x1)),(x2,F(x2))……$(x_k,F(x_k))$

To form

$F(x_i)=(d+c_1x_i+c2x_i^2….+c_{k-1}x_i^{k-1})$ mod p

where i=1,2….k.

Step 2. Solve the k equations above by Lagrange's interpolation to obtain as follows

$d=(-1)^{k-1}[F(x_1)*(x_2x_3…..x_k)/((x_1-x_2)(x_1-x_3)….(x_1-x_k))+F(x_2)*(x_1x_3…..x_k)/((x_2-x_1)(x_2-x_3)…..(x_2-x_3))…….+F(x_k)*(x_1x_2….x_{k-1})/((x_k-x_1)(x_k-x_2)….(x_k-x_{k-1}))]$ mod p

Here d is the original secret password. Voter can cast vote only if the recovered Password match with the original secret.

4. CONCLUSION

Online voting offers many advantages like increased number of voter and low cost of establishing the election process. Along with these advantages system must provide the security. In this paper we describe the design and implementation of an internet based voting system. The proposed system provides a efficient way to improve security in online voting system. As the security is an important issue in election process the proposed system provides the stronger security through the authentication.

Proposed scheme uses Shamir's (2,2) secret sharing algorithm for the authentication.

ACKNOWLEDGMENTS

Our thanks to the experts who have contributed in the area of secret sharing.

REFERENCES

[1] Adi Shamir, 1979 How to Share a Secret, in Communications of ACM, Vol.22, no.11, pp. 612-613.

[2] Prabir Kr. Naskar, Ayan Chaudhuri, Debarati Basu, and Atal Chaudhuri. 2011 A Novel Image Secret Sharing Scheme,IEEE Transaction on Second International Conference on Emerging Applications of Information Technology, Pp. 177-180.

[3] Yi-Hui Chen, Ci-Wei Lan, 2012 A self-authentication mechanism for a (3, 3)-threshold secret sharing scheme, in IEEE transaction on 9th International Conference on Ubiquitous Intelligence and Computing and 9th International Conference on Autonomic and Trusted Computing pp. 1006-1008.

[4] P.V.Chavan, Dr. M. atique 2011 An intelligent system with secured authentication using hierarchical visual cryptography-review, ACEEE International Journal on Network Security , Vol. 02, No. 04.

[5] Che-Wei Lee and Wen-Hsiang Tsai, 2012 A Secret-Sharing-Based Method for Authentication of Grayscale Document Images via the Use of the PNG Image With a Data Repair Capability, in proceeding of IEEE Transactions On Image Processing, vol. 21, no. 1,pp. 207-218.

[6] Mundalik Vijay, Sable Suvarna, Khandave Dipali and S. K. Patil, 2013 Face Based Online Voting System Using Stegenography, in proceeding of vol. 3 Issue 10.pp.462-466.

[7] Chetana Hegde, Manu S, P Deepa Shenoy, Venugopal K R, L M Patnaik, 2008 Secure Authentication using Imge Processing and Visual Cryptography for Banking Application proceeding of IEEE transaction on ADCOM,pp. 65-72.

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

[9] R. Cramer, R. Gennaro and B. Schoenmakers, 1997 A Secure and optimally Efficient Multi- Authority Election scheme in EUROCRYPT 97, LNCS 1233,Springer-verlag,pp.103-118.

[10] J. Benaloh and D. Tuintra, 1994 Receipt-free Secret Ballot Elections, in 26th Annual ACM Symposium on Theory of Computing. ACM,Pp.544-553.

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