International Journal of Computer Applications (0975 - 8887)
Volume 122 - No. 5, July 2015

Security of E-Voting System in Case of Malicious Users

Richa Sarma
Department of Information Technology
North Eastern Hill University
Shillong, India

Bubu Bhuyan
Department of Information Technology
North Eastern Hill University
Shillong, India

ABSTRACT

In a democratic country, voting is one of the most important activity. In many democracies over the years, there has been decrease in the number of voters coming for election because of the inconvenient voting system. An electronic voting scheme allows voters to vote securely from distance through internet by interacting with a set of authorities. However there is always a chance that an adversary can corrupt the users and jeopardize the voting system. In this paper, we have proposed an E-voting protocol that ensures the three most important requirements of E-voting system i.e privacy, verifiability and fairness even in case when some of the users are malicious.

Keywords

Anonymous channel, E-voting, Pseudo random generator, RSA blind signature, Secret Sharing

1. INTRODUCTION

Electronic voting refers to an election process whereby people can cast their votes over the Internet, through a web browser, with comfort from their home, or office or possibly any other location where they can get Internet access. Electronic voting is attractive due to its convenience. Though it provides convenience to the voter to vote from anywhere, the background of the voting system is complex involving many processes including voter registration,voter authentication,voting,counting,result declaration. In most of the E-voting protocols[2][3], a particular process like registration, validation, tallying is handled by a single user assigned for that particular process. Corruption of such user in any part of the system leads to an inappropriate election system affecting some of necessary requirements of an E-voting system and reduce public participation.
In the proposed protocol each procedure is controlled by multiple users and secret information cannot be revealed without the co-operation of all the assigned participants. Therefore, any attempt to undermine the procedure will require the corruption of a large number of participants. In this paper we have proposed an E-voting protocol which achieves the following three important requirements of an E-voting system even in case when some of the users are corrupted.

Privacy: No participant other than a voter should be able to determine the value of the vote cast by that voter[4]

Verifiability: It can be categorized as:

(1) *Individual Verifiability*: The ability of the voter to verify if his vote is properly received[5] and counted[6].
(2) *Universal Verifiability*: Anyone can verify that the protocol is correctly processed and tallied all valid votes.[8]

Fairness: No participant can gain any knowledge, except his vote, about the (partial) tally before the counting stage (The knowledge of the partial tally could affect the intentions of the voters who has not yet voted).[6]

Section II describes the preliminaries about the various cryptograhphic primitives used in the proposed E-voting scheme. Section III describes the proposed E-voting protocol followed by Analysis in section IV.

2. PRELIMINARIES

In this section, we state the related preliminaries about secret sharing, RSA blind signature and pseudo random number generator which has been adapted in our scheme.

2.1 Blind Signature based on RSA

In cryptography, a blind signature, as introduced by David Chaum[1], is a form of digital signature which allows a signer to sign a document without knowing the content of the document. The security of this technique is achieved if the signers do not know the content of the message to be signed.
Moreover the signers should not know the signature message pair or for whom he signed that message. It is the most popular cryptographic technique used in E-voting to provide privacy of the vote. The signature is used to authenticate the voter without disclosing the content of a ballot. The blind signature scheme based on RSA works as follows:

Let (n, e) be the signer's public key and d be his private key. The sender of the message generates a random number r such that $gcd(r, n) = 1$ and sends the following to the signer.

$B' = r^e B mod n$, where B' is the blind message

The signer signs the blind message B'.

$S' = B'^d mod n$, where S' is the signature on the blind message B'

The sender receives S' and unblinds it to obtain signature S on original message B as:
$S = S'r^{-1}modn = B^dmodn$

2.2 Secret Sharing

A secret sharing mechanism was proposed by A.Shamir[7]. The main idea of this mechanism is sharing a secret S among n users, such that any set of at least t users can recover S. We find this technology extremely suitable to construct the "separation of duties"concept; it is the key in achieving trustworthy voting. Shamir's threshold scheme is based on polynomial interpolation, and the polynomial $y = f(x)$ of degree $t-1$ is uniquely defined by t points (X_i, Y_i) with distinct X_i. A trusted party T distributes shares of a secret integer S to n users. Any t users which contribute their shares can recover S. The set-up phase is described as follows:

(1) T Chooses a prime $P > max(S, n)$, and define $a_0 = S$.

(2) T chooses $t-1$ random coefficients $a_1, a_2, ...a_{t-1}$ from a uniform distribution over the integers in $[0, P)$, defining the random polynomial over Z_p , $f(x) = \sum_{j=0}^{t-1} a_j x^j$

(3) T computes $S_i = f(i)modp$, $1 \leq i \leq n$, and securely transfers the share S_i to user P_i

Any group of t or more users contribute their shares. Their shares provide t distinct points $(x, y) = (i, S_i)$, allowing computation of the coefficients a_j , $1 \leq j \leq t-1$ of $f(x)$ by Lagrange's interpolation. The secret is recovered by noting $f(0) = a_0 = S$, the shared secret can be expressed as:

$S = \sum_{i=1}^{t} c_i y_i$
where, $c_i = \prod_{1 \leq j \leq t, j \neq i} \frac{x_j}{x_j - x_i}$

2.3 Pseudo-random generator

Pseudo-random generator (PRNG) is a cryptographic algorithm used to generate numbers that appears random known as pseudo-random number. Linear congruential generator is a type of pseudo-random generator based on a linear recurrence .Linear congruential method was first introduced by D.H. Lehmer. It is used in the proposed protocol to generate ballot id. The Validators generate a particular size of pseudo random numbers which repeat itself in some interval and all the pseudo random numbers are concatenated to form unique ballot id of the voter .We will describe the linear congruential generator[11] in brief:

We choose four numbers,
m, the modulus; $m > 0$
a, the multiplier; $0 \leq a < m$
c, the increment; $0 \leq c < m$
X_0, the starting value or seed; $0 \leq X_0 < m$
The desired sequence of random numbers (X_n) is then obtained by setting
$X_n = (aX_{(n-1)} + c)modm, n \geq 0$
This is called pseudo random number sequence or linear congruential sequence.

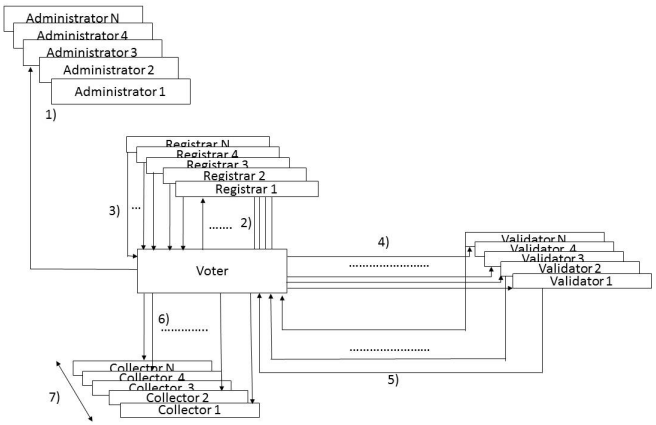

Fig. 1. The structure of proposed scheme

3. PROPOSED E-VOTING SCHEME

In this section, we describe the overall architecture of the proposed E-voting system (Fig 1).

3.1 General Description

The structure of the proposed scheme is illustrated in figure 1. The users involved in the proposed scheme are as under:

Authorities: Authorities manage the whole voting system. In our protocol, a set of equal number of authorities say N number of authorities where $N > 1$ handle each of the process required for proper functioning of the system. It includes:

(1) *Administrator*: Administrators of E-Voting system are involved in physical verification of the voter's credentials, setting the dates of registration,voting and counting .The voters once during their lifetime have to meet the administrators to verify their credentials. Once verified, the eligible person will be kept in national registration database and can vote from anywhere for all the election prevailing during his lifetime.

(2) *Registrar*: For every election, N number of registrars $(R_1, R_2, ..., R_N)$ are involved who individually verify the voters by checking their eligibility from national registration database and only the registered voter are provided the login ID and password.

(3) *Validator*: A validator is responsible to validate the ballot sent by voters during voting.N number of validators $(V_1, V_2, ...V_N)$ individually validate the ballot and produce the ballot id.

(4) *Collector*: A collector collects the validated vote during voting and counts after the voting period is over. We have N number of collectors $(C_1, C_2, ..., C_N)$ for checking the validity of the vote, collecting it and counting it.

Voter : Voter is a person who has the right to vote.

The interactions between the concerned parties shown in Fig.1 can be sufficed as follows:

(1) *Voter* $\rightarrow$ *Administrators*: Once in a lifetime every person has to physically visit the administrators to register themselves as eligible voter.

(2) *Voter* $\rightarrow$ *Registrars*: Before any election, all the voters should en-roll themselves to registrars to be eligible to vote in that particular election.
(3) *Registrars* $\rightarrow$ *Voter*: Only voters who are found eligible are provided login ID and password through email by the registrars.
(4) *Voter* $\rightarrow$ *Validators*: Eligible voter votes, splits his vote, blinds them and sends those to the validators to be validated.
(5) *Validators* $\rightarrow$ *Voter*: Validators sign on the message received from the voter and send back the message and signature to him.
(6) *Voter* $\rightarrow$ *Collectors*: Voter sends the original splits of vote and signature on it to the collectors.
(7) $Collectors_{i=1,2,...N} \rightarrow Collectors_{j=1,2,...N}$, where $i \neq j$: All the collectors collect the splits of vote from each other and count the votes.

3.2 Election stages

There are three stages in the proposed E-voting protocol i.e Voter Registration, Voting and Counting. The following sections describe the proposed protocol and events in each of the stages.

3.2.1 Voter Registration

(1) A voter has to physically visit to the registration office and register himself once in his lifetime .The administrators check his credentials and if eligible put the person in the list of eligible voters in the National Registration Database.
(2) To vote in any election a voter has to again register himself but he need not visit the registration office this time. He has to send his credentials (Name, Voter ID no. , registered email ID) through network to the registrars. The registrars check the user's particulars with the national registration database to determine the eligibility of a voter and if eligible each of them generate a part of password which is concatenated to make a complete password and sent along with the login Id (where the login Id will be the Voter ID number) to the registered email id of the voter. Therefore, the registrar cannot impersonate as voter because it doesn't possess complete knowledge of password required for successful login.

3.2.2 Voting. In voting stage, a voter must send his ballot to both validator and collector. The process of voting is described below:

(1) On the voting day ,the voter encrypts his login ID and password and sends to the validators where each of the validators obtain only some part of password to check and match with National Registration database. The validators also check whether he has voted earlier. If the voter is valid, he is provided a ballot to vote.
(2) On obtaining the ballot the voter does the following:
    (a) The voter casts his ballot and splits his vote into N parts using Shamir's secret sharing scheme.
    (b) Each N splits of the vote are then blinded using each of the N number of validator's public key respectively and choosing a random number.
    (c) The voter encrypts N blinded parts of vote and sends them to the N validators respectively to be validated.
(3) Each of the validators sign the blind message sent by the voter individually and generate a fixed sized pseudo random number (which on concatenation forms a complete Ballot id) and signs it. The blindly signed message along with the Ballot ID and signature are encrypted and sent to the voter. The Ballot id generated will be unique for each voter.
(4) The voter unblinds the N splits of vote , verifies the signature on it and on the parts of Ballot id ,encrypts them and then sends the N validated splits of vote along with id through anonymous channels to the collectors $(C_1, C_2, ...C_N)$ respectively.
(5) The collectors decrypt the message, verify the signature of the validators. If found valid, the vote is considered.

3.2.3 Counting. On the counting day all the N collectors $(C_1, C_2, ...C_N)$ co-operate to reveal the votes by exchanging the splits of votes among themselves received during the voting phase and counting of votes is initiated. The result is published through the bulletin board.

4. ANALYSIS

In this section, we prove that the proposed scheme achieves the necessary requirements of E-voting mentioned in section I.

4.1 Privacy

In the proposed protocol to achieve privacy blind signature based on RSA is used, but sometimes despite using blind signature techniques when one of the authority is malicious privacy gets broken. So, in the proposed protocol to achieve more security the voter's unique Ballot-id (which is later published on the bulletin board along with his vote) is generated by N validators instead of a single validator and each of them contribute to generate a unique Ballot-id i.e none of the validators have the complete knowledge of the voter's unique Ballot-id..In this scenario if at-least one of N validator's is not malicious then the complete knowledge of the voter's unique Ballot-id cannot be achieved to link it with the vote. Hence privacy is achieved.

4.2 Verifiability

4.2.1 Individual verifiability. After the counting phase, the voter's unique Ballot-id along with his vote is published in the bulletin board to verify that the vote has been received correctly. Moreover as in the counting stage, all the collectors collaborate to count, it is not possible that vote is listed correctly but is not counted. Hence individual verifiability is achieved.

4.2.2 Universal verifiability. In the proposed protocol, the voter's Ballot-id, splits of vote with the signature of the validators and the complete vote is published through the bulletin board. In some of the protocols[2] [3], if the voter abstains after the registration phase then the authority adds false votes. Moreover, in some cases if the process is handled by a single malicious authority then an ineligible person may vote or multiple votes are cast by a single person but this is not possible in the proposed protocol because the entire process is supervised by a number of authorities and if at-least one of them is honest then universal verifiability is achieved.

4.3 Fairness

Some of the schemes[9][10] do not ensure that the voting system is fair i.e the intermediate results are leaked. In the proposed scheme, the knowledge about the partial tally cannot be achieved because the vote is distributed among N collectors using Shamir's secret sharing scheme. None of the collectors individually can gain the knowledge of tally before the counting day because all the N collectors have to collaborate to generate the vote. Hence fairness is achieved.

5. IMPLEMENTATION

In order to implement the proposed Electronic Voting System we have used Java and Netbeans 8.0.1 is used as our editor for writing codes. Other softwares used are MySql for creating Databases and Apache Tomcat for creating server. Some third party java packages like Mysql Connector.jar necessary for connecting the system with the mysql database and servlet-api.jar necessary for creating servlets are also included in the development of the system. The encryption algorithm used in this system is RSA 2048 bits encryption system. This encryption and decryption algorithm is included in the java package javax.crypto.cipher. The client program creates a public key and private key for every voter that requests the client program. Java provides a class for creating the key pairs in the package java.security. We use the MD5 algorithm for hashing the partial password. This algorithm is called from the package java.security.message digest. As E-voting system is based on client server model,the server programs represent the server entities Registrars, Validators and Collectors. For storing different informations like the voter information, voting and results quite a large number of databases named as nric db, registrardb, validatordb, collectordb, resultdb had to be created.

No. of messages exchanged during each of the stages of the proposed E-voting system:

—**Voter Registration**
No. of messages sent from voter to N registrars = N
No. of messages sent from N registrars to voter= N
No. of messages sent from N registrars to N validators (details of registered voter) = N
Hence, no. of messages exchanged =N+N+N=3N

—**Voting**
No. of messages sent from voter to N validator during login = N
No. of messages sent as reply to login to voter by N validator=N
No. of messages sent from voter to N validator during voting=N
No. of messages sent from N validator to the voter=N
No. of messages sent from voter to N collector=N
Hence, no. of messages exchanged=N+N+N+N+N=5N

—**Counting**
No. of messages sent from 1 collector to N-1 collector=N-1
Therefore, no. of messages sent from N collector to N-1 collector=$N(N-1) = N^2 - N$
Hence no. of messages exchanged =$N^2 - N$

Phase	No. of messages exchanged
Registration phase	3N
Voting phase	5N
Counting phase	$N^2 - N$

6. CONCLUSIONS

In this paper, we have proposed an E-voting system that uses Blind signature based on RSA, Pseudo-random generator and Shamir's secret sharing scheme as security tools. Through the concept of distribution of trust and using these security tools the protocol irrespective of some of the malicious users achieves the requirements of privacy, fairness and verifiability required in an E-voting system.

7. REFERENCES

[1] D.Chaum, "Blind Signature for Untraceable Payments", Crypto'82, Springer-Verlag, $pp.199 - 203, 1983$.

[2] A.Fujioka ,T. Okamoto,K. Ohta , "A practical secret voting scheme for large scale elections", Advanced in Cryptology - AUSCRYPT'92, 1992.

[3] Michael J .Radwin "An untraceable, universally verifiable voting scheme". Seminar in Cryptology (1995)

[4] Josh Daniel Cohen Benaloh and Dwight Tuinstra, "Receipt-free secret-ballot elections". In STOC'94: Proceedings of the twenty-sixth annual ACM symposium on Theory of computing, pages $544 - 553$, New York, USA, 1994.ACM.

[5] Kazue Sako and Joe Kilian , "Receipt-Free Mix-Type Voting Scheme: A Practical Solution to the Implementation of a Voting Booth", EUROCRYPT'95, vol 921, Lecture Notes in Computer Science, pp. 393-403, Springer-Verlag, 1995.

[6] Zuzana Rjaskova, "Electronic Voting Schemes". PhD thesis, Comenius University, Bratislava, 2002.

[7] Adi Shamir, "How to share a secret Communication", ACM, $22(11) : 612 - 613, 1979$.

[8] Stefan Weber, "A coercion-resistant cryptographic voting protocol- evaluation and prototype implementation". Master's thesis, Darmstadt University of Technology, 2006

[9] W.S.Juang and C.L.Lei,"A Collision- Free Secret Ballot Protocol for Computerized General Elections", Computers and Security,4,$339 - 348(1996)$.

[10] H.Nurmi,A.Salomaa, and L.Santean,"Secret Ballot Elections in Computer Networks", Computer and Security,6, $553 - 560(1991)$

[11] Donald E. Knuth, "Semi-numerical Algorithms", volume 2 of The Art of Computer Programming. Addison-Wesley, 1969, Second edition, 1981.