Global Journal of Computer Science and Technology
Network, Web & Security
Volume 13 Issue 13 Version 1.0 Year 2013
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Proposed Secured Remote E-Voting Model based on Blind Signature

By Reham Mohamed Kouta, Dr. Essam-Eldean F. Elfakharany
& Dr. Wafaa Boghdady Mohamed

AAST University, Egypt

Abstract - We proposed a secured e-voting system model by using blind signature. Our proposed model meets all security requirements which are: (authentication, privacy, integrity, non repetition). Our proposed model depends on these main entities that are involved within the voting processes (voter registration, voting, counting, audit), and these entities are: certificate authority, ministry of interior, voter, high committee of elections (investigator), and counter. The voter can vote from any remote with secured data transfer (ballot) by using the blind signature to blinded ballot and then sign it. When it is sent to the high committee of elections (investigator) for checking the voter eligibility, there is an encrypting random value (r) that is attached with the blind ballot, using for removing blind the ballot which is encrypted by counter's public key. The high committee of elections checks the signature of voter and checks that if he is an eligible voter or not. Then removes the voter's digital signature and puts his digital signature and then sends it to the counter party. The counter party checks the signature of high committee of election and extracts the random value (r) by decrypting with his private key and removing the blind ballot and counts the vote.

Keywords : *secured e-voting system, blind ballot, certificate authority, ministry of interior.*

GJCST-E Classification : *D.4.6*

PROPOSED SECURED REMOTE E-VOTING MODEL BASED ON BLIND SIGNATURE

Strictly as per the compliance and regulations of:

Proposed Secured Remote E-Voting Model based on Blind Signature

Reham Mohamed Kouta $^{\alpha}$, Dr. Essam-Eldean F. Elfakharany $^{\sigma}$ & Dr. Wafaa Boghdady Mohamed $^{\rho}$

Abstract - We proposed a secured e-voting system model by using blind signature. Our proposed model meets all security requirements which are: (authentication, privacy, integrity, non repetition). Our proposed model depends on these main entities that are involved within the voting processes (voter registration, voting, counting, audit), and these entities are: certificate authority, ministry of interior, voter, high committee of elections (investigator), and counter. The voter can vote from any remote with secured data transfer (ballot) by using the blind signature to blinded ballot and then sign it. When it is sent to the high committee of elections (investigator) for checking the voter eligibility, there is an encrypting random value (r) that is attached with the blind ballot, using for removing blind the ballot which is encrypted by counter's public key. The high committee of elections checks the signature of voter and checks that if he is an eligible voter or not. Then removes the voter's digital signature and puts his digital signature and then sends it to the counter party. The counter party checks the signature of high committee of election and extracts the random value (r) by decrypting with his private key and removing the blind ballot and counts the vote.

Keywords : secured e-voting system, blind ballot, certificate authority, ministry of interior.

I. Introduction

Election is a fundamental instrument of democracy that provides an official mechanism for people to express their views to the government. Traditionally, the process of voting is quite complicated because voter must come in person to vote.

This problem resulting low participation rate at elections. Electronic voting system can overcome those problems in a national election, by enabling the voter to vote from his home or office or from any remote place.

Although remote electronic voting is more flexible and easier for voters than the traditional voting, but it also more vulnerable than the traditional voting due to the nature of digital processing of election data which can be easily spread, manipulated within the network, hence that may result in widespread fraud and corruption [1, 2].

For these reasons, we will propose a prototype of the remote electronic voting in this research, which may meet the security requirements of voting process [3, 4], and can reduce human errors that occurred in the traditional voting process and also reduce the fraud of voting with making the process of voting easier and more reachable for the voters (citizens)?

II. Preliminaries

Let E= {V, VA, T, CA, MOI} be the set of entities involved where V voter, VA investigator, T counter, CA certificate authority and MOI ministry of interior. Let X ϵ E, X is represented as follows. X= (PK[x], SK[$_x$], n_x), PK[x] is the public key of Entity X, SK[$_x$] is the private key of X, and n_x is the RSA constant. Recall that pub_x and $priv_x$ are multiplicative inverses to each other mod Φ (n_x), where Φ (.) is the Euler totient function. We assume $priv_x$ ϵ {MAX (p_x,q_x), Φ (n_x)-1} is a large prime for two large primes p_x, q_x, and $n_x = p_x * q_x$. We also assume for message M the following holds:

$$(M^{PK[x]}) \bmod n_x)^{SK[x]}) \bmod n_x =$$
$$(M)^{SK[x]} \bmod n_x)^{PK[x]}) \bmod n_x = M.$$

We also assume for X ϵ E, X does not knows $priv_y$ of Y ϵ E, Y ≠ X but knows the rest of Y parameters and DC_x denotes the digital certificate of X ϵ E. Thus we can represent the entities involved as follows:

1. V= (PK $[_{Vo}]$, SK $[_{vo}]$, n_v).
2. VA= (PK $[_{VA}]$, SK $[_{vA}]$, n_{VA}).
3. T= (PK $[_{TA}]$, SK $[_{TA}]$, n_{TA}).

For two entities X, Y ϵ E, Y ≠ X, a message m from X to Y is sent over a secured channel that follows the secured socket protocol as follows:

X signs on m, generating encrypt $_{privx}$(H(m)) where H is a hashing one way function, X generates a session key SK, X generates the encrypted message encrypt $_{SK}$ (m ||encrypt $_{privx}$(H(m))|| DC_x), X generates the digital envelop encrypt $_{puby}$(SK) to achieve privacy, and finally X sends both the encrypted message and the digital envelop to Y. Y opens the envelop as follows: SK= decrypt $_{privy}$ (encrypt $_{puby}$(SK)), Y gets m ||encrypt $_{privx}$(H(m))|| DC_x =decrypt$_{SK}$ encrypt $_{SK}$(m ||encrypt $_{privx}$(H(m))|| DC_x), Y verifies H(m) = decrypt$_{pubx}$(encrypt $_{privx}$(H(m)) achieving authenticity, non repudiation, and message integrity [5].

III. The Proposed Protocol

The procedures and steps that occurred at any elections must be divided into three stages:

1. The pre-voting stage (preparation).

Authors α σ ρ : Arab Academy for Science.
E-mails : mmkouta@gmail.com, essam.fakharany@gmail.com, wafae.boghdady@gmail.com

2. The voting stage (the casting of the votes).
3. The post-voting stage (counting, auditing).

1. The pre-voting stage: this phase includes all preparations that occur before the period of elections. At proposed model, this stage includes these 2 steps:
   a. Voter registration.
   b. Ballot preparations.
2. The voting stage: this phase includes all the chain of steps that occurred within the period of elections until the voter casting his vote and send it. At proposed model, these stage includes 3 steps:
   a. Voter getting ballot.
   b. Blind ballot.
   c. Validating & signing blind ballot.
3. The post-voting stage: this phase includes all the chain of steps that occurred after the period of elections ended, which include all these steps:
   a. Unblind ballot.
   b. Counting the unblind ballots.
   c. Auditing.

a) Pre-voting Stage

i. *Voter Registration*

An individual must register to be an eligible voter. This is done before the voting period. Voter registration for E-Voting is done as follows:

1. The individual generates key pair in smart card. And then generates certificate request during the generation of certificate request. The system asks for his information like name, ID address, and e-mail, etc.
2. The individual sends his certificate request to CA to issue digital certificate.
3. The CA inquires the information of voter from MOI to check if the individual are eligible or not. If eligible, the CA issues digital certificate and sends it to voter's email.
4. The voter downloads his digital certificate from his email and imports to his smart card.
5. The voter downloads ballot from the organized election website. The ballot contains unique ID to prevent multiple casts.

ii. *Ballot Preparations*

1. At this stage, the high committee of elections (investigator) starts to generate ballots with different and unique IDS which include list of candidates' names.
2. High committee of elections will send the numbers of the ballots' IDS that are generated to the counter as a list of the ballots ready for casting votes, making this for purpose if the counter received any ballot, the ID number will not be included at this list; that means that the ballot is invalid.
3. High committee of elections (investigator) will sign each ballot of these ballots using their secret key, so the voter must get the ballot **(B)** signed, which can be represented into this equation:

$$B^{SK\,[VA]} \bmod (n_{va})$$

4. High committee of elections will upload these signed ballots into the official website of the elections as a preparation step for voters to cast their votes.

b) Voting Phase

i. *Voter Getting the Ballot*

1. Voter will download the ballot from the high committee of elections (investigator) website and it must be signed also.
2. Voter will unsign this ballot using the high committee of election's public key, and then will cast his vote into the ballot.

ii. *Blind Vote*

1. The voter casts his ballot and then blind ballot as Fig (1) by generating a random value (r), such that *r* is relatively prime to *N* (i.e. *gcd(r, N)* = 1). The value *r* is raised to the public exponent *e* modulo *N,* and the resulting value r^emodN is used as a blinding factor [6].
2. Voter will encrypt these random no. (r) in two different ways:
   a. Voter will encrypt these random no. (r) using the investigator's public key, which will be the blind factor(**BF**), so the blind factor can be represented into this equation:

$$BF = (r^{PK\,[va]} \bmod (n_{va})).$$

   b. Voter will encrypt this random no. (r) using the counter's public key, which will be used in the unblind factor (**UBF**), so the unblind factor can be represented into this equation:

$$UBF = (r^{PK\,[TA]} \bmod (n_{TA})).$$

3. Voter will blind his ballot using the blind factor by multiplying his ballot with the blind factor, so the blind ballot (BB) can be represented into this equation:

$$BB = B{*}\ BF$$

4. Voter will attach the blind ballot (BB) with the unblind factor (UBF), so that will result into B'' which can be represented into this equation B'' = (BB || UBF), so

$$B'' = (BB\ ||\ UBF)$$

5. Voter will sign this B'' using his secret key, so that will be resulted into the signed B'' (SB''), which can

be represented into this equation $SB'' = (B'')^{Sk[vo]}\text{mod}(n_{vo})$.

iii. *Validating & Signed Ballot*

1. The voter sends the SB'' to the high committee of elections (investigator) for authenticating the voter and checking the voter's signature eligibility and also to check if the voter voted before or not.
2. Investigator will verify the voter's signature as Fig (2) by using his public key:

$$SB'' = ((B)*(r^{pk[va]}\,\text{mod}\,(n_{va})), (r^{PK[TA]}\,\text{mod}\,(n_{TA})))^{SK[vo]}\cancel{\text{mod}(n_{vo}})\,)^{PK[vo]}\text{mod}(n_{vo}\cancel{).,}\text{ which will resulted}$$

$$\mathbf{B'' = (BB \,||\, UBF)}$$

a. Investigator after verifying the voter signature and checking this, the first time for voter to vote will sign this B'' using his secret key; that will result into the investigator signing B'' (VSB''), and can be represented into this equation:

$$\mathbf{VSB'' = (B'')^{SK\,[va]}\,MOD\,(n_{va})}$$

While the investigator using this secret key to sign the ballot, this secret key will decrypt the random no. that encrypted by the investigator public key (BF) which will be resulted.

$$\mathbf{VSB''= ((B)^{SK\,[va]}\,MOD\,(n_{va}) * (r)) \,||\, (UBF)^{SK\,[va]}\,MOD\,(n_{va})}$$

b. Then investigator will send the VSB'' to the counter party.

c) Post-voting Stage

i. *Unblind Votes*

I. Counter will receive ballots from the investigator (VSB'') then do this process as in Fig (3) into each VSB'':

a. Counter will insert each VSB'' into a separator function, to get:

1. The unblind factor but signed from investigator (VSUF).

$$\text{VSUF} = \text{UBF}^{SK\,[VA]}, \mathbf{SO}$$

$$\mathbf{VSUF = (r^{PK[TA]})^{SK[VA]}}$$

2. The Investigator signed ballot (VSBB).

$$\mathbf{VSBB = r * (B)^{SK\,[VA]}}$$

Note the random no. (r) No longer encrypted by the investigator public key, because this encryption is removed while the investigator signing the blind ballot using his secret key.

b. Counter will verify the signature of investigator on the blind factor, which will be resulted into the unblind factor:

$$\mathbf{(UBF) = (r^{PK[TA]}\,mod\,(n_{TA}))}$$

c. Counter will decrypt the random no. using his secret key :

$$(r^{PK[TA]}\,\cancel{\text{mod}\,(}n_{TA})^{SK[TA]}\cancel{\text{mod}(n_{TA}}) = (R)$$

So will get the random no. (r)

d. Counter will use the random no. to unblind the vote by multiplying the blind ballot through the random no. versus:

$(r * B^{SK\,[va]}\,\text{mod}(n_{va}) * 1/r$, which will be resulted into the ballot unblind and signed from investigator:

$$\mathbf{Vote = B^{SK\,[va]}\,mod\,(n_{va})}$$

ii. *Counting the Unblind Ballots*

1. Counter after unblinding the vote will count it according to the voter selection.
2. Counter will declare the result about the candidates that take the highest number of ballots counted.

iii. *Audit*

1. It's the phase of auditing and reviewing the counting phase. This phase occurred especially in the case of when any one of the candidates appealed about the counted number of the votes that he have gotten, after declaring the result of elections.
2. Audit phase occurred under the supervision of high committee of elections (investigator) which will compare the number of ballots that is generated by them and the numbers of the ballots IDS received by the counter (check the ID number of each valid ballot that is counted by counter).
3. High committee of elections also checks the ballots that are counted as invalid. Ballots must apply one of 3 conditions:

a. Ballot no. ID shall not identical to the serial ID numbers of ballots that are generated by the investigator; that is these ballots are not coming from the investigator, but that is considered as fraud by any hacker.

b. Ballot received by the counter is not signed from the high committee of elections (investigator), which means that ballot was attached by attacker.

c. Ballot received by the counter is not blind (unblind) which means also these ballots are hacked by hacker. If one of these 3 cases is applied, the ballot counted as an unvalid vote.

4. The audit phase at our proposed model depends on the ballot's IDS. At this phase, the declaration of results is not only about the number of votes that each candidate got, but also about the IDS numbers of ballots that each candidate has taken; that will make the candidate check a random sample of his supporters (voters), in order to know their ballot's IDs via checking their ballots counted for each candidate.

IV. Tables and Figures

The bellow tables contain the abbreviations used in the paper. The table (1) contains the abbreviations of key pairs of entities used in the proposed model and table (2) contains the abbreviations of data items used in the proposed model.

Table 1 : key pairs of entities in our proposed model

Sk[va]	Investigator (high committee of elections) secret key
Pk[va]	Investigator (high committee of elections) public key
Sk[vo]	Voter's secret key
Pk[vo]	Voter's public key
Sk[ta]	Counter's secret key
Pk[ta]	Counter's public key

Table 2 : Main data items at our proposed model

R.	Random no. generated by voter application
B	Ballot
BF	Blind factor, which is (random no.) encrypted by investigator public key PK[VA]
UBF	Unblind factor, which is (random no.) encrypted by counter public key PK[TA]
BB	Blind ballot, which the ballot multiplies
	by random no., and this no. encrypted by investigator public key PK[VA]
B''	Blind ballot concatenate the unblind factor (BB ||UBF)
SB''	B'' signed by voter secret key
VSB''	B'' signed by investigator secret key
VSUF	unBlind factor that is signed by the investigator, using investigator secret key SK[VA]
VSBB	Blind ballot that signed from the investigator, using investigator secret key SK[VA]
Vote	Ballot signed from investigator (unblind)

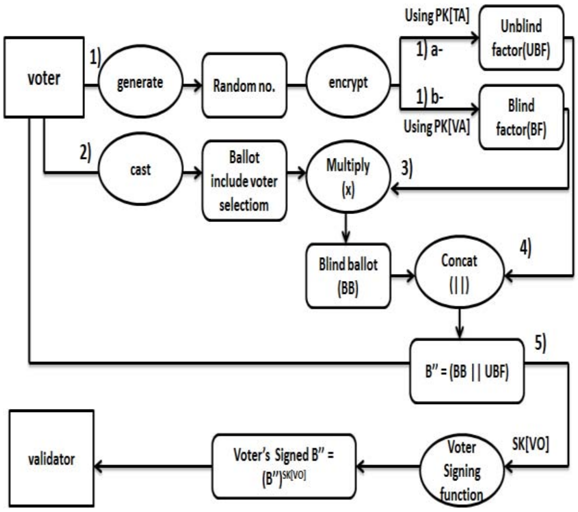

Figure 1 : Blind Phase

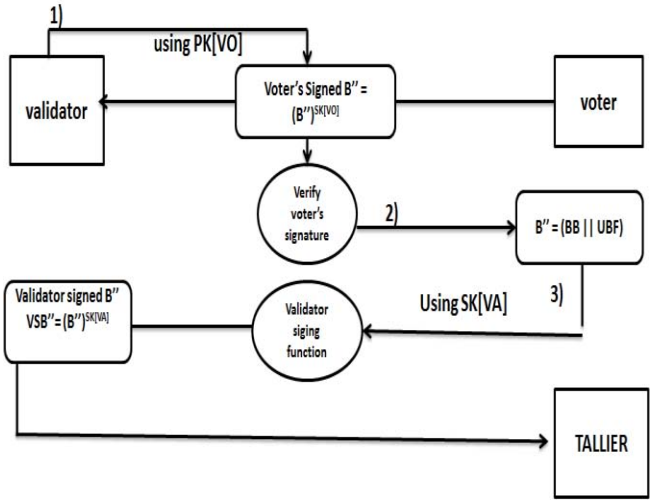
1)
using PK[VO]
validator
Voter's Signed B'' = $(B'')^{SK[VO]}$
voter
Verify voter's signature
2)
B'' = (BB || UBF)
Validator signed B'' VSB''= $(B'')^{SK[VA]}$
Validator siging function
Using SK[VA]
3)
TALLIER

Figure 2 : Validating Phase

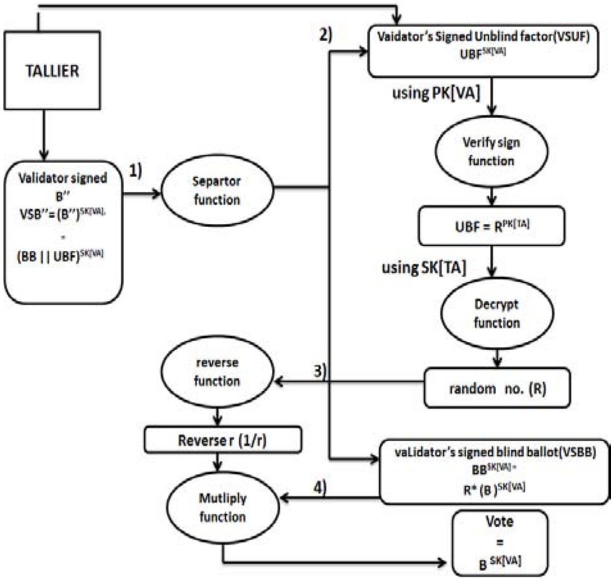
TALLIER
2)
Vaidator's Signed Unblind factor(VSUF) $UBF^{SK[VA]}$
using PK[VA]
Verify sign function
Validator signed B'' VSB''= $(B'')^{SK[VA]}$ = $(BB || UBF)^{SK[VA]}$
1)
Separtor function
UBF = $R^{PK[TA]}$
using SK[TA]
Decrypt function
reverse function
3)
random no. (R)
Reverse r (1/r)
vaLidator's signed blind ballot(VSBB) $BB^{SK[VA]}$ = $R^* (B)^{SK[VA]}$
4)
Mutliply function
Vote = $B^{SK[VA]}$

Figure 3 : Unblind Phase

V. Conclusion

We have proposed electronic voting system that meets security requirements and we expect the participations rate to be increased because the voters will not be pending in a long queue. With electronic voting, the voting will be faster than the traditional voting.

References Références Referencias

1. Subariah Ibrahim, Mazleena Salleh and Maznah Kamat, "Electronic Voting System: Preliminary Study," Jurnal Teknologi Maklumat, Vol. 12, pp. 31-40, 2000.
2. Subariah Ibrahim, Mazleena Salleh and Maznah Kamat, "Design of a Secure Web-Based Electronic Voting System," in Proceedings of Malaysian Science and Technology Congress, 1999.
3. R. Cramer, R. Gennaro, and B. Schoenmakers, and M. Yung, "Multi-Authority Secret-Ballot Elections with Linear Works." Eurocrypt '96, LNCS 1070, pp 72 – 83, 1996.
4. L.R. Cranor, and R.K. Cytron, "Design and Implementation of a Practical Security-Conscious Electronic Pollind System," Washington University: Computer Science Technical Report, 1996.
5. Stalling, W., Cryptography and Network Security, 3rd Edition, Prentice Hall, New Jersey, 2003.
6. Subariah Ibrahim, Maznah Kamat, Mazleena Salleh, Shah Rizan Abdul Aziz, Secure E-Voting With Blind Signature," Faculty Of Computer Science & Information Technology, University Technology Of Malaysia".
7. Robling Denning, Cryptography and Data Security, 1982.

This page is intentionally left blank