An Application of time stamped proxy blind signature in e-voting

Suryakanta Panda
Department of Computer Science
NIT, Rourkela
Odisha, India
Suryakanta.silu@gmail.com

Santosh Kumar Sahu
Department of computer science
NIT, Rourkela
Odisha, India
santoshsahu@hotmail.co.in

Jagannath Mohapatra
Department of Computer Science
SMIT, Berhampur
Jaga.info@gmail.com

Ramesh Kumar Mohapatra
Department of Computer Science
NIT, Rourkela
India
Mohaptra.rk@nitrkl.ac.in

***Abstract*—Voting is a way for a voter to make a decision or express an opinion or to choose a candidate. E-voting (Electronic Voting) refers to both the electronic means of casting a vote and the electronic means of counting and publishing that votes. The E - voting system has some specific advantages as compared to the traditional voting system. In this paper, a secure and efficient e-voting protocol is proposed which is based on the time stamped proxy blind signature.**

Keywords-Proxy Blind Signature; E-voting; DLP; Digital Signature; Blind Signature; Proxy Signature

I. INTRODUCTION

Many people are not going to vote as because voting booth is far away from their work place. The only solution to it is E-Voting. E-Voting has become increasingly popular in our technology driven world. It increases the security of the ballot, speed up the processing of results and make voting easier. Electronic voting also has the ability to reduce fraud, by eliminating the opportunity for ballot tampering. Due to mobility and convenience, the most important properties of e-voting, it is becoming more popular.

In general, two main types of e-voting can be identified

E-voting which is physically supervised by representatives of government or independent electoral authorities (e.g. Electronic voting M/C is located at polling stations).

Remote e-voting where voting is performed within the voters sole influence, and is not physically supervised by representatives of govt. Authorities (e.g. voting from one's personal computer, mobile phone).

E-voting is an election system that allows a voter to record his/her secure and secret ballot electronically. E-voting can reduce election costs and increase participation of voters by making the voting process more convenient.

II. SECURITY PROPERTIES OF E-VOTING

A secure and trusted e-voting must have the following properties:

i. Completeness

In the traditional voting scheme the voters identify is checked by seeing the voter in person. Completeness says that only authorized voters are eligible to vote.

ii. Accuracy

A vote cannot be altered or can't be eliminated from counting; Invalid vote should not be counted.

iii. Uniqueness

Voter can vote exactly one time. More than one time is avoided.

iv. Privacy

The definition of privacy states that no one can determine how an individual voter gave its vote. Voters also can't prove how they have voted; otherwise they may sell their vote.

v. Reliability

During major failures (e.g. Internet failure) the system should be robust and no loss of the vote should happen.

vi. Verifiability

This property states that each voter can verify that their vote is correctly counted.

vii. Mobility

Mobility is one of the basic important properties of e-voting. It states that voters are not physically restricted to cast their votes.

viii. Fairness

The property of fairness states that; no one can get the voting result before its publication phase.

ix. Anonymity

The definition of anonymity in e-voting states that no one can link the voted ballot to the voter who has cast that vote.

x. Convenience

It states that the voter cast their votes quickly and with minimal skills. The system should be user friendly.

xi. Robustness

The robustness property defines that no attacker or dishonest voter can disturb on interrupt the voting process.

xii. Efficiency

The property of efficiency states that the voting scheme should produce a specific result effectively within a minimum amount of time and unnecessary effort.

III. RELATED WORK

Chaum[1] the first to propose electronic voting. Most of the problems that are in traditional voting can be resolved in electronic voting can be resolved in electronic voting. But some problems are there, that are still cannot be eradicated. Out proposed scheme adopts the proxy blind signature mechanism for a secure and efficient voting.

Proxy blind signature was first introduced by Lin et al in 2000. Combining the proxy signature and blind signature; Later Tan et al [3] suggested a proxy blind signature scheme which was based on Schnorr blind signature scheme. In 2003, Lal et al [4] pointed out the security attacks in Tan et al's scheme and suggested a new proxy blind signature scheme based on mambo et al's [2] scheme. In 2008, yang et al [5] demonstrated a new scheme and proved that their scheme is efficient and secure. In 2013, panda et al [6] suggested a time stamped proxy blind signature scheme in which the verifier can know the time of the signer.

IV. PROPOSED SCHEME

In our scheme there are only four participants involved as follows:

1. Registration Authority (RA): Ra is a trusted party where all the eligible voter have to register in advance.

2. Administrator (A): Administrator monitors the whole process of the voting scheme.

3. Vote Counter (VC): VC has the responsibility to count the valid votes and publish the result.

4. Voter: Voter is someone who is eligible to give the vote.

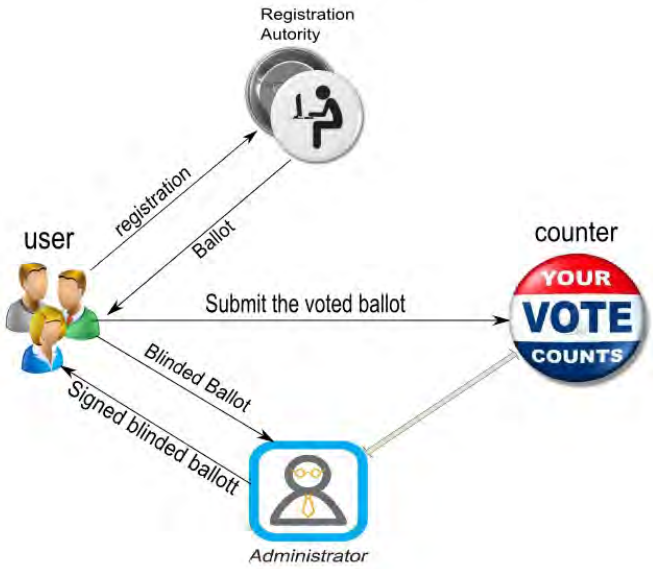
Structure of the proposed scheme

Every participants i.e. every voter registration authority, administrator, vote counter generate their public key and private key individually in advance. Everyone gets the public key of others from the certification authority (CA), by a secure authorized channel.

1. *REGISTRATION*

Voter V_i send an encrypted message to registration authority (RA) requesting for registration. The message contains the ID of the voter V_i.

After receiving the message the registration authority (RA) verifies the authenticity of the sender (Vi) and check the voting right of voter V_i. RA also checks that whether V_i has applied previously or not. With proper verification the registration authority send ballot papers to voter V_i.



Structure of the proposed Scheme

2. VOTING

The voter fills the ballot, makes blind using blind signature technique and sends to the administrator to get the administrator's signature. Administrator signs the hidden ballot and returns back to the voter.

3. COUNTING

Voter sends the signed ballot, hash value of unique number from RA to the vote counter anonymously.

Proposed Scheme in Details

The proposed scheme is divided into mainly 3 stages:

1. Registration

2. Voting

3. Counting

Registration

At the beginning the voter V_i sends an encrypted message to RA by using his secret key. The message contains ID of voter, a random number ID of administrator, time stamp. After getting the message, the RA first checks the authenticity of the message and then checks whether the voter V_i is eligible to vote then RA checks whether V_i has applied for registration or it is the first time. If voter V_i is confirmed, a unique vote no NV_i is generated by RA. Then RA sends E (IDV_i || NV_i || random_no||timestamp).

Voting

V_i: voter V_i

RA: Registration Authority

A: Administrator

VC: Vote counter

p,q: Two large prime number such that q is a factor of (p-1)

g: $g \in Z_p^*$ having order q.

$x_V, x_A \in Z_p^*$; The vote counter VC's private key and administrator A's private key.

$y_V = g^{x_v} (\mathrm{mod}\, \mathrm{p})$: VC's public key

$y_A = g^{x_A} (\mathrm{mod} p)$: Administrator's public key.

H (.): A cryptographically secure one way hash function.

vw: voting warrant

XV_i: Voter V_i's private key

The administrator gets the key for signing; first the vote counter goes for a handshake with the administrator and administrator gets the key for signing.

Vote counter VC randomly picks out $\bar{k} \in Z_q^*$ and computes,

$$r = g^{\bar{k}} \ (\mathrm{mod}\ p) \qquad (1)$$

$$s = x_v + \bar{k}.H(v_w \,||\, r) \bmod q) \qquad (2)$$

VC sends(r,s) along with the voting warrants vw to the administrator. Then, administrator after receiving (r,s), verifies

$$g^s = y_V r^{H(v_w||r)} \bmod p \qquad (3)$$

If it is correct, Administrator accepts and computers

$$s_{pr} = s + x_A y_v \bmod\ q \qquad (4)$$

As the key for signing the ballot of the voters. Administrator randomly select an integer $k \in Z_q^*$ and computes

$$t = g^{k+x_A+H(time||\, place)} \bmod p \qquad (5)$$

Administrator then sends (r, t) to voter Vi. Then Voter selects two random number $u, v \in Z_q^*$.

Vote V_i computes

$$r' = tg^u y_{pr}^v \ \bmod p \qquad (6)$$

Where $y_{pr} = g^{s_{pr}} \bmod$ p

$$e = H(r' \,||\, m) \bmod q \qquad (7)$$

$$e^* = v - e \ \bmod q \qquad (8)$$

If $r' = 0$ then voter V_i needs to select a new tuple (u, v) otherwise, Voter V_i sends e* to the administrator.

After receiving e* the administrator computes

$$s' = k + e^* s_{pr} + H(time \,||\, \ place) \qquad (9)$$

As, the signed ballot and sends it to voter V_i.

After receiving s' from administrator voter V_i computes

$$s^* = g^{u+s'} \bmod p \qquad (10)$$

Thus, the signature on voting ballot 'm' becomes finally (m, vw, s*, e).

Counting

Encrypting with VC's public key; Voter V_i sends $((\mathrm{m}, \mathrm{v}_w, \mathrm{s}^*, \mathrm{e}) \| Nvi)$ to vote counter. Vote counter verifies

$$e = H(s^* y_A y_{pr}^e \| m) \bmod q \qquad (11)$$

If it satisfies; then a vote is accepted and the final result is declared after the voting time period is over.

The Prove of verification of Eq-11 at Vote Counter is given below:

$$\begin{aligned} e &= H(s^* y_A y_{pr}^e \| m) \bmod q \\ &= H(s^* g^{x_A} y_{pr}^e \| m) \bmod q \\ &= H(\mathrm{g}^{u+s'+x_A+s_{pr}e} \| m) \bmod q \end{aligned}$$

$$\begin{aligned} &= H(\mathrm{g}^{u+k+e^* s_{pr}+H(time\|Place)+x_A+s_{pr}e} \| m) \bmod q \\ &= H(\mathrm{t}\,\mathrm{g}^{u+(v-e)s_{pr}+s_{pr}e} \| m) \bmod q \end{aligned}$$

$$\begin{aligned} &= H(\mathrm{t}\,\mathrm{g}^u (\mathrm{g}^{s_{pr}})^v \| m) \bmod q \\ &= H(t\, g^u y_{pr}^v \| m) \bmod q \\ &= e \end{aligned}$$

V. Analysis of the Proposed Scheme

i. Completeness

The attacker cannot vote as a legal voter because during registration the voter sends encrypted message to RA using his own private key which is not possible for the attacker. Again in the vote counting stage the vote counter checks the signature from the administrator with the message. So it is impossible for the attackers to vote.

ii. Uniqueness

Since RA issue a unique serial number to each legal voters only once. So that no voter cannot vote twice. RA and the vote counter can detect the duplicate votes from that unique no.

iii. Mobility

In this scheme the voter is not limited to voting in a particular voting booth. A voter can vote through the internet.

iv. Anonymity

Administrator signs the blind ballot and the voted ballot is sent in an anonymous channel to vote counter. Hence, the proposed scheme confirms this requirement.

v. Convenience

The proposed scheme does not require any additional requirement or does not need any extra skills. Hence it is convenience.

VI. Conclusion

With the rapid development of internet technology, voting through internet is a practical idea. In this scheme, a secure and efficient mechanism of electronic voting is proposed using the proxy blind signature. To make an

immune E-Voting scheme it is feasible and practical. It increases the security of the voting system and also the impartiality factor is taken care. Hence, the proposed scheme can be practically applied in large scale voting. Result of Voting can quickly calculate. For each vote there is a digital evidence is created by the involvement of voter, Registration Authority and Administrator. So it can help to mitigate against forgery and future if allegation comes for forgery then it helps to prove/justify a bitty bit of the voting process.

REFERENCES

[1] Chum, D. *"Blind Signatures for Untraceable Payments,"* New York: Crypto'82, Plenum Press, 1983, pp. 199-203

[2] Mambo, M. , Usada, K. , Okamoto, E. "*Proxy Signatures for Delegating Signing Operation*," Proc 3rd ACM Conference on Computer and Communication Security. New York: ACM Press, 1996, pp. 48-*57*

[3] Tan, Z. W. , Liu Z. J. , Tang C. M. "*A Proxy Blind Signature Based on DLP*", Journal of Software, Vol. 14, No. 11, 2003, pp. 1931-1935.

[4] Lal, S. , Awasthi, A. K. "*Proxy blind signature scheme*", http://eprint. iacr. org/2003/072. pdf.

[5] Yang, X. , Yu, Z. "*An efficient proxy blind signature scheme based on DLP*", ICESS 2008, pp. 163-167.

[6] Panda, S. , Mohapatra R. "*Stamped Proxy Blind Signature Scheme*". International Journal of Computer Applications 64(15):pp.38-41, February 2013.

[7] Chin-chen chang[a,] *, Jung-San Lee[b] ,"*An anonymous voting mechanism based on the key exchange protocol*," Computer & Security 25(2006) pp.307-314 . Elsevier.

AUTHORS PROFILE

Suryakanta Panda, Pursuing M.Tech in Computer Science & Engineering at NIT, Rourkela. He has completed B.Tech on 2010. His area of interest is Digital Signature, Proxy Blind Signature and DLP problems.

Santosh Kumar Sahu, Pursuing Ph.D. in Computer Science at NIT Rourkela. He has Completed M.Tech from Berhampur University. B.Tech from C.V. Raman College of Engineering, Bhubaneswar. His Area of research is Intrusion Detection System.

Jagannath Mohapatra working as a Asst. Prof. in Computer Science & Engineering department at Sanjaya Memorial Institute of Technology, Berhampur, Odisha. He has 5 year experience in teaching & 4 year in Industry. His area of research is Information Security and Cloud Computing

Ramesh Kumar Mohapatra working as a Asst. Prof. in Computer Science & Engineering department at NIT Rourkela. His Area of interest is Cryptography and Network Security, Theory of Computation, Pattern Recognition.