International Journal of u- and e- Service, Science and Technology
Vol.8, No.1 (2015), pp.231-238
http://dx.doi.org/10.14257/ijunesst.2015.8.1.21

GSM Verification Based Secure E-Voting Framework

Sujit Biswas

Northwestern Polytechnical University, China
sujitedu@gmail.com

Abstract

Application of computer technology in human life is increasing geometrically. People are depending on this global network technology (internet) for shopping, banking, education etc. For this technological world people live different cities for their personal jobs. At that purposes they do not want to come back to their own constituency only to apply their vote. Electronic voting (evoting) can be a viable alternative to solve this problem. In this paper, new evoting architecture has been proposed which ensure voter's annomity. By implementing this architecture any voter can employ their vote from anywhere of the world. This architecture will also allow traditional voting besides electronic voting ensuring security and unique vote per voter. In this architecture cryptographic techniques has been proposed to overcome the security threats, also ensure voter's anonymity. Considering security issue two step security has been proposed in this framework.

Keywords: *E-voting, E-voting Framework, Mobile voting, GSM application in evoting*

1. Introduction

Election is a fundamental instrument of democracy that provides an official mechanism for people to express their views to the government. In democracy, elections perform three major functions; Selection - help people to choose the people (leader) who will make government policies, acountability - people are expected to hold the government accountable, communications– elections allow citizens and elected officials to communicate with each other. By voting, people expect to at least communicate some of their preferences for government policy through their selected leaders. This leader selection process is an election. Traditionally this is done through a paper ballot. Voters employ their vote by seal or marked to ballot. Election staff ensures right voter and one vote per voter. Voter choices their future leader and sent it to ballot box. Ballot must be voter untraceable.

Traditionally, the process of voting is quite cumbersome because voter must come physically to vote. This problem results in the low participation rate of voting. Because, those who live in sparsely populated areas and who work far away from the voting venu can't employ their vote. Also large no people are involve with this election process but they have full right to apply their vote (Usually all election staff has been selected from other constituency). Evoting [10] can overcome this problem. By evoting voter can vote from anywhere of the world. To participate in evoting a voter must have some IT knowledge. Usually this is impractical especially for some developing countries where maximum people have no IT knowledge. Even, in a developed country everybody is unable to use this evoting technology. In this paper, a smart system architecture has been proposed which allows evoting besides traditional voting.

ISSN: 2005-4246 IJUNESST

2. Evoting

E-voting is an election system that allows voters to apply vote through secure and secret ballot electronically over internet. Result of evoting is just as like traditional voting, difference is that in evoting all voting process are done through internet. As a result voters can vote their preferred candidate from anywhere of the world. Many countries have implemented unique id (UID) or national id (NID) system for citizens. This can form the base of e-voting system. Some developed countries have developed their citizen database with NID/ UID and biometric information. Unique mobile no is another important identity nowdays. This information can be accessed for e-voting and it will ease the authentication process of e-voting system. It will further ensure that just one vote will cast by an individual and there will be no rigging. All citizens regardless of their level of education can employ their votes by using any of the following ways.

2.1. Voting Using Email and Mobile

This type of voting system is for educated people who have access to internet at their homes/offices or for those who are unable to stay constituency during elections and also the people who are feeling insecure for physical voting. Thus, wherever they are, they can exercise their right to vote through internet on the day of election. They can log into proposed the e-voting system with NID and password and cast their votes.

2.2. Traditional Voting

This channel is for people who do not know how to use internet or do not have access to internet. Voter enters the polling section and asked a ballot to polling officer. Polling officer ensure right voters by his/her NID and biometric or image. After confirming the right voter will sign a ballot and supply it to the voter. Polling officer will also update election commission database or list after providing every ballot. Voter vote his preferres candidate and submit it to sealed ballot box.

2.3. Why E-voting

Remote electronic voting refers to an election process whereby people can cast their votes over the internet, most likely through a web browser, from the comfort of their home, or possibly any other locations where they can get access to internet. In this internet era because of globalization people are moving within few hours from one city to another city, one country to another country. Their personal and commercial life is more important than a vote. They want to employ their vote without canceling their schedule. Moreover, a large no of voters of every country always stay aboard for different purposes. Only evoting can encourage these types of voters to vote. There are also many aspects of elections besides security that bring this type of voting into question. The primary ones are—

1. Forcibility the danger that outside of a public polling place, a voter could be coerced into voting for a particular candidate.
2. Vote selling the opportunity for voters to sell their vote.
3. Vote solicitation the danger that outside of a public polling place, it is much more difficult to control vote solicitation by political parties at the time of voting.

3. Some Terminology Used in the Paper

3.1. Blind Signature on Messages

Some verifiable transformation of a message which can only be generated by the signing entity is blind signature [1]. Using publicly available information, anyone can verify the signature. In a blind signature, the signing entity signs a message without knowing its contents. The message that is submitted for blind signature can be freely published without revealing the actual message. It is the most popular cryptographic technique in evoting by providing confidentiality of the voter's ballot.

3.2. Paillier Cryptosystem

The Paillier cryptosystem [2] is a probabilistic asymmetric algorithm for public key cryptography. The problem of computing n^{th} residue classes is believed to be computationally difficult. The decisional composite residuosity assumption is the intractability hypothesis upon which this cryptosystem is based. The scheme is an additive homomorphic; this means that, given only the public-key and the encryption of two messages m_1 and m_2, one can compute the encryption of $m_1 + m_2$.

Key Generation:

1. Two large prime numbers p and q randomly choose and independently of each other such that $\gcd(pq, (p-1, q-1)) = 1$ [this assure when both p & q are equal length]
2. Compute $n = pq$ and $l = lcm(p-1, q-1)$ Any random integer g where $g \in Z_{n^2}^*$
3. It has to ensure that n divides the order of g and checking modular multiplicative inverse $\mu = (L(g^{\lambda} \bmod n^2))^{-1} \bmod n$ where function L is defined as $L(u) = (u-1)/n$. [Here mentioned that a/b doesn't denote the modular multiplication of a times the modular multiplicative inverse of b but rather the quotient of a divide by b. so the largest integer value $v \geq 0$ to satisfy the relation $a \geq vb$]
4. The public (encryption) key is (n, g)
5. The private (decryption) key is (λ, μ)

   Encryption**:** For message m be encrypted where $m \in Z_n$; Select r random where $r \in Z_n^*$; Compute ciphertext $c = g^m * r^m \bmod n^2$

   Decryption: ciphertext C , where $c \in Z_{n^2}^*$ Compute the plaintext message as**:** $m = L(c^{\lambda} \bmod n^2) \bullet \mu \bmod n$

3.3. SMS Security

SMS security is mostly ensured by GSM operator [7-9]. Even then this paper is proposing Secure SMS (SSMS) [3] for SMS related cryptographic security. Also any other renowned SMS security [11] protocol can be used with this proposal.

4. Related Works

In paper [4], a secure mobile phone voting system has been proposed. In this proposal National Identity Card (NIC) and SIM card is used to be registration by symmetric key. Election commission server (ECS) decrypts and sends a pin to voter. This pin has been used for voting.

On the voting day ECS will send a message to voter. Voter decrypts the message by symmetric key. Voter will select their candidate within candidates list. After selecting their candidate encrypt it with ECS public key also concatenate pin, again encrypt it with voter's symmetric key finally add NIC and send it to ECS via SMS. It can be refered like (1).

$$[En_{user\_symetric\_key}(En_{ecs\_public\_key}(vote)+PIN)+NIC \quad (1)$$

Equation (1) has been sent to ECS via SMS].
ECS find symmetric key using NIC number. Decrypt the message using symmetric key and record the pin for protecting duplicate voting. Proposal is also allowing paper ballot. But how SMS vote interact with paper ballot and protect double vote is not mentioned.

O.Baudron [5] proposed an interesting multi-candidate election scheme that guarantees privacy of voters, public verifiability, and robustness against a coalition of malicious authorities. Their scheme is based on the Paillier cryptosystem and on some related zero-knowledge proof techniques. Unfortunately, the zero-knowledge arguments in [3] are not very efficient since to prove the correctness of a vote, one should encrypt each bit of j and then proves that the vote can be written as $M^j=M^{j0}\cdot\cdot\cdot M^{jk}$, where k=[log(L−1)]+1, and L is the number of candidates.

Kristian Gjosteen [6] proposed a modified protocol for evoting which allows a voter to vote multi times but only final ballot will be counted as vote. It also agrees to traditional voting but interaction process with paper voting and evoting is not mentioned.

5. Proposed Evoting Architecture

5.1. Voter Registration

First time to be registered voter must be physically presented to EC (Election Commission) office. EC office must confirm following entity in registration phase. Underlined entity must be unique. All registration process is thinking and considering evoting perspective.

1. Unique Voter ID(Identity Card)
2. Voter email address
3. Voter's personal mobile no.
4. Voter's Constituency
5. Voter's image.

5.2. Proposed Architecture

Steps (According to the Figure 1: explanation about lines (1-11) has been given bellow):

1. Voter chose his / her constituency in Election Commission (EC) website. A login form will be displayed and asked voter ID, password and temporary pin (previously Password is generated by voter).
2. ES will send a pin to voter's mobile by SMS using mobile operator's network.

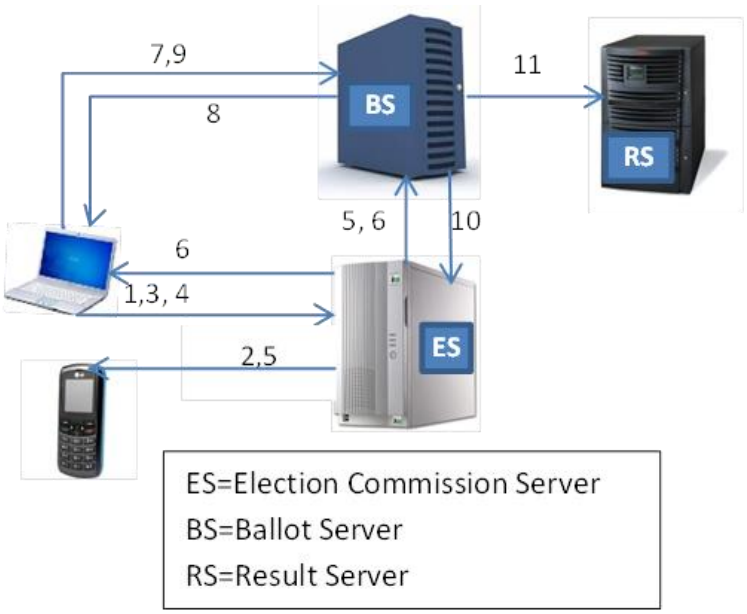

Figure 1. Proposed Evoting Architecture

3. Step 1 will be completed using step 2's pin.
4. Voter request a ballot to ES (through its website).
5. ES will check voter's constituency and vote status (previously voted or not) do the following steps.

a. Send a secret unique pin (temporary created) to voter's mobile. Simultaneously it will also be sent to BS.

6. Link of ballot with a temporary session id will be emailed to voter's email. (For every voter has different ballot link). This unique session id will be sent to BS.
7. Voter will check his/her email and click on Ballot link.

a. A temporary time session will be generated (maximum 60 sec) for log in and it will asked a pin which was generated in step 5. Voter will be allowed maximum three attempts to login using his/her pin.

8. BS will verify the pin and session id (session id will be extracted from ballot link) with previously stored (step 5) pin & Session ID. If the verification is positive then a ballot will be sent to voter.
9. Voter apply vote on his ballot and send to BS. BS store this encrypted ballot in corresponding to voter's ID (Voter ID must be stored as hash value, using a hash function)
10. BS will send an acknowledgement to ES. ES will update its database as counted vote. Also send an acknowledgement to voter's email and mobile.
11. BS send only encrypted vote to RS (without voter ID). RS decrypt the ballot using private key. And publish the result.

5.3. Interaction with Traditional Voting

Every polling station and polling officers must have unique ID and password. Before providing ballot paper polling officer ensure from Election commission website about voters vote status.If vote status no then poling officer deliver ballot paper to voter and must update voter's status in ES. Poling officer will be liable to ensure total counted vote and issued ballots are equal in his polling station

5.4. Security Mechanism

Anonymity is the very important factor for evoting. For every encryption and decryption of this framework Paillier encryption (PE) [2] technique has been proposed. Details of security mechanism have been described by 1 to 6 steps.

1. When Bob request a ballot to ES. Encrypt pin (Ep) →mobile through SMS using SSMS cryptographic technique & ES to BS by PE. Also send the ballot link to email of Bob.
2. Bob decrypt pin (D_p), Check his email and further request for Ballot to BS by using D_p.
3. BS verify Bob's credentials and send an empty encrypted and digital signed Ballot S' (E_b) to Bob.
4. Bob decrypt ballot $D(E_b)$, apply his vote to ballot (B) and send it again to BS as encrypt $S'(E_b(V))$. [He must ensure that $D_b(S'(E_b))=S'(B)$ and $S(S'(B))=B$].
5. BS again verify Bob's credential and previous sign and send to RS anonymously with blind sign $S_{bl}'(S'(E_b(V)))$. Also send a message to ES (Vote has been counted)
6. RS decrypt ballot $D(S_{bl}'(S'(E_b(V))))$, ensure that $S_{bl}'=S'$. Finally count the result.

6. Future Work

In this paper Paillier encryption system has been proposed for secured data transfer. In future more secured newly proposed encryption technique will be applied to this proposed architecture. Highly secured encryption technique will be confirmed for server and database security. A new cryptographic protocol will be proposed for increasing SMS security.

7. Conclusion

In this technology mediated world e-governance has been proved its feasibility. E-voting can be important part of e-governance also. For maximizing the benefits and minimizing the risks of evoting, a secured architecture is very important. In proposed architecture considering security issue voter's verification has been emphasized highly. To login the system, voters require 2 step verification. GSM technology beside internet has also been used for secured log in. This architecture also proposes a short session after login to vote completion which will minimize the risk. Considering the security issue verification steps has used 2 times for voter. Proposed architecture also allows traditional voting and ensure unique voter per voter that will increase the importance of this architecture in real life voting.

References

[1] D. Chaum, R. L. Rivest and T. Sherman, "Blind Signatures for Untraceable Payments", Advances in Cryptology Proceedings of Crypto 82 Plenum, (**1993)**, pp. 199-203.
[2] P. Paillier, "Public-Key Cryptosystems Based on Composite Degree Residuosity Classes", Lecture Notes in Computer Science, Springer, vol. 1592, (**1999)**, pp. 223-238.
[3] G. Belvin, "SECURE TEXT MESSAGING PROTOCOL", (A thesis of Johns Hopkins University), Baltimore, Maryland, (**2011**), May.
[4] M. Ullah, A. I. Umar, N. U. Amain and Nizamuddin, "An Efficient and Secure Mobile Phone Voting System", IEEE (**2013**).
[5] O. Baudron, P. Fouque, D. Pointcheval, J. Stern and G. Poupard, "Practical multicandidate election system", PODC (**2001**), pp. 274-283, PODC (**2001**), pp. 274-283.
[6] K. Gj_steen, "Analysis of an internet voting protocol", Department of Mathematical Sciences, NTNU, (**2010**) March 9.
[7] S. Alam, I. A. Jamil, K. Mahmud and N. Islam, "Design and Implementation of a RF Controlled Robotic Environmental Survey Assistant System", the 16th International Conference on Computer and Information Technology, IEEE, (**2014**) March 8-10.

[8] M. Sayidul, K. Mahmud, R. Halim, P. Saha, and I. A. Jamil, "Freighter fuel level detection and overload alarming system with safety notification via GSM", In Informatics, Electronics & Vision (ICIEV), 2014 International Conference on, IEEE, (**2014**), pp. 1-5.
[9] K. Mahmud, "Neural network based PID control analysis", Global High Tech Congress on Electronics (GHTCE), 2013 IEEE. IEEE, (**2013**).
[10] V. Gupta, "e-Voting: move to intelligent suffrage", SETLabs Briefings, vol. 9, no. 2, (**2011**).
[11] Y. Qiu and H. Zhu, "Somewhat Secure Mobile Electronic-voting Systems Based on the Cut-and-Choose Mechanism", International Conference on Computational Intelligence and Security, (**2009**).

Author

Sujit Biswas
NWPU, Xi'An, Shaanxi, China.
Email: sujitedu@gmail.com
Professional
Instructor, Computer Engineering Department,
Jessore Polytechnic Institute, Jessore, Bangladesh.
Currently:
M.Sc in Computer Science and Technology (Continue..)
Northwestern Polytechnical University, P.R. China.
Research Field
Android Security (Users Privacy Security), Smartphone Security.

