An Efficient and Secure Mobile Phone Voting System

Mohib Ullah, Arif Iqbal Umar, Noor ul Amin, Nizamuddin

Department of Information Technology Hazara University Mansehra Pakistan

mohibmscs.hu@gmail.com, arifiqbalumar@yahoo.com, namin@hu.edu.pk, sahibzadanizam@yahoo.com

***Abstract*— Electronic voting system provides convenience and access to the electorate without the geographical restrictions. Mobile phone is one of the emerging technologies to perform e-voting with democratic norms and privacy concern. In this paper we suggest a mobile phone voting protocol based on hybrid cryptosystem. Protocol consists of three phases: online registration; vote casting and vote collecting and result phase. Proposed protocol provides secure and efficient online vote casting and can also be implemented parallel with paper ballot voting system. Proposed protocol has efficiency, security and deployable in developing countries due to its reliance on SMS messaging without requiring internet connectivity.**

Keywords: Digital democracy; Electronic voting; Public key cryptosystem; GSM

I. INTRODUCTION

The objective of democracy is to permit the public to vote freely and let them to cast their vote according to their wishes with simplicity. The key objective of mobile phone voting is the elimination of going to polling booths, paper ballots, time and cost efficiency, tiredness and violence due to standing in line in pooling booths to cast their vote and to lessen the numbers of polling booths agents. Mobile Phone Voting System (MPVS) provides mobility feature which enhanced turnout ratio in election. However this technology faces certain security threats for its successful implementation in election. Without eliminating these security threats like vote buying and coercion, online registration, secrecy of ballot, anonymity of voter and double voting this latest technology can't be used. An efficient and reliable system is essential for the trustworthy and successful implementation of this technology.

In our propose system we design mobile phone for e-voting (electronic voting). The proposed system uses mobile phone device having: small in size, low power, low-priced as compared to computers and Direct Recording Electronic voting system (DRE's), Electronic Voting Machine's (EVM's), provide mobility feature (can be used ubiquitously) and security (can be access in a temper resistant environment making it less vulnerable to external attacks). Proposed system uses Global System for Mobile Communication (GSM) technology which is a secure and globally used mobile technology in the current situation. Mobile phone also uses Subscriber Identity Module (SIM) technology which provides user identity privacy, user identity verification and subscriber data secrecy providing more security to the proposed system.

The key features of our proposed Mobile Phone Voting System (MPVS) are:

1. Eligibility: Only authorize voter allowed to cast their vote.
2. Uniqueness: Voter can cast only one vote.
3. Accuracy: Election commission server should record the ballots accurately.
4. Integrity: No valid votes should be modified, replaced or to be deleted.
5. Fairness: The election outcome can't be accessible before the official result time ended.
6. Secrecy: No one should be able to find how someone voted.
7. Cost-effectiveness: Election system should be efficient and affordable.

II. LITERATURE REVIEW

Mobile phone voting is relatively new area of research. Here we review some of the work presented in the past.

X. Yi et al [1] proposes secure mobile phone voting system built on modular square root and blind signature system. System satisfies basic requirements of election like confidentiality of voter, secrecy of ballot, voter anonymity and has less computation cost and communication overhead. Due to third party CA (certificate authority) involvement, i.e. distribution of certificates to voters for authentication purposes, delayed occurred which make the process slow.

Y. Feng et al [2] proposes mobile phone voting system using GSM technology. In the system voter authentication is done through GSM mobile operator. Subscriber validation is done through GSM challenge-response protocol. System consists of four parts: mobile phone; authentication server; verification server and counting server. Proposed system consist of three levels: pre voting level; voting level and post voting level. Voter secrecy is ensured by using blind signature system. Due to GSM authentication setup public-key overhead is mostly reduced. Extra work is required to deal with the trust retained on authentication server, end-user device (ME) and application security.

Y. Qui et al [3] Proposes mobile phone intermediate e-voting system based on the extended Pailler's encryptions system. Aim of the system is to enforce the cut-of-the-choose method to exclude the computational zero-knowledge evidences and express effectiveness of the system. Proposed system is slightly provably safe in simulation-based prototype.

H. Sahu et al [4] propose GSM mobile phone voting system to cast vote without registering for voting in advance and going to polling booths. System prevents double voting but for security purposes no cryptographic algorithm is used is main its shortcoming.

978-1-4799-0615-4/13/$31.00 ©2013 IEEE

K. Hayam et al [5] suggested mobile phone voting system using public key encryption algorithm RSA. Protocol involves three phases: access control phase; voting phase and election administrator server phase. First phase holds validation and identification for the applied voters. Voting phase accomplished by ciphering voter data using RSA algorithm while the election administrator server phase classifies ending result by decrypting received encrypted data using RSA private key. System has shortcomings like no online registration and high computational cost and communication overhead due to RSA algorithm.

X. Yi et al [6] propose real-world electronic voting system for mobile phone. Idea is to merge mix network and blind signature protocols and blindly authorizing each vote twice. Voter verification is achieved by collaboration of SIM card and identity card (IC) fixed in mobile phone with dual SIM card holder. Proposed framework consists of mobile voter, base station (BS), certificate authority (CA), electoral commission (EC), mix server (MS) and court for election (CE). Mobile phone voting system run in three phases: setup and registering phase, voting phase and totaling phase. At least one of mix servers should be reliable and tampering proof. Certificate authority, electoral commission and mix server have own public/private keys. When mobile phone voter registers with certificate authority, CA will compute two PINs and issue an identity card and passes PIN_1 to voter via safe channel. Voter has no access to PIN_2 protected in secure memory of IC. After voter registration with election commission it will calculates PIN_3 and passes to voter via protected channel. During polling period voters reminded by SMS to cast their votes to election commission. First voter inserts SIM card and IC into his mobile phone with dual SIM card holder. Secondly voter chooses their selected candidate. Base station validates voter on the basis of SIM. If voter is authentic then base station will forwards voter request to certificate authority and then to election commission. CA and EC jointly validate voter on the basis of MAC (Message Authentication Code). During polling election commission, certificate authority and base station preserve all exchanged messages. When voting ended, election commission shows all votes in lexicographic order. Mix server collects all votes and confirms their signs. If signs are real then decrypt votes by their private key. Mix server will organize all votes in lexicographic order and forwards them to EC with its signs. Election commission validates these signs. During totaling EC and every mix server preserve all substituted messages and non-repudiation evidences of message source and message transfer for record purposes.

R. Lakhotia et al [7] proposes mobile phone voting uses global system for mobile communication technology where GSM verification system used to provide voter confirmation, enhanced security, voter mobility and reduce public-key overhead. For registration purposes user will register their mobile number to election commission (EC) of India and will get voter ID for identification purposes. Voter has to activate their mobile number for voting and only one vote will be cast on each mobile number. Protocol has three stages: Pre voting stage, voting stage and post voting stage. In pre voting stage when user wishes to vote, presses "Vote" button assumes to be exist on the set. Base station instructs user through SMS to switch off their mobile phone. Switching on again by pressing "vote" button, mobile phone will reserved only for voting purposes and no outgoing and incoming call can be received on that mobile phone. When authentic voter cast their vote will get SMS from EC of India having list of candidates, their parties name and symbols. User has to simply reply to this SMS. The message holds ten number destination field filled partly (eight digit) by base station with servers number and last two by the user for identification of different areas. The area code provided by government before the voting day. The eight number destination codes are kept secret in case of hacking makes this application secure because intruder will not be able to get the destination number. Cryptographic application will be installed earlier in the mobile phone. Message will request for voter id and mobile number. If voter ID matches with EC voter list, election commission will approved to the voter to cast their vote. Counting server receive encrypted message with encryption key from authentication centre else vote will be rejected. User will acquire acknowledgment message on same registered number after vote acceptance. To bring mobile phone in normal condition user permitted to switch on their mobile phone. Advantages of system are if SMS get hacked intruder can't cast fake vote as key already passed. If someone mobile phone stolen then user can contact with EC help center to block the number and can also register new mobile number. No need of internet as voting is done over SMS while one vote per mobile phone is the shortcoming of the system. Making authentication centre more secure and reliable is the future work of the system.

III. PROPOSED SYSTEM

Many previous studies on e-voting systems have focused on facilitating the e-voting. These systems are suffering from various weaknesses such as offline registration, extra hardware cost and compulsory polling places.

Our system is based on the lesson acquired and analysis of the several issues that play significant role in the earlier e-voting systems.

Our propose system not only provide online registration but also offline registration in case of failure of online registration. Mobile phone operator should be reliable to verify the users SIM card register with their original credentials for registration to the concern authority. System consists of five components: Mobile Phone (MP); Election Commission Server (ECS); Election Commission Databases (ECD); Vote Collecting and Result Phase Server (VCRPS) and Election Commission Office (ECO).

Proposed system consists of three phases:

A. Online registration phase
B. Voting phase
C. Vote collecting and result phase

A. Online Registration Phase

For the usage of our system user should have NIC and SIM card number registered with their credentials. Election commission server should keep two updated databases of public. First database consists of public NIC's and second database contained data about SIM cards from the concern authorities for user verification and authentication purposes at the registration time.

All the activities are done through Short Message Services (SMS) without the need of internet which reduces the cost up to some extent. ECS will generate public/private key pair. It then will keep private key secret and will put public key on its server.

Online registration phase will be a separate phase from the other two phases. Vote collecting and result phase will take part only in the system when the official time of election ended. Then decryption, counting and result displaying phase of votes will be started.

B. *Steps Required For Online Registration Phase*

1) In the first step mobile phone user will send their [NIC No + SIM Card No + Symmetric Key] encrypt with public key of ECS to ECS server.
2) Receiving this election commission server will decrypt this data with his private key.
3) ECS will verify the user credentials such as NIC and SIM card number with its two latest databases, one contained public NIC numbers and other database contained SIM card numbers.
4) If user is verified as authentic then,
5) ECS will send PIN encrypted with user symmetric key to the user. This PIN will be used for the authenticity of the voter in the later stages of the election process.
6) Receiving this user will decrypt the PIN with his/her symmetric key. User should securely keep their PIN from disclosing to others because it's disclosing will compromised confidentiality.
7) Mobile phone user will send acknowledgement message to election commission server.

   Mobile phone user will become certified mobile phone voter. In this case online registration phase will be completed.
8) This is offline registration phase which will be used in case someone registers his/herself on genuine user credentials.
9) When the genuine user registering his/herself with election commission server, ECS will send registration problem message of can't be register through online registration phase and will requested his/her to come to ECO for correction of their registration as someone already register his/herself on genuine user credentials.
10) In this case user should go to election commission office. The previous registration will be canceled and genuine user will be register.
11) Election commission office (ECO).

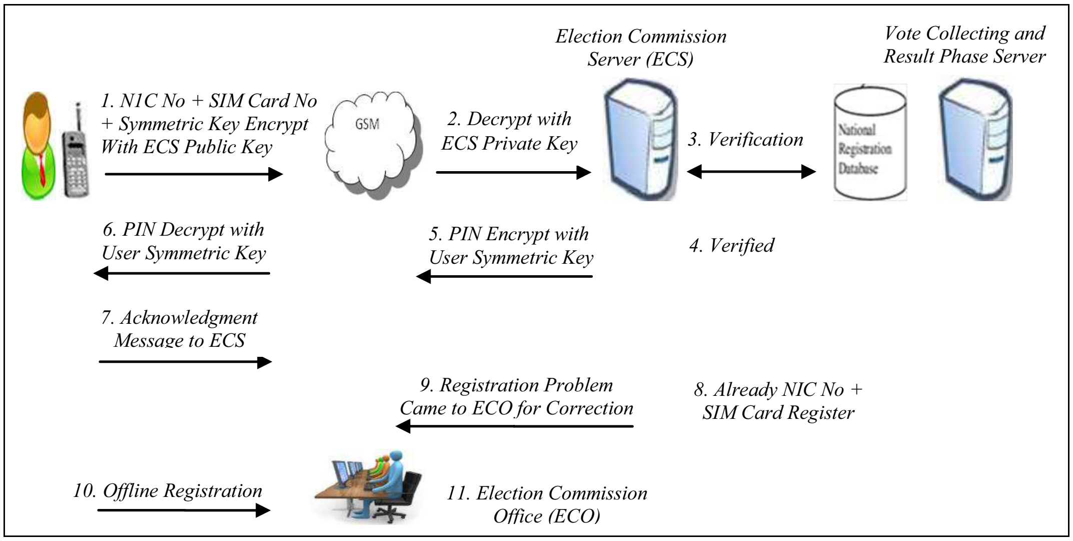
Election Commission Server (ECS)
Vote Collecting and Result Phase Server
1. NIC No + SIM Card No + Symmetric Key Encrypt With ECS Public Key
GSM
2. Decrypt with ECS Private Key
3. Verification
National Registration Database
6. PIN Decrypt with User Symmetric Key
5. PIN Encrypt with User Symmetric Key
4. Verified
7. Acknowledgment Message to ECS
9. Registration Problem Came to ECO for Correction
8. Already NIC No + SIM Card Register
10. Offline Registration
11. Election Commission Office (ECO)

Fig.1.Online Registration Phase

C. Voting Phase

1) On the voting day ECS which has the entire authenticated voter list will send candidate list to each voter according to their constituency via SMS encrypted with voter symmetric key. This will ensure that the candidate list message only send to the authenticated voter list. This method also prevents the unauthorized voter to cast vote as illegal user will not be receiving this message.
2) On the voting day after receiving the SMS, voter will decrypt the message with their symmetric key.
3) In this step voter will select their candidate from the candidate list. After selecting their favorite candidate voter will then encrypt the message with ECS public key, concatenate PIN encrypt both with user symmetric key and again concatenate NIC number and send to ECS via SMS.
4) ECS will find user symmetric key using NIC number. Then it will decrypt the remaining SMS part with user symmetric key. ECS will mark only the PIN part of the message for the record purposes and to avoid double voting. The remaining encrypted candidate list message will be forwarded to the vote collecting and result phase server.

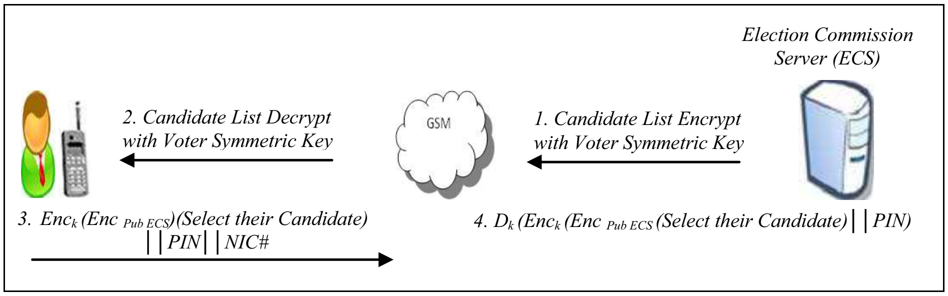
Election Commission Server (ECS)
2. Candidate List Decrypt with Voter Symmetric Key
GSM
1. Candidate List Encrypt with Voter Symmetric Key
3. $Enc_k (Enc_{Pub\ ECS})$(Select their Candidate) ||PIN||NIC#
4. $D_k (Enc_k (Enc_{Pub\ ECS}$(Select their Candidate)||PIN)

Fig.2. Voting Phase

D. Vote Collecting and Result Phase Server

1) Before the start of the election, time lock mechanism should be implemented on VCRPS. It will keep the vote in encrypted form until the official time of the election ended. Implementing this restriction on this server, the decryption of the votes will be started after the end of the election time. No third party will know the result before the official time ends, thus prevents unfair seeing of the election results. Moreover anonymity is maintained.
2) At the end of election time, each vote will be decrypt by using ECS private key.
3) At the last step of the election process, votes will be counted and the results will be officially announced to the public.

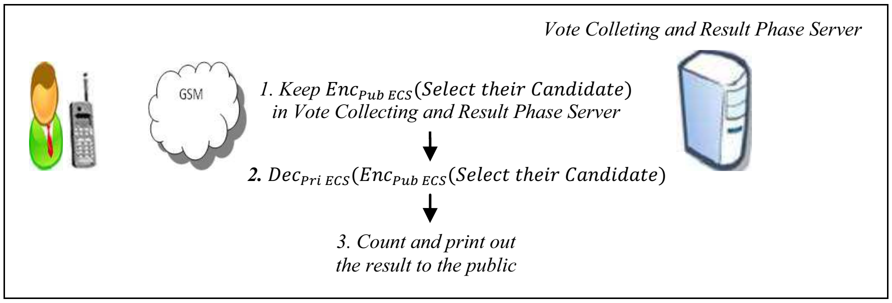
Vote Colleting and Result Phase Server
GSM
1. Keep $Enc_{Pub\ ECS}$(Select their Candidate) in Vote Collecting and Result Phase Server
2. $Dec_{Pri\ ECS}(Enc_{Pub\ ECS}$(Select their Candidate)
3. Count and print out the result to the public

Fig.3. Vote Collecting and Result Phase

IV. ANALYSIS

Our system provides online registration, which saves time, energy and provides mobility option to the voter, thus prevent double voting and offer choice to the public to cast their vote through mobile phone or from pooling booths.

A. Security Analysis

1) Voter Registration:

Our proposed system provides online registration as well as offline registration in case of registration problem. Voter will sends NIC#, SIM card number and symmetric key to election commission server by using ECS public key. Verification of NIC# and SIM card number is done through concerned authority and voter will be successfully registered through online registration phase. While in case of intruder stolen user credentials and register on user credentials then offline registration will be take place.

2) Confidentiality:

Our system satisfies the basic property of e-voting, i.e. confidentiality of PIN and ballot as:

3) Confidentiality of PIN:

In proposed system encrypted PIN is sent to the voter using voter symmetric key. As symmetric cipher such as DES, AES are secure, so confidentiality of PIN is guaranteed.

4) Confidentiality of Ballot:

As vote (selected candidate) is encrypted using ECS public key concatenated with PIN and again encrypted with vote Symmetric key. ECS will decrypt the double encrypted ballot (selected candidate) concatenated with PIN and match the PIN for authentication purposes. If voter is successfully authenticated then the encrypted vote will be forwarded to vote collecting and result phase server. When election time ended decryption, counting of votes will be stared and at the last result will be display to the public. This process guaranteed confidential credential exchange between the user and the election commission server.

5) *Avoid Vote Duplication:*

To avoid vote duplication from online and paper ballot voting, polling officer will check vote status of each voter coming for paper ballot casting via SMS. If vote already casted voter status will be marked as "vote already casted" and will deny the voter to cast his/her vote again, otherwise will be allowed to cast his/her vote.

B. *Cost Analysis*

In our system at user side one public key encryption and one symmetric key decryption performed in pre voting phase while one symmetric key decryption, one public key encryption and one symmetric key encryption performed in voting phase while no encryption/decryption performed in vote collecting and result phase.

In our system one private key decryption, one symmetric key encryption performed in pre voting phase while one symmetric key encryption and decryption performed in voting phase while one private key decryption performed in vote collecting and result phase at ECS side. Total four encryption/decryption steps performed at user side while six symmetric encryption/decryption steps performed at election commission server side. In the whole system overall ten encryptions/decryptions steps are performed.

V. CONCLUSION

This paper proposes mobile phone voting system (MPVS) with online mobile voting registration phase based on hybrid cryptosystem. System prevent double voting in case of casting ballots first from mobile phone and then from pooling booth. Proposed system is more efficient and reliable in the sense that data will be send to election commission server through secure SMS. Our system didn't need internet and any special hardware device which reduces the cost. System only required mobile phone and SIM card.

REFERENCES

[1] X. Yi, P. Cerone, and Y. Zhang, "Secure Electronic Voting for Mobile Communications," in Proc. Vehicular Technology Conference, vol. 2, 2006.

[2] Y. Feng, S. L. Ng, and S.S. Grosche, "An Electronic Voting System Using GSM Mobile Technology," Department of Mathematics Royal Holloway, University of London Egham, Surrey TW20 0EX England, England Technical Report RHUL–MA–2006 5http://www.rhul.ac.uk/mathematics/techreports, 26 June 2006.

[3] K. Kim, and D. Hong, "Electronic Voting System using Mobile Terminal," World Academy of Science, Engineering and Technology, pp. 33-37, 2007.

[4] 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, Proc. IEEE International conference on Computational Intelligence and Security (CIS'09), vol. 1, pp. 446-450, July 2009.

[5] H. Shaun, and A. Choudhray, "Intelligent Polling System Using GSM Technology," International Journal of Engineering Science, vol. 3, 2011.

[6] K. Hayam. A. Annie, M. A. Alia, and A. A. Hnaif, "E-Voting Protocol Based On Public-Key Cryptography," International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.4, July 2011.

[7] X. Yi, and E. Komodo, "Practical Mobile Electronic Election," IEEE/SICE International Symposium on System Integration (SII), pp.1119-1124, 20-22 Dec. 2011.

[8] R. Lakhotia, R. K. Jarial, and P. K. Tiwari, "Designing a Secure Protocol for Mobile Voting Through SMS," IOSR Journal of Engineering Vol. 2(5), pp.1259-1264, May 2012