Secure Voting System in a Mobile Network

Dinesh Goyal, Dr. Naveen Hemrajani, Gajanand Sharma, Ravi Sr Sharma, Dr. Ruchi Goyal
Suresh Gyan Vihar University, Jaipur, INDIA

Sharad Kumar Mahera,
JNIT, Jaipur, INDIA

Abstract: **Electronic voting (E-voting) using an internet has been recently performed in some nations and regions.**

There is no spatial restriction which a voter directly has to visit the polling place, but an e-voting using an internet has to go together the computer in which the internet connection is possible. Also, this voting requires an access code for the e-voting through the in-advance report of a voter. To minimize these disadvantages, we propose a method in which a voter, who has the wireless certificate issued in advance, uses its own cellular phone for an e-voting without the special registration for a vote. Our proposal allows a voter to cast his vote in a simple and convenient way without the limit of time and location, thereby increasing the voting rate, and also ensuring confidentiality and anonymity by using secret keys encryption and decryption.

Keywords: Voting, Mobile Terminal, Confidentiality, Anonymity.

I. INTRODUCTION

In the elections, the election of member of the assembly, the head of local/state government election, and others, a voter can cast vote after going to the designated polling place and checking his identity. This makes man directly to count the ballots and counting of votes to be long. Especially, this voting is a reason to reduce voting rate since voters always should go to the polling place. In an e-voting by touch screen, a voter directly selects candidates or the vote content appeared on a screen as the finger. This voting with fast counting time has also a problem that voters go to the polling place. In the meantime, an e-voting using internet has no inconvenience that voters should visit the voting booth. However, this voting is executed just in the environment with internet accessible computer.

In this paper, we proposes an e-voting system that allows a voter to be identified using a wireless certificate without additionally registering when a user votes using his mobile terminal such as a cellular phone or a PDA. We also present a method that ensures the anonymity of voter and the confidentiality of vote content. By our mobile voting system, a voter can cast his vote more easily and conveniently than the existing e-voting using internet, within the scheduled time period anywhere even when a voter is not able to access internet on a voting day. Our proposal can be applied all types of elections national as well as state/local elections. Our goal is not to design a cryptographically provable protocol [1] but to illustrate e-voting model and to describe a voting process.

II. EXISTING ELECTRONIC VOTING SYSTEM

In the existing off–fine voting method to select a candidate in the election such as the national assembly election, or local election, electorates go to the designated polling places and have to be identified to cast their votes, and finally voters cast their ballot. Of course, voters should be in advance registered on a poll book. To do so, a significant amount of time and cost are consumed by voting and counting of votes. In the mean time, the most important security issue for on-line electronic voting using touch screen or internet is to guarantee the anonymity of voter and the confidentiality of vote content. The followings are requirements that should be

1. The relation between voter and vote content should not be revealed.
2. The result of a poll should be retained as a secret before counting the ballot.
3. A voter can cast his vote just one time.
4. Only an identified person by an e-voting device can participate in e-voting.
5. Other people excepting a voter himself should not know the vote content.

An e-voting method using a touch screen which allows a voter to select a candidate or an option displayed on a screen has advantages in that a voter can cast his vote regardless of his assigned polling place, but in this case, a voter is still required to go to a polling booth to vote.

As other e-voting method, a voter does not have to go to a polling place if he uses internet and vote is permitted to internet user.[4] But, internet-accessible terminals are always required to vote and a voter can cast a vote in the just limited place which he can access internet. Especially, private data like personal ID might be leaked in the course of accessing to the internet. This means that anonymity of electronically voting over the internet is not satisfied. Also, confidentiality of voting might not be ensured if a candidate selection or a voting content is not encrypted.

III. E-VOTING SYSTEM USING MOBILE TERMINALS

Fig. 1 is an illustration of an electronic voting system for electronic voting over mobile communication network. E-voting system includes a mobile terminal, a mobile communication server, and an e-voting device. A mobile terminal is a device that includes wireless certificate used to verify a voter's identity. A mobile communication server within mobile communication network connects a mobile terminal to an e-voting device for e-voting service. It makes a role in transmitting data used in the e-voting process to both entities. It is not allowed to give any change of data except for deleting ID of a mobile terminal coupled with voting. An e-voting device can be a secure system managed by national organization such as a board of elections or an election

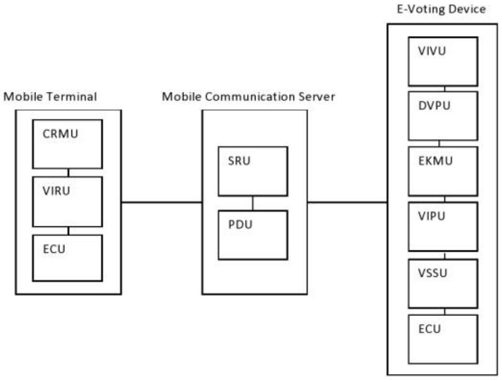


Fig 1 E-Voting using Mobile Terminal

A. E-Voting Device

E-voting device consists of 6 units for its internal functionality.

1. VIVU(Voter Identity Verifying Unit) -It verifies whether a voter is allowed to vote based on a wireless certificate received from a voter's mobile terminal over mobile communication network
2. DVPU(Double Voting Prevention Unit) - If a voter tries to access to e-voting device twice after he completes voting once, DVPU refuses a second attempt to verify his identity. This work happens if a voter accesses e-voting service again ever after already casting his vote at a polling place or finishing vote using his mobile phone.
3. EKMU(Encryption Key Management Unit) -This unit creates an encryption key to encrypt the vote content and transmits the key to a mobile terminal.
4. VIPU(Vote Information Providing Unit) - It provides vote information containing a list of possible voting selections or a list of candidates to a mobile terminal.
5. VSSU(Voting Selection Storing Unit) - It decrypts the encrypted vote content received from a mobile terminal. At this time, VSSU does not take identification information of voter since it was already removed in the mobile communication server. And, this unit stores the decrypted result to count votes after voting time is finished.
6. ECU(External Connection Unit) -This unit issues the wireless certificate to a mobile terminal. Or it may be connected to other device outside e-voting device to send a certificate to a mobile terminal.

B. Mobile Terminal

A mobile terminal includes CRMU, VIRU, and ENCU. A voter actually uses a cellular phone and PDA as a terminal.

1. CRMU(CeRtificate Management Unit) - This unit stores a voter's certificate containing a personal identification number. When e-voting process starts up, CRMU sends it to an e-voting device to prove that a voter is qualified to vote. This work is not done until a voter inputs a password or PIN to demonstrate that he begins e-voting service using his own mobile terminal. Putting password prevents others from using the certificate fraudulently.
2. VIRU(Vote Information Receiving Unit) - VIRU receives a vote information and an encryption key from an e-voting device.
3. ENCU(ENCryption Unit)- This unit encrypts voter's decision using the encryption key stored in VIRU and sends the encrypted vote content to the e-voting device.

C. Mobile Communication Server

A mobile communication server including SRU and PIDU connects a mobile terminal to an e-voting device over a mobile communication network.

1. SRU(Sending and Receiving Unit) -This unit receives an encryption key and vote information from the e-voting device and transfers it to the mobile terminal. Also, SRU receives encrypted vote content from the mobile terminal and sends it to the e-voting device.
2. PIDU(Personal Identification Deleting Unit) - It plays a part in deleting personal identification information received from the mobile terminal of voter before sending the encrypted content to the e-voting device.

In the e-voting system using a mobile terminal, a wireless certificate is used to verify a voter's identity after a voter accesses to an e-voting device for the first time. So, the certificate should be beforehand issued by a certificate authority linked to ECU of e-voting device or by other authorized entity irrelevant to e-voting device. Also, it must be stored in the mobile terminal of voter's own before a voter starts e-voting service. A wireless certificate can be used in other applications such as mobile commerce or mobile banking besides of e-voting service.

After verifying voter's identity, an e-voting device selects one secret key among a group of secret keys or its public key and sends it to a mobile terminal of voter. A voter who received the key chooses one of vote information provided by an e-voting device and encrypts the vote content. At this time, encryption is done by using secret key shared between a mobile terminal and e-voting device or using public key of an e-voting device. And then, a voter sends encrypted vote content to the e-voting device. In this process, vote information on the screen of a mobile terminal can be different to voters according to voter's place of residence, which is decided by referencing a current address of voter within a certificate.

When a mobile communication server receives encrypted vote content and ID of a mobile terminal, it always deletes ID of a mobile terminal and transmits only encrypted vote content to an e-voting device. And then, an e-voting device received an encrypted vote content can learn a vote content using a key which it created in the previous step.

IV. VOTING PROCESS USING MOBILE TERMINALS

In this chapter, we propose e-voting process using a mobile terminal. Fig. 2 shows the procedure of e-voting between an e-voting device and a voter. It is as follows:

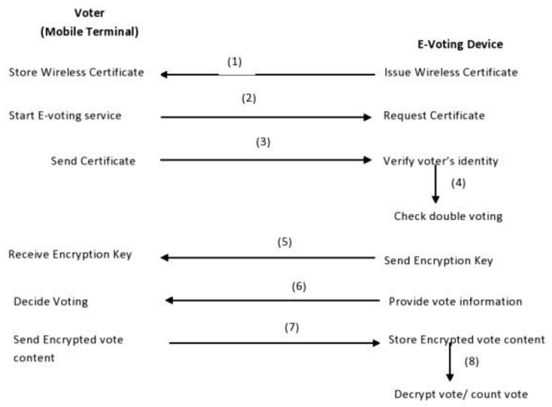


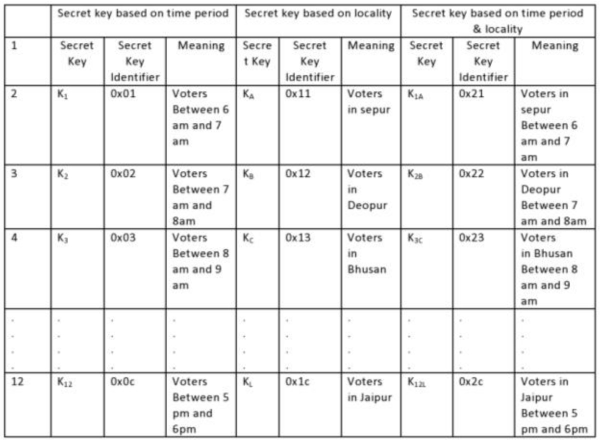
Fig. 2 E-Voting process using a mobile terminal

1. A wireless certificate is issued to a mobile terminal, that is, a voter has the certificate before commencing voting. The certificate should be kept in the mobile terminal for e-voting service.
2. E-voting service is started as soon as a mobile terminal connects to an e-voting device. If an e-voting device accepts the e-voting service, it requests a certificate to verify a voter's identity.
3. A mobile terminal sends the certificate to the e-voting device. So, a voter proves that he is a qualified person to cast a vote.
4. If the voter's identity is verified and the voter is given the right to vote, an e-voting device checks if the voter is re-accessing an e-voting device.
5. The e-voting device selects and transmits an encryption key according to the encryption method to guarantee the confidentiality of the voter. Of course, this work is done after verifying the voter's identity and checking double voting of a voter.
6. After sending the encryption key, an e-voting device continuously transmits vote information containing a list of possible voting selections and supplemental information. And then, a voter decides his voting based on the vote information.
7. A mobile terminal encrypts the vote content and transmits the encrypted vote content to an e-voting device. An e-voting device does not reveal the encrypted vote content until voting time is finished. At this moment, a mobile communication server that received the encrypted vote content and the ID of a mobile terminal always deletes ID. That is, an e-voting device receives only content of voting.
8. When voting time has passed, an e-voting device decrypts the stored encrypted vote content and checks the voting selection to count the vote.

In the process 5, the encryption key management unit of an e-voting device creates a secret key and a key identifier and transmits them to a mobile terminal. This key is sent if encryption scheme based on symmetry key is applied. On the other hand, if e-voting process employs the scheme based on public key, that unit transmits the public key of an e-voting device to a mobile terminal. If a secret key is used for each voter, the relation between a voter and his key is revealed. This makes anonymity of a voter not to be satisfied. Thus, to avoid this, one encryption key can be generated on a time period basis and then the same encryption key is assigned to voters who access at a certain time period. As well, the same encryption key can be assigned to voters in the same district by checking the address of voters from their certificates. Same encryption key identifier is used for identifying the encryption key.

Fig.3 is a table showing an example of encryption keys depending on time periods, localities, or time periods and localities. Encryption keys can be generated by creating several encryption key groups.

V. PROPOSED E-VOTING MODEL FOR INDIA



	Secret key based on time period			Secret key based on locality			Secret key based on time period & locality		
1	Secret Key	Secret Key Identifier	Meaning	Secret Key	Secret Key Identifier	Meaning	Secret Key	Secret Key Identifier	Meaning
2	K_1	0x01	Voters Between 6 am and 7 am	K_A	0x11	Voters in sepur	K_{1A}	0x21	Voters in sepur Between 6 am and 7 am
3	K_2	0x02	Voters Between 7 am and 8am	K_B	0x12	Voters in Deopur	K_{2B}	0x22	Voters in Deopur Between 7 am and 8am
4	K_3	0x03	Voters Between 8 am and 9 am	K_C	0x13	Voters in Bhusan	K_{3C}	0x23	Voters in Bhusan Between 8 am and 9 am
. . . .	. . . .	. . . .	. . . .	. . . .	. . . .	. . . .	. . . .	. . . .	. . . .
12	K_{12}	0x0c	Voters Between 5 pm and 6pm	K_L	0x1c	Voters in Jaipur	K_{12L}	0x2c	Voters in Jaipur Between 5 pm and 6pm

Fig.3: Creation of secret key in EKMU

When a secret key and a key identifier are transmitted, they are encrypted using a public key of a voter to avoid disclosing data. Fig.4 shows transferring a secret key used for encryption and decryption of vote content. The notations are as follows.

K : a secret key transferred from an e-voting device to a mobile terminal for encrypting vote content

IND : a key identifier to indicate key group

PUBU ,*PRIU* : a public key and a private key of voter *U*

PUBV, *PRIV* : a public key and a private key of e-voting device *V*

m : vote content decided by voter

E (*m*), *E* (*m*) *K PUBV* : encryption of vote content using *K* and *PUBV*

D (*m*),*D* (*m*) *K PRIV* : decryption of encrypted vote content using *K* and *PRIV*

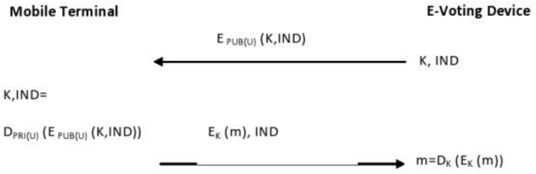


Fig. 4 Transferring Secret key and vote content

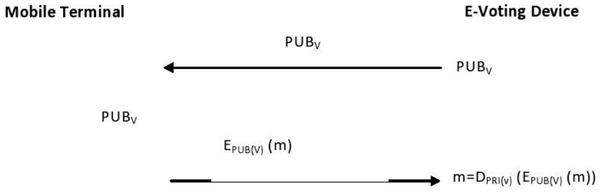
1) An e-voting device generates *K* and *IND* and encrypts them using *U PUB* included in a certificate of voter. And, the device transmits them to a mobile terminal.

2) A voter receives the encrypted information and decrypts it using his private key. And then, he extracts *K* and *IND*.

3) A mobile terminal encrypts *m* using *K* and transmits the encrypted vote content together with *IND* to an e-voting device.

4) An e-voting device decrypts the encrypted vote content using *K* and *IND* that he created.

Fig. 5 shows transferring public key and encrypted vote content.



1) An e-voting device generates its public key and transmits it to a mobile terminal.

2) A mobile terminal received the public key encrypts the vote content using that key and transmits the encrypted content to an e-voting device.

3) An e-voting device decrypts the encrypted vote content using its private key.

After transmitting encryption key, e-voting device sends vote candidate or vote information to a voter as Fig. 2.

In the e-voting process over the mobile communication network, a mobile communication server receives voter's identity, encrypted vote content, and key identifier. But, it can't know real vote content because it does not have encryption key.

Thereafter, a mobile communication server sends only encrypted vote content and key identifier to an e-voting device after it always deletes voter's ID. Therefore, an e-voting device can't know the relation between voter and vote content.

VI. CONCLUSION

Our proposal enables a voter to cast his vote using a mobile phone without additionally registering himself for voting in advance and going to a polling place. Also, proxy vote or double voting is not possible. Any entities except for an e-voting device can't know the voting result.

In this paper, we are not focusing on encryption algorithm applied for two entities. Our concern is to present e-voting system using a mobile terminal and to explain its process. As a next work, it is needed to design a concrete cryptographic protocol to guarantee the anonymity and the confidentiality of a voter. Although there are a lot of electronic voting mechanism using multiparty protocol [2,3] and anonymous communication[6], more reviews are required in the aspect of efficiency and secrecy.

REFERENCES

[1] X. Y. Cerone and P. Y. Zhang, "Secure Electronic Voting for Mobile Communications," Vehicular Technology Conference, 2006. VTC 2006-Spring. IEEE 63rd, Vol. 2, 2006, pp 836 – 840.

[2] J. D. Cohen and M. J. Fisher, "A robust and verifiable cryptographically secure election system", In Proc. 26th IEEE Symp. On Foundations of Comp. Science, pp 372-382, Portland, 1985.

[3] A. C. Yao, "How to generate and exchange secrets," In Proc. of 27th IEEE Symp. On Foundations of Comp. Science, pp 162-167, Toronto, 1986.

[4] KR Patent, Application Number: 2005-0088243, "Electronic voting system using internet", Korea, 2005.

[5] http://www.e-voting.go.kr

[6] C. S. Park, K. Itoh, and K. Kurosawa, "Efficient anonymous channel and all/nothing election scheme," EROCRYPT 93, pp 248-259, Springer-Verlag, Lecture Notes in Computer Science No. 765, 1994.

[7] Abdul Kalam, A.P.J., "Knowledge society", Employment News, 3-9 February, p.p.1, 2001.

[8] Keswani Bright., Mangal S.K., Agarwal Ashok., "e-Projects for Rural India: Status and Benefits", Journal of Commerce and Information Technology', vol.7, no.2, pp.79-84, 2007.

[9] Keswani Bright., Mangal, S.K., Agarwal Ashok, Banerjee Chitreshh., "New e-Government Model System: A Real Convenience for India", OORJA, vol. 6, no.3, pp.25-30, 2008.

[10] Gupta, M.P., Kumar, Prabhat, and Bhattacharya, Jaijit, "Government Online", Tata McGraw-Hill Publishing Company Ltd., New Delhi., 2004.

[11] Saxena, K. B. C., "Towards Excellence in e-Governance", International Journal of Public Sector Management, vol.18, no.6, p.p.498-513, 2005.

[12] Ralf-Eckhard Türke, "Towards Productive and Sustainable Forms of Interaction in Governance", Kybernetes, Vol.35, no.1-2, p.p. 164-181, 2001.

[13] Bellamy, R., Warleigh, A., "Citizenship and Governance in the European Union", Continuum, London, 2001.

[14] Dinesh, A., Mirchandani & Julius H. Johnson, Jr. and Kailash Joshi, "Perspectives of Citizens Towards e-Government in Thailand and Indonesia: A Multigroup Analysis", Information Systems Frontiers, vol.10, no.4, p.p.483-497, 2008.

[15] Haus, M., Heinelt, H., "Urban Governance And Democracy", London, Routledge, 2005.

[16] Kevin O'Toole, "E-Governance in Australian Local government: Spinning a Web around Community?", International Journal of Electronic Government Research, vol.3, no.4, p.p.58-75, 2007.

[17] Lemuria Carter and Vishanth Weerakkody, "E-Government Adoption: A Cultural Comparison", Information Systems Frontiers, vol.10, no.4, p.p. 473-482, 2008.

[18] Williams, M.D., "E-Government Adoption in Europe at Regional Level", Transforming Government:People, Process and Policy, vol.2, no.1, p.p.47-59, 2008.

[19] Mateja Kunstelj and Mirko Vintar, "Evaluating the Progress of E-Government Development: A Critical Analysis", Information Polity, vol.9, no. 3-4, p.p.131-148, 2008.

[20] Rahul De', "E-Government Systems in Developing Countries: Issues and Concerns – Discussion", IIMBM Management Review, vol.18, no.4, p.p.377-388, 2006.

[21] Sang M. Lee, Xin Tan, and Silvana Trimi, "Current Practices of Leading E-Government Countries", Communications of the ACM, vol.48, no.10, p.p.99-104, 2005.

[22] Wayne Huang, J D'Ambra, and Bhalla, V., "An Empirical Investigation of the Adoption of Egovernment in Australian Citizens: Some Unexpected Research Findings", The Journal of Computer Information Systems, vol.43, no.1, p.p.15-22, 2002.

[23] Yining Chen, Chen, H.M., Russell K.H. Ching, and Wayne W. Huang, "Electronic Government Implementation: A Comparison between Developed and Developing Countries, International Journal of Electronic Government Research, vol.3, no.2, p.p.45-61, 2007.