

Design and Analysis of Secured Electronic Voting Protocol

¹V. Kalaichelvi and ²R.M. Chandrasekaran
¹SRC, SASTRA University, Kumbakonam, India
²Annamalai University, Annamalai Nagar, India

Abstract: Electronic voting can play a really vital role in the democracy of the life. In this study, researchers propose an electronic voting protocol. The scheme does not require a special voting channel and communication can occur entirely over the current internet. This method integrates the internet convenience and cryptology. This study analyzes the various existing protocols such as simple protocol, two agency protocol, blind signature protocol and sensus protocol. In the existing protocol the Tallier has to wait until the decryption key is received from the voter. So it will consume lot of time. Instead of getting the decryption key value from the voter, the Tallier maintains the key information securely in the database. So, comparatively the proposed protocol consumes less time. This study also analyzes the various security issues involved in an electronic voting like security, privacy, authentication, anonymous, uniqueness, accuracy, fairness, efficiency and uncoercibility.

Key words: E-voting, security, privacy, anonymity, internet, India

INTRODUCTION

Conventional voting: Conventional voting consists of the following four phases shown in Fig. 1.

Authentication: Alice walks into a voting precinct and authenticates herself by showing her voting credentials; this step is public and verified by the officials present in the room. At the end of the authentication process, Alice is given a paper ballot on which to write her vote.

Vote: The vote takes place in a protected booth where she cannot be seen by anyone. Alice casts her vote by writing it with a pencil on the paper ballot; she then folds the paper ballot and puts it in the ballot box where all the votes are mixed. Since no one can see what Alice writes and there are no marks on the paper ballots, Alice's vote is anonymous.

Count votes: At the end of the voting time, the officials open the box containing the paper ballots and publicly count the votes; the results are then announced.

Verification: Various types of verification are used or possible; most procedures are indeed public and overseen by representatives of competing parties. The opposite interests of the parties warrant the first level of protection against fraud. A recount is also possible if there is a presumption of fraud or error.

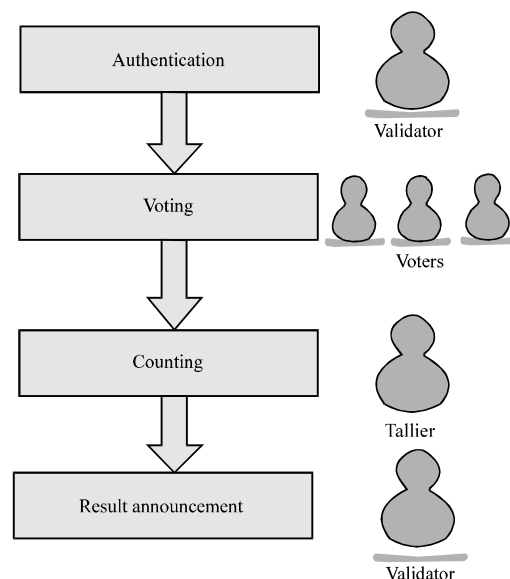


Fig. 1: Phases of conventional voting

Issues in conventional voting: Conventional voting (such as voting by paper or signature voting) has many problems:

- Printing of ballot paper is expensive
- Voting consumes lot of time
- Counting is prone to errors
- Maintaining convenient poll booths is very difficult

- There is no good relationship between the government and popular, popular cannot trust the government and depend on it, voter here is like a blind person that must rely on the other person to vote for him
- Sometimes, government coerced and carries on the voters to vote for a particular candidate and eliminate them from voting freely
- Some candidates trying to win by buy the votes from the voters
- Government can cheat by substitute the original ballot by derivative ones

According to all what is mentioned above, the whole world is moving on towards the trend of E-voting. Electronic voting systems are expected to be the solution for the weakness in traditional voting systems.

Properties/issues/requirements of an electronic voting:

The requirements in conventional voting (paper vote) are also apply for electronic voting, the requirements can be expected to be universal and any system must try to apply these requirements:

- Fairness: no one can learn the voting outcome before the tally
- Eligibility: only eligible voters are permitted to vote
- Uniqueness: no voter should be able to vote more than once
- Privacy: no one can access any information about the voters vote
- Accuracy: all valid votes should be counted correctly
- Uncoercibility: no voter can prove how he voted to others to prevent bribery
- Anonymity: there should be no way to derive a link between the voter's identity and the marked ballot
- Efficiency: the computations can be performed within a reasonable amount of time
- Robustness: a malicious voters cannot frustrate or disturb the election
- Verifiability: voters can check if their ballots have been correctly counted

Related work: In the last few years, a numerous number of researches propose different E-voting systems and some countries and states around the world implement their E-voting system. However, this numerous number of E-voting schemes can be categorized into three main categories.

The categories based on the cryptography mechanism used to build the system. The first category is E-voting system based on blind signature technique

(Fujioka *et al.*, 1992; Juang and Lei, 1997; Sako and Kilian, 1994). The second category is E-voting system based on Mix-Nets (Jakobsson, 1998; Abe, 1999). The third and the last category is e-voting system based on homomorphic signature properties (Okamoto, 1997; Jakobsson, 1998; Abe, 1999; Benaloh and Tuinstra, 1994; Cramer *et al.*, 1996, 1997; Sako and Kilian, 1994, 1995). Chaum was the first one to introduce blind signature and mixed nets. In general, this different proposed system agree that the system should not be verifiable voting system (which mean the voter has no way to prove their voting activity) as a prevent technique against vote buying problem. However, some other E-voting system allows voter to prove their voting activities. Since, the voting buying and the privacy of the voter is a critical problem in the Jordanian voting system, we design the scheme as anonymous and unverifiable E-voting system which categorize under the first category blind signature-based E-voting system.

MATERIALS AND METHODS

Existing voting scheme: This study gives a brief introduction to the approaches used in various voting schemes.

Simple protocol: This protocol is designed without employing any cryptographic techniques. In this, voters would submit their vote along with a unique identification number to a validator who would then take their name off on a list of registered voters. Then the validator would then strike off the unique identification number and submit just the votes to the Tallier who would count the votes.

Although, this system has the advantages of being flexible, convenient and mobile, this system is far from secure. If the validator is compromised votes can be easily traced back to the voter or votes could be changed. Both privacy and accuracy lack with this protocol. There is no way to ensure the voter's privacy and the Tallier accurately records the votes.

Two agency protocols: In this two agency protocols, the electronic validator distributes a secret identification tag to each voter just prior to the election. The validator then sends the Tallier a list of all identification tags with no record of the corresponding voters. Each voter sends the Tallier his/her identification tag and an encrypted file containing a copy of the tag and the voted ballot. At this point, the Tallier can make sure the identification tag is valid but the program has no way of examining the contents of the ballot. The Tallier publishes the encrypted

file and the voter responds by sending the Tallier the key necessary to decrypt it. When the election is over, the Tallier publishes a list of all voted ballots and the corresponding encrypted files. This protocol also has several problems. Most importantly, it does not protect the voter's privacy if the Tallier and validator collude.

Blind signatures: Blind signatures allow a document to be signed without revealing its contents. The effect is similar to placing a document and a sheet of carbon paper inside of the envelope. If somebody signs the outside of the envelope they also sign the document on the inside of the envelope. The signature remains attached to the document even when it is removed from the envelope (Fujioka *et al.*, 1992; Juang and Lei, 1997; Sako, 1994). The voter prepares a voted ballot, encrypts it with a secret key and blinds it. The voter then signs the ballot and sends it to the validator. The validator verifies that the signature belongs to registered voter who has not yet voted. If the ballot is valid, the validator signs the ballot and returns it to the voter. The voter removes the blinding encryption layer, revealing an encrypted ballot signed by the validator. The voter then sends the resultant encrypted ballot to the Tallier. The Tallier checks the signature on the encrypted ballot. If the ballot is valid, the Tallier places it on a list that is published after all voters vote. After the list has been published, voters verify that their ballots are on the list and send the Tallier the decryption keys necessary to open their ballots. The Tallier uses these keys to decrypt the ballots and add the votes to the election tally.

Sensus polling protocol: One of the drawbacks of the blind signature protocol is the voter has to wait till the voting has ended before the voter can verify the casted vote was the correct one which is not in line with the property of flexibility.

Sensus system is closely based on the blind signature protocol. The major difference between the schemes emerges after the voter has submitted the encrypted ballot to the Tallier. Instead of waiting till the voting ends the Tallier sends a receipt to the voter when his/her ballot has been received. This receipt is no more than a confirmation the vote has been transferred to the Tallier correctly. The voter may submit the decryption key immediately after receiving this receipt, completing the entire voting process in one session. The implemented sensus system employs a pollster agent that performs all cryptographic functions and transactions with the election programs on the voter's behalf. Tests conducted with a prototype implementation of sensus indicate that the entire voting process can be completed within a few minutes.

Proposed protocol: Before talking about the proposed electronic voting protocol, we need to define the biometric token (smart card) and the feature of it and why we use it in the system and how can it be useful for the voters in election.

Smart card: In this system, smart card is used as a storage media to store the information of the voters, other personal data and the Unique Id (11-digit number TN/99/0000012, in this TN specifies the state, next two digit specifies district Id and third one specifies the Unique id for each eligible voter) and Iris pattern (unique for each user-static one) and the public key information. But why smart token why it is the best for electronic voting? Because it is a temporarily store media and an anonymous media which provide a secure way to save the information of the cardholders. In this system, we are using 16 Kbytes EEPROM ACOS 3 smart card. The memory area provided by the card chip is basically segregated in internal data memory and user data memory. The internal data memory is used for the storage of configuration data and it is used by the card operating system to manage certain functions. The user data memory stores the data manipulated in the normal use of the card under the control of the application. Memory area is possible within the scope of data files and data records. The maximum number of data files allowed in ACOS 3 is 31. A data file can contain up to 255 records. User data files are allocated in the personalization stage of the card lifecycle. Once the personalization bit has been programmed there is no possibility of resetting the card back.

Biometric authentication: Biometrics is automated methods of identifying a person or verifying the identity of a person based on a physiological or behavioral characteristic. Examples of physiological characteristics include hand or finger images, facial characteristics and iris recognition. Biometric authentication requires comparing a registered or enrolled biometric sample (biometric template or identifier) against a newly captured biometric sample (for example, a fingerprint captured during a login). During enrollment, a sample of the biometric trait is captured, processed by a computer and stored for later comparison. Biometric recognition can be used in identification mode where the biometric system identifies a person from the entire enrolled population by searching a data-base for a match based solely on the biometric. For example, an entire database can be searched to verify a person has not applied for entitlement benefits under two different names. This is sometimes called one to many matching. A system can also be used in verification mode where the biometric system authenticates a person's claimed identity from their previously enrolled pattern. This is also called one-to-one

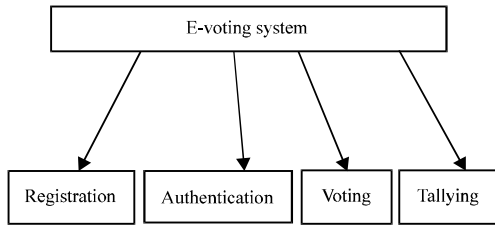


Fig. 2: Phase of electronic voting

matching. In most computer access or network access environments, verification mode would be used. A user enters an account, user name or inserts a token such as a smart card but instead of entering a password a simple touch with a finger or a glance at a camera is enough to authenticate the user. This recognition method uses the iris of the eye which is the colored area that surrounds the pupil. Iris patterns are thought unique and static one. The proposed voting scheme is divided into a number of phases as drawn in Fig. 2 and 3.

In the registration phase, validator stores the voter's information like Unique Id, Address details, Iris pattern of the voter and the public key (based on RSA 512-bit) information into the smart card. After testing the smart card, validator issues the smart card to the voter. This step has to be started and completed before the process of election. The voter authentication is the first step in the process of voting according to this system. In this phase, First the voter inserts the smart card into the smart card reader, the validator performs authentication by comparing the stored iris pattern and with the live iris pattern. If it is matched, the validator sends the authenticated message to the Tallier. Tallier checks whether he is already voted or not. If the voter is not the Tallier send's the candidate details to the voter. Once the voter is selected the candidate, the ballot is encrypted using the public key which is available in the smartcard and the encrypted ballot is transferred to the Tallier. Instead of waiting till the voting ends the Tallier sends a receipt to the voter when his/her ballot has been received and the Tallier strike off the voter's name from the registered list. This receipt is no more than a confirmation the vote has been transferred to the Tallier correctly. Immediately, the encrypted ballot is decrypted by using the corresponding private key which is kept secret by the Tallier. In the existing protocol, the Tallier has to wait until the voter sends their corresponding private key. So, this proposed protocol completes the entire voting process in one session and completes within a few minutes.

Analysis of the proposed protocol

Privacy and fairness: This scheme achieves privacy and fairness issues because no one can acquire any information about the tally result before the voting

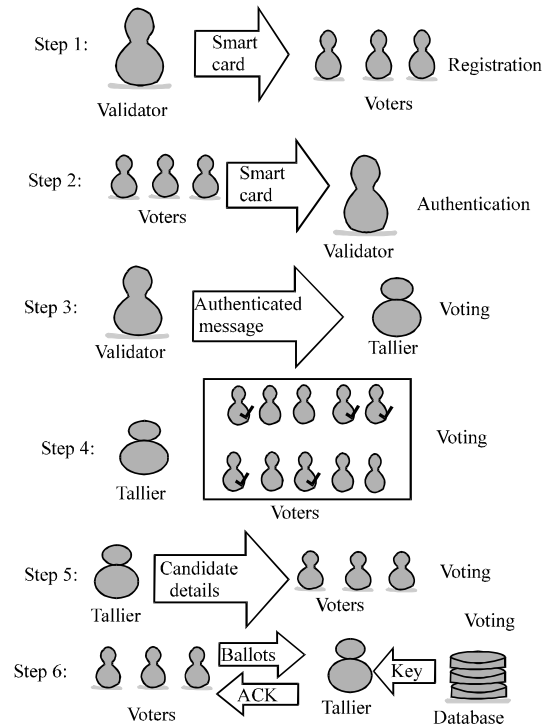


Fig. 3: Steps involved in the proposed protocol

deadline. Before announcing the election outcome, each ballot will be in an encrypted form. Therefore no one can learn or predict the outcome of each vote before the tally announcement.

Uniqueness: No voter is able to vote more than once by maintaining the status bit information; it prevents the double voting and because of this, it achieves uniqueness issue.

Efficiency: The transactions in the existing protocol are multiple as the Tallier has to send the receipt to the voter to get the decryption key to decrypt the encrypted votes. This scheme achieves efficiency because these functions are carried out in a single transaction as the Tallier does not have to wait for the decryption key from the voter. The advantages of the proposed scheme over the existing protocols are less complexity in implementation and consumption of very less time in the voting process.

Security: The proposed scheme achieves security by encrypting and decrypting the vote using RSA 512-bit public key algorithm. As the key size increased, it is very difficult for the hacker to find out the key to decrypt the encrypted vote during the time of transferring the vote from the voter to Tallier. The time to guess the key will be more and the whole process will be over by the time the key is guessed.

Table 1: Comparison of the various protocols

Properties	Simple protocol	Two agency protocol	Sensus protocol	Bind signature protocol	Proposed protocol
Eligibility	Yes	Yes	Yes	Yes	Yes
Accuracy	No	Medium	Yes	Yes	Yes
Fairness	No	No	Yes	Yes	Yes
Efficiency	No	No	Medium	Medium	High
Privacy	No	No	Yes	Yes	Yes
Security	No	Yes	Yes	Yes	Yes
Uniqueness	No	No	Yes	Yes	Yes
Authentication	No	Medium	Yes	Yes	Yes
Verifiability	No	Yes	Yes	Medium	Medium
Anonymity	No	No	No	No	Yes
Uncoercibility	No	No	No	No	No

Anonymity: In the existing protocol to guarantee verifiability, the voter's encrypted vote will be sent to the voter with the key value to decrypt that vote. By decrypting that vote, the voter can verify that the voter's vote has been counted correctly. If it is verified by the voter, it violates the anonymity and uncoercibility. So, this protocol advocate those voters not be allowed to verify their votes by themselves. It is not necessary to allow voter voters to verify (or show to bribers) their votes in the announcement phase.

Uncoercibility: This scheme does not support uncoercion, since the voter is at a remote location, we cannot be sure that the voter is who she avows to be unless we use a biometric authentication protocol. Even with the use of biometrics to authenticate both eligible person and Eve (political person) sit in front of the same system (reserved for election) doing the authentication and Eve voting or monitoring the votes as he wants. If voter wants to sell her vote and Eve is not present, she can take a picture of his voting and give it to Eve as proof. In any case, the remoteness of the voter makes the abolition of the sale of votes impossible to fulfill for online voting. In practice, this means that online voting cannot be used in elections or polls where fraud by the sale of votes or coercion is concern, like in political elections. Table 1 is the comparison of the various protocols.

CONCLUSION

Electronic voting can play a really vital role in the democracy of the life. This study proposed an electronic voting protocol and the new proposed protocol is compared with the various existing protocols. In the existing protocol, the Tallier has to wait until the decryption key is received from the voter. So it will consume lot of time. Instead of getting the decryption key value from the voter, the Tallier maintains the key information securely in the database. So, comparatively the proposed protocol consumes less time. This study also discussed about how the proposed protocol

achieves the following requirements such as fairness, uniqueness, accuracy, privacy, anonymous, authentication and un-coercion.

ACKNOWLEDGEMENTS

Researcher am grateful to SASTRA University, Thanjavur, Tamilnadu, India for providing the necessary facilities to carry out this research reported in this study. Researcher sincerely thank the management for the generous financial support under innovation fund.

REFERENCES

Abe, M., 1999. Mix-networks on permutation networks. *Adv. Cryptol.*, 1716: 258-273.

Benaloh, J. and D. Tuinstra, 1994. Receipt-free secret-ballot elections (extended abstract). *Proceedings of the 26th Annual ACM Symposium on theory of Computing*, May 23-25, 1994, Montreal, Quebec, Canada, pp: 544-553.

Cramer, R., M.K. Franklin, B. Schoenmakers and M. Yung, 1996. Multi-authority secret-ballot elections with linear work. *Proceedings of the International Conference on the Theory and Application of Cryptographic Techniques*, May 12-16, 1996, Saragossa, Spain, pp: 72-83.

Cramer, R., R. Gennaro and B. Schoenmakers, 1997. A secure and optimally efficient multi-authority election scheme. *Eur. Trans. Telecommun.*, 8: 481-490.

Fujioka, A., T. Okamoto and K. Ohta, 1992. A practical secret voting scheme for large scale elections. *Proceedings of the Workshop on the Theory and Application of Cryptographic Techniques: Advances in Cryptology*, December 13-16, 1992, Queensland, Australia, pp: 244-251.

Jakobsson, M., 1998. A practical mix. *Proceedings of the International Conference on the Theory and Application of Cryptographic Techniques*, May 31-June 4, 1998, Espoo, Finland, pp: 448-461.

Juang, W.S. and C.L. Lei, 1997. A secure and practical electronic voting scheme for real world environments. *IEICE Trans. Fundam.*, E80-A: 1-8.

Okamoto, T., 1997. Receipt-free electronic voting schemes for large scale elections. *Proceedings of the 5th International Workshop on Security Protocols*, April 7-9, 1997, Paris, France, pp: 25-35.

Sako, K. and J. Kilian, 1994. Secure voting using partially compatible homomorphisms. *Lect. Notes Comput. Sci.*, 839: 411-424.

Sako, K. and J. Kilian, 1995. Receipt-free mixtype voting scheme a practical solution to the implementation of a voting booth. *Proceedings of the International Conference on the Theory and Application of Cryptographic Techniques*, May 21-25, 1995, Saint-Malo, France, pp: 393-403.