Implementation and Analysis of Secure Electronic Voting System

Htet Ne Oo, Aye Moe Aung

Abstract: -In this technological and knowledge age, e-commerce related matters become popular. Electronic voting is one of these matters and it is able to provide convenient, less expensive, fast and secure facilities. Important basic properties of electronic voting are fairness, privacy, eligibility, receipt-freeness, coercion-resistance and verifiability. Current electronic voting systems satisfy only some of these properties. So, the proposed system aims to design and implement an electronic voting system which satisfies the required properties of electronic voting process. After implementing the system, it will be verified using mCRL2 language in order to prove the satisfaction of the security properties. The performance of the proposed system will be compared with the other existing e-voting systems.

Index Terms: -Electronic voting, fairness, formal analysis, privacy, receipt-freeness, security, verifiability.

1 INTRODUCTION

FREE and fair elections and voting are the essential ingredients for a democratic nation. Elections allow the populace to choose their representatives express their preferences for how they will be governed. Thus, the integrity and accuracy of election process is fundamental to the integrity of the democracy itself. Today, many new technological innovations are developing. So, e-commerce security and fair exchange including electronic voting is becoming a popular trend. Our country, Myanmar, is also trying to keep abreast with the other developed countries in every area. Therefore, scientists from Myanmar start to replace electronic voting instead of traditional paper voting for saving human resource and time. So, the implementation of secure electronic voting systems is very critical in every nation. The main goal of e-Voting is to provide voters a good environment so that voters can cast their votes with minimum cost and efforts. There are so many properties that have been proposed to make the e-Voting secure process. Some of these properties are the followings which must be satisfied.

(1). Eligibility: Only eligible voters are permitted to cast their ballots.

(2). Privacy: There is no association between voter's identification and a marked ballot.

(3). Uniqueness: No voter can cast his ballot more than once.

(4). Receipt-freeness: A voter does not gain any information (a receipt) which can be used to prove to a coercer that she voted in a certain way.

(5). Fairness: No partial result is available before the final result comes out.

(6). Verifiability: Voters can verify that their ballots are counted correctly. There are two types of verifiability: individual verifiability and universal verifiability.

(7). Uncoercibility: No voter can prove what he voted to others to prevent bribery.

(8). Efficiency: The computations can be performed within a reasonable amount of time.

There are many different types of voting systems. Among them the most general types of them are:

- Paper-Based Voting Systems
- Direct-Recording Electronic Voting Systems
- Public Network DRE Voting Systems
- Precinct Count Voting Systems
- Central Count Voting Systems

Paper-based Voting Systems (PVS): record, count, and produce a tabulation of the vote count from votes that are cast on paper cards or sheets. Voters may be allowed by some PVSs to make selections by means of electronic input devices. Such input devices do not record, store or tabulate independently voter selections.

Direct-recording Electronic (DRE) voting systems: record votes by means of a ballot display provided with mechanical or electronic optical components. Voter could activate these components. Such systems record voting data and ballot images in computer memory components. Also, data processing is achieved by the use of computer programs.

Public network DRE voting systems (PNDRE): Make use of electronic ballots and transmit vote data from the polling stations to other locations over a public network. The votes may be transmitted as individual ballots as they are cast, or periodically as batches of ballots, or as one single batch, at the end of voting.

Precinct count voting systems (PCVS): put the ballots in a tabular form at a particular place, say, a polling station. They provide mechanisms that store vote count electronically and transmit the results to a central location over public telecommunication networks.

Central count voting systems (CCVS): Tabulate ballots from multiple precincts at a central location. Voted ballots are safely stored temporarily at the polling station. These ballots are then transported or transmitted to a central counting location. CCVSs may, in some cases, produce printed reports on the vote count. The aim of this paper is to develop an electronic voting system which can be used for university campus election and provides security and trusted properties. And then the system properties will be formally analyzed.

Related works of the research are described in section 2. In section 3, the proposed system is stated. The system will be analyzed in section 4. The expected outcomes are in section 5 and section 6 will state the application areas of this research. The last section will conclude this paper.

2 Related Work

The major and general stages of an election process are registration, voting and counting. In order to computerize the whole election process from start to finish, there are many security and technical problems that must be addressed. There are three main kinds of electronic voting system implementation in the literature: mixnets, blind signature scheme and homomorphic encryption. The mixnet shuffles all possible votes and provides a proof of correctness of shuffling and a proof of the ordering of the voter, over secure, untappable channels. The voter submits the vote corresponding to her choice to the mixnet for the counter. In blind signature scheme, the voter first obtains a token, which is a message blindly signed by the administrator and known only to the voter herself. The signature of the administrator confirms the voter's eligibility to vote. She later sends her vote anonymously, with this token as proof of eligibility. Homomorphic public-key cryptosystems exhibit a particularly interesting algebraic property: when two ciphertexts are combined in a specific, publicly-computable fashion, the resulting ciphertext encodes the combination of the underlying plaintexts under a specific group operation, usually multiplication or addition. An immediate consequence of a cryptosystem's homomorphic property is its ability to perform re-encryption: given a ciphertext , anyone can create a different ciphertext that encodes the same plaintext. The malleability of ciphertexts in homomorphic cryptosystems limits the security of such schemes. Steve Kremer and Mark Ryan analyzed the well known FOO92 voting protocol in the applied pi calculus. The FOO92 protocol is modeled in applied pi calculus. Their research formalized three of its expected properties, namely fairness, eligibility and privacy. They used Pro Verif tool to prove that the first two properties are satisfied. In the case of third property, Pro Verif is unable to prove it directly, because its ability to prove observational equivalence between processes is not complete. They provide a manual proof of the required equivalence. V. Kalaichelvi and R.M. Chandrasekaran designed and analyzed a secure electronic voting protocol. This scheme did not require a special voting channel and communication can occur entirely over the current internet. 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 consume less time. This study also analyzed the security issues involved in an electronic voting. Ishtiaque Mahmud and Israt Jahan developed a model for describing the real life environment where voting takes place and analyze the behavior of rational adversaries. They analyzed adversarial behavior by using attack tree method. This system tried to reduce large scale attacks that will help students and researchers to realize the e-voting and security system. The system also eliminated the voting process of non-eligible voters. Subariah Ibrahim, Maznah Kamat, Mazleena Salleh, Shah Rizan Abdul Aziz developed an electronic voting system for a general election. In this system, voter's privacy is guaranteed by using a blind signature for confidentiality and voter's digital signature for voter's authentication. Hamid Reza and Hashem Haghighat presented a paper which focuses on verification of authentication-type properties of an e-voting protocol. The well-known FOO92 e-voting protocol is analyzed, as a case study, against the uniqueness and eligibility properties and their satisfaction are verified. By means of an automated formal approach, the protocol is modeled in the mCRL2 language. Then, the eligibility and uniqueness properties as two authentication-type requirements are modeled in the modal μ-calculus. These are given to a combination of dedicated mCRL2 tools to verify the properties.

3 Proposed System

The paper will propose an electronic voting system which will include the following stages: Voter list creation, List announcement, Registration, Authentication, Voting, Counting or tallying and Result announcement. The proposed system is described in figure 1. After the system is implemented, it will be formally analyzed using formal specification language mCRL2 in order to prove its security. Figure 1 describes the proposed system architecture.

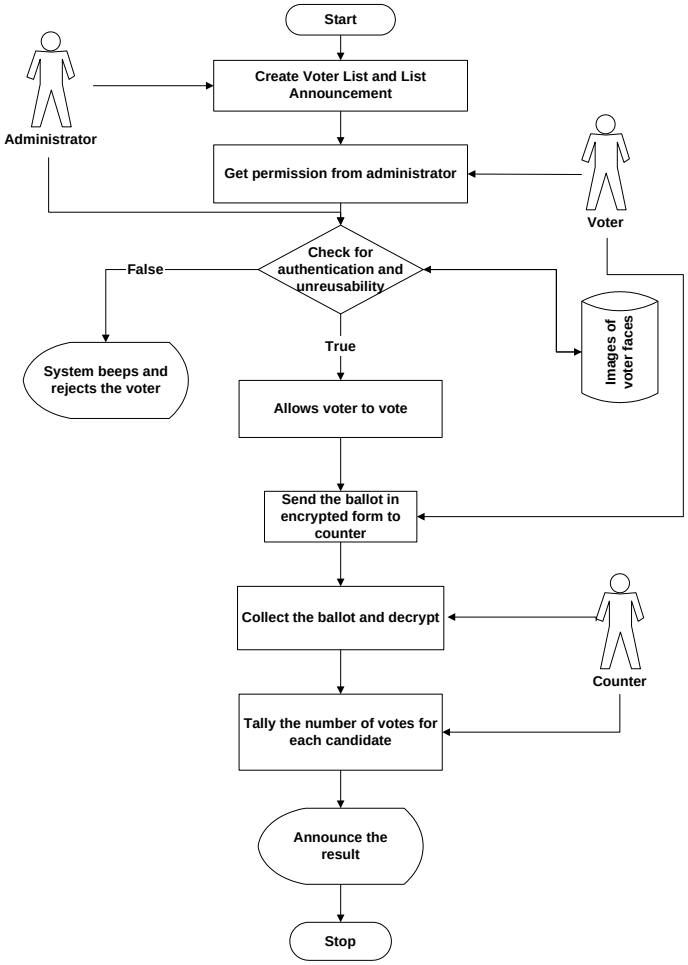

Fig.1. Proposed System Architecture

6.1 Voter List Creation and List Announcement

The first step in voting process is collecting census. In the proposed system, the data of the students from a university campus is collected for electing the pilot among nominated candidates. The voter list and the pseudo ID of legitimate

voters are stored in a database for use in checking authentication. After completing the voter list creation, the eligible voter list is announced. This step is done by the administrator.

6.2 Registration

The persons who want to vote need to register to be able to vote. The voters must send their personal data including voter name and voter ID to the authorization party in order to be checked for validity.

6.3 Authentication

The authorization party checks for validity of each voter by using the data retained in database. If the voter is authenticated, the administrator sends acknowledgement with his signature on the voter's pseudo ID. The pseudo ID of the voter will be produced on the real ID by the use of pseudo random number generator. The signature of the administrator will be produced by the use of Digital Signature Algorithm (DSA). If the voter is not authenticated person, the system will beep and reject the voter.

DSA Signatures: The Digital Signature Algorithm (DSA) is a widely used US Federal Government standard for digital signatures. The public parameters (p, q, g) and the key pairs (x, y) are identical to an ElGamal cryptosystem. If m denotes the message to sign and H(m) $\in$ Zq a cryptographic hash code of m, then a DSA signature of m is a pair with

$$a = (g^r \bmod p) \bmod q,$$

$$b = (H(m) + a \cdot x) \cdot r^{-1} \bmod q,$$

and randomness r $\in$ Zq. A given signature s = (a, b) can be verified by checking if the equation $a = (g^u \cdot y^v \bmod p) \bmod q$ holds for $u = H(m) \cdot b^{-1} \bmod q$ and $v = a.b^{-1} \bmod q$. The signature verification is denoted by $Verify_y$ (s, m) $\in$ {true, false}.

6.3 Voting

After getting permission from the administrator, the authenticated voter sends his ballot in encrypted form to the counter along with the key. In this stage, the voter will use his pseudo ID signed by the administrator in order to preserve privacy and eligibility. RSA public key encryption algorithm will be used for security and more obscurity.

6.4 Counting

The counter collects the encrypted ballots and decrypts them. The proposed system will include two talliers: one for total count of all the candidates and another for the beloved candidate of the corresponding voter. After receiving the ballot from the voter, the counter will increment the total count and the corresponding candidate vote count. After the final count is done, the counter is ready to announce the result.

6.5 Result Announcement

Final stage of voting process is result announcement. When the election deadline is over, the final result will be announced by the counter or tallier. This is important for universal and individual verifiability. The voters can verify their votes by checking the final announcement. The final result must conform to the real votes.

4 System Design and Analysis

The proposed system will include database for keeping track of candidates and voters. The database management system will manage the database. The proposed system will describe a prototype of a real polling station. The proposed system will be analyzed using mCRL2 language in order to prove that the required security properties of an electronic voting system are satisfied. mCRL2 is formal a specification language that can be used to specify and analyze the behavior of distributed systems and protocols. mCRL2 is based on the Algebra of Communicating Processes (ACP) which is extended to include data and time.

In general, the following steps are involved in the analysis of a system with mCRL2:

- A specification of the system's behavior is written in the mCRL2 language.
- This specification is converted to a Linear Process Specification (LPS).
- An LPS is an mCRL2 specification in a stricter format.
- The LPS can be modified or simplified using various manipulation tools and can be simulated using various simulation tools.
- A Labelled Transition System (LTS) or state space can be generated from the modified LPS. Subsequently, this LTS can be analyzed for errors using model checking techniques [8].

5 Expected Outcomes

This paper aims to design and implement a real application for electronic voting system. After implementing the electronic voting system, the security properties of the electronic voting system will be formally analyzed. The proposed system will satisfy the important properties: receipt-freeness and verifiability. Moreover, a comparative analysis with the other electronic voting system will be performed. The proposed system will reduce or remove unwanted human errors.

6 Application Area

This proposed system can be used in electronic voting systems to replace traditional paper voting. This study will be useful in preserving the important security properties of an electronic voting system.

7 Conclusion

This paper describes the types of electronic voting systems and essential security properties of electronic voting systems. The proposed system will implement a secure electronic voting system which satisfies the required properties. Finally, the system will be formally analyzed by formal specification language mCRL2.

ACKNOWLEDGMENT

The author would like to express her special thanks to her supervisor, Dr. Aye Moe Aung, for her invaluable guidance and kind supervisions. The author would also thank to her parents and all the teachers who taught her throughout the whole life.

REFERENCES

[1] Subariah Ibrahim, Maznah Kamat, Mazleena Salleh, Shah Rizar, Abdul Aziz, "Secure E-voting with Blind Signature", 2006.

[2] Ishtiaque Mahmud, Shamim Ahmed, A.K.M Nazmus Sakib, Quaz Emanual Alende, Israt Jahan "E-voting Security Protocol: Analysis and Solution" International Journal of Engineering Research and Application (IJERA) Vol. 2, Issue 3, May-June 2012, 2938-2943

[3] V.Kalaichevi and R.M. Chandrasekaran, "Design and Analysis of Secure Electronic Voting Protocol", Journal of Engineering and Applied Sciences 7(2), 143-147, 2012

[4] Fujioka, Okamato, Ohta, " A Practical Secret Voting Scheme for Large Scale Election", 1992.

[5] Hamid Reeza Mahrooghi, Mohamad Hashem Haghighat, Rasool Jalili, "Formal Analysis of Authentication Type Properties of an Electronic Voting Protocol using mCRL2, 2010.

[6] Feras A.Haziemeh, Mutaz Kh.Khazaaleh, Khairall M.Al-Talafha, "New Applied E-voting System", 2011.

[7] Jan Friso Groote and Mohammad Reza Mousavi, Department of Computer Science, Eindhoven University of Technology, Eindhoven, "Modelling and Analysis of Communicating Systems", 2011.

[8] J.F. Groote, Aad Mathijssen, Michel Reniers, Yaroslav, Usenko and Muck van Weerdenburg, "Formal Specification Language, mCRL2", 2007.

[9] David Chaum, "Blind Signature for Untraceable Payment". 1982