Securing a Scalable E-Voting System Using the RSA Algorithm: The Case of a Group Voting Process in a Tertiary School

Stephen Gbenga Fashoto\textsuperscript{1}, Michael Adeyeye\textsuperscript{2}, Faith-Michael Emeka Uzoka\textsuperscript{3} and Fatima Hamza Usthman\textsuperscript{4}

\textsuperscript{1}. Department of Computer Science, Kampala International University, Kasanga, Kampala, Uganda
\textsuperscript{2}. Faculty of Mathematics, Physical Sciences and Life Sciences, Sheridan College, Perth, Australia
\textsuperscript{3}. Department of Computer Science and Information Systems, Mount Royal University, Calgary, Canada
\textsuperscript{4}. Department of Computer Science, Alhikmah University, Ilorin, Kwara State, Nigeria

Abstract: E-voting (electronic voting) is a significant part of an E-election (electronic election), which refers to the use of computers or computerized voting equipment to cast ballots in an election. Due to the rapid growth of computer technologies and advances in cryptographic techniques, E-voting is now an applicable alternative for many non-governmental elections. However, security demands are paramount to electoral process in political arena. It was revealed that researchers show little interest in robustness of E-voting system compared to other E-voting requirements [1]. This paper shows that RSA (Ron Rivest, Adi Shamir and Leonard Adleman) cryptography algorithm can be incorporated into E-voting process as a whole. The RSA cryptography algorithm ensures that votes casted are secured, thus maintaining the privacy of votes. The performance of the cryptography algorithm is tested on a university E-voting system over a public network. The E-voting process is initiated by a server system that other computer nodes are connected to. The system is such that when the votes are cast on the nodes, the RSA technique encrypts the vote that is sent to the server system using both node and vote identity number. The system performs consistently and reliably which in return gives good level of confidence of votes count.

Key words: Cryptography, RSA algorithm, E-voting, paper ballot.

1. Introduction

E-voting is recording, storing and processing of electoral data of a voting system as digital information [2]. E-voting system is employed to enable stress-free election and increase the attendance at polls like in Austrian Students Association in 2009 and Estonia Parliamentary Election in 2007 [3]. Although a wide variety of E-voting systems exist, the basic process of any electronic election is almost the same. O. Cetinkaya and D. Cetinkaya [4] explained that any E-voting system should include the following entities.

(1) Voter: is an entity with voting right and possibility casts a vote in the election.
(2) Registration Authorities: are entities with power to register eligible voters before the day of election. The registration authorities also ensure that only registered voters can vote and each voter is entitled to a single vote on the day of election. Registration authorities may be registrar, authenticator, authorizer, ballot distributor or key generator.

(3) Tallying Authorities: are entities that collect cast votes and tally results of the election. The tallying authorities may be counter, collector or tallier.

The E-voting system involves these four phases: registration, authentication, voting and tallying as shown in Fig. 1.

Registration: is the act of registering voters by registration authorities and compilation of list of eligible voters before the day of election;
Fig. 1 A typical E-voting process [4].

- Authentication/Authorization: is the verification of credentials of those attempting to vote and permission of eligible registered voters;
- Voting: is the process of casting votes by eligible voters;
- Tallying: is the counting of votes by the tallying authorities and announcement of election results.

Cryptography conceals and protects integrity of information being transferred. Cryptography deals with the construction and analysis of protocols to overcome the influence of third parties and ensure the security of communications [5]. Cryptography relates to several aspects of information security such as confidentiality, data integrity, authentication and non-repudiation.

1.1 Problem Statements

In several electoral processes, the following challenges have been identified.

1. Inaccuracy and inconsistency in number of votes. In paper ballot voting system, elections are easily rigged and votes are usually manipulated by malicious elements which consequently lead to an inaccurate number of votes.

2. Violation of voters’ privacy. As voters cast votes on a receipt E-voting system, the voters’ credentials are printed by E-voting system on a paper-format which reveals the voter’s identity and how voters cast their vote.

3. Improper verification and validation. Most elections on E-voting systems are usually not tested in compliance with required standard as to whether they perform intended functions.

4. Low voter turnout. In paper ballot voting system, optimal voter turnout is not usually achievable. The use of E-voting systems helps eliminate this challenge by providing adequate convenience to voters.

It is therefore important to design a robust voting system that addresses and eliminates these challenges.

2. Literature Review

E-voting has come to limelight with the rapid growth in computer and information technology. It is an integral aspect of e-election (electronic election). E-voting is the use of computers or computerized voting equipments to cast ballots in an election. It is quite an important part of the most current political scene, though not limited to politics [4]. Application of E-voting exists in various environments such as government, parliaments, academia and industry [6].

The E-voting system is a technological advancement of the ICT (information and
communications technologies) to improve electoral process. Due to this advancement, many applauses as well as criticism have been made concerning the E-voting system. Many proponents of technology agree that computers by nature are more accurate, efficient and reliable than humans while others are of the opinion that the exclusion of human involvement out of the voting process will likely lead to errors that will pass unnoticed [7]. Some people are even of the opinion that the E-voting system is quite complex and that the physical ballots can provide better audit trails than purely electronic systems [8]. The central question relates to the physical representation of the paper ballot and its virtual equivalent in the E-voting system that is, the paper ballot system is more transparent as it can be monitored by anyone at any stage of the voting process when compared to its virtual “e-vote” in the E-voting system.

The E-voting system presents several benefits that outweigh the arguments presented against it. Remmert [9] considered reasons why an E-voting system is implemented in political election or referendum in Europe and these include:

1. Enabling voters cast votes from a location other than the polling station in their voting district;
2. Enabling each voter casts his/her vote with ease and convenience;
3. Enhancing broad participation in elections and referendum for all those who are eligible particularly for citizens not within the physical geographical region;
4. Widening access to voters with disabilities or those having other difficulties in being physically present at a polling station and using the devices available there;
5. Increasing voter turnout by providing additional voting channels;
6. Bringing voting in line with new developments in society and the increasing use of new technologies as a medium for communication and civic engagement in pursuit of democracy;
7. Reducing, over time, the overall cost to the electoral authorities of conducting an election;
8. Delivering voting results reliable and more quickly;
9. Providing the electorate with a better service in pursuit of democracy, by offering a variety of voting channels.

The descriptive representation of E-voting system architecture is shown in Fig. 2.

2.1 E-Voting Requirements

The following are the basic E-voting requirements [2, 4]:

Privacy: It is the inability to link a voter to a vote. The privacy of voters must be preserved during the election as well as after the election.

Eligibility: Each voter is validated before participation in election. Each voter should register before the day of election and only registered eligible voters can cast votes.

Uniqueness: Each voter should be entitled to a single vote. It is important to note that uniqueness does not mean un-reusability, where voters should not vote more than once.

Uncoercibility: Any coercer, even the authorities, should not be able to extract the value of the vote and should not be able to coerce a voter to cast his vote in a particular way. Voters must be able to vote freely.

Receipt-freeness: It is the inability to know what the vote is. Voters must neither be able to obtain nor construct a receipt which can prove the content of their vote to a third party both during and after the election. This is to prevent vote buying or selling.

Fairness: No partial tally is revealed before the end of the voting period to ensure that all candidates are given a fair decision. Even the counter authority should not be able to have any idea about the results.

Transparency: The whole voting process must be transparent. Bulletin boards may be used to publicize the election process. Voters should be able to possess a general understanding of the whole process.
Securing a Scalable E-Voting System Using the RSA Algorithm  
The Case of a Group Voting Process in a Tertiary School

Fig. 2  E-voting system architecture [2].

Accuracy: All cast votes should be counted correctly. Any vote cannot be altered, deleted, invalidated or copied. Any attack on the votes should be detected. The uniqueness should also be satisfied for accuracy.

Robustness: In order to achieve confidence of voters in election results, the robustness should be ensured. However, there are numerous ways for corruption. For instance, registration authorities may cheat by allowing ineligible voters to register. Also, ineligible voters may register under the name of someone else. The ballot boxes, ballots and vote counting machines may be compromised. To combat all of these inadequacies, the system has to be to a good extent fault tolerant.

Cost-effectiveness: Systems should be affordable to purchase by the electoral commissions and must be efficient.

Convenience: Voters should be able to cast votes with minimal equipment and with little or no assistance.

Auditability: There should be reliable and demonstrably authentic election.

Verifiability: It should be possible to verify that votes are correctly counted for in the final tally.

2.2 Some Barriers to E-Voting

As observed by Gritzalis [2], the following are some of the barriers to E-voting:

1. Lack of common voting system standards across nations;
2. Time and difficulty of changing national election laws;
3. Time and cost of certifying a voting system;
4. Security and reliability of electronic voting;
5. Equal access to Internet voting for all socioeconomic groups;
6. Difficulty of training election judges on a new system;
7. Political risk associated with trying a new voting system;
8. Need for security and election experts.

3. Methodology

The problems in the section above are systematically addressed as follows. The literatures on E-voting and E-voting systems that implement cryptography are thoroughly considered. A specific
Cryptographic algorithm, RSA, is chosen to secure the E-voting system. The RSA algorithm is implemented using three steps: key generation, encryption and decryption. Then, flowchart to describe the working of E-voting system and incorporated RSA algorithm is presented. The verification and validation check is performed at each stage of the E-voting system design.

3.1 Description of the Existing System: Paper Ballot

The paper ballot voting system is the type of voting system in which votes are cast on a piece of paper and are dropped in a ballot box, ensuring the secrecy of votes. The system is basically made up of ballot boxes and printed paper ballot, on which the names and parties of the nominated candidates appear. Voters can vote for the candidates of their choice on the paper ballot as shown in Fig. 3. The voting system is set up at the polling stations on the Election Day for voters/candidates to cast their votes.

3.2 Evaluation of the Paper Ballot System

The present voting system used for conducting the RUNMASS (Redeemer’s University Mathematical Students Society) is the paper-ballot system. The voting process includes the following:

Voter: is any current member of the departmental students’ society.

Registration Authorities: these are the departmental students’ society electoral committee; they register the voters (on a paper) and give them the paper ballot before the voters proceed to the ballot box and cast their votes sequentially in the box.

Supervisory Authorities: one or two delegates from the university’s student association electoral commission are present at each polling station to supervise the election.

Tallying Authorities: these include the university’s student association electoral commission chairman, the supervisory authorities and the registration authorities. They collect the cast votes and tally the results of the election.

On the Election day, the student voter goes to the polling station and is authenticated by their ID (Identification) Card by the registration authorities. After being authenticated, the voters are authorized to vote and are registered with the registration authorities, who give them the paper ballot to cast their votes. The
voter makes his/her choice on the paper ballot and then drops the ballot into the ballot box in the presence of one or more of the registration authorities.

At the end of the election period, the ballot boxes are taken to the university students’ election commission office by the registration authorities, accompanied by the supervisory authorities for tallying. The ballot boxes are then opened and the votes are counted manually by the electoral commission chairman, with at least two of the registration authorities and one of the supervisory authorities (all making up the tallying authority), recording the counts of the votes on paper via the tally system. The results are compiled, released and announced to the students’ society.

3.3 Benefits of the Paper Ballot System

The system preserves the privacy of the voter as no voter can be linked to its vote. It is transparent because the voters and candidates can easily believe and accept the election results as being authentic since the tallying authorities is comprised of trustworthy personnel.

3.4 Problems of the Paper Ballot System

Cost: The overall cost of conducting the election is expensive. The cost of buying and printing of ballot papers etc.

Labour: The process of counting/tallying of the ballots is sometimes tedious and tiring.

Inaccurate Result: The election results may not be perfectly accurate (one or more counts may be missed in the counting/tallying process).

Malicious Votes Cast: Multiple votes can be counted for a voter who maliciously voted more than once without being identified by the Election Authorities.

Election Result: The release time of result is not immediate. The result of the election may take quite a while to be released and announced due to the manual counting process.

3.5 Overview of the New System

The proposed new system for conducting elections for RUNMASS is an E-voting system. The E-voting system, as defined by O. Cetinkaya and D. Cetinkaya [4], is the use of computers or computerized voting equipment to cast ballots in an election.

The E-voting system is a Direct Recording Electronic (DRE) voting system using a public network. A Public network DRE voting system, as defined by Ofori-Dwumfu and Paatey [10], is an E-voting system that makes use of electronic ballots and transmit vote data from the nodes at the polling stations to other locations over a public network. In ref. [10], it was explained further that the votes in a public network DRE voting system may be transmitted as individual ballots (that is, as they are cast) or periodically as batches of ballots or as a single batch at the end of the whole voting process.

The E-voting system, shown in Fig. 4, consists of a series of microcomputers, with one of them being the main system, “The Master Tallier”. The votes casted on the other computers (the nodes) are transmitted to the “Master Tallier” immediately after voting and counted. Each node used for voting also has its own counter or tallier to track the number of votes. Thus, at the end of the election, the votes on the individual nodes are compared to that of the “Master Tallier” to verify the accuracy of the tallied votes.

The E-voting system consists of the front-end and the backend interfaces. As a proof of concept, prevalent technologies have been used to demonstrate how E-voting can be achieved. The prevalent technologies are programming tools and languages, such as MySQL, Netbeans, Phpmyadmin and Java. The RSA algorithm, which secures the votes, works through the front end and backend interfaces.

JDK (Java Development Kit) using Netbeans IDE 6.8 is used to develop the front end design of the system which is a GUI (graphical user interface).
Fig. 4  Overview of the new system.

The Back end design is a database developed by MYSQL using Wamp Server's with phpMyAdmin.

The database contains the basic details of every current member of the Mathematical Students Society. The details are:
- Name of the Student;
- Matriculation Number of the Student;
- Gender of the Student;
- Level of the Student.

The database contains additional details, strictly for the candidates of the election:
- Position the candidate is vying for;
- A Picture (soft copy) of the candidate.
3.6 The Security of the E-Voting System

The security of the E-voting system is very essential in the development/building of an E-voting system. The voters need to be assured that votes cast are correctly recorded and not interfered with or modified by any force such as adversary program or computer viruses. This E-voting system employs the RSA algorithm to secure its data (votes) as they are cast as well as they are recorded.

Asymmetric or public key cryptosystems separates the capacities of encryption and decryption. These systems make use of two keys, a private key that should be kept secret, and a public key that can be published. Each pair of keys has the following properties: (a) Anything encrypted with one key can be decrypted with the other key; (b) Given the public key it is computationally infeasible to discover the private key. In order for a user A to send a private message to another user B, A has to look up the public key of B and use it to encrypt the message. The message can only be decrypted with the corresponding private key, which is only known by the user B. With two keys, one secret and one public, a major problem with symmetric cryptosystems can be solved, namely key distribution. Asymmetric cryptosystem can also be used for authentication. Any user can sign a message by encrypting it with own private key. Any recipients can the decrypt the message with the corresponding public key and verify the sender [11]. RSA is an example of an asymmetric cryptosystem.

The application of the RSA algorithm is extensively used for digital signature and key exchange. It, a subset of the RSA algorithm, is also used in hardware devices such as smart cards. The RSA algorithm performs session key encryption for message integrity and uses message hashing to protect digital signature [12]. The RSA algorithm is employed for the following reasons because:

- It has a high practical application and is used in a variety of software products [12];
- The encryption security has a large range of number, thus easing computational difficulty [13];
- RSA Laboratories have published challenges for breaking RSA encryption. The challenges involve factoring \( n \) of a particular size to find the two factors \( p \) and \( q \). The intent was to track the cutting edge in integer factorization, and thus to give an indication of which key sizes that are still safe. The largest number to be factored consisted of 200 decimal digits, or 663 bits, and took 18 months with an unspecified number of computers [14].

The DES (data encryption standard) was a widely used symmetric encryption technique, but it is now regarded as insecure because a brute force attack is practically feasible. In the early 1970’s the U.S NBS (National Bureau of Standards) recognized the need for protecting sensitive data. Cryptography was historically studied extensively at the Department of Defense and the Department of State but the very nature of the information they were encrypting made it difficult to release any material used there to the general public. Therefore NBS was assigned the responsibility of developing an encryption algorithm that would be standardized and released publically. NBS contracted IBM, which continued their work on the algorithm Lucifer, and in 1976 the algorithm was standardized and named Data Encryption Standard, DES. During development, IBM worked with the NSA (National Security Agency) which was responsible for analyzing the strength of the algorithm [14].

DES is a block cipher using blocks of 64 bits and using substitution and permutation to encrypt data. These two techniques are applied in sequence and then the procedure is repeated for 16 rounds, or cycles. The algorithm makes use of a 64 bit key, although only 56 bits are actually used for encryption; the remaining 8 bits are often used as a checksum or may even be discarded. Due to the secrecy imposed on the development by NSA, details regarding the design of the algorithm were not publically released for many years. This led to speculations that the NSA had
Securing a Scalable E-Voting System Using the RSA Algorithm  
The Case of a Group Voting Process in a Tertiary School

included “back doors” in the algorithm in order for the agency to easily decrypt messages. But the design principles were released as differential cryptanalysis were developed and published in 1990 in a paper by Eli and Adi [15], and even extensive public scrutiny has not found anything that could indicate a back door.

The most serious question regarding the security of the DES is the length of the key used in the algorithm. As mentioned before, the length of a key determines how many possible keys there are. DES uses a key with the fixed size of 56 bits, thus there exist 256 possible keys. Diffie and Hellman [16] argued that a 56 bit key was too short. With the hardware available in 1977 it was unfeasible to conduct an extensive search but they argued that over time more powerful hardware would eventually surpass the strength of DES. Twenty years later, a team of researchers won a contest sponsored by the organization RSA Security, as they broke a message encrypted with DES using extensive search. They used a distributed system consisting of at most 14,000 machines on the Internet to find the key in over four months (www.computerprivacy.org/archive/03171998-4.shtml).

3.6.1 The RSA Algorithm

The RSA is the first public-key/asymmetric algorithm and it is extensively used. It was developed and publicly described in 1977 at MIT (Massachusetts Institute of Technology) by RSA (Ron Rivest, Adi Shamir and Leonard Aldeman). It makes use of two different keys for encryption and decryption: the Public Key and the Private Key respectively [17].

According to Ref. [16], the RSA algorithm comprises of three steps namely: Key Generation, Encryption and Decryption.

Key Generation step involves generating the public key and the private key, which are used for encrypting and decrypting messages respectively. This is achieved by the following steps:

- Choose at random two distinct prime numbers (call them $p$ and $q$) that have the same bit-length. This can be effectively done with the aid of the primality test.
- Compute $n = pq$ where $n$ is the modulus for the public key and the private key;
- Compute $\phi(n) = (p-1)(q-1)$ where $\phi$ is Euler’s quotient function;
- Choose an integer (call it $e$) such that $1 < e < \phi(n)$ and also $e$ and $\phi(n)$ are relatively prime. Thus, $e$ becomes the public key exponent;
- Determine $d$, the multiplicative inverse of $e$ mod $\phi(n)$ that is,  
  $$d = e^{-1} \mod \phi(n) \text{ or } de = 1 \mod \phi(n).$$  
  Thus $d$ becomes the private key exponent.

The Public key is $(n, e)$ and the Private key is $(n, d)$. It should be noted that mod $\phi(n)$, $d$, $p$, $q$ and $\phi(n)$ must be kept secret.

For Encryption, a User A can transmit his/her public key $(n, e)$ to User B while keeping the private key secret. When User B wants to send a message $M$ to User A, he/she has to turn message $M$ into an integer $m$, such that $0 \leq m < n$ by the padding scheme (an already agreed-upon reversible protocol) and computes the cipher text $c$ as

$$c = m^e \mod n$$

Thus, User B transmits $c$ to User A.

For Decryption, User A recovers $m$ from $c$ with the aid of the private key, $d$ using the formula

$$m = c^d \mod n$$

Now having $m$, User A can recover the original message $M$ by simply reversing the padding scheme [18].

3.6.2 Adaptation of RSA Algorithm for E-Voting System and Implementation

As a voter chooses his/her candidate on the E-voting system and confirms the vote, the RSA immediately encrypts (through the public key) the vote in the Tallying Table (Tallier), so no one (not even the election officials) knows how the voter voted. At the end of the election, the encrypted votes are decrypted (through the private key) and the result of the election is revealed [24].
Step 1: For all authorized voters, $V_i$ (for $i = 1, 2, 3 \ldots$) that cast their electronic vote, $C_i$ (for $I = 1, 2, 3, \ldots$) on the E-voting system, the RSA algorithm, by the public key $(n, e)$, encrypts the whole vote, $c_i$, details of voter, $V_i$ in the Tallying table called tallier (this table stores the votes) such that no one knows voter $V_i$ and how he/she voted.

Step 2: The votes, $C_i$ remain encrypted in the Tallying table (Tallier) until the decryption command is given, which makes the private key $(n, d)$ of the RSA, decrypt the whole details of the votes, $c_i$ and reveal how the votes were cast.

This flowchart in Fig. 5 describes how the RSA algorithm works with the E-voting system. It shows how the vote $C_i$ is cast and encrypted and later, decrypted to get the details of the vote $C_i$.
4. Interface Documentation

This documentation describes the interfaces of the RUNMASS E-voting system.

The election administrator logs into the server system via this interface. The Administrator inputs its “user name” and “password” in Fig. 6 then, clicks on the “login” button and is consequently, issued access into the E-voting system (the main interface).

The main interface of the E-voting system shown in Fig. 7 is expected to be displayed first before the start of the election. Before the election is initiated, the key pairs (the public and private keys) are to be generated, basically for the purpose of securing the votes.

**The Key Generation**

On the main interface (the server system), the “edit” button is clicked and the option “Generate key pairs” is given. On clicking, the option “Generate key pairs”, the public and private keys are generated and stored in the Netbeans project file for the E-voting system.

![Admin login interface (server system).](image)

![The main interface.](image)
As seen in the Fig. 8, the next step to starting a new election is to click the “New Election” button, which pops out a dialog box, signifying that the Election Administrator should input the number of posts that are available for the election. After the number of posts available had been specified, MySQL generates tables for each of the posts under the “Post Table” and thus, there is a pop up (a form) called the “Election Post Entry”, in which the posts are entered into.

After the entry of the posts has been made, the “add” button, in Fig. 9, is clicked and MySQL applies the given post names to the tables it had created.
The succeeding step is to add the candidate’s details to the database table called “Candidate Table”. This is initiated by clicking on the “Add Candidate” button in Fig. 10 on the main interface, which pops up a form to fill in the required details of the candidates. These details include the “post” the candidates are vying for and this makes MySQL relate the “Candidate Table” to the “Post Table” in order to establish the post each candidate is actually vying for.

Note that for this system, all the students of RUNMASS (the voters) are all registered for the election because their details have been inputted and stored in the database (on the “Voters_Table”); there is no need for any form of individual registration of the voters for the election again.

On the nodes (where the voters cast their votes), the election administrator clicks on the “File” button in Fig. 11 on the Admin User Interface and chooses the option “Set Central IP address” to input the IP address of the Server system into the node system; this is to establish that the nodes are connected with the Server system over a Public network. After this, the Election Administrator logs into the system with his/her User name and Password.

Consequently, the voters go to the nodes of the E-voting system to cast their votes. The user click the “vote” button on the Main interface of the node in Fig. 12 and then, a dialog box named “Voters Confirmation” pops up. All the voter needs to input is his/her Matriculation Number and press “Enter”; the remaining details of the voter will be revealed and the voter can then click the “Confirm” button to certify that his/her details are correct.

The “Voter Card” will be the output of the voter confirming his/her details. The Voter Card contains the posts and the details of the candidates vying for...
Securing a Scalable E-Voting System Using the RSA Algorithm
The Case of a Group Voting Process in a Tertiary School

Fig. 11  Configuring the nodes with the Server system over a public network.

Fig. 12  The voting interface (voter authentication to vote).

the post, that is, their names and pictures. The voter can thus vote for his/her candidate and consequently, lick the “Cast Vote” button in Fig. 13 to send the vote into the database. The RSA algorithm (Primary Key) encrypts the vote and stores it in the database so that no one knows the details of the casted vote.

At the end of the election, the election administrator clicks on the button “Vote Statistics” in Fig. 14 to view the election results (still in cipher text). The election administrator then clicks on “Decrypt” button to view the election result in plain text (performed by the RSA Private Key). The election result only reveals the ID number and name of the candidate voted for, thus, ensuring the secrecy of the identity of the voter. Thus, the election result can then be printed out and published.
Securing a Scalable E-Voting System Using the RSA Algorithm
The Case of a Group Voting Process in a Tertiary School

Fig. 13  Voter's card.

Fig. 14  RSA-encrypted vote result (via RSA public key).
5. Conclusions

This study shows how cryptography can be incorporated into the E-voting process, in order to ensure that the integrity of the process is preserved, and that privacy is maintained with respect to votes cast. The RUNMASS E-voting system works over a public network, initiated by a server system that other computers (nodes) are connected to. The system is such that when the votes are cast at the nodes, the RSA algorithm encrypts the votes before transmission to the server, with the identification information on the transmitting node. This in return, generates a high level of confidence in the electoral process.

There have been encrypted E-voting systems in literature. However, the use of E-voting systems in micro settings (e.g. in university students’ union elections) is not very common, especially in developing countries. The RUNMASS E-voting system ensures that the votes cast are secured, while anonymity and privacy are maintained. Unlike the E-voting system developed by RU (Rice University) called votebox (which has a few usability concerns), the RUNMASS E-voting system has been evaluated by users as being user friendly and secure. The RUNMASS E-voting system is capable of running on different platforms, such as: Windows, Macintosh, Unix and Linux operating systems, unlike some other university based E-voting systems (e.g. UCL (University College London) E-voting system and the RU system), which can only be used when integrated with Microsoft PowerPoint on both PCs (Personal Computers) and MACs (Macintosh).

While the RUNMASS E-voting system is capable of protecting voter’s identity and ensuring integrity of the voting process, the system has not been tested in a data intensive environment. The scalability and strength of the system is yet to be determined, since there was no stress test on the system. However, it forms an initial basis of applying security strict security algorithms in E-voting environments, especially in small to medium group settings.

References

Securing a Scalable E-Voting System Using the RSA Algorithm
The Case of a Group Voting Process in a Tertiary School

Johor, Malaysia.


