Analysis Cryptographic for Electronic Votes in Systems of Distributed Architectures

Segundo Moisés Toapanta Toapanta¹, a, Nathaly Vanessa Orellana Vélez¹, b, Danny Wilfrido Barona Valencia¹, c, Luis Enrique Mafla Gallegos², d

¹Computer Science Department, Universidad Politécnica Salesiana Ecuador, Robles 107 Chambers, Guayas, Guayaquil, 042590630, Ecuador
²Faculty of Engineering Systems, Escuela Politécnica Nacional, Ladrón de Guevara E11-253, Quito, Pichincha, 022976300, Ecuador

a toapanta@ups.edu.ec, b norellanav@est.ups.edu.ec, c dbarona@ups.edu.ec, d enrique.mafla@epn.edu.ec

Keywords: electronic voting, security, voting platform, cryptography, Smartmatic, privacy, ballots.

Abstract: It was considered that electronic voting is revolutionary around the world because of the new technological trends that are improving over time with their security and privacy in the different voting platforms; this problem is notable in all underdeveloped countries. The objective is to analyze and determine a cryptographic system to improve the security with efficiency and effectiveness in the electoral processes at the moment of paying and having a vote count, maintaining the transparency and integrity of the data. The deductive method was used to analyze the different cryptographic algorithms used in electronic votes that provide greater knowledge in the new trends of electronic votes. It was determined the operation of the Smartmatic that allows to identify the methods when making the electronic votes around the world, each of these systems implements an exclusive security for their voting systems, so that the voter carries out the action of paying and this vote is keep intact and transparent for the system and for the general public, achieving high reliability and integrity of the data, in addition a change in society will be noted, promoting democracy and honesty. It was concluded that electronic votes show a high level of trust, although this depends on the age and education of the voter who must have some knowledge in the field of computer science, this refers to the elderly who sometimes do not have the comfort and adequate confidence in many cases. This system can be an alternative to implement electronic voting in Ecuador to improve democracy.

1. Introduction

Currently, electronic votes are becoming more profitable for many developing countries, so we must take into account the cryptographic methods that maintain the information integrity to protect
and have consistency of the data when making a vote count giving anonymity and reliability of the voter when carrying out the suffrage [1]. The electronic voting systems that have been successful are because they are adapted to meet the specific requirements of a jurisdiction or country in which it will operate [2]. Certain countries are familiar with using ballots instead of electronic votes [3], problem that occurs is that there is no standard cryptographic system, to choose it according to our environment [4].

Why implement electronic voting in Ecuador using secure cryptography? Because in Ecuador, the system of printed ballots is used, which is a method that entails many shortcomings from corruption by altering the ballots[5][6], to environmental problems when using logging for the impressions of ballots and more tools for these processes, with the change that is made by using electronic voting systems open more security for the voter, with a cryptographic system we can have greater security by knowing the processes that will be carried out without alterations or loss of information.

The objective of this analysis is to understand the use of electronic votes in a safe way and the management of them in order to have a centralized distributed system for the admission of the same. Electronic voting is essential to avoid some kind of fraud by increasing public confidence[5].

A hypothetical deductive method is used to analyze the types of cryptographic algorithms for electronic voting to analyze the information of the referenced articles.

It turns out that the Smartmatic system has all the security advantages for the voter and the staff that manages this system to control the statistics of the votes; having a hash, electronic signature and fingerprint biometric to authenticate the voter who can try to pay in several places without this, and what the system will not allow is that the process advances because the voter made the vote in their respective place of suffrage.

It is concluded that the electronic voting systems in the world are very safe, because the results are not altered before being delivered to the controlling entity, therefore, electronic voting requires a security method that can guarantee the authenticity of the data of the voter before voting[1][7].

A robust and high speed E-voting algorithm using ElGammel CryptoSystem [8], Secure and easy internet voting [9], Secure E-voting with blind signature [10], Comparative study of electronic voting models and a proposed security framework for the implementation in Mauritius [11], From piloting to roll-out: Voting experience and trust in the first full e-election in Argentina [12], E-Voting Requirements and Implementation [13].

2. Materials and methods

2.1. Materials.

The types of security in the electronic voting of the most developed countries are analyzed in order to know the different types of cryptography with a system that should only know the result of the vote, without revealing the exact vote. In certain countries, the automated elections generate a large percentage of confidence in the electoral population, which is carried out through a safe and transparent process, eliminating the margin of human error [7] [8].

2.1.1. Traditional voting and pilot test of electronic voting in Ecuador (Latin America).

The votes in Ecuador have been made with the traditional method of printed ballots, which has caused a great negative impact on society since voters are not sure that they are accounted for correctly when making their vote, this being the first step for corruption. Certain citizens are chosen to be part of the polling station members, which before the voting day, citizens are trained to know their function depending on the role that has been assigned. After the voting, the members of the
voting table must count the votes, but in these cases there are always human errors since the votes can be altered or modified before delivery to those in charge of receiving the ballots and performing the scan.

2.1.2. Electronic votes in Argentina and Colombia (Latin America).

The pilot tests of electronic voting in Colombia and Argentina have had a great impact on society since it shows a higher level of confidence in these devices, they noticed that when interacting with the machine it gave very simple and understandable instructions, using a touch screen and showing the option to vote, this facility is given thanks to the age and knowledge of voters [12] of electronic systems in general.

The devices are used.
- Direct electronic recording (DRE)
- Optical Scanners (OS).

The touch screen reviews the list of candidates and a numeric keypad to record the vote, these machines are equipped with smart card readers as opposed to the optical scanner which gives voters a greater degree of privacy and the voter made the vote on a ballot and entered it into a scanner which showed the data that the voter selected on the screen.

At the moment that the user finishes his voting, he will not be able to change his vote since the information is stored digitally in the machine. The aforementioned devices use a VVAT (Voter Verified Audit Trail), which provides the voter to verify that the issued ballots were processed without altering the data. It was observed that the people who vote have more confidence in the DRE technology than those who use OS [1].

2.1.3. Electronic votes in Fujioka, Okamoto and Ohta (Japan).

In Japan, in several countries a system called Sensus is used, not only for electoral or political processes but also for surveys through computer networks using blind signatures, which refers to cryptographic protocols that hide the content of their data, using it for reliability and the digital signature to authenticate the voter [10], which allows the voting user who is registered, to make his vote only once. The system uses encryption algorithm like the RSA (Rivest, Shamir and Adleman) is an asymmetric algorithm, which uses a public key that is in charge of the distribution and another private one that performs the encryption of the data and keeps it secret, these algorithms are sufficiently strong so that the encrypted votes cannot be corrupted or usurped without the proper key.

![Figure 1 Schematic illustration Sensus system.](image)

Figure 1 shows the operation of how voters encrypt their votes with a public key which is sent to
the validator.

1) The function of the validator is to remove the voter's signature and verify that the voter is the registered voter, in case the verification has satisfactorily concluded this vote will be registered, this prevents the voter from taking votes consecutively.

2) The function of the indicator is to publish the encrypted file, but first the voter must send his password so that the indicator can decipher it, since this will allow the voter to confirm that his vote was counted appropriately in case the voter thinks he / she presented a fraud; The voter can protest by presenting his encrypted file or vote and the password.

3) The validator and the indicator have a very important role in this scheme because if they do not interact in a correct way they will not be able to protect the voter's data. To obtain greater security and privacy, the validator, indicator and the voter's machine must be run on separate machines[6].

2.1.4. Electronic votes in the country Switzerland (Europe).

In Switzerland-Zurich, a study was carried out from 1998 to 2006, which ended with the pilot tests of an electronic voting system developed in the same Canton mentioned. This system allows you to make the payment through cell phones thanks to a SIM card or via the Internet because in Zurich you have a dedicated VPN for this canton called LeuNet and the data that will be sent and imported will take an ELM (Electronic Marking Language) format that fits the requirements of the Swiss government. The security of this system is based on the Information Security Management System (BS7799). The encryption that is done is two steps.
- The voter's device encrypts the voter's vote and data through an SSL channel with an encryption of 1,024 bits.
- The electronic voting system is responsible for verifying the data and then re-applying another 1,024-bit encryption, so that they can be transferred to the vote storage database [9].

The steps that are carried out for the electronic voting process are shown in Figure 2.

In Figure 2, the steps are executed.
1) The voter proceeds to register in an electronic list.
2) An email will be received with a password designed exclusively for this electoral process.
3) The voter carries out the payment in any medium such as computers, PDA / WAP, or mobile

![Figure 2 Operation of electronic voting in Zurich.](image-url)
phone.
4) The voter proceeds to send the results to the voter registration software.
5) A vote counting is performed on the server’s side.
6) The votes made are shown by a statistic.

2.1.5. Electronic votes in the country Mauritius (East Africa).

The architecture used in Mauritius has been designed taking into account the environment, infrastructure, geographic size, economy and the amount of population. The system implemented is the Smartmatic model. The system adapts to different climates, and the effectiveness of this system that uses cryptography of public keys and fingerprints for voter authentication has already been demonstrated. Voters will use a touch screen on the voting machine by which they must authenticate themselves through a biometric system before gaining access to the voting system, using a network server to authenticate voters' personal information, send a list of candidates to the voters and also receive encrypted ballots with a public key.

One of the main advantages of using voting machines is the action of making counts automatically, so the risk of errors will be drastically reduced. As in most electronic voting systems this works through a distributed architecture, it will have several servers where it will distribute its processing. Servers can be both to store the incoming votes and to store credentials that validate that such person made his vote. To encrypt the data that will go to the vote count, cryptography is used to generate a public key and to decrypt the information it is done by means of a private key [11].

2.1.6. Functioning of Distributed Architecture.

A distributed system eliminates the direct physical interaction with the system since everything is handled in a virtual way, which guarantees a better process and integrity in the processes of votes managing in an adequate way so that there is no collision in the servers keeping the whole process in an equitable way[13]. This architecture is essential to apply electronic voting, this helps to distribute the processes that should have the voting, such as counting, saving receipts, save data to access the systems.

2.2. Methods

For this study, a hypothetical deductive method is applied to analyze several types of cryptographic systems and algorithms for electronic voting and in the future it can be implemented in Ecuador.

What will be done first is that all the available information will be analyzed on the different electronic voting systems and identified which would be the best option to be able to apply it for our social environment.

As a second activity, it will choose one of the algorithms and conduct a pilot for Ecuador at the time of future elections.

The main objective for the use of electronic votes, will be that there will be no difficulties of surplus votes at the time of making the counts since this new system will maintain the reliability and integrity of the data, and at the same time will be within a distributed architecture that helps to have better processing by dividing the work overload and supporting the data.

3. Results

The analysis of this research has the result of making known the different methods when making
the electronic votes, each of these systems implements an exclusive security for their voting systems, that's why the Smartmatic in Figure 3. System was taken for the durability of their equipment and saving time when counting votes. This system is perfectly coupled to the distributed architecture since, when receiving the electronic vote, the machine sends the vote to the counting center that will later be stored in a database.

![Figure 3 Operation of the Smartmatic.](image)

In Figure 3, the steps are executed.

1) The voter shows up at his meeting showing his identification.

2) The representative of the board verifies if it appears in the system, making a search in the whole register verifying the voter.

3) The voter places his finger on a fingerprint scanner, capturing it and comparing it with a previously stored fingerprint.

4) The network server will confirm the authenticity of the voter and then send the list of candidates.

5) After the voters have cast their votes and confirm their selection, the votes will be encrypted with a public key and will be transmitted through a local area network to the server of the ballot and a proof of suffrage is printed that is deposited in an amphora

6) The encrypted vote will be sent to a server that is responsible for storing all the votes

7) The votes are transferred to the server of storage of votes whose main function is to decipher the votes by means of a private key.

8) Finally, the results are shown in a statistic

Figure 4 explains how the counting of votes works at the moment of receiving them physically and electronically and the comparison that is made at the end to verify that the votes were processed satisfactorily.
4. Discussion

The main result of Smartmatic is the robustness of its equipment and its function of printing a voucher that helps to make a comparison between electronic and physical voting. What is missing in society is to have the new trends that will help people to have a new system that facilitates the counting of votes. A comparison with the other systems mentioned above is that they use different types of securities to be able to keep their votes fully integrated. The biggest consequence would be that there are people who want to manipulate and extort votes already stored in a main server.

5. Future Works and Conclusions

The agency in charge of a country's electoral elections envisaged the application of any alternative for the assurance of the integrity of the electoral data; you must define the processes using different techniques as conceptual models.

Electronic votes show a high level of trust, although this depends on the age and education of the voter who must have some knowledge in the field of information technology, especially in current technology, this refers to the elderly who do not feel the comfort and adequate confidence in many cases. By using the Smartmatic system in our society, the processes of democracy will be improved, giving the Ecuadorian people adequate confidence. This increase in democracy and the correct election of a leader by means of voting will boost the economic and industrial growth of the country. This system can be an alternative to implement electronic voting in Ecuador; once the processes for the application of Smartmatic operation have been defined.

Acknowledgments

The authors thanks to Universidad Politécnica Salesiana del Ecuador, to the research group of the Guayaquil Headquarters “Computing, Security and Information Technology for a Globalized World”
References