ASTES

Advances in Science, Technology and Engineering Systems Journal Vol. 4, No. 4, 292-299 (2019)

www.astesj.com

ASTESJ

ISSN: 2415-6698

Prototype of a Security Architecture for a System of Electronic Voting for the Ecuador

Segundo Moisés Toapanta Toapanta[*,1], Gabriel Enrique Valenzuela Ramos[1], Félix Gustavo Mendoza Quimi[1], Luis Enrique Mafla Gallegos[2]

[1]*Departamento of Computer Science, Universidad Politécnica Salesiana (UPS), Guayaquil, Ecuador*

[2]*Facultad of Systems Engineering, Escuela Politécnica Nacional of Ecuador (EPN), Quito, Ecuador*

ARTICLE INFO

Article history:
Received: 08 July, 2019
Accepted: 26 July, 2019
Online: 07 August, 2019

Keywords:
Electronic voting.
Security architecture
Cryptography

ABSTRACT

To be able to perform a better voting system, it is important to go to ICT and its various platforms designed for electoral purposes, which are being used in several countries in Latin America. In Ecuador are being used digital mechanisms during the process, but with certain errors and he is being considered to implement electronic voting, although it remains a project. The objective of this study is to analyze the prototype of a security architecture for a system of electronic voting for the Ecuador. In this study applied a quantitative, deductive, non-experimental descriptive criteria allowing to analyze the documents of reference. It was observed that the laws governing the franchise in the country have been well designed to provide facilities to the greatest number of voters, whether people with certain physical disabilities or with deprivation of liberty; In addition gives to know how to vote and the rapid counting system. It is concluded that architecture deserves a protocol that protects information throughout the electoral process and also the use of cryptographic algorithms with special software, that allows to work quickly and provide security properties, integrity and authenticity.

1. Introduction

Electronic voting is a challenge for Latin American countries and Ecuador is not far behind, we aimed to start with a pilot plan 2018, but budget cuts could not be achieved; This situation is similar to what happens in other countries of South America, because they have implemented new technologies for rapid counting and transmission of final results, but only two countries used it in its entirety, Brazil and Venezuela. This happens also in other continents; in Asia only India, uses it throughout the country, changing us, France and Canada are used in some areas or States. Other countries have been unwilling to use it, despite having the required platform. This situation reflects the complexity in the implementation of electronic voting, due to the infrastructure, as well as by the education which they must venture, both for those who wish to implement, such as citizenship, for correct use.

According to the author Pacheco, combining access to information technologies with the confidence and security in the electoral process is not an easy task; but with the increase in the recent years, Internet applications, telecommunications and audiovisual and electronic technologies, has been given a gradual change in these [1].

There are two major categories of electronic voting: face-to-face and not face to face.

Non-Presential vote. -Is that which can be done through the use of electronic devices such as the internet the computer, cell phone or other device near or far site.

Presential vote. -Is done directly in the electronic ballot box is where managed vote in traditional places.

The two types of voting are effective, but require their respective care and security protocols. So also this kind of gathering of electronic votes is done is through two ways:

- The direct recording electronic voting.
- Collection by reading eye. -Storage and automation is given up to the counting of votes and then rapid publication of results.

[*] Segundo Moisés Toapanta Toapanta, Email: stoapanta@ups.edu.ec

https://dx.doi.org/10.25046/aj040437

This leads to plant the idea of a security architecture that provides confidence to users, that the results of the elections will be not changed at the end or during the process.

2. Materials and Methods

2.1. Materials

To carry out this study we considered several scientific articles, documentary bibliography and projects inside and outside the country, which provided a contribution to the proposed topic. The author Garcia-Barrera believes that ubiquitous, cyberspace, netizens, homo digitalis, virtual communities, telematic networks, e-democracy, e-elections politica.com are terms that are presented in the glorifier speech of the new technologies, corresponding to this era post-industrial.

Al Gore, from the American Vice President, announced "the new era of democracy" and the Internet guarantees direct, global, virtual, interactive democracy by survey and electronic voting [2].

The use of ICT, platforms and knowledge of those involved in the issue, make it possible that applies a security architecture in e-voting. Also the Constitution of Ecuador provides several articles of law for the benefit of citizens, but this requires that the Government invested in different platforms, training and search for the appropriate use of these resources, to avoid results unexpected, as well as the untimely intervention of persons unrelated to the National Electoral Council (CNE) who wish to affect the system.

The articulated in the Constitution of the Republic of Ecuador, designated the duties and rights for voters, as article 62 which says: "people enjoyment of political rights have right to vote universal, equal, direct, secret and counted publicly"[3].

Likewise it is the electoral function, which is responsible for ensuring the correct fulfilment of the rights of every citizen to vote. You could also be observed that the electoral function has three bodies that are involved in electoral processes, security and the respective protocol in each vote: The National Electoral Council, the Electoral contentious Tribunal and the receiving voting together.

2.2. Methods

This study maintains an approach to quantitative, deductive logic, correlation criteria and qualitative, conducted analysis to the various revised texts. Considering the important aspects regarding e-voting, can be established a prototype of a relevant to electronic voting security architecture in the country.

The Constitution expresses the popular will or the will of the people in the electoral system, which requires certain Protocol, protection, allocation of seats and organisation so that it complies.

The author Aguirre Board, notes that in the coincidences of some forms of participation it affects the State, either because the proposed citizens obtain recognition, transform some public policy or, if possible, institutionalize procedures e instruments of political participation, to ensure the permanence or regularity of a desirable action, such as voting, require transparency in public spending and obtain accountability of rulers, etc. [4], allowing that is expand the visibility of the instruments of social expression, with the encouragement of citizen participation.

Likewise the articulated in the Constitution indicate that people with disabilities also have the indispensable right of participation in electoral processes, even new ways in which they can vote, have adapted According to their condition. At the same time they also have legislation which protects their right to suffrage adapted to his condition.

The Convention on the rights of persons with disabilities, according to the legal norms in disability in Ecuador, are local or foreign, require direct their chance to vote. The author Quesada believes that the decision of one or another form of registration is not exclusive, on the other hand, are recommended in various ways so that between them they are complementary and, in this way, to achieve greater inclusiveness of voters abroad, so is privileged that it idea previously mentioned the principle of universality [5].

Similarly, the Constitution of the Republic of Ecuador, the code of democracy and also the rules for the participation of people with disabilities, have articles which guarantee the right of the political exercise of each person. To implement electronic voting in these cases, required instruments enabled for this purpose, as well as security protocols that take care of the decision of the voters.

I) Digital voting (electronic)

Digital voting is being implemented in several States, as noted by VALVERDE, who refers to that in several countries there are three modalities for the vote: by post, personally, in the embassies or consulates or online, through internet [6]. However, according to Legorreta, the issue of the security of electronic voting may be the aspect where the lack credibility is more evident. In this sense, the technologies of e - vote are not exempt from problems [7].

The experience in Ecuador has been through phases, first implemented new technologies for the rapid count and emission results.

There was carried out a project to start e-voting and had great reception, but the plan did not continue due to high costs that demanded. There was carried out a project to start e-voting and had great reception, but the plan did not continue due to high costs that demanded. But it has not ruled out the continuity of the project, since the benefits are large.

II) Stages of e-voting

According to Montes the stages of the process of voting on a modern voting system, can be distinguished into three stages:

- Creation of the vote: the voter selects somehow among the options available and 'creates' vote, in any format.
- Anonymous receipt of voting: the vote is sheltered along with other votes to anonymize.
- Vote count: after completed the time available for voting, count the guarded votes [8].

To use the vote Electronics is required to work with citizenship and thus obtain the expected results, therefore, is important to have several requirements, such as those set out below.

3. Requirements of electronic voting

There are two prerequisites:

- The voter confidence in the proper functioning of the system.
- The ease, comfort and simplicity that present.

In addition, a digital voting system must have other requirements that must be met, among those are: guarantee the anonymity and privacy of who exercise the vote, so that each one can be done with total freedom.

Another requirement that should have a digital voting system is to be eligible and genuine, is that they can make the vote of those who are authorized, in addition to this be done only once.

Another need is that it is full, it there is no fraud in the process, i.e. that the votes may not be disposed of or much less modified.

Electronic voting is synonymous with integrity, but not during the electoral process, but before, since the pre vote also has its own requirements, which should be considered as part of the process, not in isolation, so the results will be more optimal.

Objectives of the electronic vote, should be established so that it can be evaluated, but the participation of persons designated for such purposes, must be fundamental, so will keep the integrity of the information, you can review processes and will contain limitations of access for people that are not part of the electoral institution of the country.

Table 1: Objetives

Objectives of the electronic voting	
Data Integrity	During and after the electoral process.
Audit	It may be auditable completely at any stage of the process.
Confidentiality	Integrity and no-denegation.
Security in the user interface	That the interface can be subsequently used by anyone.

The system should be, also, accurate and verifiable. All information that will be recorded along with the votes made must be very well stored. It is reliable, is to say that all data and votes that you enter are not lost that this effective operation is essential.

Which is easy to use is other requirements you must have the system so that it can be used by all persons without complications, including persons who are responsible for the scrutiny of the data.

Another proposed requirement is to not be coaccionable, i.e. that people who exert the vote may not reveal by whom or who they have voted. The author Charles Leija the vote represents the form of most widespread citizen participation and, in many cases, the only exerted by population [9].

Finally, another requirement is to be verifiable by the voter, i.e. it must verify that it exercised their right to vote.

4. Functional requirements for electronic voting: Software, network, and security.

4.1. Software requirement

They must be grouped into modules of authentication, voting, counting and results; so make your application more feasible. Each of these modules will have certain functions. Then mentioned the functions of each module, among them are:

Authentication functions:

- Regularize the participants receiving the vote tables, to verify if those who vote enabled are to cover.
- Verify that the personal data of the user (ID, name, and precinct numbers) match those registered in the database.
- Compare the list of people who have voted with those recorded in the database of the receiving Board vote.
- Generate verified lists of those who exercised their right to vote.
- Verify that the voter has enabled access to digital ballots.
- Others.

Vote modules consist of the following functions:

- Facilitate access to the candidates in the voting, also have a braille system for visually disabled people so that they can also vote.
- There should be the option to vote blank or null and that count as valid decision for the voter.
- The encryption of data and voting should be included as part of the security.
- You must include an endorsement with digital signature enabled and authorized voter.
- Availability of authentication that do not have access to vote those who are not registered.
- Have assistance of the vote in the case of people with reduced mobility.
- Immediate impression of the vote.

Counting modules consist of the following functions:

- Decoding and transfer of the feedback received.
- Generate reports of the vote that it could not decrypt.
- Do blank votes count.
- Creating reports automated with the results of the votes.
- Generate and print digital reporting based on the final results of the voting process.
- Export of results information to be able to be checked in other platforms.

All these functions must be carried out so that it can fulfil the requirement of software.

4.2. Network requirement

You need a high-performance network, also must take into account population growth, to provide vote receiver boards which may be necessary; It is necessary to consider the bandwidth and also the fault tolerance.

4.3. Security requirement

Within the safety features, Jeff Schmidt points out that while there are many important aspects that guided development, should highlight the following general characteristics of e-voting:

- Separation of the identification of the voter and the urn; both systems must be independent. All the information needed to operate must be previously loaded.
- All functions of the system should be stored in blogs that can be extracted later for audit purposes. These logs can also be used as duplicates of the documents required by the legislation in force.
- Absence of communication between devices (URN and Padrón). This prevents that you handling a system from the other and that gives greater assurance and confidence in the secrecy of the vote.
- Print proof of voting. Once the voter manifests his election will proof, that voter will see to confirm its decision to be printed and then this is deposited automatically in an urn.
- Use of free software. While it is true that access to the source code is not a guarantee of reliability, yes we can make what an application of electronic voting whose source code not be auditable must be ruled out entirely. This decision covers also the operating system on which applications will be implemented to develop [10].

There are institutions that apply systems SAFE created by CISCO, which provides defense in depth and a modular design and architecture is aimed to detect threats in the network systems.

5. Voting Counting

Incorporated by electronic vote counting systems, these, are a hit at the time of results, since the automation of data, speeds up the query and display of information. Valverde Loya opinion has as alternative of internet voting is considered fast, low cost, through a website with restricted access with individual password for each voter in each election [11].

This technological mechanism requires the review of institutions to increase confidence in the process.

5.1. Traditional and remote voting systems

According to the storage system one of the best known and currently do not use traditional calls ballots, they are DRE and OCR systems. Among the most commonly used types today are buttons, mini switches and those who have a touch screen.

It is important to consider that electronic voting poses stages to be followed, as Chungata suggests, Jussibeth (2017), raises a sequence in the Presential vote and a system of remote that it is not very different to the traditional methodology, this being the following:

5.2. Traditional or face-to-face system

This system uses your voter from locally and face-to-face, where picks up their vote by means of different methods and issued a check, this environment is completely controlled or supervised by the responsible authority that checks your process.

Within this system are used different methods, such as perforated card, electronic ballots, machines of levers or camshaft and electronic ballot boxes; These different technologies:

- Optical character recognition, or OCR readers.
- DRE electronic record direct, using touch screens for receiving and storing the chosen option. Each one differs in the form that stores the information received, directly by optical scanning or directly in memory. These systems are usually applied in developing countries, with low levels of literacy, extensive geography and ethnic diversity.

5.3. Remote system:

This method is what allows that the voter is not specifically directed at the electoral college, this often performs it in a place other than tables, this often works with a connection to internet, intranet, or any other mobile device, as the cell phone through an SMS.

With this system there is no control by the authorities at the time of issue or receive votes, so the reliability of this is highly questionable, in turn, is considered an obstacle is the lack of total internet access in households not fully Universal [12].

Finally, in accordance with the established schedule of receipt of votes, the authorities of each table will be electronic urns can be counts and issue findings in the case thus required with proper safety of the case.

6. Prevent threats on electronic voting

E-voting while it has high safety standards, however, these can become to be also violated and present certain threats.

Among them are human threats, natural and environmental threats.

According to Bast in electronic voting systems, it is necessary to protect:

- Indefinitely the privacy of the voter: even after after the election, given that where any intruder get a digital copy of rows that allow to relate the voter with their vote, would have all the time to try to figure it out. All people want to maintain their privacy assured indefinitely, and it would be very serious to be know by a voter who voted in particular. For example, knowing the trajectory as a current candidate voter could influence the electorate.

- The security of the data of the votes while lasts the electoral process: the protection of the information of the votes issued only must support the length of time that corresponds to the voting process, given that the proposed model only records the data of the votes and voters and after the scheduled time not publicly known [13], the resulting count information, i.e. the results of the election.

The characteristics of use of security processes in the use of electronic voting, being the data those who agree are vulnerable, you can see in table 2.

Table 2: Data requiring security and/or privacy

	Confidentiality	Integrity	Availability
Electoral Padron	NO	YES	YES
Votes	YES	YES	YES
Candidates	NO	YES	YES
Charges	NO	YES	YES

6.1. Encryption of data

Data are the most important elements to the moment of electronic voting, there is very personal, sensitive information that must be cared for and protected. So says Garcia that the same is true in the field of computer security in general, and on cryptography in particular. One of the reasons for this phenomenon, passes by the large increase in the volume of information available.

Any new method that appears is quickly made available a huge critical mass that assesses and generates any changes it deems necessary.

Simultaneously the geometric growth of the ability to attack a cryptanalyst required a cryptographic system to show security so undeniable, and must apply rigorous formal mathematical techniques.

- One of the applications with highest demands in this regard is the electronic voting. The results of a vote define important power relations and the management of important economic resources. Consequently, it is essential to make two key points.
- Scrutiny must reflect the will of citizens in a transparent manner.
- A voter must have the guarantee that your vote will be kept anonymous indefinitely [14].

This deals with such aspects in such a way to ensure the security of this process. Currently asymmetric cryptography, symmetric cryptography, and figures can be uses several types of cryptography, which are crypto algorithms. The first are mathematical functions that are structured as a finite set of steps, which help to encrypt and to decrypt the data.

In symmetric cryptography is commonly used the same password or key to be able to encrypt and decrypt the information, here comprise the DES (Data Encription Standard) triple DES, AES (Advanced Encription Standard), IDEA (International Data Encription Algorithm).

In asymmetric cryptography two keys, one public and private, are used here comprise the RSA, DSA, and elliptic curves.

So that cryptographic systems work, requires a Protocol, allowing follow the respective steps, to avoid the manipulation of some external agent and allowing to achieve the proposed objectives. It should not underestimate any level of security, so we must be aware of some weakness filed with any steps that are not fulfilled as expected.

6.2. Multi-layered security architecture

The development of an architecture, there are several methods, the sequential and progressive; the sequential stipulates the collection of requirements, development, testing and delivery; in the progressive are the requirements, design, implementation and review.

In this case, it is recommended a system that uses components to the highest levels, such as authorization, access controls, authentication and audit models; These require an architecture specific and adapted to these elections.

Applications use multilayer systems and each communicates with the previous layer according to their functionality via a defined interface.

Table 3: levels of a safety mechanism

Authorization and Access Control	
Authentication	Supervision
Safe Communication	
Cryptography	

The electronic protection relies on several features that must be fulfilled and protected:

1. Inviolability: Strict access code.
2. Usability: For benefit to its social environment.
3. Monitoring/audit: Quality assurance and compliance processes.
4. Software development: Creates and builds the software according to the needs of the nation.
5. Scalability: That the Software has the ability to grow.
6. Protocol attacks: Decrease the likelihood of malicious attacks.
7. Versatility: Making the system very flexible and adaptable.
8. Maintenance: To ensure the proper functioning of the software and its infrastructure.

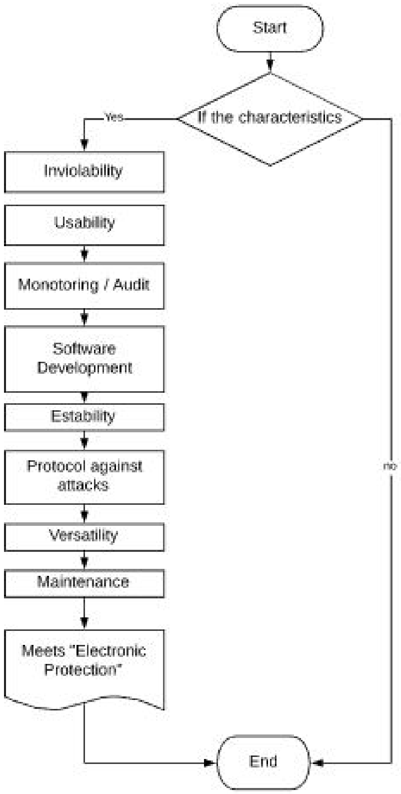

Figure 1: Electronic protection

6.3. Encryption algorithm using Diskcryptor:

This software presents tools that allows to determine the speed of encryption and decryption in megabytes per second of AES algorithms and combinations with other algorithms.

6.4. Audit

Importantly go monitoring and verifying the operation of the components during the electoral process, using blogs, reviewing the minutes of opening, the generated receipts and analyzing the final acts.

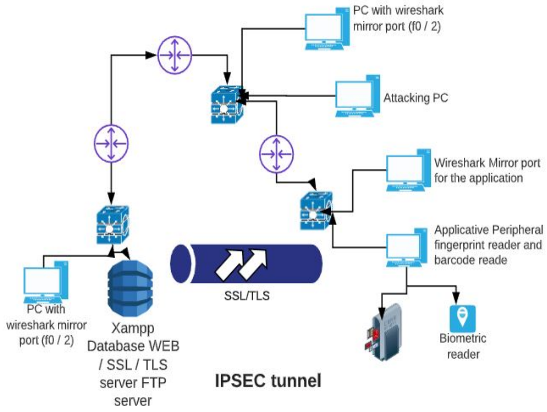
PC with wireshark mirror port (f0 / 2)
Attacking PC
Wireshark Mirror port for the application
Applicative Peripheral fingerprint reader and barcode reade
SSL/TLS
Biometric reader
PC with wireshark mirror port (f0 / 2)
Xampp Database WEB / SSL / TLS server FTP server
IPSEC tunnel

Figura.2. Security and Audit Protocol

The audit becomes a valuable requirement to establish a security architecture, but requires care processes are fulfilled accurately and avoid the intrusion of strangers and Protocol problems before, during and after of the electoral votes. the CNE must then combine aspects of the audit and security technology in the electoral process.

7. Results

For the design of a security architecture is needed of the law, as first articulated, then establish the process by software and its application to the respective vote.

Combined encryption makes possible the security of electronic voting. The use of the Diskcryptor system for a quick and appropriate encryption and decryption of the information on the electoral process.

There are systems that are used by some institutions, but only apply to identify threats in the network modules, then fight them. But also complementary procedures that complete security architecture is needed.

During the process is required to conduct audits allowing to know if the mechanism used is fulfilling their purposes, if the vote of voters is being protected and if the results are being provided Correct and timely.

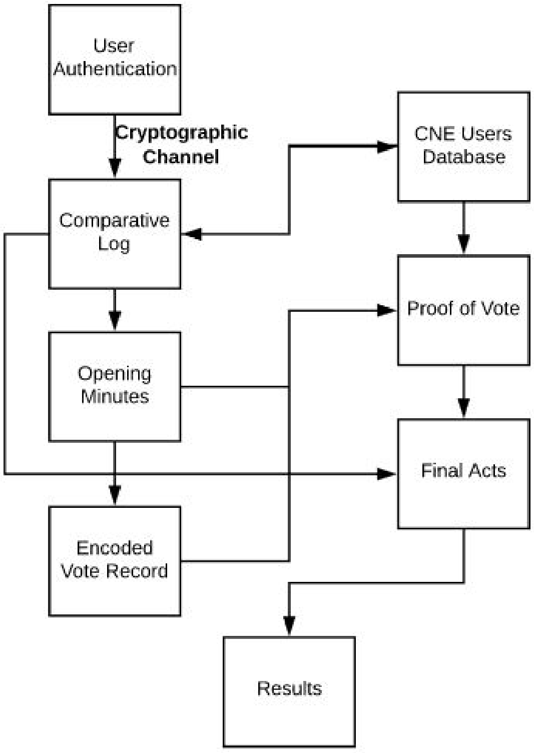

Figure 3: Prototype

1. User Authentication.
2. It encrypts the information through a cryptographic channel.
3. It decrypts the information and it occurs in the middle of a comparative log, is the comparison of the information in the database of the CNE.

4. If the data are correct, it gives way to the Act of opening which allows you to create proof of e-voting.
5. To generate the proof of e-voting, you must find the user in the Act of opening and have registered their electronic vote.
6. Once approved the above steps generates the final act and demonstrates the results.

8. Discussion

E-voting is an alternative used in few countries of Latin America and in Ecuador even these proposals not materialize by lack of decision or budget or mistrust in the political parties. With a good program, following protocol, their implementation could guarantee security, speed and efficacy, before, during and after the electoral process.

All voting system either digital or traditional will need prerequisites for its execution. However, there is a voting system that provides the security and integrity of the information; most, however, there are aspects which may be taken into consideration so as to prevent certain attacks.

In accordance with article "e-voting considerations" Miguel Montes, Daniel Penazzi and Nicolás Wolovick quoted in Nardi & Maenza, mentioned several requirements for the use of electronic voting and their respective security measures:

1. Reinsurance Individual, i.e. that not disclosed the identity of the voter.
2. Transparency, meaning that access to the code must be opened in such a way that any person can be inspected by other.
3. Separation of functions, i.e. the electronic count must be carried out by another different machine.
4. Non-electronic auditability, the vote must be printed on a paper in machine-readable form for all persons for verification and possible conduct of audit.
5. Independence of voter identification, i.e. that the identification of the elector occurs independently to the electronic ballot box.
6. Protection against unauthorized, i.e. readings that there is protection against attacks that want to be from some other device, whether this person or not.
7. Backup of keys [15].

These suggestions proposals are relevant to the proper use of the electronic medium. There is extensive coverage in relation to the information and the care of the system, but it will be necessary to maintain updated programs.

In a complementary manner, it is suggested to complete security architecture, adding an audit during the process, allowing you to monitor the compliance of each stage of scrutiny, this is relevant, at the discretion of specialists that may emit criteria to the logs of information that has been used.

9. Conclusions and Future Works

9.1. Future Works

Design of security measures in the voting systems that provide immediate feedback to the user in case present a computer plagiarism in your vote.

Audit of security technology, allowing to go to monitor the implementation of phases during electoral processes.

9.2. Conclusions

E-voting requires a security architecture that allows to avoid that the citizen decision be changed to benefit of any candidate. For this, you must set the fulfillment of the articulated law, which consists of the Constitution of Ecuador, also is needed to implement technological structures effective, with symmetrical or asymmetrical, encryption systems that prevent the manipulation of results, using the Diskcryptor software; Finally the participation of public bodies in the company of international participants will audit stages of scrutiny and give its approval to the processes and the different mechanisms implemented in the votes, which handles the electoral institution of the nation.

As indicated us Aguilar soul: analyzing the reasons for voting, are mostly reasons of trust, usefulness and interest. Level country established themselves confidence and technical reasons. These contrast with their respective visions of the situation in the country [16]. But electronic voting is not yet run, used modern technological structures in the count, and communication of results.

Acknowledgment

The authors thank the University Politécnica Salesiana of the Ecuador, to the research group of the headquarters of Guayaquil "Computing, security and Informatics for a globalized world" (CSITGW) created in accordance with resolution 142-06-2017-07-19 and the Secretariat education higher science, technology and innovation (Senescyt).

References

[1] S. L. Pacheco, "towards electronic voting in the State of Mexico electoral practice: elementary considerations," pp. 51-81, 2015.

[2] M. e.. García Barrera, "paperless Court, one step of the e-Justice TT - Paperless Courts, One More Step of Electronic Justice," Rev. IUS, vol. 12, no. 41, pp. 133-154, 2018.

[3] Constitución de la República del Ecuador. (s.f.). Organización de los Estados Americanos. Obtenido de https://www.oas.org/juridico/mla/sp/ecu/sp_ecu-int-text-const.pdf.

[4] J. F. Aguirre Sala, "The potential of digital media to traditional civic participation and in the participatory budget", new era, no. 22, pp. 211-229, 2014.

[5] P. A. Quesada, "Costa Rican vote abroad: a new national challenge," pp. 85-112, 2013.

[6] V. Loya, "reflections / REFLECTIONS."

[7] P carolina, G. Legorreta, P. Carolina, and G. Legorreta, "available at: http://www.redalyc.org/articulo.oa?id=211032011004," 2014.

[8] M. Montes, D. Penazzi, and N. Wolovick, "Considerations on the vote electronic," 10° Simp. about computer science in the State, pp. 297-307, 2016.

[9] H. A. Charles Leija, A. J. Torres García, and L. M. Colima Valadez, "socio-demographic characteristics of the voting members by 2015: an analysis of spatial Econometrics," Rev. Col. San Luis, vol. 8, no. 17, p. 107, 2018.

[10] J Schmidt-Peralta y J. Gutierrez - Alfaro, "towards the development of a prototype system of electronic voting for Costa Rica," Rev. Tecnol. in March, vol. 29, no. 3, p. 146, 2016.

[11] M. O. Gómez, "Vote of the Mexicans in the outdoors," Mexico before and after political alternation, pp. 133-138, 2018.

[12] J T. Places Chungat, E. R. Portilla Lopez, o. D. León Granizo, and M. Botto-Tobar, "reliability and considerations of electronic voting, a global vision", J. Sci. Res. Rev. Cienc. e research., vol. 2, no. 5, pp. 26-38, 2017.

[13] S. Bast, "model of data of the system of voting electronic classroom OTP-Vote", pp. 23-37.

[14] P Garcia, G. Montejano, S. Bast and E. Fritz "Seguridad Incondicional para el Anonimato en Sistemas de e-Voting", pp. 2-5.

[15] J. Leandro and r.. Rita, "electronic voting, vulnerabilities and solutions to prevent attacks," pp. 61-71.

[16] D. E. Aguascalientes, A. Lilia, S. Aguilar, C. Gutiérrez, L. Cristina, and P. Howlet, “Electronic voting : reliability and implementation of technology,” pp. 77–83, 2017.