OFFICIAL VOTING SYSTEM FOR ELECTRONIC VOTING: E-VOTE

Marco Antonio Dorantes González,
Martha Rosa Cordero López, Jorge Benjamín Silva González

Escuela Superior de Cómputo I.P.N México D.F.
Tel. 57-29-6000 ext. 52000 y 52021.

mdorantesg@ipn.mx, mcorderol@ipn.mx, jorge.ben.silva@gmail.com

ABSTRACT

This paper describes the Official voting system by electronic ballot: E-Vote, which aims to streamline primary electoral processes performed in the country, beginning with the District Federal benefits and improvements. The principal benefices are economic and ecological time, taking into account process security features and the integrity of the captured votes. This system represents an alternative to the currently devices and systems implemented in countries like Venezuela, Brazil and the United States, as well formalized as a prototype able to compete with others developed by the Institute Federal Electoral District (IEDF).

KEYWORDS

Biometrics, Privacy, Fingerprint, Security, Electronic voting, Voting, Vote.

1. INTRODUCTION

The use of computerized systems in electoral processes is not new. Although certain actions are still made by hand, others have sophisticated technology. For example, aggregation of results is typically done electronically, although remaining paper backing can be checked with the provided data.

Thus, the electronic voting studies normally do not cover the phases and the computing process. But the introduction of electronics in the electoral process kernel, is the moment at which citizen people emit their vote. Currently, this is done by introducing a paper sheet vote into an urn. It can be possible that such operation can be computerized. Precisely, our approach adopts narrowly this kind of electronic voting and analyzes various forms to perform it.

While a controlled environment, as current boxes, we can not exclude the possibility of immediate coercion, voting from home or from the workplace leaves the door open to possible extortion.

Dhinaharan Nagamalai et al. (Eds) : ACITY, WiMoN, CSIA, AIAA, DPPR, NECO, InWeS - 2014
pp. 69–80, 2014. © CS & IT-CSCP 2014 DOI : 10.5121/csit.2014.4508

Electronic voting present many advantages compared to current processes vote. Are ecological, they make faster and more agile counts and ratings long are cheaper.

Despite all the benefits, many experts believe that the main vulnerability of electronic voting is the integrity of the vote, that is, the voter is satisfied that Your vote will be counted as the did. Having taken into account this problem, have sought various solutions to this, ranging from the total suspension of use of electronic voting to implementation and testing of better security systems.

That's why we propose, through a study of the problem, an accurate and economically viable solution. The proposed system aims to meet the security needs and counting of votes from a number of electronic modules. These modules will be presented below.

PRINCIPLE

Our methodology uses the spiral method. Basically, it consists in repetitive spiral series of cycles starting from the center (see Fig. 1). Usually, it is interpreted as within each cycle of the spiral method follows a waterfall, but it is not like this.

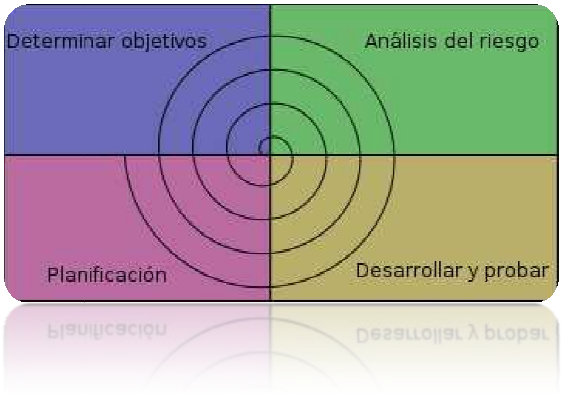

Fig. 1 The Spiral Methodology

The spiral evolutionary method combines the iterative nature of MCP model with the controlled and systematic aspects of the waterfall model, adding the risk management.

We designed our system with three layered architecture: Presentation, Business, and Data.

1) Presentation Layer

The presentation layer serves as the interface among users with the system. The layer processes carried out bio-data capture, deployment, and user data, as well as configuration ballots and the summary of the electoral exercise activities.

2) Business layer

The business layer takes the collected Data by means of the presentation layer, performing operations related to the voting exercise. This layer authenticates the processes by taking the

voter registration and the vote counting. This is where the interfaces are contained in the management of database users and voting and voting and candidates.

3) Data Layer

This layer are contained in the database voters and users, as well as the candidates' database and votes. The layer is accessible only through the functions and processes established in the Business layer.

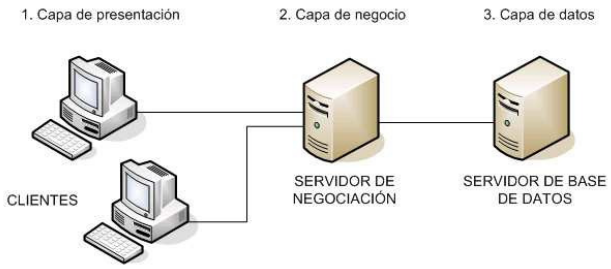

Fig. 2 Three layers architecture

Likewise, the Official Voting System for E-Vote electronic ballot box, our system uses specific modules to the following functions: recognition, authentication, digital signature, encryption, and decryption.

1. Identification RFID Module

The radio frequency identification system Frequency (RFID) stores and retrieves data using devices like remote labels, cards, transponders, or by RFID tags. The fundamental purpose of RFID tag is an object's identity (a unique serial number) using radio waves.

Fig. 3 Reader, cards and tags RFID

We used RXTX Java library to implement the RFID module. It serves as the communication interface between the serial and parallel ports with our development toolkit in Java or JDK.

Currently there is no way to access the serial or parallel ports with the standard Java API. This includes all versions up to 1.6 of the JDK. The communication of Java API provides the

necessary support for the communication with the Serial and parallel port. Currently, CXR is the most complete implementation of this API.

2. Fingerprint Authentication digital Module

We think that human has ID cards integrated, easily accessible and virtually with unique design : the fingerprints.

Fingerprints allow to grab things more easily, because they have tiny "ridges and valleys" of skin. These “valleys and ridges” are very useful until nowadays. They are produced from the combination of genetic and environmental factors, like the fetus position at a particular moment, the exact composition and density of surrounding amniotic fluid.

Fig. 4: Features of the fingerprints

Fig. 5: Pattern of fingerprint

A fingerprint reader function performs two tasks:

1) To get a picture of the fingerprint.

2) To compare the pattern of “ridges and valleys” with image patterns stored in the traces DB.

The reading or the scanning capacitance are the two main methods for obtaining fingerprint images.

The module fingerprint recognition implemented in our system has been developed using the U.are.U 4000 model.

The Digital Person Sensor Company produces. A scanning device, offering an application programming interface or API that allows to integrate the following functions: the fingerprint reader, the fingerprint Registration, the fingerprint Verification, and the fingerprint Baja.

3. Data Security Module

Our system, **E-Vote** has a unique module for ensuring that certain information, such as database or public keys are known only to the charge of the polls.

Thanks to the cryptographic algorithm called RSA, is possible to generate two keys (public and private) and to encrypt/decipher these information. RSA uses the prime factorization and the arithmetic functions.

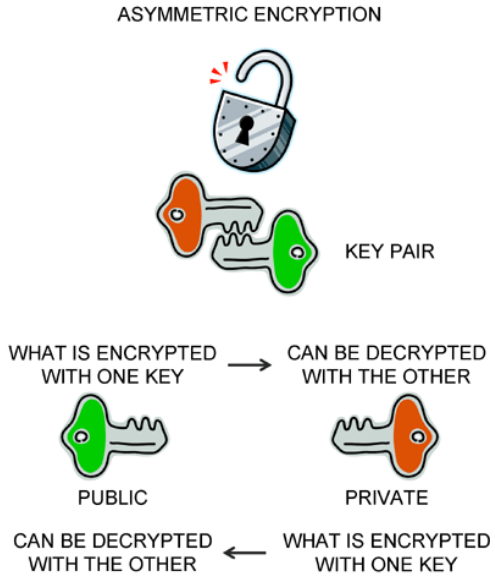

FIG. 5 Asymmetric encryption RSA

The the most safest and efficient cryptographic algorithm is RSA created by Rivest, Shamir, and Adleman . However, recently the RSA algorithm has suffered different attacks, because not only can be broken when using keys of 1024 bytes, although this problem can be easily solved just by extending the key size to 2048 bytes.

The digital signature is a mathematical scheme that perimenopausal verify the integrity and authenticity of a message. Thus, we can identify whether or not our the key database has not undergone any change over his transfer. Yielding a digital signature is a mathematical residue which is compared to the original that the representative can confirm if the message is corrupt.

The digital signature module can be made to different files and obtain a residue which we verified whether or not there are drawbacks.

Electronic voting and Operation Scheme: E-Vote

Official Voting System for E-Vote electronic ballot includes two operation schemes: -the overall system, including the involvement of the central shrine system and the electronic voting; -the operation of the scheme as such electronic ballot. The latter is located within the former.

1) Operation E-Vote System

The voting system is composed of four phases: History, Home, and End Exercise.

At the stage of **history** voters? will go to the central shrine system to be discharged by an authorized officer.

In this phase, the voters, together with personal data, provide the fingerprint. The official in turn, gives high associating RFID card with biometric voter registration, for electronic voting later use. In the initial phase, which is based on a streamlined electoral process, candidates are set to choose, and the criteria by which biometric references to candidates will be split to stay in each of the deployed electronic voting machines. These references divided fragments of the database, packed, encrypted and signed electronically to be stored on USB storage devices that can have its own security system fingerprint, to add additional insurance to the operation of the data transported.

In the exercise phase, once the polls and storage devices have been transferred to the place of voting, the officer assigned to the operation of the urn will identify it with your card, fingerprint and password. Only in this way will be able to set the time of voting, attempts to identify voters and begin and end the exercise.

To set the total time and start voting the same, voters will go to cast their vote by the scheme transaction narrate later.

At the end of time, the votes will be packed, encrypted and digitally signed to return to the central shrine described by the media before. The results of the choice of the particular electronic ballot box displayed on the screen.

In the final stages USB storage devices with the votes of the polls deployed will be checked, decrypted and imported by the central shrine in the database, which will host the final count and the issuance of the results.

Fig 6 Operation E-Vote System

2) Operation of the electronic ballot box E-Vote

The operation of the electronic ballot box has action in the **Exercise** phase of the system, and comprises three phases: authentication, the election and confirmation of the vote, which will be described below.

In the **authentication** phase currently voter presents the identification card with RFID chip. Then, a view confirmed this card existence within the chunk of data belonging to the specific urn. For complete identification the fingerprints are submitted.

In the **choice** phase, an electronic template candidates is selected for the E**xercise** will be displayed on screen, the voter may well choose the desired or cast a blank vote.

Once the choice is performed, in the **confirmation** phase, the voter has the opportunity to correct your choice, when you are sure, the urn will tell you the number of ballot box and the exact time of your choice. Through this information, voter can ensure the vote at the end of the year without being publicly linked with it. Thus, fulfilling the electoral exercise as confidentiality.

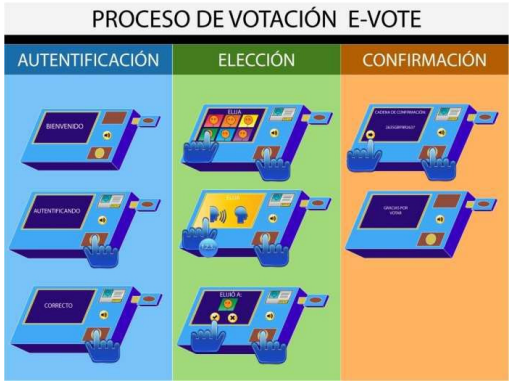

Fig 7 Operation of the electronic ballot box E-Vote

3. EXPERIMENTAL RESULTS

According to the extension of this project as opposed to the time set for execution, prototypes were developed central shrine and electronic ballot on two laptop computers, one with a touch screen, which is a housing manufactured allow a modular host computer and reading devices and RFID fingerprint.

Tests were performed with data fragmentation modules described above, in which successful results obtained in the 90% of cases to compress, encrypt and sign the content, as well as a 95% success to verify electronic signatures, decrypt and sign the votes generated by the electronic ballot box.

Were tested for reading RFID tags in electronic voting, the maximum reading distance of 10cm was with direct line of sight and interference 5cm with housing, which was more than enough for identification purposes.

As for fingerprint reading we test registration and authentication, check that the device performed successful readings in the 98% of cases regardless of the lighting conditions. Regarding the identification all successful tests established with FAR 2.0% error.

As for the average voting time per person, the amount was accounted for 3 minutes, so as an exercise of the federal elections of 2006, having four polls for the 130, 488 boxes, and the total

time of the vote would decrease by 40% from 10 hrs to 6 hrs. Looking at the whole electoral roll, which usually is not presented in its entirety.

From the economical point of view, each urn costs $10,000.00 M.N using 4 polls for the box, for 10 years of lifetime. By contrast, for electronic voting we consider investments of $521,952,000 M.N for electronic voting machines, $50,604,380 for the credentialing of the whole electoral roll. In addition, 7.49% and 0.72% of the average annual budget allocated $6966.44 IFE MDP.

Some results are

- The process of authentication, in this image shows the message of “welcome”.
- The voter inserts the RFID in this urn.
- The voter inserts the fingerprint in this urn.

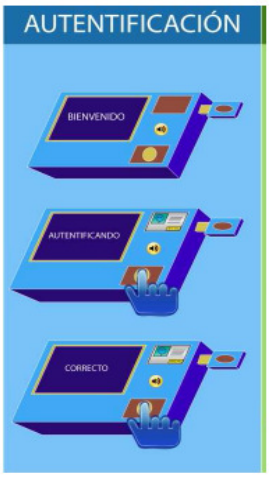

Fig 8 authentication

The following image shows the general project:

Fig. 9 Welcome a “E-Vote”

Fig. 10 Begin vote

Fig. 11 Window of begin of operation

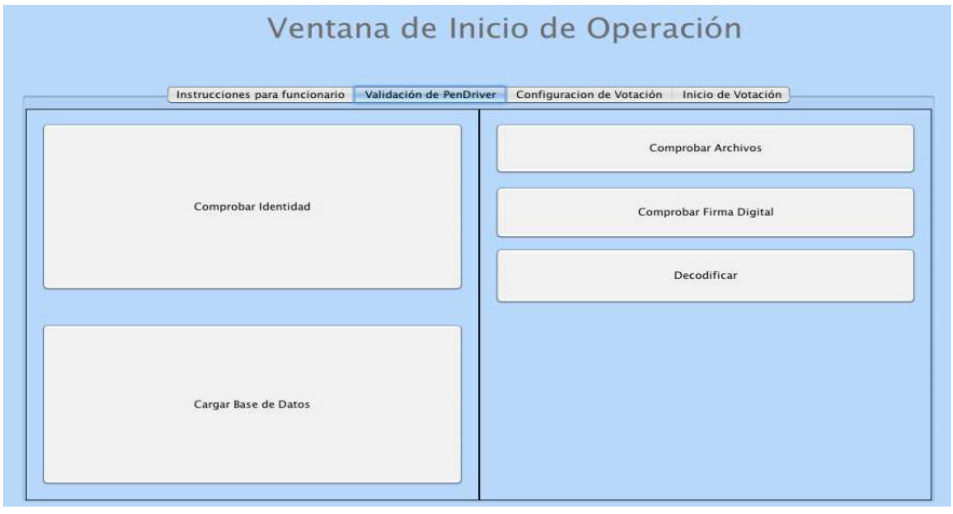

Fig. 12 Window of begin of operation

4. CONCLUSIONS

Electronic voting systems are gaining acceptance in the world. Our E-Vote system has been validated for the Mexican Electoral Institute, in the Coahuila state and the Jalisco state. They have declared to be satisfied with the results and they will plan to use the E-Vote system for the upcoming local elections. As a future research work, we will redesign the engineering process, including the identification and authentication mechanisms for RFID. The fingerprint will be complemented with better electronic devices.

During this study, we observed that these technologies are viable, affordable, and secure. This approach preserves the right of choice and national sovereignty for any country. Besides, this kind of systems, significantly reduce the alarming environmental impact, like that represented by the more than 60 tons of printed paper sheet vote as well as urn votes generated each elections without any dedicated computer system.

With regard to the restructuring of the voting process , though perhaps being the most ambitious of our project aspect , I have to say that is even more efficient than the current , carries in itself the same difficulty for implementation, however, sometimes a complete change for improvement is necessary.

In developing the system , we note that , despite the mistrust arising electronic voting procedures and counting, capture system itself may be more accurate , fast and economical long-term paper procedures . In addressing the risks posed in the analysis , we note that most of the causes of failure, as in the ballot paper , is represented by malice and desire premeditated to boycott the elections , a factor that is beyond the scope of any computer system in catastrophic events such as theft or destruction of equipment . There are also related failures inexperience or lack of user training , which in the case of our system are provided with the materials necessary training for operators and voting , as well as a simple and user-friendly interface.

ACKNOWLEDGE

The authors thank the School of Computing, National Polytechnic Institute (ESCOM-IPN, Mexico) for the economical support and the facilities provided for the development of this research work.

REFERENCES

[1] Kendall, Kenneth E.; Kendall, Julie E. Análisis y diseño de sistemas. 3° ed. México, Prentice Hall, 1997.
[2] Calculan 27.6 mdp operación de urnas electrónicas [online]. Available: http://www.elimparcial.com/EdicionEnLinea/Notas/Noticias/07102010/472309.aspx .
[3] El IFE registra cobertura del 99.57% de votantes en México [online]. Available:http://www.elsiglodetorreon.com.mx/noticia/427523.el-ife-registra-cobertura-del-99-57x-de-votan.html.
[4] El universal IFE estudia instalación de urnas electrónicas [online]. Available: http://www.eluniversal.com.mx/notas/660728.html.
[5] Hackers brasileños no pudieron vulnerar urnas electrónicas [Online]. Available:http://www.fayerwayer.com/2009/11/hackersbrasilenos-no-pudieron-vulnerar-urnas-electronicas/.

[6] El voto electrónico [online]. Available: http://www.larepublica.pe/archive/all/larepublica/20101017/6/node/295583/todos/15.
[7] Número de habitantes [Online]. Available: http://cuentame.inegi.gob.mx/monografias/informacion/df/poblacion/default.aspx?tema=me&e=09
[8] Ahorro millonario en comicios con la urna electrónica [Online]. Available: http://eleconomista.com.mx/notasimpreso/politica/2009/10/04/ahorro-millonariocomicios-urna-electronica-tellez.
[9] The History of Voting Machines By Mary Bellis [Online]. Available: http://inventors.about.com/library/weekly/aa111300b.htm
[10] Remote Voting Technology, Chris Backert e-Government Consulting
[11] U.S. Election Assistance Commission: 2005Voluntary Voting System Guidelines. Manual deprocedimientos para el sistema de votaciónvoluntaria de 2005.
[12] U.S. Federal Election Commission: DirectRecording Electronic. http://www.fec.gov/pages/dre.htm
[13] Instituto Tecnológico de Informática: Líneas I+D+I:Biometría [Online]. Available: http://www.t2app.com/index.php?derecha=ayuda/controlbiometrico.htm
[14] SAB - Sociedad Avanzada de Biometría. Available: http://www.sabiometria.net/
[15] Aplicación con Biometría Vascular. Available: http://www.kimaldi.com/aplicaciones/control_de_acceso/control_de_presencia_y_acceso_mediante_biometria_vascular_a_entornos_ofimaticos_y_de_pc_de_alta_seguridad
[16] Investigación y desarrollo de lectores biométricos [Online]. Available: http://www.by.com.es/es/lectores-deproximidad.html
[17] M1 – Biometrics About This Committee INCITS/M1, Biometrics Technical Committee [Online]. Available: http://standards.incits.org/a/public/group/m1
[18] The BioAPI Consortium [Online]. Available: http://www.bioapi.org/
[19] Identificación biométrica por huellas digitales [online]. Available: http://www.inegi.gob.mx/inegi/contenidos/espanol/ciberhabitat/hospital/huellas/textos/identificacion.htm
[20] Cómo Funcionan los Lectores de Huella [online]. Available: Digitalhttp://www.tecmex.com.mx/promos/bit/bit0903-bio.htm
[21] Roger Smith: RFID: A Brief Technology Analysis, CTO Network Library, 2005.RFID Journal [Online]. Available: http://www.rfid.org/
[22] Tipos de tags RFID [Online]. Available: http://www.idautomatica.com/informaciontecnica/tipos-de-tags-rfid.php
[23] Tipos de tags o etiquetas RFID [Online]. Available: http://www.rfid-a.com/index.php/2008/05/06/tiposde-tags-o-etiquetas-rfid/
[24] Lemmons, Phil; Robertson, Barbara (October 1983)."Product Review: The HP 150".
[25] Investigaciones del Laboratorio de Investigación Eléctrica de Mitsubishi (MERL) en interacciones con pantallas táctiles.[online]. Available: http://diamondspace.merl.com/
[26] Criptografia simetrica y asimetrica Dr. José de Jesús Ángel Ángel [Online]. Available: http://www.virusprot.com/Art1.html
[27] Seguridad en JAVA, Sergio Talens-Oliag, Instituto Tecnológico de Informática (ITI) [Online]. Available: http://www.uv.es/sto/cursos/seguridad.java/html/sjava-13.html
[28] Funciones Hash Criptografia [Online]- Available: http://www.monografias.com/trabajos76/funcioneshash-criptografia/funciones-hash-criptografia2.shtml
[29] Curso Seguridad de Redes y Sistemas. Autor: Msc.Walter Baluja García. CUJAE.“MD5 by Professor Ronald L. Rivest of MIT” [Online]. Available: http://userpages.umbc.edu/~mabzug1/cs/md5/md5.html
[30] The Legion of the Bouncy Castle [Online]. Available: http://www.bouncycastle.org/
[31] http://www.truecrypt.org/docs/
[32] How to use Model-View-Controller (MVC), Steve Burbeck, Ph.D. Roger Pressman, “Ingeniería de Software” Ed.8”

AUTHORS

M. Sc. Marco Antonio Dorantes González. Was born at Córdoba, Veracruz on 28 June, 1968. He had done his graduation in Electronics from ITO, Veracruz, México in 1990. After that he had completed his M. Sc. Degree in Computing in CINVESTAV in 1996 and M. Sc. of computing technologies in CIDETEC-IPN in 2008, research professor of ESCOM (IPN). He has been research Professor since 1996. He is interested in: Mobile Computing, Software Engineering, Data Bases. He has directed more than 70 engineering degree theses. Technical reviewer of interested areas books of publishers (McGraw Gill, Thompson, Pearson Education), He has participated in several research projects and has held some administrative positions in the IPN, also has experience in the industrial sector in the area of instrumentation and electronics; has done graduate studies in some fields, he has participated in several television programs and publications in scientific journals.

M. Sc. Martha Rosa Cordero Lopez. Was born at México D.F on 25 March, 1972. He had done his graduation in degree informatics from ITO, Veracruz, México in 1994. After that he had complete his Master Science Degree in Computing in CINVESTAV (IPN) in 1996, Master of computing technologies in CIDETEC-IPN in 2008, research professor of ESCOM (IPN) since 1995, her areas of interest are: Software engineering, Mobile Computing, Data Bases, affective computing, she has been director of in more than 70 theses to date, technical reviewer of interested areas books of publishes (McGraw Gill, Thompson, Pearson Education, among others). He has participated in various research projects and has held various administrative positions in the IPN also has experience in the private sector in the area of systems development; has done graduate studies in some areas, has been assistant mMcanager of technology intelligence unit in the technological development of the IPN, has participated in some television programs and publications in scientific journals.

Engineer Jorge Benjamín Silva González: Computing Systems Engineer from ESCOM (IPN) México D.F.