Automated Election System

Hipolito, Jovellano, Pachico

Abstract

The Philippines has been adopting the Automated Election System after years of adhering and relying on the Manual Voting System. It has been proven that the process became more efficient and generates results in a lesser time frame. However, complications are still evident in present time. For instance, electoral fraud still continues to remain through the existence of memory cards especially for the counting/transmission of election returns. There are many factors to consider in determining the causes of result manipulation that includes the humans accessing the system extensively. A physical object like the memory card is easy to exploit though many seem to think that transmitting/counting the results using memory cards are reliable and dependable. This study aims to produce a new system in which transmitting and counting of the votes does not require physical contact with other entities besides the system itself.

INTRODUCTION

Background of the Problem

After years of having a manual voting system, the Philippines have finally adopted an Automated Election System (AES) in 2010. This was mandated by Republic Act No. 9369 which is the Amended Elections Automated Law. The law stated that there would be paper-based election system defined as “a type of automated election system that uses paper ballots, records, and counts votes, tabulates, consolidates, canvases, and transmits electronically the results of the vote counts.” (Angkaya, 2011).

By standards, the new technology should be significantly more accurate and reliable for the voters; however, there were still some problems that might prove the acquired AES otherwise. For instance, the current automated election system with SMARTMATIC uses compact flash (CF) cards for the configuration of the Precinct Count Optical Scan machines in different provinces. These CF cards are pre-loaded with the precinct’s ballot depending on its specific geographical data. Then the same CF cards will also be the ones to store the data of the votes of the people. To look at it clearly, the cards are pre-loaded and will also be the storage of the votes and elections results. Now, this situation gives candidates, who want to sabotage the election, an easy time to manipulate the data in the system because it can definitely be intercepted through physically tampering with these so-called CF cards. The study aims to find a way to reduce electoral fraud in the counting and transmission part of the automated election system in order to achieve an indeed accurate and reliable system.

The Automated Election Systems in the Philippines follows a sequence of process. Focusing on the counting and transmission module of the system, the process starts when the polling precincts closes on the election day. The PCOS machines transmit the vote counts or election returns to the corresponding servers and canvassing centers. It is done chronologically with a hierarchical structure composed of the precinct level, municipal level, provincial level, regional level, and national level. From the PCOS machines, the ERs are transmitted to the central server, to a transparency server, and to the municipal board of canvassers (MBOC). From the MBOC, the results are brought to the provincial board of canvassers (PBOC) or the regional board of canvassers (RBOC), where the results are collected and then transmitted to the national board of canvassers (NBOC), where the results for national positions are canvassed. The MBOC and PBOC also separately send ERs to the central server. Moreover, the canvassing system processes the ERs that were transmitted. Public telecommunication networks are assigned to be the main channel when transmitting the ERs. There are back-up plans made if the network fails to accomplish its task. For example, transmissions can be made via satellite to avoid delays when problems occur.

During the course of the counting and transmission of ERs, electoral fraud is inevitable. There are a lot of issues concerning the effectivity and efficiency of the machine during the elections. For instance, the current voting system does not incorporate digital signature when transmitting the election returns from precincts to canvassers even if it is stated in the law. According to the republic act 9369 section 22, *“The election returns transmitted electronically and digitally signed shall be considered as official election results and shall be used as the basis for the canvassing of votes and the proclamation of a candidate”.* This means that BEIs are required to digitally sign the ERs that would be transmitted. As stated in the law, the ERs that would be recognized officially are the ones that were authenticated and validated by the administrators. However, during the past three automated election system, the AES failed to meet the requirements prescribed by the law. A possible reason is that the system being used allows humans to intervene in the process of the election. This is one of the reasons why it is easy for any unofficial institutions/organizations to ambush and manipulate the elections. For example, in Mindanao armed men prevented the citizens from voting. They controlled the precinct and made it impossible for the voters to cast their votes. Many eye witnesses claim that a wholesale ballot shading was conducted. Meaning only the same people casted many ballots inside the PCOS machine without the control of the BEIs. Without the existence of a digital signature provided by an authenticated agency, the election returns being transferred would still be considered not reliable because the digital signatures are used to verify the validity of the transmitted ERs. A public key infrastructure is practiced to guarantee that the votes are secured during transmission. A system should be designed to ensure that before transmitting the votes, ERs are equipped with digital signatures. Another solution that could be made to reduce the chances of this type of cheating is to incorporate the idea of GPS or global positional system in the machine used in the elections. GPS tracking uses both the time and location components that could provide data to the users. It is an effective way of navigating where the machine should be placed or located via a system the receives data from the satellites in space.

Statement of the Problem

How can the Philippine election system prevent electoral fraud specifically for the counting and transmission of the election returns?

Objectives

General

* To know the vital issues currently present in the counting and transmission of the votes
* To propose a system that would prevent electoral fraud in the counting and transmission of votes in the election system

Specific

* To develop a system that would transmit election returns without any human intervention (e.g. physical transportation of election returns)
* To design a database that would cater to the need of the proposed system

Significance of the Study

The findings of this research will benefit the following key players:

To the Filipino Citizens

This study will benefit the Filipino citizens for ensuring the security of the casted votes. Also, it would prevent malicious individuals from manipulating the votes. Although the nature of automation easily provoke fear to ignorance of using technology, this study will educate some of those users that still lack computer literacy foundation. Indeed, education can bridge the existing gaps and even remove the unnecessary fear from automation. This will leave the citizens better equipped for the future of the Philippine automated election system.

To the COMELEC

This research would significantly contribute to the goal of the COMELEC to conduct a fair and transparent election. Considering the impact of the elections in the overall condition and future of the Philippines, it is important to make sure that the voters’ choice reflect the outcome of the election. To do that, the system should be able to prevent and mitigate electoral fraud while ensuring that the voters have casted their votes in a way that is convenient and voter-friendly. This study will aim to determine the most appropriate methods to achieve the kind of system that does not manipulate the vote of the people in any way through data gathering and research. In this manner, the people will be knowledgeable about how the system works and be informed and wise voters themselves.

To the Future Researchers

As the Philippines adjust to this kind of voting system, more and more developers would also contribute to the AES aspect of software development. In that case, the system that would be created can serve as a guide and inspiration for other developers who would want to pursue the prospect of automated election system too.

Scope and Limitation

The scope of the study would only include the issues and possible solutions for the counting and transmission part of the automated election system in the Philippines. Further study on the other parts of the automated election system will no longer be covered.

REVIEW OF RELATED LITERATURE

Related Literature

**How does the current automated election system work?**

How the aes works: <http://www.rappler.com/newsbreak/iq/91663-philippine-automated-election-sytem-explained>

**How can electoral fraud occur in the system?**

Digital signature removed: <http://romeocayabyab.com/controversial-2010-philippine-automated-elections-revisited/>

Secret Servers

During the 2016 elections, Bong Bong Marcos’ camp believes that there exists a “Fourth Server” or also known as the “Queue Server”. It has been revealed that the Comelec and Smartmatic has been keeping it from the public. Instead of letting the ERs be directly transmitted to the three official servers, namely the Municipal Board of Canvassing Server, Comelec Server, and the Transparency server, the results were first being processed and consolidated in the “Queue Server”. Another problem with the secret server is that the source code being used was never reviewed despite of it being a requirement in the law. Moreover, there were no poll watchers assigned for these servers making it questionable to both the public and the administrators. According to a statement made by Rodriguez, a representative of Marcos’ camp, the integrity of the 2016 May elections has been questioned because of the unexpected situation made by the Comelec and Smartmatic. The ERs that were presented to the public did not come directly from the transparency server. Alternatively, the results were first transmitted to a “Queue Server” where they were “consolidated and processed” and the “Queue Server” sends the data to the transparency servers which is against the law. The law clearly states that (\*\*\*INSERT LAW\*\*\*) (Retrieved on August 10, 2016/ http://www.manilatimes.net/smartmatic-admits-using-unofficial-servers/275442/)

The Philippine Government in collaboration with the Department of Information and Communication Technology and Department of Science and Technology established an Integrated Government Philippines Project. It seeks to lower the cost of government information and communication technologies (ICT) by using cloud computing services. The project aims to increase productivity, to develop excellent services, and at the same time to reduce the value spent on this development. The agencies that would first be targeted by this project are the National Government Agencies and Government-Owned and Controlled-Corporations (GOCCs), including State Universities and Colleges (SUCs). (Retrieved on August 10, 2016/ http://i.gov.ph/philippines-cloud-first-policy-draft-4/)

Following the controversial secret server, the Commission on Elections is also a part of the target audience of this project which means that if the counting and transmission of the ERs are to be done under this project then there will be a chance that electoral fraud can be lessen. The said project is already being developed to provide high-speed communication and to increase the security of the data being kept. This is design to prevent hackers from attacking or penetrating government-related information in the cloud. It also promotes transparency which is also a requirement during the local and national elections. The project being conducted can be one of the possible solutions that can be done to prevent electoral fraud in the counting and transmission module of the automated election system.

**How can the automated election system be secured specifically for the counting and transmission?**

Philippine National Public Key Infrastructure: <http://i.gov.ph/pnpki/>

Related Study

EA Case Study for Tablet Election: <https://www.42gears.com/case-studies/case-study-electionadministrators/>

The Future of Election: <http://www.ccao.org/userfiles/14%20Oct%202nd%20Weds%20CCAO-OAEO-final-3.pdf>

THEORETICAL BACKGROUND

Include comprehensive discussion on theorems, definitions, fundamental algorithms and mathematical models/formula.

Dichotomy for voting systems: <http://www.sciencedirect.com/science/article/pii/S0022000006000924>

PDF: <http://ac.els-cdn.com/S0022000006000924/1-s2.0-S0022000006000924-main.pdf?_tid=3cd2a74e-6026-11e6-9dbf-00000aab0f26&acdnat=1470962982_4d631b942875a4a3d55e3dd9804aeac5>

Design and Implementation of a Practical Security-Conscious Electronic Polling System: <http://openscholarship.wustl.edu/cse_research/394/?utm_source=openscholarship.wustl.edu%2Fcse_research%2F394&utm_medium=PDF&utm_campaign=PDFCoverPages>

PDF: <http://openscholarship.wustl.edu/cgi/viewcontent.cgi?article=1394&context=cse_research>

PROPOSED SOLUTION TO THE PROBLEM

Must be the focus of the paper