A Trustable Electronic Government Voting Management Framework Using TPM

Mervat Adib Bamiah
Staffordshire University, UCTI
Technology Park Malaysia
Kuala Lumpur, Malaysia
mervatbamiah@yahoo.com

Ali Dehghantanha
Asia Pacific University College of
Technology and Innovation
Technology Park Malaysia
Kuala Lumpur, Malaysia
ali_dehqan@ucti.edu.my

Bridget Archibald
Asia Pacific University College of
Technology and Innovation
Technology Park Malaysia
Kuala Lumpur, Malaysia
bridget@apiit.edu.my

***Abstract* — one of the critical systems is Electronic voting systems, in sense of security-critical computing. One of the critical and complex parts of Electronic voting system is the voting process, which is responsible for storing the preference of the voters accurately and securely. The integrity of the election process is fundamental to the integrity of democracy itself. That requires good secure voting system, whether electronic or traditional paper ballots, to guarantee the voter's and candidate trust of the system and the results. This paper presents the issues in Electronic Voting system, Proposed Framework based on the literature review and Quantitative study. Finally Trusted plat form technology as a part of the proposed framework.**

***Keywords*-Electronic Voting Systems, Trusted Platform Module (TPM), Security**

I. Introduction

Critical systems that have vital impact on nations destiny and future has to be secured in highest level, and given the most priority , governmental voting system is one of these vital systems as it decides the nation's leader. Many countries have adopted Electronic Voting (E-Voting) to facilitate the process, and to overcome the traditional voting problems especially in counting the votes, in addition including citizens overboard, and disabled people. E-voting "Is the use of computerized voting equipment to cast ballots in an election securely by implementing the cryptographic voting protocols to make electronic voting secure and applicable"[1].

E-voting applications are growing in relevance as the population of the world becomes more reliant on technology. The major issues faced the adoption of E-Voting systems are on security part and usability, which prevented the voter from trusting the e-Voting systems. Solutions were provided to increase the security as will be described in the related work next section. The suggested artifact framework is developed through implementing Trusted Platform Module (TPM) as Trusted Computing Standard (TC) attractive security solution for use in voting machines because of its unique identity, wide range of security functions, hardware protection of cryptographic keys and software attestation. Voters are more likely to trust a voting system that is more transparent and allows source code inspection. The main priorities are election integrity and having voters understand the system. [2]

This paper is organized as follows. The next part will present understanding of E-Voting context and issues, and related work of E-Voting system. The second part will discuss TPM, Third part will be on the propose solution framework addressing for the identified problems in E-Voting system, finally conclusion and references.

II. E-Voting channels

There are different technologies for E-Voting, which can be used alone or integrated that can involve electronic counting schemes of traditional paper ballots, touch screens, kiosks, internet voting (I-Voting), Interactive voice response (IVR) landline telephone voting and Mobile voting (SMS) text message voting, and Digital television voting (IDTV)[3]. These channels have to be highly secured to gain voters and users confidentiality of the E-Voting system to increase the voter's turnout and peoples trust of the election results.

III. Related Works

E-Voting system was introduced by Chaum in 1981 as a simple flexible protocol that enables voters to create a receipt for their preference. In 1988 Colin Boyd introduced another scheme which was designed for *"Yes/No"* voting, quantity of options can be increased by adding new encryption keys, voters were verified by authorities. He tried to improve his system in 1989 by adding voter's second private key to assure full privacy. [4]Up to 1992 A. Fujioka et al. Invented protocol that combines the techniques of blind signatures and anonymous channels. While in 1997 Okamoto introduced a schema based on Unstoppable channels that made it possible to design a receipt-free schema. It has a weakness of lost property, if the coercer provides the voter with information

for the trap-door bit commitment scheme which made his schema hard to implement [4] In 2002 and 2004, D. Chaum proposed a method to provide voters with a coded receipt that reflects their vote but does not reveal it to anyone else, cost to implement D. Chaum's scheme is relatively high because of its requirement that all voting machines be equipped with special printers.[5]

In 2005 Researchers from University of Pisa, Italy introduced SEAS which is defined as a secure system for polling over computer networks.. SEAS require a list of eligible and registered voters to be available before the election takes place. But it does not assure that no one can view votes before the end of the election. And does not assure uncoercibility and it enables only universal verifiability; fraud can be detected after the voting ends. [4]

By 2007 Cetinkaya and Odanaskoy introduced DynaVote protocol, that secures all of requirements listed in the *general overview* section as follows; The *dynamic ballot* ensures diversity of votes which prevent coercibility. The *PVID* scheme that solves the anonymity problem *uses* blind signatures and has two main security flaws: The coercer may buy voter's signed identity or just make voters give it directly to the coercer to send a vote in place of the voter. The Authorities may replace votes in place of voters that have not taken part in the election because only the authorities' signature is verified [4]

Yee Designed a Direct Recording Electronic (DRE) voting machine with a greatly reduced trusted code base to simplify software inspections, but the Inspections cannot prevent malicious tampering of the DRE immediately prior to operations. Jorba, *et al* Scytl architecture using a hardware security module to protect chained digital signatures. The issue was they were Vulnerable to compromise through theft and replacement of the media [6]

Still researchers are trying to improve E-Voting systems, Chaum, and other researchers introduced End-to-End (E2E) systems such as Punchscan, Pr^et-_a-voter, Three Ballot, Scantegrity and Scantegrity II, in these systems Voters can check that their votes are recorded accurately using a receipt, and observers can verify that the tally is correctly constructed, without compromising ballot secrecy. The weakness is that they require special kind of paper ballots format. Punchscan ballots4 require two sheets of paper, and Prêt à Voter ballots randomize candidate name order [5].

TPM was introduced as a trusted solution to overcome previous E-Voting systems issues, and was first used by Arbaugh for voting in on-line protocol to attest systems through a central server. The weakness was that he Omitted key design details. Followed by Rössler, *et al* that used TPM in postal-voting where each voter submits a ballot encrypted with a public key to the tallying server, also Omitted key design details.[6]

As for Paul and Tanenbaum proposed E-Voting system architecture incorporating TPMs, but the issue is that TPMs' role assures only presence of correct software the platform state, and it is not bound to the casted ballot. Feldman, *et al* using technology from the TCG, but could not prevent malicious code from changing future votes by altering data before it was sent to the storage device. As for Pearson *et al* gave comprehensive overview of TPMs, and Challener provided an excellent practical guide to the TPM for software developers. Although TrouSerS introduced an open source implementation of the TSS, Strasser provided an open source TPM emulator to aid development. While Sevinc Described key distribution protocol that sends secrets from a server to a TPM-enabled client, but the weakness is that server has no way to attest the software state of the client.[6]

For overcoming all those past TPM issues Fink, R., and Sherman, A., Combined End-To-End Voting with Trustworthy Computing for Greater Privacy, Trust, Accessibility, and Usability, E2E features achieve many E-Voting system goals, but several gaps remain because of E2E untrustworthy software and poor usability. [6]

IV. E-VOTING ISUUES

Security can be external issues due to voters and attackers, and internal issues such as system developing and administrating even just inheritance of some objects in the source code are unsuitable can cause the voting system crash. Weaknesses of the current E-Voting systems, they are vulnerable to attacks and network threats such as, sabotaging the e-voting devices to stop them from running (Denial of service) or changing the election results by changing votes in some key precincts [7] also they can be vulnerable to fraud; *Fraud by Election authorities*; they may cheat by knowingly allowing ineligible voters to register, allowing registered voters to cast more than one vote, or systematically miscounting or destroying ballots. *Fraud by Ineligible voters*; they may register (often under the name of someone who is deceased) or eligible voters may register under multiple names. *Fraud by Registered voters*; eligible and non-eligible voters may be impersonated at the polls, and ballot boxes, ballots, and vote counting machines may be compromised.

The possibility of an over voting (or making more selections than permissible) or under voting (when a voter makes fewer than the maximum number of permissible selections in a contest), Internet voting is subject to potential risks due to the inherent insecurity of both the user's machine and the network connection by which it connects to the central server or tabulator. The users' machines may have many different forms of computer viruses, "worms", "spyware", or "Trojan

horse" applications or spoofing attacks when one of the communicating parties is tricked into opening a secure connection to a site controlled by an attacker.

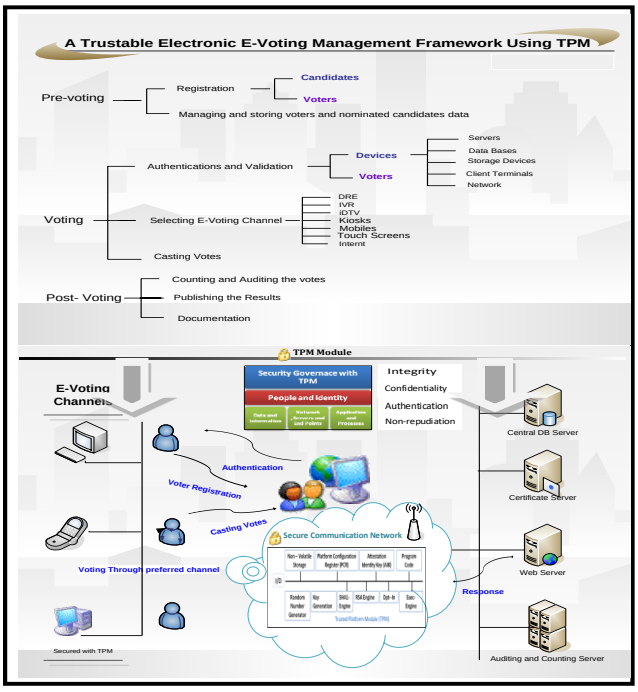
V. TPM PROPOSED SOLUTION

Trusted Computing (TC) with the usage of TPM increases privacy by ensuring the correct software is running. TC helps enable optimum usability and accessibility by making it possible to build trustworthy electronic interfaces. And helps voters catch problems in the polling location, making voting safer and better for everyone at the cost of more complicated engineering design and key management. [6]Trusted Computing TPM can benefit three critical areas: Privacy is platform attestation used to control signature keys only allows voting when the system has booted the correct software, mitigating the risks of unauthorized software disclosing private information, such as Scantegrity II ballot codes. Second TPM controls can reduce reliance on trusted chains of custody by ensuring that only the correct platform can access valid data. Finally verifying correct software operation is crucial to detecting problems early and for more usability. [6]

In addition to catching under votes and over votes prior to casting, managing the device signature key in hardware and sealing it to the correct platform state would allow the ballot to be signed only when the correct software was running. Also, sealing to the TPM prevents theft of the signature key. In this research framework will be developed based on the TPM module, and will be provided from the initial stage of E-Voting securing the information storage devices, network , communication and channels preferred for casting votes, such as mobiles and pc's.

VI. PROPOSED FRAMEWORK

The main propose of developing this framework is to manage a secure trustworthy E-Voting system by implementing TPM as chain of trust that combines hardware and software security to provide trusted client device. This TPM chip provides Protected Capabilities, Integrity Measurement and Storage as Roots of Trust, Integrity Reporting and Attestation. For securing; data, network, servers, communication channels, storage devices and user devices.



"Fig. 1" E-Voting Management Framework

The proposed framework consist of two parts, the first part concerns the E-Voting processes. The second part consists of TPM implementation in the whole operation of E-Voting processes. These two parts will be explained as follows:

- *Part One - E-Voting Management Process*

Preparation for the election considers: Human factors such as voters, candidates, employees, Technology Factors such as the devices, operating systems, application and networks.

Pre – voting

At the beginning of the election the organizers of the election campaign; will announce the information and the duration time of the E-Government Voting process, then they determine who is eligible to vote at the permitted time, after that ballot preparation and distribution this phase includes election information , candidates and voters identification. In addition to the **awareness campaign**, there should be **training** for the employees on the election process including the use of the E-Voting system. The administrative and technical personnel should be trained on the ethical, business and technical issues before the elections. As for managing the election process there should be three teams that are supervised by technical team as follows: *First*; the **Electorate Registration** System: for building the official database of voters.

Second; The **Candidates Registration** System: for managing and updating Candidate's information and verifying their eligibility to run in the election. *Third;* the **Voter's Identity**

Verification System: for ensuring the authentication of voters' identities using an ID card or a passport. The Voter identification and registration is used to identify the person either male or female, for the purpose of registering has a right to vote, thus identifying legitimate voters.

This will be done through authenticating the identity of the legal person allowed to vote in a contest, and to authenticate each person's voting rights. Voter identification and registration ensures that only legitimate voters are allowed to register for voting. Successful voter registration will ensure the authenticity and anonymity of the voter, and will result in legitimate voters being given a means of proving their right to vote to the voting system in a contest. Depending on national requirements or specific voting

Validation of E-Voting channels, as for the internet voting method validation**.** There must be some consideration taken when voting by internet, that voters are voting on different operating systems, and on different devices which provide the necessity for the websites to be usable, user friendly and secured. E-Voting system must be adapted to the different systems used by users, such as, for example, internet navigators. The other thing E-Voting system must check upon the voters if they voted online they will not vote again physically at the polling place, to avoid over voting not to mention checking the identity of the voter who is voting online to avoid dead people vote or redundancy of voting. Other channels such as mobiles, DRE's …etc also must be validated for the accuracy of votes results. After validating the channels also maintenance and validation of the system devices as they should be ready for the voting operation next step.

Voting

This process includes the e-voting channels and devices, such as touch screens, kiosks, voting websites, the voting database, the encryption system, the vote counting system and results presentation system. The primary function of E-Voting system is to capture voter preferences reliably, and report them accurately. The critical process is between capturing the voter vote and voting on an e-voting system (machine), as the system should be able to prove that a voter's choice is captured correctly and anonymously from his/her selected voting method, and that the vote is not subject to tampering. Voters can choose between casting their votes physically at the election place (poll site), remotely by internet voting (online / email) or by Mobile SMS according to the different channel voters preference, after authenticating and authorizing themselves by providing identification to a trusted official workers, for preventing over or under votes administrators validates the credentials of those attempting to vote when the election process begins.

Post – voting

After voters have casted their votes, the administrators collect the votes, then votes are processed and an election result is audited calculated and presented. Audit is the process by which the election authority representatives can examine the process used by which the vote is collected and counted to prove the authenticity of the result. Then publishing the final results and documenting the e-voting process. The system provides a facility to perform recount if there is any complaint about the results.

- *Part Two - Implementing TPM on E-Voting System*

This technical part should be done according to the security requirements such as privacy, eligibility, uniqueness, fairness, receipt-freeness, accuracy, verifiability, and elaborate checklists presentation [1].Then applying TPM module through all the E-voting phases as follows;

Phase 1: System initialization to check the integrity of the electoral roll before the poll opens, and to make sure that the virtual urn is empty and that the vote counters are set to zero, also securing the devices with TPM by sealing the storage, and the electronic devices.

Phase 2: Registering all the legible voters and storing their information in a secured database (secured by TPM), Verifying and authenticating the voters and the candidates. The voter must prove his/her identity to the manager of the electoral roll. The procedure used may range from the use of an identifier combined with a PIN code to use of a smartcard, in this proposed framework usage of TPM key generation for better security.

Phase 3: Securing E-Voting channels and devices by TPM, for an example as voting by the internet (I-Voting) protecting the voters passwords with a TPM, so that the servers on the other end can be assured who the user really is as the password is backed with the guaranteed identity from the TPM, and the user can be assured that access to the services can only be made from the computer with the TPM installed.

Phase 4: If the voter is authenticated, he/she is credited with a random number, giving him/her the right to vote. The voter then makes, from his/her virtual polling station, the selection, or selections, appertaining to the poll. Next is validation of the vote (check to ensure the voter has not already voted).
Phase 5: After casting the votes, and when the poll closes, the managers analyze the vote's then audit and count them, finally publishing the results and the documentation, if needed recount.

VII. CONCLUSION

The need to further exploration on the re-design of the electoral process and consider procedural security in view of the increased complexity of the E-Voting processes, which

can involve multi-channel E-Voting options, and the increase in the number of agents involved in the administration of elections. Security is a problem because, to date, the commercially available technology does not provide a completely secure e-transaction environment. It is not the aim of this research to address the future technical advances of security in E-Voting, but rather, how to improve the level of security of the E-Voting procedures, within the limitations of technology available. The proposed framework addresses all these issues through providing TPM as a solution to develop trustable E-Voting system.

REFERENCES

[1] O. Cetinkaya, "Analysis of Security Requirements for Cryptographic Voting Protocols (Extended Abstract)," *Availability, Reliability and Security, 2008. ARES 08. Third International Conference on*, 2008, pp. 1451-1456.

[2] A. Xenakis and A. Macintosh, "Procedural security in electronic voting," *System Sciences, 2004. Proceedings of the 37th Annual Hawaii International Conference on*, 2004, p. 8 pp.

[3] Peng Shuanghe and Han Zhen, "Design and Implementation of Portable TPM Device Driver Based on Extensible Firmware Interface," *Multimedia Information Networking and Security, 2009. MINES '09. International Conference on*, 2009, pp. 342-345.

[4] D. Rusinek and B. Ksiezopolski, "Voter non-repudiation oriented scheme for the medium scale e-voting protocol," *Computer Science and Information Technology, 2009. IMCSIT '09. International Multiconference on*, 2009, pp. 325-330.

[5] D. Chaum, A. Essex, R. Carback, J. Clark, S. Popoveniuc, A. Sherman, and P. Vora, "Scantegrity: End-to-End Voter-Verifiable Optical- Scan Voting," *Security & Privacy, IEEE*, vol. 6, 2008, pp. 40-46.

[6] R. Fink, A. Sherman, and R. Carback, "TPM Meets DRE: Reducing the Trust Base for Electronic Voting Using Trusted Platform Modules," *Information Forensics and Security, IEEE Transactions on*, vol. 4, 2009, pp. 628-637.

[7] K. Weldemariam, R. Kemmerer, and A. Villafiorita, "Formal Specification and Analysis of an E-voting System," *Availability, Reliability, and Security, 2010. ARES '10 International Conference on*, 2010, pp. 164-171.