Journal of Information Security and Applications 36 (2017) 69–89

Contents lists available at ScienceDirect

Journal of Information Security and Applications

journal homepage: www.elsevier.com/locate/jisa

A practical, secure, and auditable e-voting system

Kareem M. AboSamra[a,*], Ahmed A. AbdelHafez[b], Ghazy M.R. Assassa[c], Mona F.M. Mursi[c]

[a] Faculty of Engineering, Higher Technological Institute, Egypt
[b] Communication Dept., Military Technical College, Egypt
[c] Faculty of Engineering, Shoubra, Benha University, Egypt

ARTICLE INFO

Article history:
Available online 29 August 2017

Keywords:
Electronic voting
Secret ballot
Security
Cryptography
Verifiability

ABSTRACT

A cryptographic electronic voting system is proposed, to replace the conventional voting methods, which are widely used in most developing countries in the Middle East and North Africa (MENA) region. The proposed e-voting system is based on the concept of Prêt à Voter, which is a paper ballot e-voting scheme. Mixnet based e-voting schemes such as Prêt à Voter use mix servers to create anonymous channels. These schemes have some shortcomings; Mixnets need complex protocols for generating and maintaining shared mix keys, as well as for mixing and proving correctness of the shuffles. Moreover, Mixnets are complex to implement on a large scale. Mixnets are also vulnerable to corrupt or faulty mix servers as well. The proposed e-voting scheme eliminates the need for anonymous channels to anonymize the votes in Mixnet based e-voting schemes, yet provides comparable level of security and vote anonymity with less system complexity. The proposed e-voting scheme uses paper ballots, due to its familiarity among the public, but with strong cryptographic algorithms with proven security features, to provide enhanced level of ballot secrecy, verifiability and security. The proposed scheme is simple, secure, practical, and auditable. Security evaluation is conducted based on the critical and desirable properties of e-voting to support the claimed aspects. Threat analysis of the proposed e-voting system had been conducted to prove its resistance to well-known attacks on e-voting schemes and systems. A proof of concept implementation and simulation of the proposed e-voting scheme was developed to elucidate its efficiency, practicality, and scalability. The research proposal has the potential to be deployed as a trustworthy e-voting system, to replace the conventional voting methods in developing countries.

1. Introduction

Traditional voting systems have been developed to ensure that the principles required for democratic elections and referendums are met, namely the guarantee of the freedom to vote, the secrecy of the vote, the non-modification of the expressed intention of the vote, and lack of intimidation and coercion during the vote process. It is essential that these principles are not undermined by the introduction of new voting methods. E-voting is the term used to refer to the act of voting using electronic systems to cast and count votes in elections. Forward-thinking countries and election commissions are very motivated to explore how it can help them improve their elections. For some nations, automated elections mean that people can trust the results because it allows for a process that is so auditable, transparent and secure. Of course, e-voting also helps reduce human error. E-voting is very good at making voting more accessible, meaning it's easier for disable people to vote independently. Every country has different needs. That's why every e-voting solution is different for every country.

The conventional elections methods suffer from many drawbacks. These drawbacks include long period of preparation, fake and faulty voting, mistakes in count of votes, long period of votes counting, and high cost of the election process. Despite that, these conventional election methods are still being used in the developed and developing countries. Nowadays, Information and Communication Technologies (ICT) are being introduced in various stages of the electoral process. Electronic voting introduced ICT to the election process in order to increase the possible benefits such as speed release of election results and ease of voting. Electronic voting aims to decrease the time needed for vote casting and vote counting, to reduce the cost of the election process, and to improve the accuracy of the results.

An e-voting scheme is expected to satisfy certain general security requirements determined by the application, and also some specific requirements related to system's implementation. To be considered secure against adversarial attacks, an e-voting scheme must also satisfy additional security requirements. An exhaustive

* Corresponding author.
E-mail addresses: karimabosamra@gmail.com (K.M. AboSamra), aabdelhafez@gmail.com (A.A. AbdelHafez), dr.ghazyassassa@feng.bu.edu.eg (G.M.R. Assassa), monmursi@yahoo.com (M.F.M. Mursi).

http://dx.doi.org/10.1016/j.jisa.2017.08.002
2214-2126/

set of definitions for the requirements of e-voting schemes and systems have been derived from the literature [1]. These requirements may be divided into voter related, scheme related, and system related requirement. Voter related requirements include eligibility, authentication, uniqueness/non reusable, privacy, convenience, transparency, and walk away. Scheme related requirements include dispute freeness, fairness, non-coerce-ability, and practicality. System related requirements include soundness, accuracy/completeness, integrity, reliability, robustness, flexibility, auditability, Certifiability, cost effectiveness, voter mobility, receipt freeness, verifiability (including individual, universal, and end-to-end), verifiable participation, efficiency, and scalability.

Developing countries need to keep up with the advancements in information technology. Therefore, these developing countries need to replace their conventional voting methods, so as to gain the possible benefits of electronic voting. The aim of this paper is to create a framework upon which an electronic voting model can be developed and deployed in developing countries. The framework should provide the guidelines that leads to the translation of the developed e-voting model into an e-voting scheme. Such an e-voting scheme should be applicable for direct deployment as an e-voting system to replace the conventional election methods.

As a case study, The Arab Republic of Egypt was chosen from the Middle East and North Africa (MENA) countries to develop such framework. The framework should be applicable to conduct electronic voting in presidential elections, parliamentary elections, and public referendums. Voters in developing countries are familiar with the traditional paper ballot voting systems rather than electronic voting machines. The framework should consider the digital divide in Egypt as a main factor that would affect the public acceptance of an e-voting scheme. Therefore, among the functional requirements that would be critical for the framework is scheme simplicity, and familiarity in terms of voters' participation, and their ability to learn and interact with a new e-voting system. This familiarity comes from paper ballots that Egyptians used to cast their votes in their latest presidential elections in 2014 and parliamentary elections in 2015.

Voting in Egypt is currently using the conventional paper-based voting in government elections and referendums. Lately, the Egyptian government is showing great interest in an e-voting system as an alternative to conventional voting with all its problems and deficiencies. This interest in an e-voting system is an attempt to utilize technology to avoid the drawbacks of the existing conventional system. The main problems of the conventional paper-based voting method in Egypt are Illiteracy (in both computer and basic reading and writing), accuracy of election results, communication infrastructure, lack of verifiability, integrity of voting sheets, loss of votes, human resources, and voters' turnout.

In order to address the transference to electronic voting, several factors and requirements need to be taken into consideration. The convenience requirement states that all physical restrictions must be eliminated, and the number of voters having to learn complex methods in order to vote must be decreased to a minimum. Therefore in order to increase the voter turnout, the framework should consider simplicity as a main factor in order to be successful and gain public acceptance. Using paper ballots thus satisfies convenience because voters should be able to cast votes with minimal skills. Critical requirements relative to the security of e-voting schemes have to be considered as well to provide election security in terms of vote fraud, vote for others, duplicate votes, and voters' bribe & coercion.

An e-voting scheme must protect the privacy of the voter at time of casting the vote and provide ballot secrecy as well. An e-voting scheme should not have assumptions and requirements that may be difficult to implement on a large scale. Voters should be able to verify or get proper assurance that their votes were correctly included in the final tally. Votes should not be able to be modified, and in such case, any alteration should not go without detection and proper recovery. Another desirable property is the voters' mobility; that the voters need not be restricted to a certain geographical region to cast votes. Partial tally should not be revealed when the voting phase is in progress. It is crucial to have a trust-worthy voting system that delivers accurate results without human errors. All the previously mentioned factors and requirements should to be taken into consideration, handled with persistent efforts, and effective regulations need to be put into place to govern the transference from conventional to electronic voting in Egypt.

This paper is organized as follows. Section 2 reviews the related work. In Section 3, an overview of the proposed electronic voting scheme is presented. Section 3 also details the new scheme by presenting an abstract of the cryptographic operations of the proposed e-voting scheme. In Section 4, the core cryptographic operations are expanded for further details. Section 4 also presents the key security features that characterize the new e-voting scheme. These features are analyzed and compared against the desirable security requirements of a trustworthy e-voting scheme. Section 4 also presents a threat model of the proposed scheme to illustrate its resistance to well-known attacks on e-voting schemes and systems with proper mitigation measures where needed. Section 5 presents the implementation aspects of the proposed e-voting system. The implementation targeted the core cryptographic operations as a proof of concept and to illustrate the practicality of the proposed scheme. Section 6 details the simulation of the proposed e-voting system. The aim of the simulation is to build a simulation model of the proposed electronic voting system. Section 7 concludes our work and points out future work.

2. Related work

To achieve true confidence in electronic voting is to allow the voter to directly inspect the actual cast vote record, and therefore confirm to be correct, and later to verify that his vote was counted in the final tally. There exist some e-voting schemes that try to achieve this. Most of them rely on complex procedures and often require a level of experience and skill that an average voter may not have. This would impact their public acceptance, and therefore renders these schemes useless. Also some of these schemes rely on various assumptions and requirements that would be difficult to be realized or used on a large scale.

There exist many approaches in the literature towards e-voting schemes and systems. Among these approaches is the blind signature approach, which was initiated in [2]. Blind signature is a cryptographic protocol that can be used to authenticate a voter without disclosing the content of his ballot. Blind signatures are the electronic equivalent of signing carbon-paper-lined envelopes. Writing a signature on the envelope leaves a carbon copy of the signature on a slip of paper within the envelope. When the envelope is opened, the slip will show the carbon image of the signature. This approach was introduced for e-voting in [3,4].

Another approach is the homomorphic encryption approach. The homomorphic property allows the encrypted votes for each candidate to be summed into a single total, without being individually decrypted. This generally applies to "Yes/No" votes. The homomorphic approach was introduced in [5,6], and was improved in the work of many authors [7–11].

Mixnet based approach is one of the main approaches to deploy secret and verifiable electronic elections. Mixnet is a technique to create anonymous channels; a multistage system consisting of cryptography, shuffling and permutations. The function of a Mixnet is to randomize a sequence of mutated messages such that the inputs and outputs of the Mixnet are not link-able. Mixnets in