Design of Web Service-based Secured Distributed I-Voting System

Teha Abrar
HiLCoE, Computer Science Programme, Ethiopia
Ministry of Finance and Economic Development, Ethiopia
observe_nature@yahoo.com

Fekade Getahun
HiLCoE, Ethiopia
Department of Computer Science, Addis Ababa University, Ethiopia
fekade.getahun@aau.edu.et

Abstract

Processing large scale voting manually is complex, time taking, incurs high cost, causes recurrent vote rigging, and finding the vote result can also be beyond the planned schedule [1, 2]. The aim of this research is to develop a secure distributed Internet Voting system using web service technology. In a voting system, maintaining the security of data and privacy of voters are main concerns. Advancement in computer networking and cryptographic techniques facilitate the implementation of Internet-based voting. To analyze and design the system, object oriented design approach is used. The backend system is designed using Oracle database enterprise edition, Oracle SQL developer, and XML. The frontend is designed using Oracle Fusion Middleware JDeveloper. The web pages are designed using JSP, Servlet, HTML, and web services.

To realize the system, a prototype is developed to simplify the process of organizing elections and let voters vote remotely from a controlled environment using Internet while taking into consideration security, anonymity, verifiability, and providing audit capabilities. We used digital signatures and cryptography for privacy and security.

Keywords: Internet Voting; Digital Signature; Cryptography, Security, Distributed System; Web Service

1. Introduction

Public voting is one of the common ways of making decisions. It is a basic technique to know the opinion of individuals, groups, citizens, etc. on a given matter. Public voting serves not only for general election but also to make decisions on other public issues such as policy, politics, socio and economic issues. The current voting system in Ethiopian is manual. Having a voting system which is easily accessible, secured, user friendly, highly available, transparent, verifiable, equal suffrage and with high throughput will have great impact in building consensus among the society of a country. Recently countries such as Estonia, Switzerland, United States, and India introduced electronic/Internet voting system nationwide, on state level or target specific categories of voters [1]. Also the countries' experience has shown that the election conducted at regional level can scale up nationwide using distributed Internet voting system.

The main objective of this research is to design and develop a Secured Distributed Internet voting system using web service technology for Ethiopia as supplementary to the existing manual voting system. To achieve the objective, data are collected using interviews, questionnaires and document review. The data are analyzed through familiarization, categorization, and interpretive analysis. Furthermore, object oriented design tools, Oracle Fusion Middleware JDeveloper and Oracle database enterprise edition, are used to develop the system.

2. Related Work

The most common flaws in Internet voting as stated in [3, 4] are: unauthorized vote casting, voter impersonation, ballot stuffing, voter privacy compromise, voter coercion and vote buying, vote modification, publication of non-authorized intermediate results, a voter does not have any means for verifying the correct reception and count of her/his vote, denial of service, not enough election

traceability, malicious software, SQL injection, insufficient procedures and legal protections. Moreover, cyber attack is a very real threat. There must have updated cyber security strategy that puts into consideration changes in technology and threats [13].

Traditional cryptology methods like SSH, Cryptography, SSL, TLS, and IPSec use cryptology algorithms that are more venerable [10]. Encoding classical data on quantum states in a way that any attempt of an unauthorized entity to extract the secret data leads to either the attempt fails, and the amount of information revealed is negligible, or the measure taken by that entity damages the coherence of the quantum signals, and by that reveals its presence [9]. If properly implemented, it is inherently unbreakable. However, the technology is still in experimental stage and is evolving [11, 12].

Single sign on is a session/user authentication process that permits a user to enter the same user name and password in order to access multiple applications. When the user tries to access high risk applications, the single sign on software requires to use a stronger form of authentication. Single sign on improves user productivity, development productivity, and simplifies administration. However, it is a single point of enterprise failure if not properly designed, as it could simplify attackers' effort on finding out only one password [8].

Several remote electronic voting models have been implemented worldwide using various security controls. In this paper, two Internet voting models: Estonian and Switzerland are analyzed in-depth which address most of the security issues.

2.1 Estonian Model

In Estonia, each citizen has a unique identification card that allows secured remote access. Online voting is conducted within scheduled and predefined days before the actual election day. Once the advance voting period ends, list of citizens who voted electronically is complied and sent to polling stations to prevent double voting. If an elector votes by paper ballot on election day, his/her pervious electronic ballot is deleted. The system is deployed in four machines: Vote Forwarding, Vote Storage, Log Server, and Vote Counting [1, 2, 13]. The vote forwarding server (VFS) is the only publicly accessible server. It verifies voter eligibility and sends an encrypted and signed vote ballot to the vote storage server (VSS). The VSS stores encrypted votes during the online voting period. It verifies voted data format and voter's digital signature using an external Online Certificate Status Protocol (OCSP) Server but cannot decrypt the vote. Only the vote counting server can decrypt the vote and count. The VSS can unwrap the digital signature and mark the vote by timestamp or any other means and then can send this to the vote counting server (VCS). The VCS is never connected to a network and is only used in the final stage of the election. Officials use a DVD to copy encrypted votes (with their signatures removed) from the VSS. The VCS is attached to a hardware security module (HSM) that contains the election private key. It uses the HSM to decrypt the vote, count them and output the official results. Log Serve is an internal logging and monitoring platform that collects events and statistics from the VFS and the VSS.

2.2 The Switzerland Model

Switzerland uses different voting procedures in the different cantons (federal states). The remote Internet model used in Geneva is an adaptation of its postal model. All voters are sent with a voting card, which is to be presented when voting by paper ballot, mailed back with a postal vote or used to obtain codes which permit online voting. In terms of security, Geneva does not use digital signatures. Once cast, the ballot is encrypted with alphanumerical characters, which masks its content (the first envelope is sealed). When a voter confirms and attaches his/her identity to the ballot, it is encrypted with another protective layer (second envelope). Once the vote is received, the identity and the ballot (the two envelopes) are kept in different files. Before the ballot box is opened, the ballots are shuffled so that they do not correspond

with the voter registry. The voter receives electronic confirmation that a ballot has been cast [1, 2, 6].

The main problems of the Estonian and Switzerland voting systems are:

a. A client computer could be infected with malware since the voter could not have the knowledge to examine the fingerprint or is too lazy to do it. So especially phishing mails and malware installed on the client PC are security problems. [Both]
b. The voting is only in Estonian language although there are a large number of Russian speaking Estonians. [Estonia]
c. A sealed envelope or a sealed bag does not hinder somebody from breaking the seal and counterfeiting a new one later. [Switzerland]

Based on comparative study of security aspects of these two selected Internet voting models, our proposed model is then developed.

3. The Proposed Solution

The current ICT infrastructure and information security landscape in Ethiopia do not warrant sufficient level of security (with respect to authentication, identification and transmission of cast votes) and accessibility to implement a full-scale remote Internet voting in the country [7]. Hence, manual voting is still a major option in many parts of the country. However, to reach all eligible voters, the voting process should guarantee accessibility (voting right) using different voting methods that assure the voting requirements. For instance, for voters in cities, universities, for those living abroad, and who travelled far away from their registered polling station, implementing Internet voting is an option. For physical impairments, elderly people and people in hospitals, manual proxy voting is a better option. However, to use kiosk Internet voting there should be a reliability test trusted by all stakeholders due to security and secrecy concerns.

In a general election, Internet voting at poll stations allows voters in person authentication, to configure site to site security protocols, and to monitor and install anti-malware (antivirus) on client machines to reduce client side threats.

3.1 System Model

The dynamic nature of the system is modeled using a UML diagram. Use case diagrams are used to gather the high level requirements of a system including internal and external influences. Figure 1 shows the use case diagram of the system. Actors identified for the system are:

1. ConstituencyElection Official: declares election and the election details. She/he Manages election setups, centers, schedule, candidates, voters, parties, poll station election official, and other system users.
2. Voter: A citizen who has a legal right to vote and registered to vote.
3. External Citizen Database System: An external system that provides citizen information.
4. Poll Station Election Official: Registers voters and coordinates election at the polling station.
5. Representatives: Observe and hear grievances during election days.

To registered voters, citizen data is imported from the external system. The poll station election officer registers eligible voters and provides authentication means for voting. Casting is performed on local languages after the voter authentication. A voter casts her/his vote in a way that protects secrecy, and the authorized individual records are updated. The voter ensures the reception of his/her vote to whom s/he votes. Online voters are allowed to change part of his/her pervious vote for that election during the online voting period. The vote replacement process does not violate the vote equality principle. The vote data along with the voters' list is consolidated from the region or sites to the central repository. After the vote integrity is verified, the election officer announces and publishes the election result on a scheduled date.

Result integrity verification also takes place in case a voter or any other interested party requests to verify that any of the aforementioned election procedures have been conducted properly.

3.2 Architecture of the System

The I-voting system has N-tier architecture. N-tier application architecture provides a model for developers to create a flexible and reusable application [5]. The proposed I-voting system has client tier, web tier, business tier, and data tier. The system is developed in Java EE that supports multi-tier architecture. Both the web tier and the application tier run on Java Enterprise Edition (EE) Server. The system architecture of the proposed prototype is shown in Figure 2,

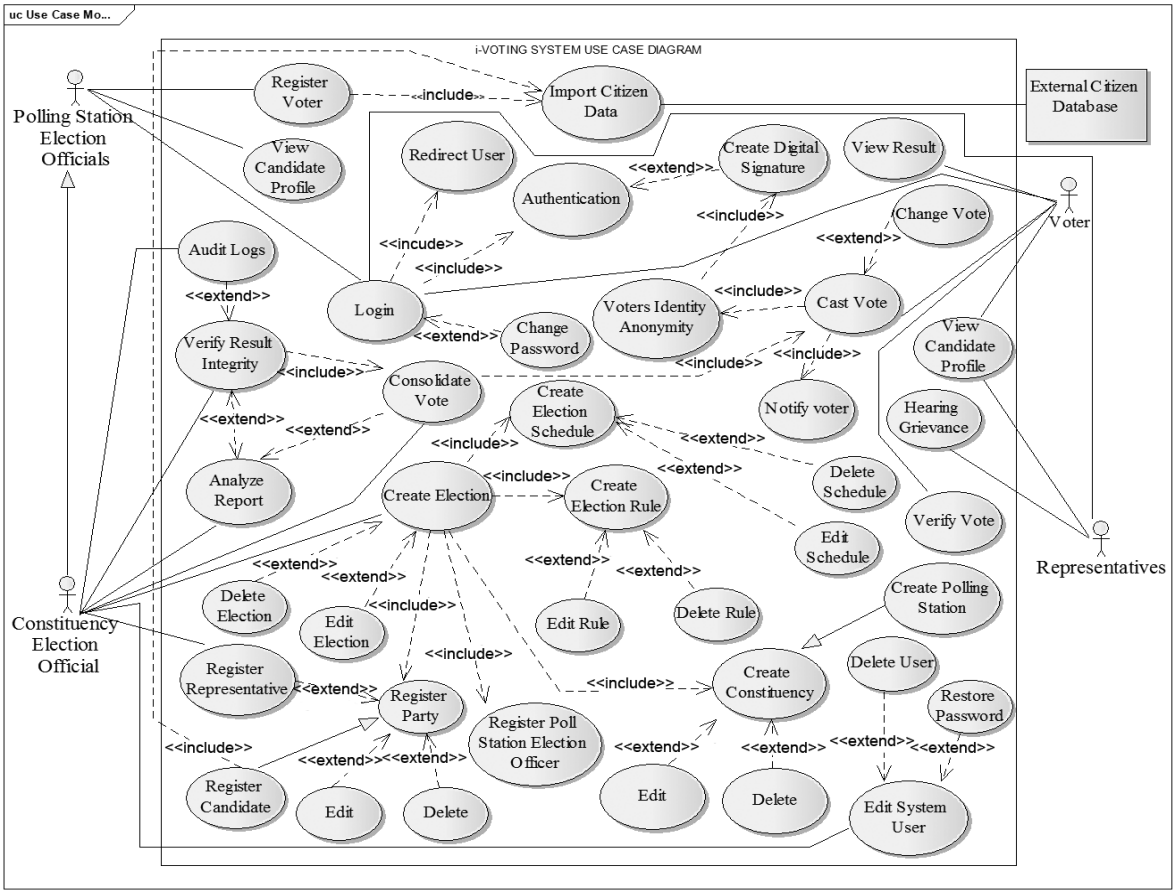

Figure 1: Use Case Diagram

The Client Tier

It is a dynamic thin web client that displays a web browser and acts as an interface between the user and the WebLogic server which are generated by web components running in the web tier. It consists of style sheet and user level user input validation scripts.

The Web Tier

It interprets the request received from the client, does some basic business logic processing and invokes the business layer for more complex business processing. Oracle WebLogic Server supports the Java EE architecture security model for securing web applications. It consists of JSP pages and Servlets components of the voting system. The web tier maintains the state of data for a user's session and performs basic logic and holds data temporarily in managed beans.

Business Layer

This tier moves and processes data between the surrounding web tier and data access layer. Citizen data are imported from an external system in an XML format in batch once or each time during registration. The business rules and data validation, domain concepts, and data access logic are handled using business layer components such as cast vote, register, verify integrity, authentication, manage user, anonymous voter, analyze report, etc.

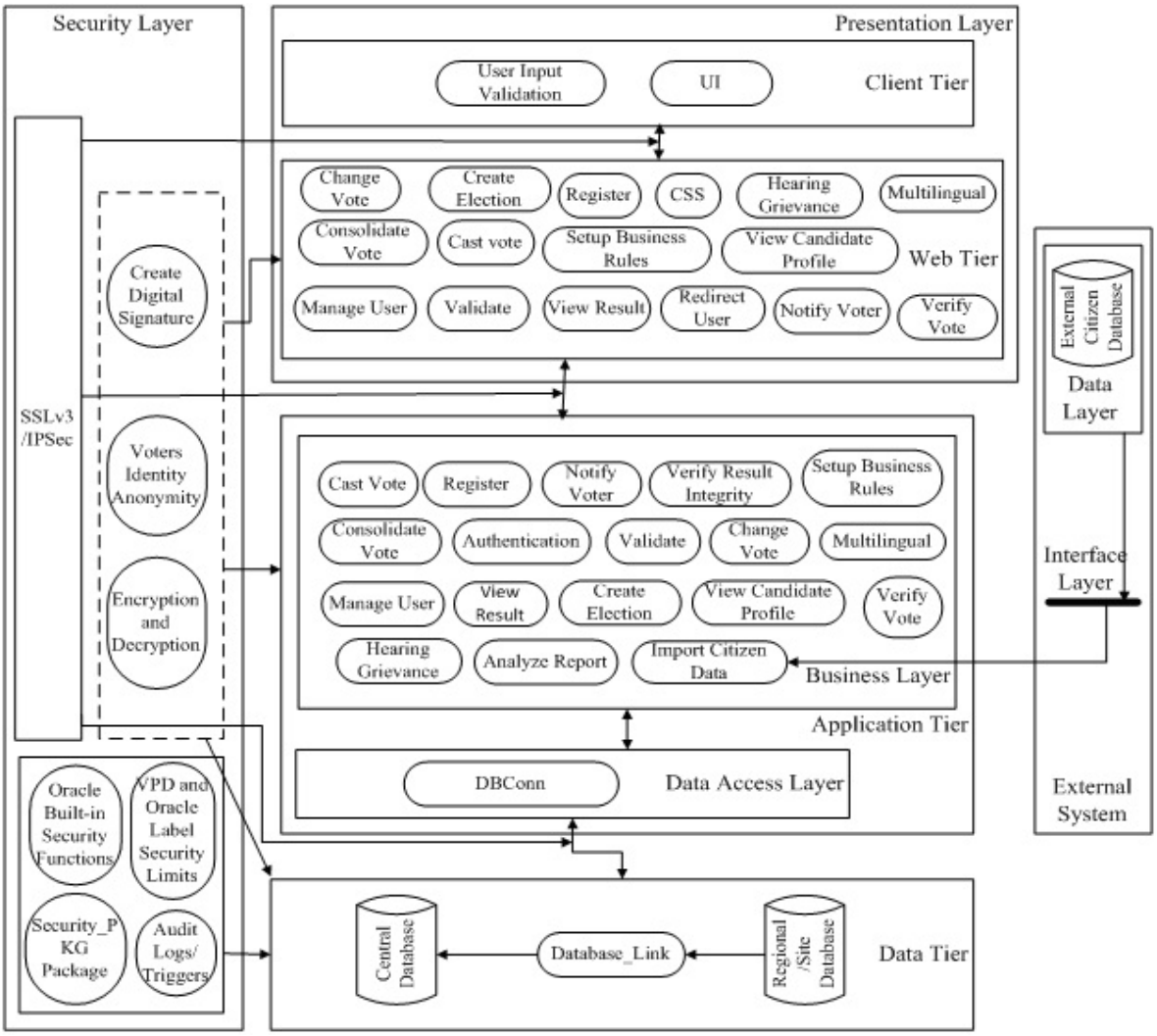

Figure 2: The Proposed System Architecture

Data Access Layer

It receives data from the business layer and performs the required DML and DDL operations into the database. The DBConn class uses JDBC connection.

Data Tier

Data tier is the core service for storing, processing and securing data. The voters' records, candidates' record and election results data reside on this tier. This tier is also responsible for authenticating voters and administrators' authorization. Using Oracle task scheduler and database link, data are pulled to the central database servers from regional/district database servers automatically on a given time interval. ImportDataToCentralWS web service provides additional features for the system user at the central database to pull data from the regional/site database to the central database.

Security Layer

This component performs authentication, authorization, validation and protection. During data transmission it uses the more secure IPSec that needs site to site configuration. To authenticate users during login and voting, digital signature is used. The voted data and users' password and username are encrypted using digital signature for protection. In all tiers, the data are secured using encryption and digital signature. Business dependent DML SQL queries do not function unless the security class is wrapped into the database. To limit backend access, these DML queries are implemented and function at the

application level and only accessed at database level based on responsibility. The audit triggers also record all DML actions on basic tables; the time, user, the IP address of the machine, and the type of action. Applying virtual private database policy and Oracle label security limits and prevents end user actions.

External System

In Ethiopia, a national electronic identity card (e-ID) with an asymmetric key is not established. So, to verify a voter, it is assumed that there is an external system that provides citizen information and citizen national unique id. The system is interfaced with the external citizen information system to import citizen data in XML format. Before the data is imported, it is hosted on the external system gateway machine or its local machine. The interface layer provides methods to communicate the two systems.

4. Implementation

The prototype is developed using Java EE (Oracle JDeveloper 12c) and Oracle 11gr2 enterprise edition database. Two databases are created to test the distributed nature of the system. Database link is created between the two instances and Jobs are scheduled to consolidate data from site databases to the central database. It includes the following processes:

a) Voter and Candidate Registration

The system imports citizen information in XML format from the external citizen information system, then maps and inserts to the corresponding table schema in the internal database. Election officer registers voters at polling station. The system creates unique registration number, user name, temporary password and sends to the voter.

b) Authentication

To authenticate a voter, the system uses user name, password, registration number and creates digital signature of these fields.

c) Vote integrity

Cast votes are vulnerable from being tampered by attackers that gain access to the voting system. Digital signatures can be used for both integrity, verification and identification purposes. To secure the system more, each staff's access/responsibility is limited.

d) Auditablity

The system creates triggers to register sensitive operations audit logs files on basic tables (voted_datas, registered_voters, users, and candidates tables). It takes care of not registering information that can compromise voters' privacy. The system notifies the voter the receiving of the vote by sending the private key of the voter during voting. A voter verifies his/her vote.

e) Data Consolidation

To consolidate data to the central database, first a database link is created between the central database and the site databases. The data consolidation is done using two methods.

Method 1: Using Oracle scheduler, the data is pulled to the central database from site databases automatically based on defined job schedule.

Method 2: Using a web service module to import data from each site to the centralized database.

f) Voter Anonymity and building public trust

The system assures voters' privacy at two levels. First it creates unique registration number and hashed value of the national id of the voter during voter registration. Then, during voting, the system creates digital signature from a hashed value of a registration number based on RSA algorithm. At every step, the data is encrypted/decrypted using the election board's private and public keys. Due to security reason the data is not imported in batch. However, each voter data is imported when s/he is registered.

g) Validity

The validity of the voted data is checked by comparing the decrypted digital signature value with the hashed value of the registration number for each record. Invalid records are filtered and inserted into the invalid voted data table.

h) Redirect User

To redirect a voter to the appropriate application, the system does not use single sign on; rather it uses

user level option. In the user level option, each region or sub region and the head office have applications that authenticate users. A voter selects his/her voting region or sub region from the redirect page before s/he logs in. Figure 3 shows user redirect default page.

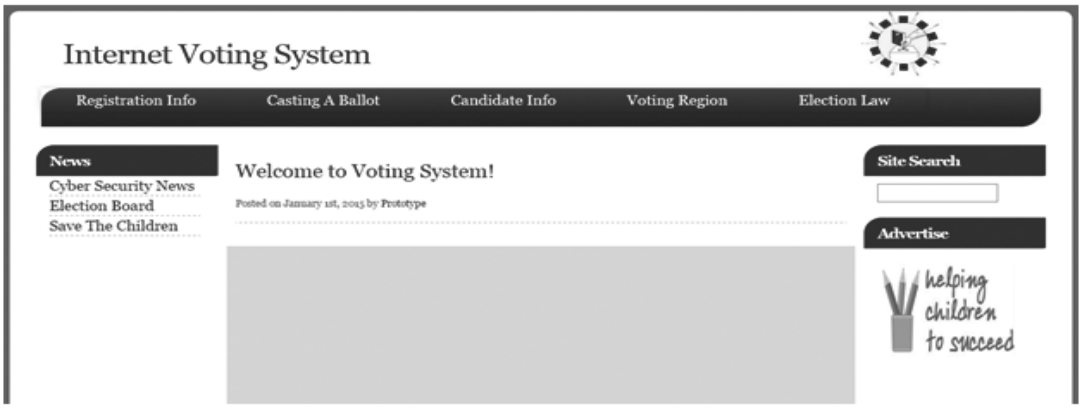

Figure 3: User Redirect Default Page

i) Voting and secrecy protection

A logged in voter is required to conform his/her eligibility by entering his/her password and registration number. If it is valid, the system displays list of candidates information who can run at the poll station that the voter is registered, avoids double vote, creates digital signature from registration number, allows more than one time online vote before the last election day, i.e., before the paper voting day. During this period, only the last vote is valid since the pervious votes are override. It provides user interface to enable authenticated voters to check their own vote to whom it is counted. It also enables an authenticated voter to delete all his/her pervious vote during online voting date. Figure 4 shows the voting page.

j) Election Setups

It creates and modifies election setups. It includes creating constituencies, poll stations, creating election calendar, business rules, election and sub election types, and allocate election officers.

Figure 4: Voting Page

k) Supporting Languages

It is a multilingual and supports English, Amharic and Afaan Oromo languages which can also be easily extended to other ethnic/regional languages of the country.

l) User management and report analysis

It modifies system users and user responsibility. It designs different report formats, and analyses the integrity of the result using backend queries and designed report.

5. Conclusion and Future Work

The proposed system uses digital signatures and advanced encryption standard to authenticate users and voters and also to secure the whole data in the database. It uses IPSec to secure the data during transmission in the network. Digital signature is used for integrity, verification and identification purposes.

To warrant vote right for physical impairments, elderly people, and people in hospitals, the proposed system will be extended to mobile environment with multimedia authentication methods.

References

[1] J. B. Esteve, B. Goldsmith, and J. Turner, "International Experience with E-Voting: Norwegian E-Vote Project", https://www.regjeringen.no/globalassets/upload/KRD/Prosjekter/e-valg/evaluering/Topic6_Assessment.pdf, Last accessed on Mar. 03, 2014.

[2] Elections BC a non-partisan office of the Legislature, Internet Voting Discussion Paper, Province of British Columbia, Victoria, British Columbia, 2011, http://www3.elections.bc.ca/docs/Internet-Voting-Discussion-Paper.pdf, Last accessed on Mar. 03, 2014.

[3] S. Mudana, "Security Flaws in Internet Voting System", Computer Science Department, University of Auckland, https://www.cs.auckland.ac.nz/courses/compsci725s2c/archive/termpapers/sr.pdf, Last accessed on Mar. 03, 2014.

[4] A. Al-Ameen and S. Talab, "The Technical Feasibility and Security of E-Voting", The national Arab Journal of Information Technology, Vol. 10, No. 4, July 2013.

[5] M. Papagelis, Web App Architectures Multi-tier (2-tier, 3-tier) & MVC, http://queens.db.toronto.edu/~papaggel/courses/csc309/docs/lectures/web-architectures.pdf, Last accessed on Apr. 14, 2014.

[6] Michel Chevallier, Michel Warynski, and Alain Sandoz, Success Factors of Geneva's e-Voting System, State Chancery, Republic and Canton of Geneva,Switzerland, http://www.ejeg.com/issue/download.html?idArticle=78, Last accessed on Jul. 17, 2014.

[7] M. Baron, "The Impact of Telecommunications Services on Doing Business in Ethiopia", Addis Ababa Chamber of Commerce and Swedish Agency for International Development Cooperation, SIDA, December 2010 http://www.ethiopianchamber.com/Data/Sites/1/psd-hub-publications/the-impact-of-telecommunications-services-on-doing-business-in-ethiopia.pdf, Last accessed on Dec., 2014.

[8] E. Cakir, Risks and Opportunities of Using SSO (Single SignOn) in a Complex System Environment with Focus on Overall Security Aspects, Linnaeus University, School of Computer Science, Physics and Mathematics, http://www.diva-portal.org/smash/get/diva2:605900/FULLTEXT01.pdf, Last accessed on Dec., 2014.

[9] I. Bregman, "Public Keys and Private Keys in Quantum Cryptography", Unpublished PhD Dissertation, Hebrew University, May 2008, http://shemer.mslib.huji.ac.il/dissertations/W/JMC/001486952.pdf, Last accessed on Mar, 2015.

[10] Network security Protocols: IPSec vs. TLS/SSL vs. SSH Part II, http://www.k2esec.com/secure-communications/network-security-protocols-ipsec-vs-tlsssl-vs-ssh-part-ii, Last accessed on Mar, 2015.

[11] C. Guenther, The Relevance of Quantum Cryptography in Modern Cryptographic Systems, GSEC Practical Requirements, December 16, 2003, http://www.sans.org/reading-room/whitepapers/awareness/relevance-quantum-cryptography-modern-cryptographic-systems-1334, Last accessed on Mar, 2015.

[12] A. G.Pillai, Quantum Cryptography, University of Washington, https://courses.cs.washington.edu/courses/csep590/06wi/finalprojects/pillai.do, Last accessed on Mar., 2015.

[13] D. Springall, T. Finkenauer, Z. Durumeric, J. Kitcat, H. Hursti, M. MacAlpine, and J.A. Halderman, "Security Analysis of the Estonian Internet Voting System", University of Michigan and Open Rights Group, U.K., https://jhalderm.com/pub/papers/ivoting-ccs14.pdf, Last accessed on July, 2015.