The Technical Feasibility and Security of E-Voting

Abdalla Al-Ameen and Samani Talab
Department of Information Technology, University of Neelain, Sudan

Abstract: *An Electronic voting (E-voting) system is a voting system in which the election data is recorded, stored and processed primarily as digital information. E-voting may become the quickest, cheapest, and the most efficient way to administer election and count vote since it only consists of simple process or procedure and require a few worker within the process. The main task of this paper is to introduce the idea of the internet voting systems. It discusses the different ways in which voters can vote, then we introduce the concepts of E-voting system .This paper observes the security threats that may affect E-voting system. This paper discusses technical and secure attributes of a good E-voting system and the reason for each attributes with respect to the voting process. In this paper we analyze some researcher's efforts in E-voting systems in order to minimize the threats that compromise E-voting systems. We end with our opinion about technical feasibility of E-voting in developing countries.*

Keywords: *E-voting, EML, threats, security, authentications schemes, integrity.*

Received May 4, 2011; accepted July 28, 2011; published online August 5, 2012

1. Introduction

An Electronic voting (E-voting) system is a voting system in which the election data is recorded, stored and processed primarily as digital information.

The research on E-voting is a very important topic for the progress of democracy. If a secure and convenient E-voting system is provided, it will be used more frequently to collect people's opinion through cyberspace.

Traditional paper-based voting can be time consuming and inconvenient. E-voting not only accelerates the whole process, but makes it less expensive and more comfortable for the voters and the authorities as well. It also, reduces the chances of the errors. E-voting system should provide all basic features that conventional voting does, further should furnish more services in order to make the process more trusted and secure [13].

In this paper, we use the phrase “E-voting” to refer to E-voting over the internet. Unlike traditional voting systems in which voter choices and intentions are represented in form of a paper ballot or other means like a punch card, Internet Voting (I-Voting) uses electronic ballots that are used to transmit voters' choices to electoral officials over the internet.

This paper focuses on introducing E-voting systems, requirements that E-voting system must meet, E-voting threats, challenges that can compromise the electoral process and some proposed E-voting solution.

The rest of this paper is organized as follows. In section 2, we provide a general description of E-voting systems. In section 3 we present the concepts of an E-voting system and the phases of the voting process. In section 4, we describe the different threats that can compromise the various areas of E-voting systems. In section 5, we give a description of desirable characteristics that should exist in any good E-voting system and the reason for each characteristic with respect to the voting process. In section 6, we analyse some proposed E-voting solution. In section 7, we discuss the possibility of applying E-voting in Developing Countries. Finally, we give our opinion about technical feasibility of remote E-voting over the internet.

2. The E-Voting Description

Electronic elections gain more and more public interest. Some countries offer their citizens to participate in elections using electronic channels. E-voting is generally any type of voting that involves electronic means [9]. The letter E is associated with anything that involves web based or computers these days. However, the terminology of E-voting is nascent, and a crucial distinction lies between the various different ways in which voters can vote.

E-voting is similar to classic “paper-form” voting. In classical “paper-form” voting voters entering the polling station have to be identified. If identification is passed, they are able to vote. The whole scenario of classical voting can be seen in Figure 1.

There are two recognized types of E-voting systems. The first one is based on visiting a polling station as illustrated in Figure 2. In this case voters are still identified by using identification cards. Voters do not fill voting cards as in the paper form but push buttons on various electronic devices.

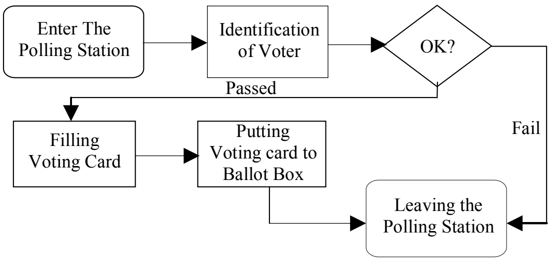
Enter The Polling Station
Identification of Voter
OK?
Passed
Fail
Filling Voting Card
Putting Voting card to Ballot Box
Leaving the Polling Station

Figure 1. The classical voting process [7].

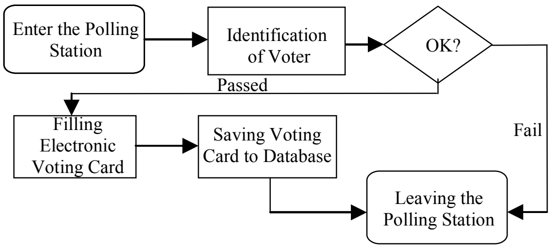
Enter the Polling Station
Identification of Voter
OK?
Passed
Fail
Filling Electronic Voting Card
Saving Voting Card to Database
Leaving the Polling Station

Figure 2. The in-site E-voting system [7].

The second type of E-voting system is based on remote technology. Usually voters have the chance to vote by using computers at remote locations or at polling stations. They use computer and internet networks for voting. Voters can vote out with the normal interval for voting (usually office hours). They can also, vote from abroad. These constitute the most important advantages of the remote-based voting system. This idea is usually called I-Voting. The whole scenario of I-Voting can be seen in Figure 3.

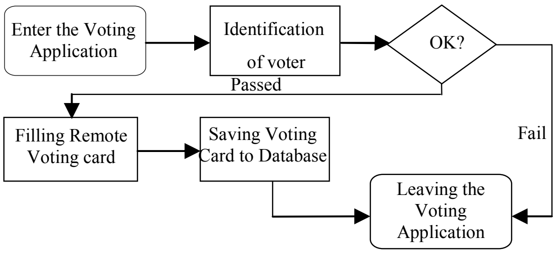
Enter the Voting Application
Identification of voter
OK?
Passed
Fail
Filling Remote Voting card
Saving Voting Card to Database
Leaving the Voting Application

Figure 3. The remote voting process [7].

3. Concept of An E-Voting System

From a conceptional perspective, E-voting can be split up into three phases:

- Pre-Voting Phase.
- Voting Phase.
- Post-Voting Phase.

Considering E-voting systems this way follows the high level models of election systems given by The Organization for the Advancement of Structured Information Standards (OASIS). The OASIS consortium specifies a so called Election Markup Language (EML) [15] especially for the exchange of data within E-voting processes. Therefore, OASIS drafts a high level overview and a high level model dealing with the human view and a high level model dealing with the technical view.

These models should be the initial point of creating E-voting concepts. EML is in particular useful for interoperability reasons. Separating the process into these phases gives a good abstraction of an election process. Moreover, these models provide a common terminology and a conceptional perspective.

3.1. Pre-Voting Phase

As depicted in the human view of the OASIS high level model shown in Figure 4, the major tasks provided within this phase are:

- *Candidate Nomination Process:* There might be various ways to become nominated as a candidate to be elected depending on the national legislative. A candidate has to meet some legal restrictions, e.g., he must be old enough, etc., the candidate suggested might have to accept his nomination, he has to decide whether to accept or decline his nomination. Finally, nomination process results in a list containing all candidates, the so called candidate list. The EML model considers referenda as well. Thus, the model includes the referendum options nomination process in parallel to the candidate nomination process [15]. In principle, they are quite similar beside the different legislative restrictions. Even the options nomination process leads to a resulting options list. In this paper we limit our scope only to elections.
- *Voter Registration Process:* Depending on the local laws, voters have to register for voting explicitly. On the other hand, in many countries citizens are registered for voting automatically. However, the result of this process is an election list containing all persons allowed to vote.

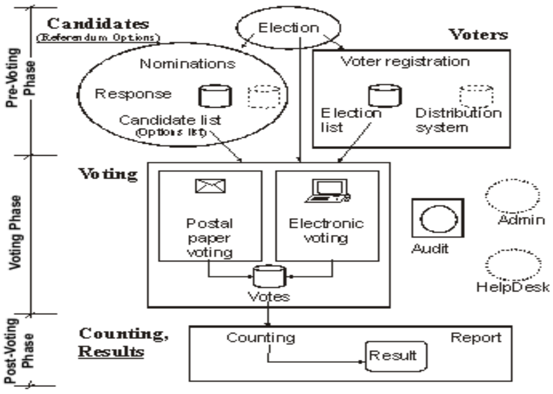

Figure 4. The human model stated by EML [15].

3.2. Voting Phase

Based on the results of the pre-voting phase, the voting phase enables all eligible voters to make their decisions and cast their votes. Thus, by the use of the election list the voter has to authenticate herself as an eligible voter and he has to cast his individual vote.

Since the voter should have an alternative to E-voting and since conventional voting with paper ballots must be provided in parallel, the model has to consider multiple possibilities. Especially the interfaces and cutting edges between electronic and conventional elections have to be considered in the conceptional design.

3.3. Post-Voting Phase

The post-voting phase deals with the juicy bites of the E-voting process. This phase covers counting and result reporting mainly.

- *Counting:* Counting is one of the most critical steps. Here, the possibility of recounting must be considered as well. Therefore, counting has to be re-runnable and the input needed, such as the cast votes in particular, have to be archived.
- *Result:* Close to the counting mechanisms, an analysis system is needed. Such a system provides the auditing team and the election officials with various reports. One of the most important reports is of course the final result of the counting. The form and the precise schema of such reports are out of scope of the model provided by EML.
- *Audit Administration:* Beside the phases and roles given above, there are some other important actors and elements in the model. Very important are the audit mechanisms needed along all phases of an election. On the one hand, it is important to have possibilities to prove the correctness of the process as such. On the other hand, it is crucial to do not violate the main principles and security requirements, keeping a vote an inviolable secret in particular. However, audit is necessary to prove the authenticity of the result of the election. Thus, a special set of persons, e.g., election officials and candidate's representatives, should be allowed to gain access to auditing information.

System administration is critical as well, since administrators are allowed to access the system. Nevertheless, administration is necessary and therefore the security concept of the E-voting system has to protect critical data and components, the secrecy of the ballots especially. This affects the organizational aspects of the security concept either. Not only technical security mechanisms can guarantee this. The administrative staff has to be elected in respect to reliability as well.

4. E-Voting Threats

E-voting systems threats exist in many different forms; they can compromise an E-voting system in various ways. Different threats can compromise the various areas of security leading to untrustworthy systems.

4.1. Denial of Service

Denial of Service (DoS) attacks that are carried out have devastating consequences and in most cases the extremely affect the ability to provide availability to a system. The following two methods described are how a hacker may compromise the availability to a voting system.

4.1.1. Ping of Death

The ping of death relies on a flaw in some Transmission Control Protocol, Internet Protocol (TCP/IP) stack implementations. The attack relates to the handling of unusually and illegally large ping packets. Remote systems receiving such packets can crash as the memory allocated for storing packets overflows. The attack does not affect all systems in the same way, some systems will crash, and others will remain unaffected [5].

4.1.2. Packet Flooding

Packet flooding exploits the fact that establishing a connection with the TCP protocol involves a three-phase handshake between the systems. In a packet flooding attack, an attacking host sends many packets and does not respond with an acknowledgment to the receiving host. As the receiving host is waiting for more and more acknowledgments, the buffer queue will fill up. Ultimately, the receiving machine can no longer accept legitimate connections [5].

4.2. Viruses

A computer virus is a computer program that can reproduce itself and may cause undesired effects in computers where it is active. To do its malicious work, the virus needs executing. Usually viruses are located together with other code that is likely, will be executed by a user. As long as the virus is active on the computer, it can copy itself to other files or disks when they are used [23]. Viruses made could destroy E-voting systems. This could compromise the availability at election time forcing governments and institutions to perform re-elections.

4.3. Worms

A worm is a type of virus that does not change any existing program or file to spread itself. Instead, it makes copies of itself within an infected computer and spreads to become active on other systems. It is intentionally destructive, overwriting portions of the files with random data [23]. This damage is non-repairable, so files may need reinstallation or restoring from a backup. Worms could overwrite files and change results of votes if programmed to do so, brining the integrity of the votes into question.

4.4. Trojan Horses

Trojan horses are pieces of computer code that download to a computer while connected to the internet. They may be harmless, but it could possibly delete or modify an important file from the computer, plant a harmful virus, or even steal user's passwords [23]. This makes all sorts of fraudulent schemes possible.

Once inside a computer the Trojan horse can access passwords, screen names and other personal information and then distribute this confidential data to the attacker. Trojan horse represents an immense threat to systems confidentially and integrity of information of E-voting systems.

4.5. Physical Attacks

Numerous physical attacks can be carried out on E-voting system to sabotage an election. Vandalism of E-voting systems would make them inoperable for the day of the election. Saboteur's could remove network connections and pull plugs out of E-voting systems causing votes to be lost. Attackers may remove hard drives or smart cards replacing them with falsified data. E-voting machines could be stolen with attackers discovering sensitive voting information about users.

5. Technical and Secure Attributes of a Good E-Voting System

The following is a description of desirable characteristics that should exist in any good E-voting system and the reason for each characteristic with respect to the voting process.

5.1. Accuracy

"A system is accurate if 1). It is not possible for a vote to be altered, 2). It is not possible for a validated vote to be eliminated from the final tally, 3). It is not possible for an invalid vote to be counted in the final tally [2]".

Accuracy is one of the most important factors to any system. If the input is not correct, then the result will not be correct. Not only should the system be accurate in counting votes and maintaining the integrity of cast ballots, the system should be accurate in identifying voters.

5.2. Verifiability

"A system is verifiable if anyone can independently verify that all votes have been counted correctly" [2]. Currently, many experts believe that the best method to verify votes and perform recounts is with paper ballots. In addition, the voter should be able to verify that their ballot is entered correctly and allow them to adjust their vote if necessary. The process needs to verify the validity of the voter as well. Perhaps the use of a nationwide database of registered voters' information and a method of non-intrusive biometrics could identify participants. The system should also, verify that the E-voting system has not been compromised.

5.3. Democracy

"A system is democratic if 1). It permits only eligible voters to vote and 2). It ensures that each eligible voter can vote only once [2]". This characteristic can be accomplished by incorporating accuracy and verifiability. Currently, many counties require that voters vote in their own precinct so, that they can sign their name in the approved voter list. Some counties have implemented a database that tracks voters. A voter must be able to show proof of their identity, the database is then updated, which prevents that voter from going to another precinct and voting again.

5.4. Privacy

Privacy is one of the most important properties of an information system must satisfy, in which systems the need to share information among different, not trusted entities [3]. "A system is private if 1). Neither election authorities nor anyone else can link any ballot to the voter who cast it and 2). No voter can prove that he or she voted in a particular way [2]". Privacy is a concern to all users of a voting system. While it is important to have an audit trail available to verify the system, aggregate data should be accessible as opposed to an individual's vote. Some voters have problems using the voting machines, this requires that a staff volunteer assists them and this can interfere with the privacy of the voter. "The second privacy factor is important for the prevention of vote buying and extortion. Voters can only sell their votes if they are able to prove to the buyer that they actually voted according to the buyer's wishes [2]".

5.5. Convenience

"A system is convenient if it allows voters to cast their votes quickly, in one session, and with minimal equipment or special skills [2]". The introduction of touch screens into the voting process was first used to aid the disabled population [1]. This increased convenience of touch screens could lead to higher voter participation and decreased time at the polls. If the system utilizes technology that society is already comfortable using, voters will perceive the system to be more convenient.

5.6. Flexibility

"A system is flexible if it allows a variety of ballot question formats, including open ended questions. Flexibility is important for write-in candidates and some survey questions [2]". It is probably less common now for voters to write in candidate choices; however, the system should be dynamic especially in our ever-changing fast-paced society. Additionally, the system should be able to accept more than one method of input to accommodate both voters at the polls and absentee ballots.

5.7. Mobility

"A system is mobile if there are no restrictions (other than logistical ones) on the location from which a voter can cast a vote [2]". Mobility in the system could allow voters the capability of voting anywhere internet access is available. This characteristic is better suited for an online E-voting system. However, the designs of the physical machines need to be small enough to accommodate various polling locations where space could be an issue.

5.8. Reliability

A system is reliable if it performs and maintains its functions continuously. Reliability in the system requires that there be alternative methods should failure occur. For example, in the event of a power failure, the system should have an uninterruptible power source or an alternative paper method. Many polls did not open on time because of machines malfunctioning.

5.9. Consistency

A system is consistent if it operates efficiently at each location, in each situation, and the functions perform exactly as designed [6]. Each voting machine must be an exact duplicate of the other to ensure consistency and quality control. This also, increases usability as the voting process does not vary between locations, especially important for our mobile society.

5.10. Social Acceptance

A system has social acceptance if it has favorable reception and is perceived as being an effective system by the voting population [16]. It can be easy to overlook the users involved in a system. Even if the system is sound, users are what make or break the system. Perception is crucial. Currently, society views the majority of E-voting as inaccurate, unusable, and not private.

6. Countermeasures of Threats Against E-Voting Systems

In an effort to minimize the above mentioned threats, researchers have proposed a number of mitigation controls and in the following paragraphs we summarize some.

6.1. Authentications Schemes

In literature [12, 18], some researchers have suggested that physical and logical access to the voting systems should be based on credential and rights granted either on role based or need to know policy. Voters and administrators must gain access with nontrivial authentication mechanisms that may require use of smartcards [20] for stronger security.

In Estonian E-voting System (EstEVS) [25] the national Public Key Infrastructure is applied and voters use their authentication and digital signature certificates for casting votes. In Secure Electronic Registration and Voting Experiment (SERVE), performed in the United States of America, it is possible to vote any time within 30 days before the election day until the closing time of polls on the election day. Every voter can vote only once. There are no public key infrastructure and ID-cards used in SERVE [25].

However, some authentications schemes which offer a strong authentication require either a user to memorize complex credentials or they are technically expensive in monetary and privacy terms. This is because users may be required to buy end user authentication devices like cryptographic calculators and biometric readers; additionally, transfer of biometric data over public networks raises privacy concerns on the side of users.

6.2. Virus

From literature [21], it is clear that sensitizing users into knowing the dangers of keeping update versions of software and being careful on the type of software they install on their computers can tremendous reduce the risks. Though most antivirus software is commercial, there are also, non commercial versions of software that voters could use before a voting process to ensure that their computers are free of viruses. However, these problems cannot be easily solved for all client computers participating in an election where people are voting from their homes.

6.3. Solution to Phishing Scams

Social phishing scams can be prevented through educating of E-voting system users about the various means through which phishing scams can be launched [4, 18]. However, this requires that the educators themselves keep updated with current methods of exploitation. Otherwise, taught methods of attack and defences for the voters could be out dated and could still leave the voters vulnerable to social phishing scams. More importantly, technical phishing scams are more dangerous that social ones, since their effect can be easily wide spread in an election process. However, the solution equally solves the problem on a wide scale. Strong authentication is required in the E-voting system by means of mutual authentication. Mutual authentication schemes require the clients to be authenticated to the server software, and the server software also, authenticated to the client. In that way, voters protected from technical phishing scams.

6.4. Integrity Threats Solutions

System changes must be prohibited throughout the active stages of the election process. Voting systems need to be verified by independent non partisan bodies that will look at the source code and verify that it does exactly what it was designed to do. The use of cryptography exchange of messages can guarantee integrity of information exchange. Indrajit and Indrkshi [17] developed an algorithm that protects voters' votes by use of cryptographic keys, in which it is not possible to link a voter to a vote unless the voter has cooperated. The requirements of vote secrecy and voter anonymity has not been a problem in itself, but achieving both of them (secrecy and voter anonymity) at the same time has been a problem to vote accountability and dispute resolution after voting process.

6.5. Subverting System Accountability Solutions

Although, in some literature [14, 18], researchers have advocated for use of encryption and checksums on audit trails to help in detecting changes to file system audit trails, additional use of audited open systems code on the server environment can also, minimize the risks of running source code with undesirable side effects [10].

6.6. Network Infrastructure

Through redundancy, use of cryptograph, and the concept of honey spots, attacks on network infrastructure can be minimized. However, we note that it is fairly difficult to prevent some attacks along the communication channels like DoS [7].

6.7. Legal Protection

Attacks on mission critical systems in countries like the USA and UK are being handled as criminal cases [6, 21] for which culprits have to be prosecuted. The act of hackers/crackers gaining unauthorized access to computer system can be compared to someone breaking into a house as a means of checking whether it is secure.

6.8. Open Source Systems in E-Voting

In literature [11, 19, 24] a concept of using open source systems for E-voting has been proposed. The debate rages on whether it is a good idea to have open source systems powering E-voting over the internet or not? The question of whether open source systems can be trusted more than closed source systems still stands? A Ken Thompson in his article entitled "Reflections on Trusting Trust" indicates you can't trust code that you did not totally create yourself [24]. The paper by Ken presents an ingenious piece of code which can be used to create another program from itself in a way that is not easy to detect my non sharp-eyed programmer. Software written in a similar comportment can be used to introduce trap and back doors in an application.

7. E-Voting in Developing Countries

It is true that the application of E-voting system requires many resources such as qualified computer network infrastructure and computer machines, knowledge in computer systems and internet technology, good human resources to manage online system, and 'culture' to use computer in society.

In developing countries, the quality of data communication infrastructure is not quite good and only available in certain areas. The governments still has to spend a lot of money to develop communication infrastructure, while providing qualified human resources to manage that. Besides, the level of education in society is not quite high.

Many people do not know what computer is, and how to operate it. In other word, most of them are not familiar with computer. Due to limited budget, a lack of qualified human resources and computer knowledge, E-voting system is not a good choice to be applied in the public election at the moment.

E-voting will be easier to be implemented in developed countries than in developing countries because it will takes a large portion of fund to be invested and need more educated people to get involved through it. On the other hand, those developing countries usually have limited national budget to run the new system and most of their people are still live under poverty and undereducated.

The most well-known use of E-voting is Estonia, where since 2000; internet access is considered a fundamental human right. Estonia was the first country to use I-Voting in a nationwide public election. In 2005, 9,317 Estonians voted online (approximately 1.85% of all voters). In 2007, Estonia again used I-Voting in their national parliamentary elections, and 30,275 people voted online (5.4% of all voters).Voter identification is achieved using Estonians' national identification cards, which contain a microchip that enables the voting system to identify the voter. To vote online, voters need to purchase card readers and special software [25].

The need for E-voting in the world's developing countries tends to be overshadowed by the nation's deficiencies in physical infrastructure. Consequently E-voting may be inadequately addressed by governments and supporting agencies in their plans for stimulating democracy.

8. Conclusions

Over the last year, there has been strong interest in E-voting as a way to make voting more convenient and, it is expected, to increase participation in election process. E-voting systems are among those being considered to replace traditional voting system.

E-voting may become the quickest, cheapest, and the most efficient way to administer election and count vote since it only consists of simple process or procedure and require a few worker within the process.

The main task of this contribution was to introduce the idea of the I-Voting systems. Security plays a major role in the development of any E-voting system. Availability, integrity, confidentiality, non-repudiation, and authentication are key areas in computer security; by amalgamating these areas of security, together they form a cohesive bond that helps guarantee voter trust in E-voting system.

However, there are many threats that exist, that many hinder E-voting system to function correctly such as DoS attacks, worms, viruses, and Trojan horses to name a few. It is imperative to correct all weaknesses of E-voting systems to ensure a full voter trust compared to that of traditional voting.

Many methods can be used in order to face E-voting problems as mentioned in section 6.

A desirable voting system should be accessible to all potential voters. In some societies like in the developing countries, not all voters have access to a computer and internet. In fact a good number of them do not have knowledge of computer usage and the internet. In such cases, the internet can be used as an option to improve voter turnout. However, if the election is only facilitated by internet voting, then the technology would end up becoming a barrier to voter participation

Therefore, we recommend that before applying E-voting system, developing countries governments should consider to fulfill the requirements mentioned in section 7 and tested many times before this system is released.

References

[1] Bellis M., The History of Voting Machines Inventors, available at: http://inventors.about.com/library/weekly/aa111300b.htm, last visited 2009.

[2] Cranor L. and Cytron R., "Design and Implementation of a Security-Conscious Electronic Polling System," *Technical Report*, Washington University Computer Science, 1996.

[3] El-Sisi A., "Fast Cryptographic Privacy Preserving Association Rules Mining on Distributed Homogenous Database," *The International Arab Journal of Information Technology*, vol. 7, no. 2, pp. 152-153, 2010.

[4] Espiner T., "Microsoft Launches Legal Assault on Phishers," available at: http://news.zdnet.co.uk/0,39020330,39258528,00.htm, last visited 2009.

[5] Evans M. and Furnell S., "Internet-Based Security Incidents and the Potential for False Alarms," *Electronic Networking Applications and Policy*, vol. 10, no. 3, pp. 238-245, 2000.

[6] Friedenberg M., Heller B., McCracken W., and Schultz T., "E-voting System Requirements: An Analysis at the Legal, Ethical, Security, and Usability Levels," available at: http://www.marcfriedenberg.com/wp-ontent/evoting.pdf, last visited 2011.

[7] Gibson S., "Distribute Denial of Service Attack," available at: http://www.grc.com/dos/drdos.htm, last visited 2011.

[8] Hollinger R. and Lanza-Kaduce L., "The Process of Criminalization," *The Case of Computer Crime Laws*, vol. 26, no. 1, pp. 101-126, 1988.

[9] IPI, "Report of the National Workshop on Internet Voting: Issues and Research Agenda," *Technical Report*, Internet Policy Institute, Washington, 2003.

[10] Jefferson D., Rubin A., Simons B., and Wagner D., "Analyzing Internet Voting Security," *Communications of the ACM*, vol. 47, no. 10, pp. 59-64, 2004.

[11] Jefferson D., Rubin A., Simons B., and Wagner D., "A Security Analysis of the Secure Electronic Registration and Voting Experiment (SERVE)," *Technical Report*, available at: http://www.servesecurityreport.org, last visited 2009.

[12] Kohno T., Stubblefield A., Rubin A., and Wallach D., "Analysis of an Electronic Voting System, Security and Privacy," *in Proceedings of IEEE Symposium on Security and Privacy*, USA, pp. 27-40, 2004.

[13] Leenes R. and Svensson K., "Adapting E-voting in Europe: Context Matters," *in Proceedings of EGPA*, 2002.

[14] Neumann P., "Security Criteria for Electronic Voting," *in Proceedings of the 16th National Computer Security Conference*, Maryland, pp. 478-482, 1993.

[15] Organization for the Advancement of Structured Information Standards, available at: http://www.oasis open.org/committees/election/index.shtml, last visited 2003.

[16] Parakh A. and Kak S., "How to Improve Security in Electronic Voting," *Ubiquity Information Everywhere*, vol. 8, no. 6, pp. 1-7, 2007.

[17] Ray I. and Narasimhamurthi N., “An Anonymous Electronic Voting Protocol for Voting Over the Internet,” *in Proceedings of the 3rd International Workshop on Advanced Issues of E-Commerce and Webbased Information Systems*, CA, pp. 188-190, 2001.

[18] Rubin A., “Security Considerations for Remote Electronic Voting over the Internet,” *Communications of the ACM*, vol. 45, no. 12, pp. 39-44, 2002.

[19] Schneier B., The Problem with Electronic Voting Machine, available at: http://www.schneier.com/ blog/archives/2004/11/ the problem wit.html, last visited 2010.

[20] Sun H., “An Efficient Remote use of Authentication Scheme using Smart Cards,” *IEEE Transactions on Consumer Electronic*, vol. 46, no. 4, pp. 858-961, 2000.

[21] Symantec Security Response, available at: http://securityresponse.symantec.com/avcenter/security/Advisories.html, last visited 2011.

[22] Tavani H., “Defining the Boundaries of Computer Crime: Piracy, Breakins, and Sabotage in Cyberspace,” *ACM SIGCAS Computers and Society*, vol. 30, no. 3, pp. 3-9, 2000.

[23] Falk H., “Computer Intrusions and Attacks,” *The Electronic Library*, vol. 17, no. 2, pp. 115-119, 1999.

[24] Thompson K., “Reflections on Trusting Trust,” *Communications of the ACM*, vol. 27, no. 8, pp. 761-763, 1984.

[25] Triinu M. and Buldas A., “Practical Security Analysis of E-voting Systems,” *in Proceedings of Advances in Information and Computer Security, Lecture Notes in Computer Science*, vol. 4752, pp. 320-335, 2007.

Abdalla Al-Ameen received his BSc degree in computer science from International University of Africa, Sudan in 1997. He completed his MSc in information technology form AL Neelain University, Sudan. Currently, he is working toward PhD degree in department of computer science and information technology at AL Neelain University, Sudan. His fields of interest are in data security, web design and web application modelling with UML.

Samani Talab received his BSc, MSc and PhD degree in computer science from department of computer science, University of Khartoum, Sudan in 1989, 1995, and 2001 respectively. Currently, he is working as dean, associate professor of computer science faculty of computer science and information technology, AL-Neelain University, Khartoum, Sudan. His research interests include data structures, algorithms, teaching and learning, compiler design and numerical computation.