# SECURITY THREATS ON E - VOTING SYSTEM IN NIGERIA

**1. Isah Baba Ahmed *,2. Uzairu M. Gwadabe ,3. Abubakar. M. Isah , 4. Nasa'i M. Gwadabe , 5. Usman A. Yakubu**

1 Department of Computer science, Niger State Polytechnic, P.M.B 1, Zungeru
kasuwa65@yahoo.com

2 Faculty of Economics and Management Sciences, University Sultan Zainal Abidin, 22300, Kuala Terengganu, Malaysia
uzairumg@gmail.com

3 Government Day Secondary School Takatuku,
Bodinga Local Government,
imilan1984@gmail.com

4 Faculty of Humanities,
Northwest University Kano, Nigeria
ngwadabe@gmail.com

5 Faculty of Science,
Northwest University Kano, Nigeria
usman.abbas84@yahoo.com

**Abstract**

A remote voting system allows voters to participate in the electoral process if they are granted access to the election. They can do so regardless of their location at the time of voting. However, this scheme needs a secure, private network to connect the poll stations, which is usually very expensive. Also, the scheme suffers from declining participation due to the inconvenience to the voters in reaching the poll stations. This type of voting is user convenient, as it allows voting from over the internet. However, the online voting is exposed to threats, as there are many malicious programs, software and network applications, like worms, viruses, identity theft, phishing, online fraud which dents confidentiality of democratic decision-making process and implementation bugs that will need to be addressed before using the same scheme in practice. The rest of the paper is organized as follows: Section two introduces, in brief, the notion on both the poll site and remote voting, section 3 Conceptual Discourse, methodology and theoretical framework, section 4 briefly discusses the types of attack, Section 5 security threats and section 6 recommendation and conclusion.

**Keywords:** Security, Threat, Internet, Voting and Democracy

## Introduction

Democracy follows the rule of law where equal rights are given to all the electorates (Okedira et al., 2011). An election is well - defined as a formal decision - making process by which a population chooses an individual to hold public office. Also, election is a process to affirm democracy (Howard, 2001). The integrity of voting processing is central to democracy (Olaniyi et al., 2012). However, internet voting systems enable a voter to vote over the internet while providing accuracy and security. Internet voting can be of two types - poll - site and remote voting. Poll - site voting enables the voter to vote over the internet, at a voting poll. Remote voting allows the voter to vote from anywhere around the globe thus removing geographical restrictions. Advancement in the ICT world has penetrated all facets of life without leaving behind the voting system, thereby introducing the use of computer technologies in voting (Okedira et al., 2011). The automation of voting could be a vehicle for fraudulent acts such as electronic ballot spoofing, vote falsification, vote rigging and invalid votes by erring administrators and eavesdroppers (Olaniyi et al., 2013). The security is one of the main concerns, such as authentication, confidentiality, integrity and non - repudiation. It is not an easy task to achieve secure e-voting.

## Problem Statement

In Nigeria, there are lots of irregularities surrounding the conduct of elections. These irregularities are usually characterized by ballot box snatching, vote buying, manual registration of voters; there was neither any database for voters nor any technology introduced to minimized double registration if not by 2011 thereby undermining the credibility of the election. As a result of the above, if e-voting is introduced, it would lead to the correction of these unusual or flaws associated with the conventional voting in Nigeria. However, attractive e-voting is, the complexity of building secure electronic voting is

challenging. The challenges such as Denial of service attack increased vulnerability to security threats like malware and Man – in – Middle attacks making e-voting system vulnerable to security threats.

**Conceptual Discourse**

We can bank online, so why cannot we vote online? There is a good reason, argued security experts. We do everything online; book doctor's appointments, manage our bank accounts and fix dates but we still cannot yet vote from our Personal Computers or Smart phones. The United Kingdom (UK) has run trials for local elections before 2002, 2003 and 2007 – and Estonia famously became the first to offer online voting for its general elections for parliament in 2007, but critics continue to call for cautions, saying electronic voting is not secure enough to trust for the basis of our democracy – and many never be. Kitcat(2007) argued there are three requirements for robust political elections: Security, anonymity and verifiability. "Meeting those three requirements is a complicated problem quite unlike other transactions ". Online banking suffers problems, but refunds are possible after checking the balance statements, but cannot be provided to check the vote selling and coercion."

At present, there are some trials of these systems being carried out worldwide. Proponents of e-voting have argued that it will have the following salutary effects: increased participation for disadvantaged communities, an antidote to voters apathy, greater voter convenience in terms of voting time and location, access for people with disabilities, money saving, and greater accuracy(Mohen and Glidden, 2001). However, some authors have raised cautions that e-voting possess many security issues (Mercuri, 2002; Neumann, 2001). Availability: - An e-voting system must remain available during the whole election and must serve voters connecting from their devices. Notably, the e-voting system must be prepared for high workload, because there will be periods where many voters will place their votes simultaneously. Eligibility: - Only eligible voters are allowed to cast a ballot, while only one vote per voter counts. If it is allowed to vote multiple times (also called re-vote), the most recent ballot will be tallied, and all others must be discarded.

**Integrity**: - The integrity of the vote must be guaranteed. Voting systems must ensure that the ballots are not altered during any step of the election. Otherwise, we cannot trust this system.

**Anonymity and Election Secrecy**: - The connection between the vote of a user and the user herself must not be reconstructable without her help.

**Fairness**: - the Voting system must ensure that no(partial) results are published before the tallying has ended. Otherwise, voters can be influenced by these results and vote differently.

**Correctness**: - The elections results must be counted appropriately and correctly published.

**Robustnes**: - The system should be able to tolerate (some ) faulty votes. Attackers might try to cast malicious ballots, but these ballots must be detected. A voting system has to recognize these ballots to prevent vote – manipulation or attacks on the servers.

**Universal Verifiability:** - After the tallying process, the results are published and must be verifiable by everybody. The electronic voting system must provide mechanisms to verify the election's outcome. This depends on the building blocks the system is built upon and must not break other preliminaries.

**Voter Verifiability**: - The voter herself must be able to verify that her ballot arrived in the ballot box. That ensures that the voter is sure her vote was counted and was not modified.

**Coercion Freeness**: - Voting systems must provide security mechanisms to present a coercer from being able to force the voter place a vote for a specific party, candidate etc. or even to see that she voted. This is also called receipt-freeness. A voting system must be built coercion – resistant to guarantee that a voter can place her vote as intended even in the presence of a coercer. Even vote – selling must be unattractive or too expensive. Coercion is a significant problem in voting systems.

These requirements are necessary for a secure e-voting, which adds complexity and makes secure design and a user interface more difficult. The big challenge for voting systems is to fulfil as many requirements as possible and create a secure voting system that is easy enough for everybody to understand and to use.

Also, it may not be possible to prevent widespread vote selling. Since this could be done from an offshore location, jurisdictional sanctions may not exist. There are also internet infrastructure problems that make voting susceptible to denial of service attacks. That could be carried out selectively to

disenfranchise voters in particular neighbourhoods.
Internet voting systems are vulnerable to all forms of the security flaws, such as denial of service attacks, spoofing attacks, malicious code attacks, spyware attacks, remote management attacks, and automated vote selling schemes. These attacks are powerful enough to compromise large numbers of votes, either disenfranchising voters, spying on their votes, changing their votes or buying votes. These attacks can often succeed, possibly changing the results of an election, and yet go completely undetected (Wolchok, E.W., Isabel.D & Halderman, A.,2012). According to David Jefferson(2004), these vulnerabilities are fundamental. They cannot be designed around or fixed with the current generation of personal computer hardware and software and the current internet protocols. Until security architectures of the internet and the personal computer have been completely redesigned and, the new designs widely developed, which is probably at least a decade away, internet voting in public elections must remain out of the question.

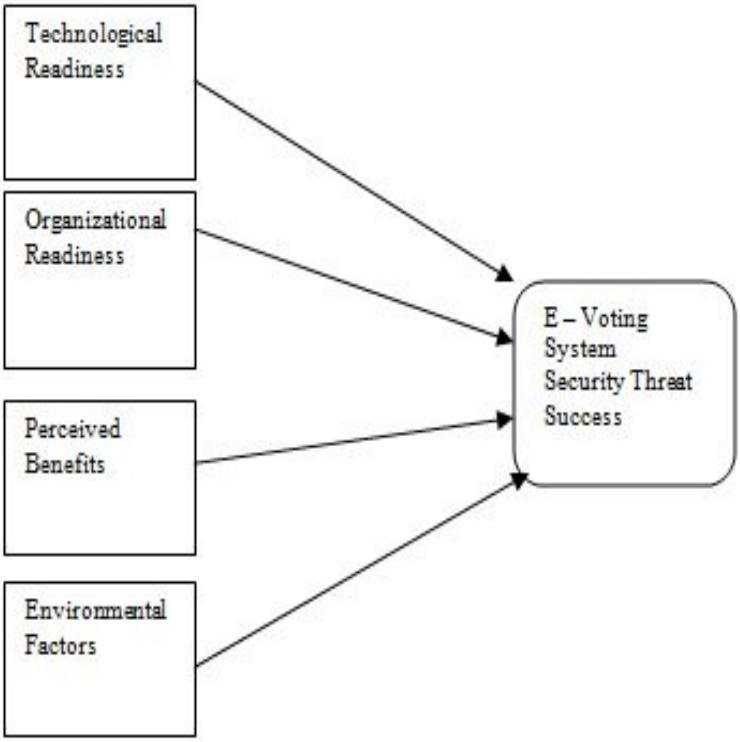
**Methodology and theoretical framework**
To further investigate the security of the e-voting system, we set up a copy of the system in our lab, reproducing the software and configuration used for the 2013 election. While pen testing during a real election would have involved numerous legal and ethical problems (Robinson et al.,2011), our laboratory setup allowed us to play the role of an attacker in our mock election without any risk of interfering with real votes.

**Mock Election Setup**
To reproduce the e-voting servers, we used the source code published on Git Hub by the election authority(Halderman, J. et al. 2014). We set up the servers by following published configuration documents(Springall, D. et al. (2014)and matching step – for – step the actions performed by election workers(https://www.youtube.com/channel). As part of this process, we generated our key pairs for the web server TLS certificate and the selection key. Some components were missing from the published server code, but we attempted to recreate them as faithfully as possible. In real elections, Estonia uses a hardware security module(HSM) to handle the private election key and decrypt votes. Since we did not have compatible hardware available, we emulated the HSM in software using OpenSSL and Python. Since deviating from the fielded setup, we ensured that none of our attacks depends on vulnerabilities in the HSM. Since we did not have access to actual Estonian ID cards, we had to emulate them. We replaced the ID card on the client with a software-based emulator that speaks the protocol expected by the voting client application. Once again, we ensured that the success of our attacks does not rely on the changes we made. We assume for this study that the ID cards and associated infrastructure are secure.

**Theoretical Framework**
The need to understand the adoption of IT innovations factors in the organizational context has witnessed the development of theories on the subject matter (Tomatzky et al.1990; Rogers, 1995; Lacovou, et al. 1995). Research findings equally shows that combining related factors and integrating constructs of similar or same factors for a specific adoption study from these theories to develop a conceptual model assist in better understanding of the determinants factors influencing such adoption(Scott, et al. 2008; Oliveira, & Martins, 2011; Salimonu, et al. 2013). In this research, factors and constructs from Diffusion of Innovations (DOI) proposed by (Rogers, 1995). Technology – Organization – Environment (TOE) offered by (Tomatzky, et al.1990), and Lacovou et al., proposed by (Lacovou, et al. (1995) were adapted and integrated to form the basis for our research model(see figure 1). The dependent variable is the e-voting security threat (EST), which is the variable of interest in this research. We attempt to explain variance in this dependent variable by the four independent variables of (1) Technological Readiness (TR), (2) Organizational Readiness(OR), (3) Environmental Factors(EF), and (4) Perceived Benefits(PB). TR is the degree to which the organization is ready technologically to threat IT security; TOE (1990) model supports this. OR refers to the degree to which an organization is prepared for the threat IT security in line with their internal structural characteristics, this variable is supported by(Tomatzky, et al.1990; Rogers, 1995 and Lacovou, et al., 1995) models. EF identifies those factors external to the organization which can minimize the successful threat of IT security; TOE's model supports it. PB is the benefits derivable by the organization for minimizes the IT security threat, this can be direct or indirect. Lacovou et al., model support this variable.

**Technological Readiness (TR)**
This variable defines the degree to which the organization is ready technologically to adopt IT innovation. Tomatzky and Fleischer (1990) describe technological factor (context) in terms of availability and characteristics of the technologies (internal and external) relevant to the firm or organization. Findings of Oliveria and Martins (2011) confirm that technological capacities among other factors played an essential role in the IT diffusion process at the organizational level. Alvar (2011) identify the aspect of

technology such as its reliability, its level of security and its relationship with existing technology contributing to the overall framework of a factor of the security threat. Technological factors are the most obvious factors which an organization must establish and asses about its present organizational structures and culture to make an explicit threat decision of its readiness and ability about happening in technology threat (Alvar, 2011). Technological Readiness (TR) is expected to measure the technology metrics such as reliability, user ability, and security of e-voting as a critical determinant in the threat process. This variable can be used to measure the readiness of INEC in terms of technology resources such as hardware, software and other ICT equipment made available to achieve e-voting threat success.




**Organizational Readiness (OR)**

Organizational readiness define the degree to which the organization is ready for IT innovation. Tomatkzy and Fleischer (1990) describe organizational context (willingness) as the characteristics and resources of the organization, including the organization's size, the degree of centralization, the degree of formalization, managerial structure, human resource, amount of slack resources, and linkages among the employees. Rogers(1995) include interconnectedness as a significant construct to measure organizational determinant factor to the reduction of a threat to the security of IT.

**Environmental Factors (EF)**

Environmental Factors variable establish those factors external to the organization which can impact the reduce threat on the security of IT. The environmental context is the place in which an organization conducts business. This includes the industry, competitors, regulations, and connections with the government. These are factors external to an organization that present limitations or restrictions and prospects for technological innovations (Rogers(1995), (Tomatzky, L.et al.1990).

**Perceived Benefits (PB)**

Perceived Benefits (PB) variable describe the understanding of the benefits to be derived from the reduction from the IT security threat innovation. A variable derived from, Lacovou, C .et al. (1995) model. Perceived benefits refer to the expected advantages that IT security threat can provide to the organization. The benefits are both direct and indirect. Immediate benefits measure operational cost savings and other internal efficient arising from the IT security threat, while indirect benefits measure

the opportunities that originate from the IT security threat, such as better service delivery and the capacity for the process reengineering. At the level of technology, the perceived benefits take into consideration the appropriate interests of an IT security(Chwelos et al.2001). The research model is expected to measure indirect benefits of e-voting technology to the organization under study in terms of, Accuracy of the vote count, Stoppage of multiple registrations, and eliminating of numerous voting, Ballot stuffing, Vote manipulation, and Ease of use.

**The Client and Server Related Security Issues**

With today's hardware and software architectures, penetration attacks involve the use of a delivery mechanism to transport a malicious payload to the target server or host in the form of the remote control program or a Trojan horse. Once executed, it can spy on ballots, prevent voters from casting ballots, or, even worse, modify the ballot according to its instructions, thus having a direct effect on the election, and bringing the integrity of the entire process into question. What makes the latter threat particularly insidious is that it can be accomplished without detection, and such security mechanism as encryption and authentication(e.g., secure socket layer(SSL)) and secure hypertext transport protocol(https)) are impotent against this kind of attack in that its target is below the level of abstraction at which those security protocols operate(e.g., the operating system or browser). Virus and intrusion detection software is also likely to be powerless against this threat because detection mechanisms generally look for known signatures of malicious programs or other signs of unauthorized activity. These stealth attacks usually emanate from unknown or modified programs and alter system files to effectively "authorize "the changes made (after which they might disable further virus protection). This attack could originate from anywhere in the world.

These malicious payloads can be delivered either through some input medium(e.g., CD – ROM or Optical drive), download, or email, or by exploiting existing bugs and security flaws in such programs as Internet browsers. Activation need not be the intention(e.g., double-clicking an icon), but can also occur by executing compromised code that users intentionally download from the internet(e.g. device drivers, cookies, and multimedia) or unknowingly download(e.g., Active X controls associated with Web pages they visit). Even the simple viewing of a message in the preview screen of an email client has, in some cases, proved sufficient to trigger execution of its attachment.

A Trojan horse, once delivered to its host and executed, might be activated at any time, either by remote control, by a timer mechanism, or through detecting certain events on the host( or a combination of all three). If such a program were to be widely distributed and then triggered on or about Election Day, many voters could be disenfranchised or have their votes modified. Attacks do not have to be confined to the individual or random voters but can be targeted on a particular demographic group. Remote control software introduces a similar concern in that those monitoring the host's activity may compromise the secrecy and integrity of the ballot. In principle, poll site voting is much less susceptible than remote voting to such attacks.

The Software on voting machines would be controlled and supervised by elections officials and would be configured to prevent communication with any Internet host except the proper election servers. Election officials and vendors could configure voting clients so that voters and poll workers would be unable to reboot the machines or introduce any software other than the voting application. Careful monitoring of the system could reduce the risks even further. Opportunities for attack and insider fraud, however, would still exist, especially since voting jurisdiction may have difficulty getting the reliable technical support they need to administer their system correctly.

**Attacking Ballot Secrecy**

While we focused on attacks against the integrity of election results, we also considered ballot secrecy issues, since the secrecy of the voter's ballot is a critical defence against voter coercion and vote buying in Germany. The internet voting system implements relatively strong protection against in – person, individual coercion by allowing voters to cast replacement votes online or to cancel their electronic ballots entirely and vote in person on Election Day in Germany. More sophisticated attacks remain possible, however, including spyware on the voter's PC or smartphone, as well as server-side attacks. Server-side attacks on ballot secrecy are particularly troubling, since preserving ballot secrecy is the primary goal of the system's cryptographic double – envelope architecture. The internet voting design attempts to ensure that votes remain private by breaking the association between voters' digital signatures from their plaintext votes. The encrypted ballots are separated from the signatures and copied to an isolated machine before being decrypted and counted. Note that this machine, the counting server, have access to the complete association between the encrypted ballots and the plaintext votes.

An attacker who can smuggle this information out through a covert channel can compromise every voter's secret ballot.

**Related Work**

**E-voting in Nigeria**

In countries such as Nigeria, e-voting has been considered a necessity(Hapsara, M. et al.2016) and as the only solution for credible elections (Salimonu, R. et al2013). Nigeria has set its eyes on e-voting since 2011(Hapsara, m. et al. 2016, Adewumi, D. et al.2011) and, undeterred by the problems found during its implementation(Salimonu, R. et al2013, Verity, F., et Al.2016), seems determined to proceed with the technology. In Nigeria, the traditional voting system was believed to have allowed significant irregularities and a lower level of probity, accountability and transparency(Adewumi, D. et al. 2016), and have overseen corruptions, oppressive acts and administrative failures [Hapsara, M. et al 2016, Salimonu, R. et 2016, Musa, M.et al 2013). Nigeria, e-voting, for instance, had a considerable effect upon research one e-voting in other African Countries. Interestingly, it was not until Nigeria planned to employ the technology in 2011(Hapsara, M. et al. 2016, Adewumi, D. et al. 2011) that there was a sudden, significant growth in the number of publications. Many countries, especially the underdeveloped and developing, have found it almost impossible to adopt the use of e-voting system in their electoral processes due to a barrage of problems. None or only a few have been able to engage substantially electronic means of voting. This contrasts with countries in advanced economies, including Austria, Australia, Brazil, Canada, Switzerland, Estonia, France, Great Britain, Japan, Russia, Sweden, and the USA, that have gone beyond holding pilots and trials, to legally binding e-voting or remote e-voting implementation(Zissis, D.,2011).

An e-voting system must be accessible to every eligible voter, and provide a high level of security. However, this system is vulnerable to various security challenges and threats, including stored central data leakage/ disclosure, selling of votes, and the presence of specific malware on voter's machine, to mention but a few(Musa, M. et al. 2013). Although there are robust encryption schemes applicable to address issues concerning confidentiality, integrity, and authenticity, there is a need for further technological implementations to address the problems of availability, which consequently enhances overall security. Essentially, electronic voting requires a level of protection higher than the other components, including e-commerce(Salimonu, R., et al 2013). It is a complex system where every stage of its implementation must be secure.

**Security Threats to Internet Voting System in Nigeria**

There is no way at present for designers of internet voting systems to ensure that the voters' home computers have not been compromised in such a way as to call into question the reliability of the voting process. Securing the connection between the voter's home computer and the central server is also problematic, but in this area, at least the correct use of public – key cryptography allows a degree of confidence in the integrity of this communication channel. Specifically, the SSL (Secure Sockets Layer) and TLS( Transport Layer Security) protocols used by web browsers and servers to create secure channels for e-commerce and internet banking, for example, were designed to prevent the so-called " man in the middle" attack whereby a network transmission is hijacked by an attacked who has managed to control the channel through which the two end – points of the transaction communicate with one another(WM.A. Wulf, 2001).

SSL uses signed encryption keys which have been verified by a trusted "Certificate Authority Global Sign "to make it impossible for such an attacker to modify the contents of this communication, without revealing that the attack has taken place. Unfortunately, even if this technology is used correctly, it is still vulnerable to other types of attacks, which may be characterised as either "denial of service " attacks or " spoofing " attacks. A denial of service attack is said to take place when the attacker, even if unable to alter or interfere with the substance of a communication, can prevent the communication from taking place, typically by overloading one or the other endpoint of the communication. A spoofing attack is said to occur when one of the communicating parties is tricked into opening a secure connection to a site controlled by an attacker.

A variety of spoofing attack, popularly known as " phishing ", has become extremely widespread in recent years, typically involving an email containing an obfuscated link to a site which has been created to perfectly mimic a particular target website(e.g that of a financial institution,) along with an urgent request to "re-enter" sensitive personal information(credit card numbers, passwords ,etc). This is related to a more general form of attack commonly referred to as " social engineering "; that is, bypassing technical security measures by targeting the users of the system, who often have a poor

understanding of these security measures.

Despite the widespread deployment and use of the internet for banking and other sensitive transactions, it must be emphasised that guaranteeing the security of voting via the internet is a fundamentally more difficult problem, for two important reasons. First, unlike financial transactions, in most constituencies no connection may be made between the voter and his or her vote; record – keeping and auditing capabilities which are standard in the financial world are therefore not applicable to online polling systems. Secondly, the discovery of anomalies or errors in the transmission or recording of votes cannot feasibly result in a correction of these results after the fact. At best, such discovery can only lead in the invalidation of any votes so affected; at worst, in the invalidation of the election itself. Needless to say, such an outcome could have disastrous effects in terms of public confidence in the legitimacy of the entire process.

**6. Recommendations**

Secure Platform:- We assumed that we could trust the voter's computer she /he is voting with. But many computers are infected with viruses; some reports say that about 32% of all computers in the world are infected with viruses and malware (Wolchok S. et al. 2012). The real number does not matter, but we can be sure that there will always be security issues in our computer systems and that there might be some viruses attacking the ballots of electronic voting systems from the voter's computer. So, we have to research how to prevent malicious software might being able to attack and manipulate electronic voting systems.

Programming Languages:- The Civitas used Jif in their implementation, which is an unpopular programming language with only a few people being able to use this language. The Cornell University, who invented Civitas, also developed Jit, which extended Javas with the support for information flow – control and access control. We should make this an object to analyze other languages and check, if they are more suitable for securing – critical applications, like voting systems. In further research, we should also concern about different programming paradigms like, logical or functional programming, and try to evaluate, which is the best choice in voting systems.

Usability Analysis; - Usability is a critical point: if the voters do not understand how to use the voting system, they should not try it. Therefore some guidelines should be designed to simplify voting systems and to have a road map, how the components should look like in the front – end.

**7. Conclusion**

E-voting may become the quickest, cheapest, and the most efficient way to administer election and count vote since it only consists of a simple process or procedure and requires a few workers within the process. Internet voting is widely claimed to improve voter turnout and reduce costs. This paper introduced the idea of electronic voting systems. It discussed the different ways in which voters can be a vote. We summarized the importance of security in e-voting. The reasons for the growing interest in e-voting in some Countries, e.g. Nigeria were identified. This paper observed the security threats that may affect the e-voting system. In our opinion transition to e-voting method should proceed slowly by implementing it in small pilot populations. First and the widening the scope gradually. If mistakes are made along the way, they will not be catastrophic and widespread. Given the current state of widely deployed computers in peoples' homes, the vulnerability of the internet to denial of service attacks, and the unreliability of Domain Name Service, we believe that the technology does not yet exist to enable electronic voting in public election. The implementation of such a system poses many security challenges and risks for system developers and governments. Therefore, without appropriate security measures, electronic-based elections can be a challenge. Contrary to remote internet voting methods, we suggest that solutions based on Virtual Private Networks (VPNs) and reinforced with strong security layers pose as more viable approaches to implement reliable and robustly secure e-voting system.

**9. References**

Alvar, N. (2011). *Technology adoption decision framework* (Doctoral dissertation, The College of

Chwelos, P., Benbasat, I., & Dexter, A. S. (2001). Empirical test of an EDI adoption model. *Information systems research*, *12*(3), 304-321.

Danchev, D. (2010). Study finds the average price for renting a botnet. Zdnet. Retrieved from *http : // www. Zdnet.com/blog/security/study - finds - the average - price - for - renting -a - botnet/6528.*

David, J. (2004). If I can shop and bank online, why can't I vote online?. Verified Voting Foundation. Retrieved from *- voting/vote -online.*

Estonia Internet Voting Committee, (2013). In Estonian. Retrieved from *http : // www.youtube.com / channel*

Halderman, J. A., Hursti, H., Kitcat, J., MacAlpine, M., Finkenauer, T., & Springall, D. (2014). Security analysis of the Estonian Internet voting system. *Nr. May.*

Hapsara, M., Imran, A., & Turner, T. (2016, October). E-Voting in developing countries. *International Joint Conference on Electronic Voting* (pp. 36-55).

Hoglund. G., Butler. J. (2005). Rootkits : *Subverting the windows kernel*. Wesley: Addison

Howard, M. (2001). E-Government across the globe: How will "e" Change government? *Government finance Review,* Vol 17(4), pp.6 – 9.

Iacovou, C. L., Benbasat, I., & Dexter, A. S. (1995). Electronic data interchange and small organizations: adoption and impact of technology. *MIS quarterly*, 465-485.

Kitcat, j.(2007). A noted report into Estonia's e – voting System. Retrieved from *https://www.youtube.com/channel/*

Mediati (2013). How to remotely install apps on your Smartphone. TechHive. Retrieved from *http: //www.techhive.com/article/2067005/how -to -remotely - install -apps - on -your smartphone.html*

Mercuri, R.(2002). A Better Ballot Box. *IEEE Spectrum*,31,10, 46 -50.

Musa, M. A., & Aliyu, F. M. (2013). Design of electronic voting systems for reducing election process. *Int. J. Recent Technol. Eng*, *2*(1), 183-186.

Neumann, P. G. (2001). Risks to the public in computers and related systems, ACM SIGSOFT. *Software Engineering Notes*, 26, 1, 14 – 38.

Okediran O. O., Omidiora, E. O., Olabiyisi S. O., Ganiyu, R. A. & Alao, O. O. (2011). A framework for a multifaceted electronic voting system. *International Journal of Applied Science and Technology*, Vol. 1(4), pp 135 – 142

Olaniyi O. M, O. T., Arulogun, E. O., Omidiora, A., & Omitoso, O. B. (2012). Design of a secured model for electronic voting system using Stegano – Cryptographic Approach. Proceedings of the 7th International Conference on ICT Applications, Application of ICT to Technology, Research, and Administration(AICTTRA 2012), National Defence College Abuja, pp 84 – 89

Olaniyi, O. M., Arulogun O. T. & Omidiora E. A. (2013). Design of secure electronic voting system using multifactor authentication and cryptographic harsh Functions. *International Journal of Computer and information Technology,* 2(6) : 1122 – 1130

Oliveira, T., & Martins, M. F. (2011). Literature review of information technology adoption models at firm level. *Electronic Journal of Information Systems Evaluation*, *14*(1), 110.

Raidma, S. & Kase, J. (2014). Kohaliku Omavalitsuse. Volikogu valimiste e – haaletamise Protseduuride hindamise Lopparuanne in Estonia. Retrieved from *http : // VVK.ee/ Public/KoV13/ Lopparuanne_2013*

Robinson, D. G., & Halderman, J. A. (2011). Ethical issues in e-voting security analysis. *International Conference on Financial Cryptography and Data Security* (pp. 119-130). Springer, Berlin, Heidelberg.

Rogers, E. M. (1995). Diffusion of innovations: modifications of a model for telecommunications. *Die diffusion von innovationen in der telekommunikation* (pp. 25-38). Springer, Berlin, Heidelberg.

Salimonu, R., Osman, S., Jaleel, A., Shittu, K., & Jimoh, R. G. (2013). Adoption of e-voting system in Nigeria: A conceptual framework. *International Journal of Applied Information Systems*, *5*(5), 8-14.

Scott, S. D., Plotnikoff, R. C., Karunamuni, N., Bize, R., & Rodgers, W. (2008). Factors influencing the adoption of an innovation: An examination of the uptake of the Canadian Heart Health Kit (HHK). *Implementation Science*, *3*(1), 41.

Springall, D., Finkenauer, T., Durumeric, Z., Kitcat, J., Hursti, H., MacAlpine, M., & Halderman, J. A. (2014). Security analysis of the Estonian internet voting system. *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security* (pp. 703-715). ACM.

Tornatzky, L. G., Fleischer, M., & Chakrabarti, A. K. (1990). The processes of technological innovation: Issues in organization and management series. *Lexington Books. Retrieved from http://www. amazon. com/Processes-Technological-Innovation-Organization/Management/dp/0669203483. Accessed June*, *10*, 2013.
UCTv2y5BPOo-ZSVdTg0CDIbQ/videos

Verity, F., Pattinson, D., & Goré, R. (2016). Modular Synthesis of Provably Correct Vote Counting Programs. *E-Vote-ID 2016*, 55.

Wolchok, S., Wustrow, E., Isabel, D., & Halderman, J. A. (2012). Attacking the Washington, DC Internet voting system. *International Conference on Financial Cryptography and Data Security* (pp. 114-128). Springer, Berlin, Heidelberg.

Yasinsac, A., & Wulf, W. A. (2001). A framework for a cryptographic protocol evaluation work bench. *International Journal of Reliability, Quality and Safety Engineering*, *8*(04), 373-389.

Zissis, D. (2011). Methodologies and technologies for designing secure electronic voting information systems, 2011. Unpublished PhD thesis, university of Aegean.