IST-Africa 2018 Conference Proceedings
Paul Cunningham and Miriam Cunningham (Eds)
IIMC International Information Management Corporation, 2018
ISBN: 978-1-905824-60-1

Online Voting System with Reliable Voter Authentication Protocols

Julius MUTEBI[1], Emily BAGARUKAYO[2], Ivan SSEMPEBWA[3], Michael KALANDA[4]
Makerere University, P.O. Box 7062, Kampala, 00256, Uganda
[1]*Tel:+256706659351, Fax:+256414540620, Email: banks3man@gmail.com*
[2]*Tel:+256702511076, Fax:+256414540620, Email: ebagarukayo@cit.ac.ug*
[3]*Tel:+256700250958, Fax:+256414540620, Email: ivanmic47@gmail.com*
[4]*Tel:+256754378432, Fax:+256414540620, Email: kalmike256@gmail.com*

Abstract: A detailed and critical analysis was done on manual and e-voting systems implemented. These systems exhibited weaknesses of unreliable protocols, denial of service attacks hence the need to implement the public-key encryption e-voting system. Using Makerere University as a case study, the major aim of the public-key encryption e-voting system is to assure reliability and security of the protocol hence guaranteeing voting convenience. Interviews and document review were used to determine inputs, processes and outputs. As a result of the requirements specification, the system was summarized into three processes: access control process which involves identification and authentication phases for eligible voters. Secondly, the voting process was done by encrypting voter's electronic ballot before submitting to the server. Finally, the final result was sorted through deciphering the received encrypted information. The System is more efficient than other E-Voting systems since voters can vote from their devices without extra cost and effort, and encryption ensures the security.

Keywords: online voting, Protocols, reliability, security

1. Introduction

Voting is a patriotic right where voters choose their representatives, which allows them to express their opinions [1]. Elections and voting practices are of very much importance to all countries that practice democracy [2]. A trustworthy voting system is crucial to a population's consent, as democracies are built on this consent. The base of democracy is to allow people vote freely, so the election result is accepted by voters' committee [3]. In most countries, like Uganda, the fundamental right of choosing a leader is done mainly in manual form which makes it prone to various electoral problems such as double-voting, wrong count, impersonation, lost ballot, spoilt ballot, declining turnout of voters, difficulty of auditing after voting, poor documentation [2]. Electronic voting schemes must provide the same security protocols as traditional voting. The security requirements of such protocols among others include integrity and voter authentication since it is easy to eavesdrop on connections or tamper with protocols by connecting extra devices wirelessly, therefore integrity and authentication are the most important requirements for voter authentication protocol [4]. There are several cryptographic primitives that allow one to create secure e-voting schemes thus the designed system applies a type of this technology known as the RSA (Rivest-Shamir-Adleman) public key encryption standard in the voter authentication phase. The RSA public-key encryption protocol describes three steps for electronic voting system by using the Public-key E-Voting protocol. These steps are: the system access control process that is to authenticate the voter on the election server, the voting process, and collecting data process. The access control process involves the identification and authentication phases for the eligible voters.

In public-key authentication, there are two pair soft keys involved. The first pair is maintained by each user who is trying to authenticate to the server. The private Key for each user is maintained on the user's personal workstation or other client system, not the Server to which the connection is being made. The public key of each user is maintained in that user's "authorized keys" file and not in a central repository. Thus, there is no equivalent of the password/shadow file existing on the server for an attacker to steal. The second pair is maintained by the server itself, and is for authenticating the server to the user. While the private key of this pair is maintained on the server, it is irrelevant because it does not provide authentication of the user on the server. Rather, it is an extra step guaranteeing (when configured correctly) that the user is making connection to the same server they last Connected to by that name or address (or else lots of alarm bells go off). Put together, this means an attacker would have to hack into each client system to gain access to the server for that user, rather than hacking into the server directly. It is a lot more work than hacking the server side. However, the client system will be fortified against attack by requiring the private key on the client to itself be encrypted with a pass phrase, which is only feasible where the user in question is an individual person and not a mechanized account or "bot". There are also "hardened" or "locked-down" systems where it is impossible to remove keys from the server-the keys need to be generated & stored elsewhere, and the server only allows a small whitelist of programs to use them after it imports them. Even if one does obtain the key, they should also be password-protected, and obtaining that password would be difficult to guess / brute force if done properly.

The paper-based voting system introduced in Uganda during the first general elections [5] has resulted in a number of issues and problems that include majorly time - consuming factor as (i) voters leaving without voting because of long queues, (ii) a very high intolerable percentage of lost, stolen, or miscounted ballots, (iii) high number of unclear or invalid ballot, (iv) limited or no accommodation for people with disabilities (PWDs), (v) bad weather causes people to avoid walking long distances to stations to cast their votes, (vi) intimidation of voters by agents [1]. As the case for Uganda, E-voting has not been administered; there is still enormous dwell on the traditional system even though there was an increase in the telephone usage [6]. According to [7], presidential elections in Uganda, invalid votes accounted for 4% of the votes. This makes the issue of invalid votes in manual voting systems a big problem.

Different methods, like the secret ballot method or the punch card systems have been used to carry on electoral processes, proving effective ways of casting votes. Due to fast evolution of Information Technology, electronic voting systems have emerged, which allow a voter to be part of an automated process [8]. These modern voting systems and equipment evolved through the years with technology advances from traditional paper-based voting system to paper punching machines to the latest Internet voting system, i-voting [1]. Most voting systems are based on the concept of majority rule or plurality. For example, in an election, a candidate with a plurality receives more votes than any other candidate, but does not necessarily receive the majority of the total votes cast [9].

E-voting systems have the potential to improve traditional paper-based voting procedures by providing convenience and flexibility to the voter. Due to the numerous benefits of e-voting systems, several countries have since introduced e-voting solutions either as a pilot system or in its entirety. Countries that have found e-voting satisfactory include Brazil, Belgium, United States, Canada, UK, India, Ireland, Geneva Venezuela, and Estonia. E-voting is being piloted in a number of African countries like Kenya, Ghana and Nigeria [10]. Recently, mobile technological revolutions have become one of the most important ICT trends with an effect to human lives [11]. The problems associated with traditional electoral process include pre-ticked ballots, irreconcilable tallies of votes in polling stations, ghost voters, delays in the commencement of voting and ballot stuffing

[12]. E-voting has problems resulting from human unreliability in cryptographic protocols, and denial of service [3]. Therefore, this raises need for a reliable Online Voting System with a secure authentication protocol, which will ensure voting convenience.

2. Objectives

The main objective was to develop an online voting system with a reliable and secure voter authentication protocols to ensure voting convenience.

3. Methodology

Interviews are a forum for talking to people and they may be structured, unstructured or semi- structured. The interviews conducted were on a random sample of 100 students (voters) to identify and specify functional and non-functional requirements to determine requirement specification. Students were interviewed to get their view of the system under development because they were the target audience to use the system to vote once implemented. The university was used as a starting point and for prototyping before the system could actually be adopted and used for general elections. The system has not been tested in the real world yet. The interviews were both semi-guided and unguided and also contained both closed and open-ended questions and the obtained data was mainly about the operation of the existing system; its problems, strength, information flow and processing of the current system.

A review of the relevant documents, guides and laws governing the voting system in use for the past years was undertaken. The processing methods used to come up with the accurate records such as gathering information on concepts and challenges of the manual voting system were reviewed and reports examined which helped to identify the inputs, processes and outputs. The preferred sources of the documents reviews were in the form of the Constitution of Uganda, other books of literature, internet resources and journals.

From the data gathered about the existing systems through interviews and documentation review, it was found that manual voting systems are widely used in Makerere University elections. Data was analyzed to identify user, functional, non-functional, software and hardware requirements that guided the design and implementation of the Online Voting system to automate the manual voting process. The user requirements include the following: -

- Allow users to cast votes efficiently and effectively
- Process user's tasks as fast as possible
- Provide a user-friendly interface with interface metaphors, mapping, affordances, constraints, visibility, feedback and other user-friendly qualities of an interface.
- The user expects consistent predictable results / information from the system after a request.
- Users access the system, that is, high reliability during the voting period.

The OVS Functional Requirements include system authentication and approval of all users provided correct credentials are supplied, registers voters and candidates, enables voters to vote online, provides e-ballots, dynamically counts and tallies votes during voting process and admin views and declares voter results. Non-Functional Requirements relate to emergent system properties such as reliability, availability, response time, storage capabilities, security due to implemented voting protocol, portability and high performance for reasonable short time response.

System Design was done by Process Modelling using Data Flow Diagrams to show processes and external entities in the system with a detailed description of process model as the end product; and Data Modeling achieved using Entity-Relationship Diagrams to show data requirements and model. In process modelling a Context Diagram and Level 1 DFD

were modelled. The diagram depicts system effectiveness and efficiency Diagram 0 decomposes the OVS context diagram and shows major internal processes, data flows and data stores. It consists of the entities and data flows that appear in the context diagram. The architectural design shows how OVS is comprised of different subsystems like Data Collection, Data Processing, Data Storage and Data Display. A data model was built by identifying data requirements for the OVS database, identification of entities and attributes making up the system and relationships between these entities, an Entity Relationship Diagram (ERD). The relationships indicate multiplicities between entities.

4. Technology Description

OVS was implemented using various software tools, programming languages and development kits like Wamp Server, Hypertext Preprocessor (PHP), MYSQL, Cascading Style Sheets (CSS) were used with HTML to define the layout and the look of text and other elements. Java applications (MIDlets) were embedded in mobile phones or simulated to support the voting processes of the OVS. Extensible Markup Language (XML) was used to design User Interface layouts and screen elements constituting the System. XML coding was used to create validations for different modules of the system and parse framework to provide backend services.

OVS offers multiple advantages over traditional paper-based voting systems-advantages that increase citizen access to democratic processes and encourage participation. The advantages are explained below;

1. ***Reduced costs:*** OVS reduces the materials required for printing and distributing ballots. Internet based voting, in particular, offers superior economies of scale in regard to the size of the electoral role.
2. ***Increased participation and voting options***: Online voting offers increased convenience to the voter, encourages more voters to cast votes remotely, and increases the likelihood of participation for mobile voters.
3. ***Greater speed and accuracy placing and tallying votes***: Online voting's step-by-step processes help minimize the number of miscast votes. The electronic gathering and counting of ballots reduces the amount of time spent tallying votes and delivering results.
4. ***Greater accessibility for the disabled and the sick:*** Because they support a variety of interfaces and accessibility features, e-voting systems allow citizens with disabilities-especially the visually impaired-to vote independently and privately.
5. ***Flexibility:*** Online voting can support multiple languages, and the flexible design allows up-to-the-minute ballot modifications.

OVS enables legitimate voters to cast their vote from wherever they are using their mobile devices unlike other means that require the voter to appear at the polling station. This helps alleviate the nuisance of long queues at poll-sites which waste a lot of time. It also eases the vote-counting process which is now done instantly as the voting progresses and a graphical display is available on a site (attached to the system) for all stakeholders to view progress, hence ensuring transparency.

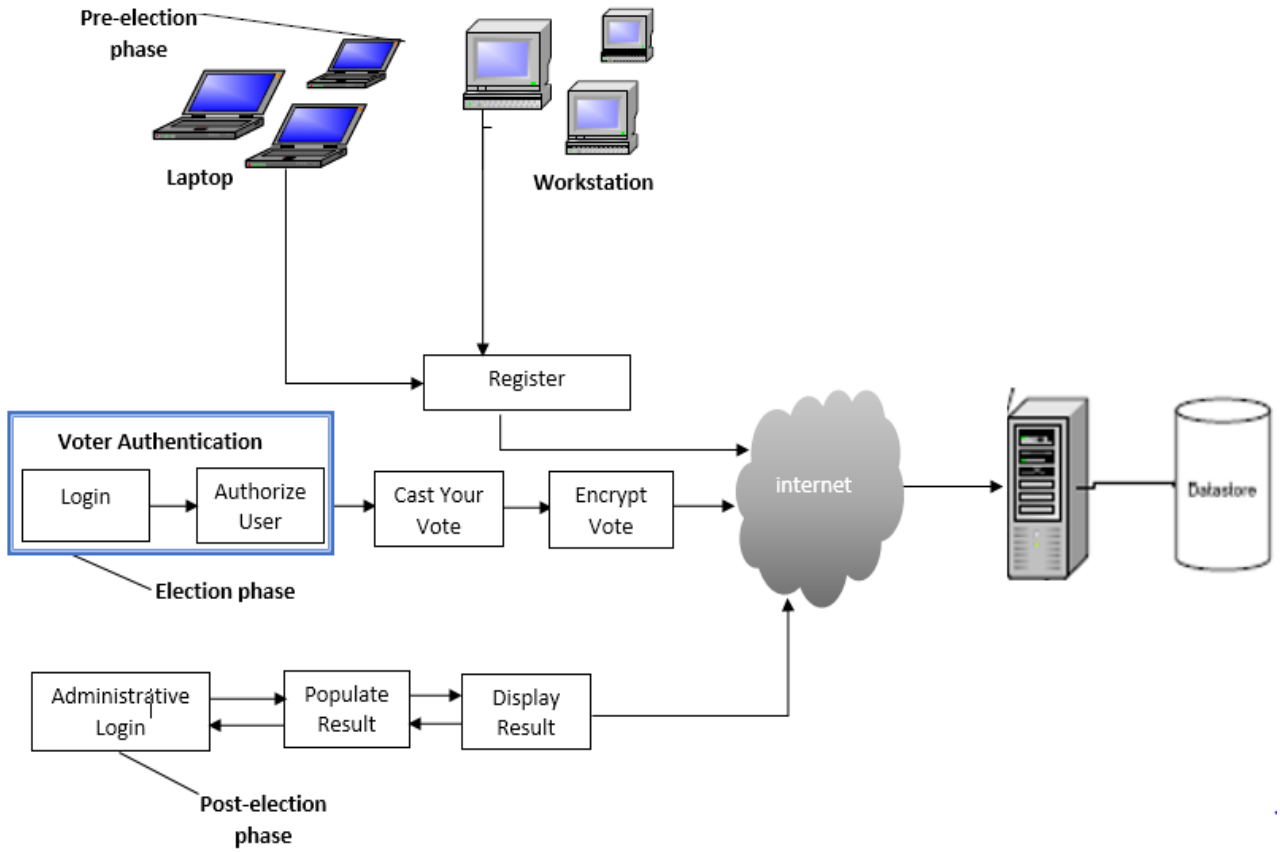

Figure 1: Architectural Design for the System

The OVS was tested by developers and users to identify any bugs or errors. The developer used Test Drivers to simulate higher level units and Test Stubs to simulate lower level units. The system testing was conducted by performing the unit, integration, compatibility and acceptance testing. As the project team traversed through the coding stage, every finished module was tested in order to enable early debugging. This was conducted on the different modules of the OVS to determine whether specific functionalities were in proper flow within the system. Integration and Compatibility Testing was performed to expose defects or faults in the interfaces and interaction between integrated components or modules. The researchers tested interaction among OVS modules like login module and registration module. A compatibility test was done to check whether the system is compatible with various devices, compatibility between OVS and other voting software. An acceptance test was conducted with a sample of 20 voters to verify that the system satisfies users' expectations and functional requirements. After interaction with the system, the users were interviewed for feedback and recommendations were analyzed and used to make adjustments accordingly. The feedback from the users about the system was got through interviews and questionnaires. For example, users interacted with the system to determine whether there was need to change certain system aspects, and feedback was captured using questionnaires. After interaction with the system, users were interviewed for feedback and recommendations were analyzed and used to make adjustments accordingly.

5. Results

Online Voting System (OVS) will operate in parallel with the existing manual and automated voting processes and enable legitimate voters cast their vote from anywhere using mobile devices. This alleviates long queues at poll-sites which waste a lot of time and

ease the vote-counting process, done instantly as the voting progresses and a graphical display will be available on a site (attached to the system) for all stakeholders to view progress, hence ensuring transparency. The risks include third parties, Errors and technical malfunctions and Unreliability. The challenges include Security -voter authentication, Reliability. OVS can be trusted as a platform to conduct free and fair elections in a secure and transparent manner if well implemented. Mutual authentication, integrity, voter anonymity and system accountability are some of the critical functional requirements that e voting Systems should have. With the OVS, there will be little or no invalid votes due to the use of option buttons on the electronic ballots to represent candidates. The e-voting methods have weaknesses like non-satisfying security protocol and mechanisms, voters' exhaustion, the required hardware cost, and the mandatory polling places. As new technology for electronic voting, this protocol replaces the unreliable previous voting protocols such as the Cryptographic Voting Protocols, since voters feel justifiably confident that their votes are counted and unaltered. The system needs only basic requirements such as; PC or standard smart phone and internet connection. Therefore, the system minimizes the voters' exhaustion since it allows the voter to vote from their own PC without any extra cost and effort.

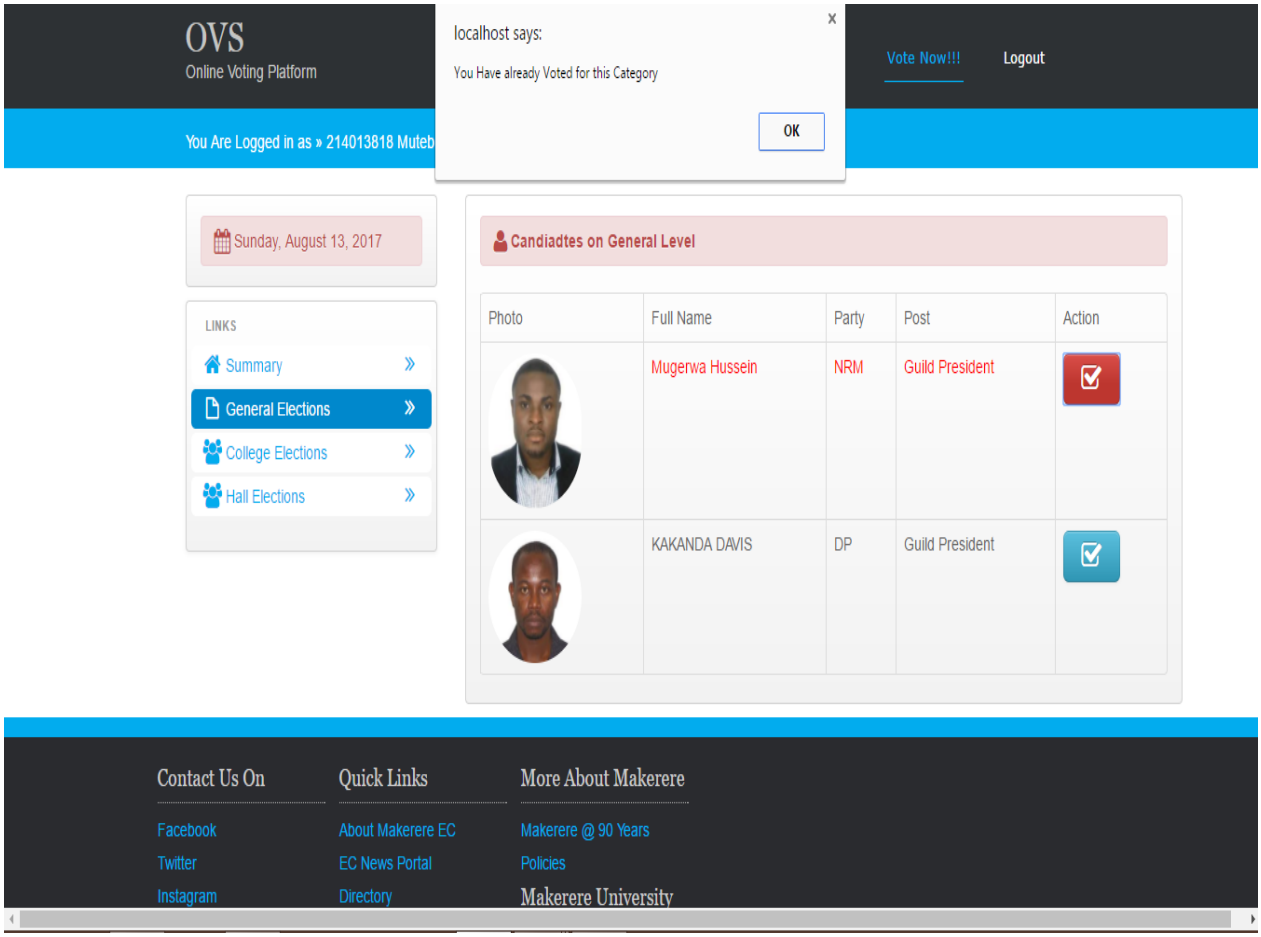

Figure 2: Vote Casting

Validation was done to check the System's usage, usefulness to the users and its usability so as to ensure that the input and output data of the system is complete and accurate and performs functions as expected and to the satisfaction of the users' needs. This involved checking of text visibility in the selected language (English), use of appropriate and easily understood words, navigation between screens, and verification of functionality. This system can be installed and run on any Operation System ranging from windows XP upward and Ubuntu. The system is compatible with all computers with appropriate storage

and memory capacity. The system was presented to end users and Makerere University Guild Election Commission who verified and confirmed that the system addresses the requirements and satisfies intended user needs. Users interacted with the system to determine whether there was need to change certain system aspects, and feedback was captured using questionnaires.

Respondents recommendations, criticism and impressions were analyzed and as a result, adjustments were made accordingly to make the system more user-friendly and accepted by users. Having interacted with the system, users were asked to rate the usefulness of the system out of 10. The system met the users and system expectations of simplicity, high responsiveness, accessibility, security and portability. Users were asked to rate the system in terms of navigating through the interface, and their feedback showed that they found no difficulties in exploring the systems interface, and interacting with different components of the system's interface. Users were asked if they think the OVS system provides a solution to the current voting system's problems and they agreed that it might solve their voting issues and opted that if it works out well, it could even be implemented in other universities or even in the upcoming 2021 Uganda elections. The respondents were asked what they have liked about the system interface. They appreciated and showed contention with the system navigation tools followed by the Content. The OVS has very limited images incorporated on the interface and color on the interface is consistent and less attractive as reflected in the respondents' response. Implementation and testing of the E-Voting System was done successfully and the system is now ready for use by the voters and University Guild Election Commission to ease their work.

6. Business Benefits

The target group at university level elections are students or people eligible to vote for their leaders in different categories and departments of the university. The target group at national elections level are the citizens who are eligible to vote. Voters and election officials will benefit from further development in this area since there is need to influence progress of electronic voting, mass voter participation and ensuring transparency, freedom and fairness of the election process. This study is of significance to:

- The public in understanding the new advancements undertaken by the electoral body and approving them to enhance better interaction, transparency and collaboration. Consultation with and involvement of people affected by changes reduces resistance which is otherwise experienced when change is introduced.
- The Government of Uganda understanding the benefits of adopting the electronic voting system towards promoting voting-exercise efficiently in a socio-political arena.
- In order to bring the product to market, there must be support from the electoral body of the university to use and approve this system. Also, the system must be endorsed by the Government of Uganda if it is to be used for national elections.

7. Conclusions and Recommendations

This research aimed at improving speed, ease and transparency of the electoral process. There is need to guarantee improved quality of service, reduced election malpractices, increased efficiency in tallying, increased voter participation, decreased invalid votes and voting errors; prevent digital divide, and allow for better voter registration management. The research offered greater knowledge and helped the researchers to identify the advantages of using the new Public Key Cryptography OVS as opposed to manual voting system. According to the current Information Technology evolutions and advancements, electronic voting can provide reliable, convenient, and effective voting platforms that create a remarkable paradigm shift from the highly flawed traditional voting systems once all the

important issues pertaining to the harmonious functioning of the system in question are clearly and fully addressed. Especially issues to do with security of the system in question. The OVS has fully satisfied all these questionable areas.

The OVS system needs to be adopted because it will help to guarantee improved quality of service, reduced election malpractices, increased efficiency in tallying, increased voter participation, decreased invalid votes and voting errors; prevent a digital divide, and allow for better voter registration management. The research offered greater knowledge and helped the researchers to identify the advantages of using the new Public Key Cryptography OVS as opposed to manual voting system. The system application showed success of the research conducted. The researchers recommend that the system be officially used by the electoral bodies such as Makerere University Guild Election Commission, and later on be adopted by the Electoral Commission of Uganda and other countries because the system can administer the election processes fairly, effectively and efficiently.

These kind of projects needs exhaustive and meaningful research in order to implement a system that fully addresses the issues surrounding that topic such as; issues to do with the reliability and authentication of system, voting security, ease of use, among others. It is crucial to involve users in the development of the project. More research should be conducted to improve the system's functionality, high responsiveness, accessibility, ease of use by the end user and security. More research is needed in the security of the system because new threats occur as technology evolves. The project was initially done to address the challenges of the electoral body of Makerere University, as a starting point that will lead to greater research on how to use the system for general elections.

For future developments and improvements, the researchers intend to improve the system to incorporate much more robust and sophisticated security technologies like biometric features.

In conclusion, the research offered greater knowledge and helped the researchers to know the advantages of using the new Public Key Cryptography OVS as opposed to manual voting system. The system application showed success of the research conducted. The researchers recommend that the system be used by the electoral bodies such as Makerere University Guild Election Commission, the Electoral Commission of Uganda because the system can administer the election processes fairly, effectively and efficiently. In future we intend to improve the system to incorporate a biometric feature.

References

[1] Steyn, J., and Van Greunen, D. (Eds). (2014). ICTs for inclusive communities in developing societies. Proceedings of the 8th International Development Informatics Association Conference, 372-385, Port Elizabeth, South Africa.

[2] John, K.A., and Kofi S.A.M. (2014). IJCSI International Journal of Computer Science Issues. A Trustworthy Architectural Framework for the Administration of E-voting, 11 (3), 97.

[3] Hayam, K., et al. (2011). E-Voting Protocol Based On Public-Key Cryptography. International Journal of Network Security & Its Applications (IJNSA), 3 (4), 87-96.

[4] Drijvers, M., Luz, P., Alpar, G., & Lueks, W. (2013). Ad Hoc Voting on Mobile Devices. WIC Symposium on Information Theory in the Benelux. U.S. Department of Commerce, Washington D.C.

[5] Sekaggya, M. (2010). Uganda Management of Elections. The Open Society Initiative for Eastern Africa. Open Society Foundations

[6] Uganda Bureau of Statistics. (2015). Statistical Abstract- Pg 66

[7] Lumu, D.T. (2011) Election Rigging. The Observer. Retrieved on 25th February 2011, from http://www.observer.ug/index.php?option=com_content&task=view&id=12352&Itemid=59.

[8] Eliver, P.V., Gina, G., Gualberto, A.T., Héctor, F.G. (2013). Implementation of Electronic Voting System in Mobile Phones with Android Operating System. Journal of Emerging Trends in Computing and Information Sciences. CIS Journal, 4 (9), 728-737.

[9] Ofori-Dwumfuo, G. O., & Paatey, E. (2011). The design of an electronic voting system. Research Journal of Information Technology, 3 (2), 91-98.

[10] Enguehard, C. (2008). Transparency in Electronic Voting: The Great Challenge. M-Voting.

[11] Roberto, B., C. (2010). M-Cognocracy. Building participatory democracy through the electronic voting mobile ICT.
[12] Kaka, J. (2016). Uganda's 2016 Elections: Another Setback for Democracy in Africa. Retrieved from The Global Observatory website: https://theglobalobservatory.org/2016/02/ugandas-2016- elections-another-setback-for-democracy-in-africa/
[13] Uganda: Biometric Voter Registration - Lessons from Uganda Elections. (2016). Retrieved from the All Africa website: http://allafrica.com/stories/201603041336.html