FINGER PRINT ONLINE VOTING SYSTEM

A. Muhammed Haaris
M.Tech CFIS,
Department of Computer Science and Engineering,
Dr. M.G.R Educational and Research Institute,
Maduravoyal, Chennai-600 095.

Mr. Arun Raj S
Professor,
Department of Computer Science and engineering,
Dr. M.G.R Educational and Research Institute,
Maduravoyal, Chennai-600 095.

Dr.S.Geetha
Head of Department
Department of Computer Science and Engineering,
Dr. M.G.R Educational and Research Institute,
Maduravoyal, Chennai-600 095.

Ms. Sri Laksmi R
Coordinator
Department of Computer Science and engineering,
Dr. M.G.R Educational and Research Institute,
Maduravoyal, Chennai-600 095.

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 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- E-voting system; Public encryption key; security

I. INTRODUCTION

Electronic voting schemes must provide the same security protocols as traditional voting. The security requirementsof such protocols among others include integrity and voter authentication since it iseasy 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 . There are several cryptographic primitives that allow one to create secure evoting 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.

II. LITERATURE SURVEY

(ICTs for inclusive communities in developing societies. Proceedings of the 8th International Development Informatics Association Conference) The Information and Communication for Development (ICT4D) research landscape can be described as a dynamic,

fragmented adhocracy and hence, predictably, attempts at producing a shared conceptual framework for the field have had mixed success. Given the multi-, inter- and trans-disciplinary nature of ICT4D it may be impossible to reach complete consensus on such a framework.

However, many basic research activities, such as guiding novice researchers and structuring information sources for efficient access, necessitate a shared vocabulary and generally agreed concepts and hence the quest continues. The purpose of this paper is to propose a non-prescriptive, dynamic conceptual framework for ICT4D. An initial representation was developed based on a literature review and an informal expert interview and this was used to categorize the papers in the ICTD2013 conference proceedings. The results were then used to refine the initial framework from the Computer Science and Information Systems perspectives. This paper presents this framework as point of departure for an ongoing discourse with the purpose of structuring the ICT4D research domain.

(Steyn, J., and Van Greunen, D) One of the key areas of concentration in achieving harmonious democracy is transparency in the electoral processes. Some countries like Ghana, Sierra Leone, Liberia and Kenya have recently had issues of doubt and mistrust of the administration and the management of their Electoral Commission and hence a suspicion of election fraud which has prone threats of violence, economic declination and on the peak, legal implications. There was a claim of double registration, duplicated ballots, lost ballots, wrong count of ballot, failure of biometric registration system, impersonation, and alteration of counted votes in the immediate past election in Ghana, which led to series of court cases. Therefore, this paper seeks to optimize the voting processes and governance of the Electoral Commission of Ghana by proposing a trustable e-voting theoretical framework which dwells on biometric data of various candidates as the basis for encryption of ballot, dedicated channel for transmission of counted ballots and, connecting and disconnecting the database server before and after voting. Various literatures are considered to help propose a robust framework.

(E-Voting Protocol Based On Public-Key Cryptography) In this paper we propose a new secure E-Voting protocol based on public-key encryption cryptosystem. This protocol is summarized in three processes: firstly, access control process which involves the identification and authentication phases for the applied citizens. Secondly, the voting process which will be done by ciphering the voter information using public-key encryption cryptosystem (RSA), to be submitted over an insecure network to the specified government election server. Finally, the election server administrator will sort the final result by deciphering the received encrypted information using RSA private key. Actually, this E-Voting protocol is more efficient than others E-Voting protocols since the voter can vote from his/her own personal computer (PC) without any extra cost and effort. The RSA public-key encryption system ensures the security of the proposed protocol. However, to prevent a brute force attack, the choice of the key size becomes crucial.

(Hayam K Al Anie , Adnan Hnaif) In this paper we present two publishing methods for the votes and the result of an election, the TreeCounting and alternative TreeCounting method. These methods make the verifiability of public boards more achievable by publishing the result of an election as a tree. Both can be parametrized to increase the average number of times each node of that tree has been checked.

(Jerome Dossogne Olivier Markowitch) Voting must respect several criteria to be democratic. In this paper we determine whether electronic voting can simultaneously protect secrecy, be transparent, accessible and resistant to intimidation and fraud.We consider different types of e-voting ranging from Direct Recording Electronic voting systems to remote internet voting. We show that there are major contradictions between the constraints of democratic elections and the possibilities offered by computers. In particular, electronic voting appears to make massive and invisible fraud possible to achieve by small groups of people with the necessary skills. At

present, it is not a realistic possibilility to design an electronic application, remote or not, that could cope with the demands of democratic elections**.**

(Enguehard, C) To many people, the exercise of democracy and participation in politics has become a synonym for election, an event where ordinary citizens are the leading actors only on the voting day, once every two or four years. This causesthe decrease of citizen participation in the world, bringing about what has been called the crisis of political parties. The use of information technologies and communication technologies (ICTs) and new ways of participation in city governments through the exercise of the so-called Participatory Budgeting (PP) arean effective means to reverse the apathy of citizens. But in order to obtain the desired effect, these new ways of participation must have two characteristics. The first one is to reach the greatest number of citizens, who should be able to exercise their right to participate in a simple and safe way; and the second one, that they somehow summarize the citizen preferences through results that represent them. This paper presents a new way of citizen participation called m-cognocracy, that using mobile "Visión de Futuro" Año 7, Nº1 Volumen Nº13, Enero - Junio 2010 communication technology and mathematical aggregation operators Ordered Weighted Averaging (OWA), provide a new model for citizen participation in the government of cities.

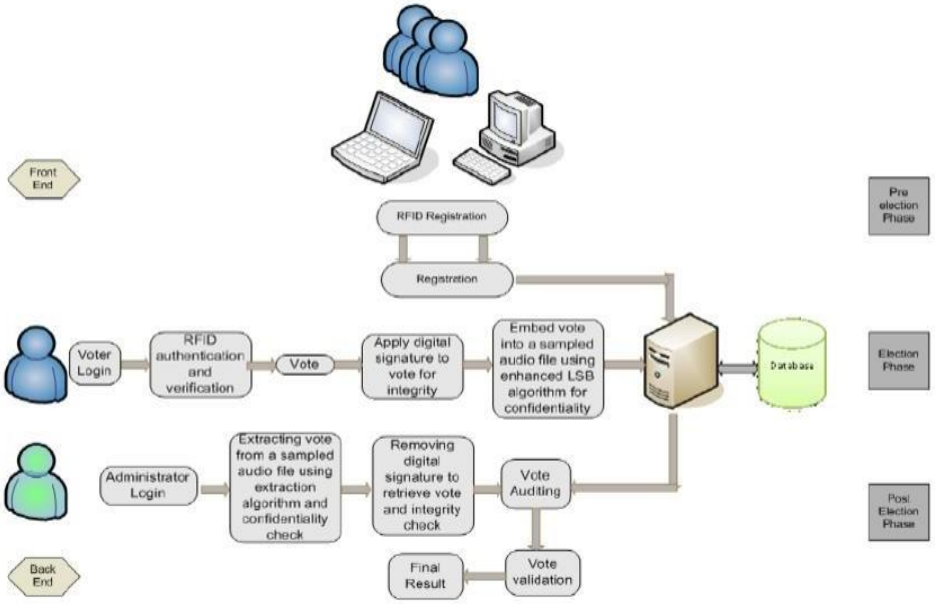
III. EXISTING SYSTEM

Assess current accepted standards on voters' anonymity for traditional and internet-based voting systems. evaluate the core elements of lawful relaxations to the principle of secret suffrage, and especially those traditionally associated to different forms of remote voting, and assess whether they can be applied to internetvoting; and study how current technical developments in the field of elections may result in further relaxations of the principle of secret suffrage in the future.

IV. PROPOSING SYSTEM

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.

V. ARCHITECTURE DIAGRAM



5.1 Architecture Diagram

VI. LIST OF PHASES

There are 6 phases

1) Admin Module
2) User Module
3) Candidate Module

1. ADMIN MODULE:

This module is used to help the server to view details and upload files with the security. Admin uses the log key to the login time. Before the admin logout, change the log key. The admin can change the password after the login and view the user downloading details and the counting of file request details on flowchart. The admin can upload the file after the conversion of the Zip file format.

LOGIN: Admin was login in server page.

VIEW NOMINEE DETAILS:

***** candidate are check in age eligblity criteria.

*Register in all identification mark.

*Candidate are not invoved in crime activity

VIEW USER DETAILS:

*User are register in face recogination and authentication mark

*Eligibility for voting age.

VOTE DATA:

*User and candidate details are uploaded in server.

*Select the candidate for voting.

*Registered vote in server**.**

***display result

LOGOUT:

*After complete process admin will be logout

2. USER MODULE:

REGISTER:

*USER ARE REGISTER FOR VOTING.

LOGIN:

*User are enter into admin.

*After enter vote for eligible candidates.

1. LOGOUT:

*Finally complete the voting process system will be logout.

3. CANDIDATE MODULE:

REGISTER:

*Candidate are register in vote election nomination**.**

LOGOUT:

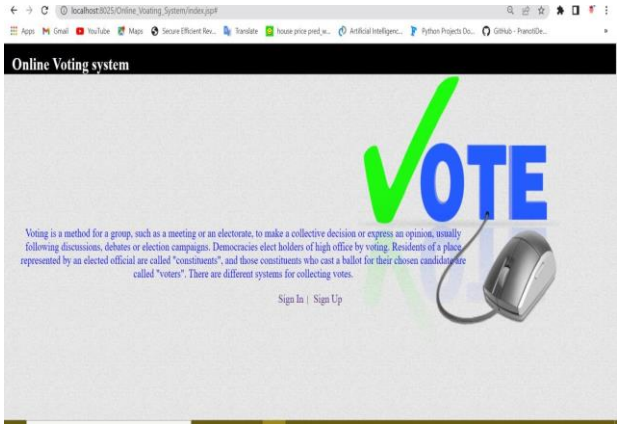
*After completing nomination process

*Candidate are know the status of the result.

*Finally know the result system will be logout.

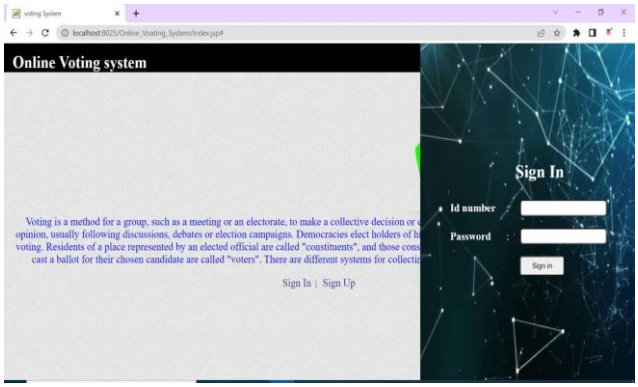
SCREEN SHOTS

7.1 Home pagE



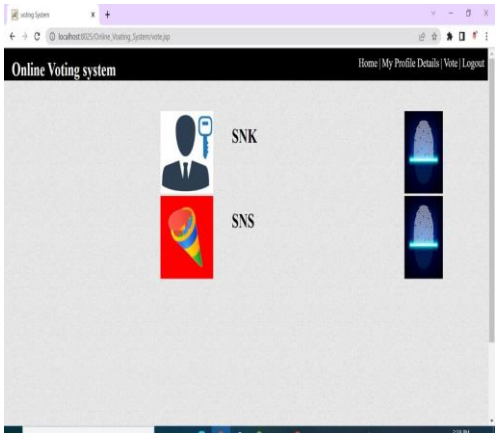
7.1 Home page

7.2 Sign In Page



7.2 Sign In page

7.2.1 Profile page

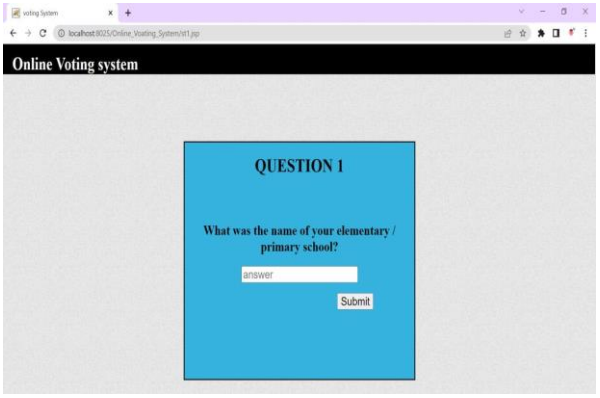


7.2.1 Profile page

7.2.2 Main Page

7.2.2 Main Page

7.2.3 Security questions

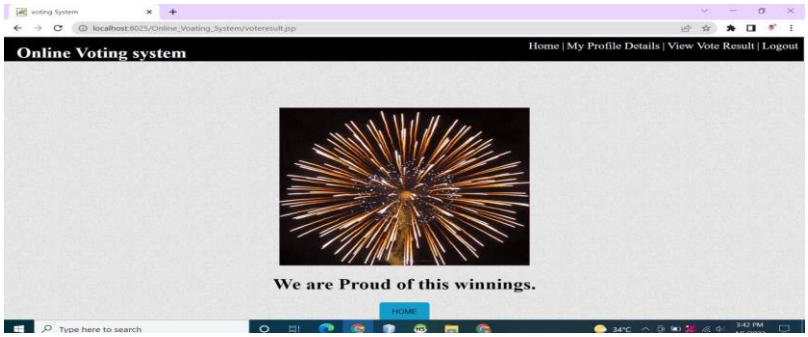


7.2.3 Security questions

7.2.2 OTP verification

7.2.2 OTP verification

7.2.3 Vote result page



7.2.3 Vote result page

VII. CONCLUSION

This research aimed at improving speed, ease and transparency of the electoralprocess. 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 Copyright © 2018 The authors www.IST-Africa.org/Conference2018 Page 8 of 9 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 touse 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 asMakerere University Guild Election Commission, the Electoral Commission of Uganda because the system can administer the election processes fairly, effectivelyand efficiently. In future we intend to improve the system to incorporate a biometric feature.

VIII.REFERENCE

[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