A Trustworthy Architectural Framework For the Administration of E-voting: The Case Of Ghana

John Kingsley Arthur[1] and Kofi Sarpong Adu-Manu[2]

[1] Department of Information Technology, Valley View University
P.O.Box VV44, Oyibi – Accra - Ghana

[2] Department of Computer Science, Valley View University
P.O.Box VV44, Oyibi – Accra - Ghana

Abstract

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.

Keywords: *E-voting, theoretical framework, biometric data, security, encryption.*

1. Introduction

Elections and voting practices are of very much importance to all countries that practice democracy. It is through the process of elections for which citizens have the opportunity to choose the leaders and representatives of their choice. Rexha et al.(2011) mentions that in most countries the fundamental right of choosing a leader using a voting system is done mainly in manual and paper form. However, the administration of the voting process when done manually makes it prone to various electoral problems such as over-voting, wrong count, impersonation, lost ballot, spoilt ballot, declining turnout of voters, difficulty of auditing after voting, poor documentation (Rexha et al,2011 & Nu'man, 2012). This situation calls for immediate attention to the methods used in voting. Around of Africa, some countries such a Sierra Leon, Rwanda and Uganda have had riots because of the poor administration of the Electoral process and in all of these these countries, the manual paper forms are used for voting.

According to the official website of the Electoral commission of Ghana (2013), the EC is mandated to be in charge of free and fair elections in Ghana. Since 1957 for which Ghana achieved its independence, the EC has been responsible for the organization of the elections till date. However, the last elections in December 2012 brought a new dimension in the history of Ghana, where the major opposing party had doubts of the results and hence launched a court case against the winning party. The party disagrees with the results from the EC and saids it is fraudulent. This calls for the fact that an effective and trustworthy system would be required to replace the manual system to enhance the trust of the citizens of Ghana in the voting system. Therefore, this research work seeks to examine the lapses in the existing voting system and proposes a trustable e-voting system framework for which when adopted and implemented would solve majority of the problems faced.

2. Related Research Literature

There are several research works done by some researchers in the area of e-voting security and trust issues. In the research of Bamiah et al.(2010) they proposed a framework to manage a secure trustworthy E-voting system, by securing each and every side of the system from its initial stage to finishing stage by implementing Trusted Platform Technology (TPM). The TPM serve as a chain of trust that combines hardware and software to provide trusted client device. However, in their research they failed to provide the design of the TPM and how it was used to

secure the vote, channel, the computers, and mobile phones in their framework. Also, on their proposed framework the entire voting process is obscured from the voter and polling agents. They only get to know the result from the polling station only when the entire voting process has ended. This will affect the trust of the voters.

Rexha et al(2011) proposed an e-voting framework that will enhance the security of their immediate manual system if they adopted their framework. To enhance the security they implemented it using smart cards and digital certificates. However their framework is expensive because at every polling station they implemented two (2) ARC(Archive) redundant servers which invariable stored small amount of records. Also, to secure records, the systems were configured by the national election commission. Their research did not cover the polling agents at this level, for which it can implicate the trust of the system by the voters.

Rexha et al.(2012) in their research work proposed a framework aimed at improving authentication and transparency in e-voting systems. Their systems framework was to replace the manual system so then their citizens will be able to vote from any polling station. This concept was derived from dynamic queue list which is based on voters' arrivals and identification at the polling station. However, the system could not address how the centralized database could be protected to check for content; whether there are votes or no votes already in the in database before voting starts. Again, their research work did not consider the integrity of casted votes during the time of voting.

The work of Alkassar et al.(n.d.), in their work proposed a solution to security of online voting systems bringing to bare how unsecured malware and corrupt voters activities on the voting system could affect the trustworthiness of the voting process and the voting system entirely. Their solution was based on Trusted Computing in combination with secure operating systems. However, they did not consider the security breach based on amount of time spent within the network and the number of attempts of logging onto the system. Their framework could have been very much effective if a defined set of parameters were identified breaches to use of the voting system. Their framework could not detect exactly who is voting, this is because it is done online. The framework lacks physical system administration and monitoring. No mechanisms were defined to tell genuine citizens are identified to vote anywhere. Therefore, there is the need for a framework that identifies each voter before the ballot is casted.

3. Framework of the existing manual system

3.1 Voting Process

Without any unforeseen circumstances, voting takes place only on the day of election starting from 7am to 5pm. This is not to say one cannot vote when it is 5pm while he/she is already in queue to vote. It is only persons who get to the polling stations at 5pm who would not be allowed to vote. The voter goes through the following processes:

- The voter is required to check His/her name in the reference list so as to identify himself/herself as eligible to vote. This is done by showing your voters' ID card to the officials who would in turn cross check to see whether you are in the voters' register and also place your thumb on the biometric machine to verify if you are truly the card bearer.
- After all necessary information checks out, your finger would be dipped into an indelible ink. This is also a measure to prevent double voting. But one must be sure not to stain the ballot paper with that finger since a soiled ballot paper would be rejected.
- After receiving your ballot paper, carefully check whether it has the ECs official stamp on it before you go and vote otherwise that is also invalid.
- Voting is done in two(2) ways; presidential and parliamentary. After receiving the presidential ballot first, you would proceed to a voting booth where you find an ink to dip your thumb in and then carefully vote in the space provided for your candidate of choice. After which you wipe your finger first and gently fold the paper into the ballot boxes.
- Finally you proceed to the next table for the parliamentary ballot paper and also follow the same procedure as the presidential one above and drop the ballot paper in the parliamentary ballot box.

3.2 Predominant Challenges of the manual system

- **Poor documentation and recording:** In the past elections there were several situations of poor recording of total ballots in some of the polling stations. For example; 270 writing in words as twenty seven zero. Their respective meanings are completely different.

- **Alteration of votes:** Votes can easily be manipulated because they are directly recorded on

paper. The records can be exposed to any voter or official with malicious intention. According to Mercouri(2002) electoral personnel always replicate the votes which at the normal circumstance would not have been so as compared to e- voting which is claimed to be devoid of such.

- **Voter Error:** Voters sometimes makes errors. For example voter may unintentionally thumb print against the picture of a candidate for which he did not intend to have voted for**.** However, you cannot make changes to the selected option. Also, if voter do not fold their ballot papers well, the ink can spread to another candidate column, and hence the vote is disqualified and nullified. The Official website of Electoral commission, R&M Department of Ghana provides a summary of rejected ballots from 1992 to 2008 as follows: 3.03, 1.53, 1.58, and 2.13 2.32. by observation, it is clear that from year to year the total percentage of spoilt ballots are increasing. In 2012, December election, 251, 720 out of 11,246,982 total votes casted were nullified because they either voters voted for two(2) different parties same time or were left blank.

- **Deferrals in showcasing final results**: According to Ofori-Dwumfuo and Paatey(2011), it has been gathered that it takes the EC of Ghana about three(3) days to eventually publish a presidential election result. This situation prevails because they manually do the collation of results from all the various polling stations, constituency and then the national levels, which is very tedious and cumbersome to be finished within an hour.

- **Ballot design and Count:** Recently biometric registration and verification were introduced into the electoral processes. However, when voting is done, all the ballot papers are mixed and no voter can be linked to any ballot paper. Also, counting is very difficult, because ballot papers are mixed up in one ballot box and are unorganized. After voting, counting is manually done for each party. Errors may occur during a large count and hence would affect the result.

- **Unsecured medium for transfer of ballot count:** Transferring votes from one polling station to the constituency involved faxing and was alleged that transferred votes did not match counted votes at polling station. Methods for transfer would therefore have to be improved.

4. The Proposed Solution: E-voting System

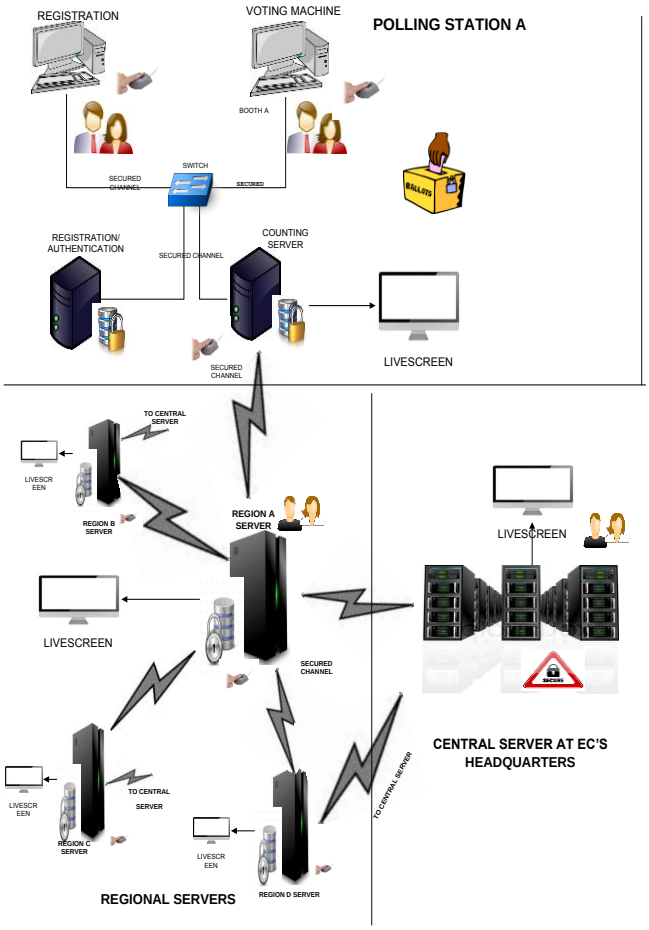

Fig. 1 Proposed architectural framework for implementing e-voting.

4.1 Ensuring Security

In this section appropriate methods and techniques for ensuring security on the e-voting architecture is discussed. The network architecture for which the voting software is going to run and the design of the database are considered.

4.1.1Network Architecture

The system architecture is going to be based on 2-tier architecture. In this architecture, the client or the e-voting system handles the e-voting application whiles there is a server that will handle the database at the backend. When the client starts it establishes a connection to the server and communicates as needed with the server while running the client. The client computer usually cannot see the database directly and can only access the data by starting the client. This means that the data on the server is much more

secure. Now users are unable to change or delete data unless they have specific user rights to do so.

The client-server solution also allows multiple users to access the database at the same time as long as they are accessing data in different parts of the database. One other huge benefit is that the server is processing data that allows the client to work on the presentation and business logic only. This mean that the client and the server is sharing the workload and by scaling the server to be more powerful than the client, you are usually able to load many clients to the server allowing more users to work on the system at the same time.

4.1.2 Master Database

Before the process of voting begins, party agents who are assigned cryptographic keys have to append to attest the fact that the database count is zero. The same agents would have to append their keys to encrypt and isolate the database. Then they would append to encrypt a secured channel from the system to the database server. Voters can then be allowed to cast their votes after channel to the database has been secured by the various political party representatives.

4.1.3 Algorithm of System

- **Setting database record count to zero**
  -Use biometrics from party agents
  E.g. $X_i \longrightarrow [R_i]$, where X is party agents, R is the biometric reset sequence generated by system
  for
  $X_1 \longrightarrow [R_1]$
  $X_{2=} [R_1]+[R_2]$
  $X_{n=} [R_1]+[R_2\}+\ldots\ldots[R_n]$
  $X_1 + X_2 +\ldots X_n$ = empty db
  db = 0

- **Disconnecting Database From Application Before Voting**
  Party agents confirm and disconnect db for authorized connections only.
  E.g $X_i [R_i]$, where X is party agents, R is the biometric reset sequence generated by system
  $X_1 \longrightarrow [R_1]$
  $X_{2=} [R_1]+[R_2]$
  $X_{n=} [R_1]+[R_2\}+\ldots\ldots[R_n]$
  $X_1 + X_2 +\ldots X_n$ = disconnected db

- **Secure direct encrypted connection for eligible voters.**
  E.g. assuming we have polling booth [A, B, C] at a polling station,

  At booth A: n number of party agents are required to establish a secured connection from the system to the db.

Booth A = $X_1 + X_2 +\ldots X_n$
BA = $X_1 + X_2 +\ldots X_n$
[BA $X_1 + X_2 +\ldots X_n$]

Booth B = $X_1 + X_2 +\ldots X_n$
BB = $X_1 + X_2 +\ldots X_n$
[BB $X_1 + X_2 +\ldots X_n$]

Booth C = $X_1 + X_2 +\ldots X_n$
BC = $X_1 + X_2 +\ldots X_n$
[BC $X_1 + X_2 +\ldots X_n$]

4.2 Flowchart of the Existing System

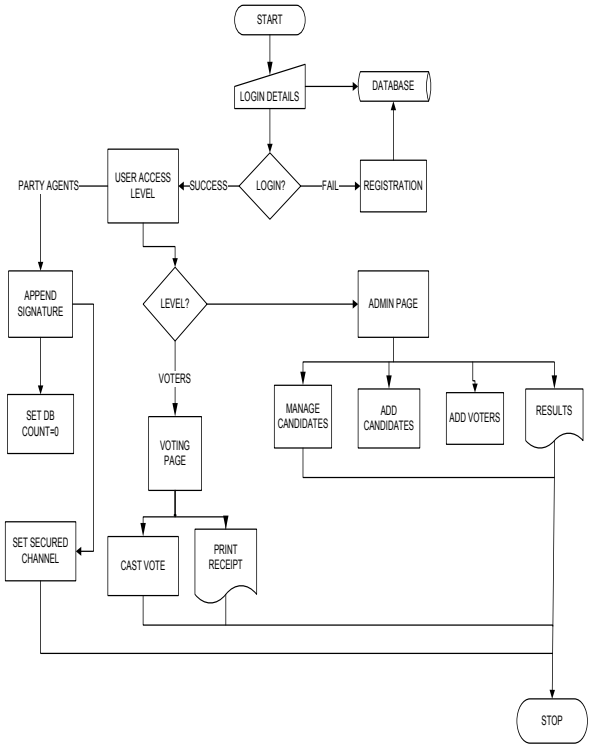

Fig 2: Flowchart of Existing System

5 Increasing Trustworthiness

5.1 Preliminary Level

- **Auditing of the voting system:** To enhance of the trustworthiness of the voting system, the system would have to be tested thoroughly. The modules or scripts of the voting software and the dedicated channel would have to tested and tried by an auditing team made up of computer programmers and ethical

hackers from each of the representing political parties. This will help the parties to understand and accept that the system is robust and hence no errors are going to emanate from the use of the system.

- **Registration:** The registration is done at the second phase after the system has been tested thoroughly. All legible voters will come along with their voters ID card and their details as specified by the Electoral Commission would be captured including their finger prints. Upon completion of the registration, the voter is assigned a unique voters ID that is generated from a set of random numbers.

- **Securing database and dedicated channel:** This process is also carried out before the Election day where various representatives from the political parties are assigned biometric keys. These keys are to be appended to connect and disconnect the database before and after the main voting. This is to set the database to zero(0) vote count and also the secure the channel for voting.

5.2 Voting Level

Voting interface: Here, the voter is required to enter his/her unique ID and biometric data before access to the voting panel where he/she is presented with the two main voting categories of presidential and parliamentary to vote is granted. Upon selection of each category, the voter is presented with the various candidates‟ names and pictures for voting. Voting for a candidate in this category is acknowledged and that category immediately disabled to prevent double voting. A receipt is then issued out to the voter which states the political party voted for. This receipt is then placed in a physical ballot box for recounting later in case of disputes. Voting process is made possible when party reps append their signatures to secure voting channels to database. All these processes must appear graphically on a live screen.

5.4 **Event After Voting**

Counting and tallying: ballots cast is shown on the live screen prior to this stage to show live results and to also make sure ballots cast are equal or less than number of people registered. In case there still some doubts, the receipts placed into the ballot boxes can be recounted.

Election results from each polling station are then sent to a regional server in a secured encrypted manner which is also authorized by the party agents. At the regional level, various party reps can be assigned with biometric keys to receive data from polling stations and then also send them securely to other regional servers as well as the Electoral Commission's central server. The process of exchanging data between the regional servers before sending them to the central server is to prevent the process of someone hacking into the network to change data on one communication channel. If such a person even succeeds on that channel, we would have nine(9) additional regional servers to cross check data for accuracy.

6. Conclusion And Recommendations

The researchers have demonstrated considerably the use of a more authenticated but simple approach which is user friendly and can be used by a voter with no difficulty when provided with the necessary training. The proposed framework when implemented will do away with most of the inconsistencies in the vote processes and will be very effective.

However, in the current situation of Ghana, some people could not be verified although their biometric data were previously collected during the registration period. Therefore an alternative to biometric data would be very important for further research. Also, most of the existing e-voting systems do not consider the illiterates. Therefore an alternative such as voice instruction should be further studied to see how they could be integrated into voting systems as an addition to the use of the usual input devices(such as keyboard and the mouse).

References

[1] B. Rexha,, V. Neziri,, and R. Dervishi. "Improving authentication and transparency of e-Voting System Kosovo Case". International Journal of Computers and Communications. Issue 1, Volume 6, 2012

[2] B. Rexha, R. Dervishi, and V. Neziri. Increasing the Trustworthiness of e-Voting Systems Using Smart Cards and Digital Certificates – Kosovo Case. 2011. .Retrieved from https://www.google.com.gh/#bav=on.2,or.r_cp.r_qf.&fp=6399758690bf4ee6&q=Increasing+the+Trustworthiness+of+eVoting+Systems+Using+Smart+Cards+and+Digital+Certificates+%E2%80%93+Kosovo+Case on 7th August, 2013.

[3] A. Nu'man."A Framework for Adopting E-Voting in Jordan". *Electronic Journal of e-Government* Volume 10 Issue 2 2012,pp133 – 146, 2012.

[4] M. A. Bamiah, A. Dehghantanha, and B. Archibald. A Trustable Electronic Government Voting Management

Framework Using TPM. 2010. Retrieved from http://www.academia.edu/643254/A_Trustable_Electronic_Government_Voting_Management_Framework_Using_TPM on 15th August, 2010.

[5] A. Alkassar, A. Sadeghi, and M. Volkamer, "Towards Trustworthy Online Voting".n.d. Retrieved from https://www.cosic.esat.kuleuven.be/wissec2006/papers/17.pdf on 10th April, 2014.

[6[A.Yeboah."Electronic Voting in Ghana: Is It The Solution To Ghana's Perceived Electoral Challenges After Biometric Registration?". Journal of Information Engineering and Application, Vol. 3, No. 1. 2013.

[7] G.O. Ofori-Dwumfuo and E. Paatey. "The Design of an Electronic Voting System". Research Journal of Information Technology 3(2): 91-98, ISSN: 2041-3114. 2011.

[8] The official website of Electoral Commission of Ghana(2013).