A Secured Cloud-based E-voting System using Information Dispersal Algorithm

John Kingsley Arthur
Valley View University
Computer Science Department
Accra, Ghana

Kofi Sarpong Adu-Manu
Valley View University
Computer Science Department
Accra, Ghana

Charles Adjetey
Valley View University
Computer Science Department
Accra, Ghana

ABSTRACT
The introduction of the electronic voting (e-voting) system has received much attention by researchers in recent years. E-voting has been of interest to stakeholders and political party leaders in most countries (that is developed and developing) practicing democracy. Academics and technocrats have delved into technical issues related to e-voting system that could foster its smooth implementation and this have encouraged it's full acceptance in many countries. The challenge however, is how to secure and maintain a trustworthy e-voting system devoid of security breaches especially from hacking and hijacking. The challenge still remains an open area that calls for novel designs into high level security infrastructure that may enhance and improve the security of e-voting systems to gain the full trust, acceptance, and adoption by the citizenry. Ghana deploys computerized system for registration and verification during the electoral process. During the 2016 election, the Electoral Commission of Ghana adopted the electronic transmission of results although the elections were conducted manually. In this paper, a novel secured framework for electronic voting relying on the principle of the Information Dispersal Algorithm (IDA) is proposed. In our approach, upon voting, the voters vote record is encrypted and split for distribution on several virtual cloud servers. At the end of the voting period, the split vote records are reassembled into their original state for counting to take place. The splitting of the vote records and its assembling are performed by the IDA. The paper further discusses the design and implementation of the IDA in a typical e-voting environment.

General Terms
Security, Algorithms, Information Dispersal Algorithm, E-voting

Keywords
E-voting, Information Dispersal Algorithm, Electronic Voting System

1. INTRODUCTION
Elections have been in existence for decades, and the very core mandate of every election in a democratic system is to have a transparent, free and fair elections that seeks to promote the peace and stability of a country or group persons. Elections are conducted for several portfolios including but not limited to presidential, parliamentary, school leadership or association and whatsoever position that may be. In the past decades, leaders were elected mainly through the use of steel ballot boxes and counting centers to choose preferred candidates. The electoral processes have improved over the years especially in Africa with innovations such as biometric registers for registration and the use of verification machines to verify the voter during the election process. Vote counting in-situ has also brought improvements in the electoral processes. It is expected that future elections in Africa will be equipped with new methods and procedures especially with the use of technology to greatly improve the sanity and the security of the elections from the registration process to results coalition. Technology has tremendously improved the election procedures to the next level especially with the presence of the Internet. Several mobile and web applications have been developed for voting purposes. Hence, the introduction of electronic voting systems popularly known as e-voting systems.

E-voting is the act of using electronic means to cast and count votes during the elections. Countries such as the United States of America, India, Russia, the other European countries across the world uses e-voting systems to elect leaders in the country and by the same means the results of the electoral process is announced to the citizenry (Jones, 2011).

Although the use of e-voting systems enhances and makes the management of the entire electoral process easy, it is not popular in Africa due to several constraints which include lack of the needed Internet connectivity, cost of logistics, lack of technical know-how, mistrust among the populace and general lack of integrity in persons overseeing such systems. This reason accounts to why e-voting systems have not been widely implemented in Africa. Stakeholders and political leaders issues with the security of the e-voting system and the robustness of its entire management framework.

Some of the current e-voting systems suffer challenges as that of the manual system such as over voting, impersonation, fault intolerance and insecure transmission mediums results in elections [cite]. Given this background, the authors of (Tornos et. al. 2014; Arthur and Adu-Manu, 2014; Malviya, 2014; Ofori-Dwumfuo and Paatey, 2011, and Ofori-Dwumfuo and Paatey, 2011, investigated how to secure channel for transmission of votes to enhance trust in the e-voting system. Although these contributed enormously to the trustworthiness of e-voting system, the fault intolerant level of the e-voting systems are very high. There is no robust representation of voters vote record in the storage sections of the e-voting system. Also, most of the e-voting systems are highly fault intolerant and hence any hack on a section of the network will mean a total shutdown of the e-voting system.

This paper proposes a comprehensive and robust cloud e-voting system that relies on the secure capacity of the Information Dispersal Algorithm (Rabin, 1990; Bestavros, 1994) to split voters vote record and randomly assign them to a defined set of virtual servers in the cloud. The split vote records of each voter are then reassembled at the end of the voting process for tallying and counting as indicated in Figure 2. The proposed framework as shown in Figure 1 can only be taken over by hackers when they have access to all the

defined set of virtual servers in the cloud.

The paper further introduces different party representatives in the electoral process for the purposes of fostering transparency and gaining trust in the administration of the e-voting system. The party representatives are given keys which are to be appended for the encryption of votes before the entire voting process begins. After voting, the party representatives append their keys once again to decrypt ballots before result are displayed.

2. ELECTIONS IN GHANA

Ghana's elections take place every four years to vote into power a president and members of parliament. The parliament of Ghana has 275 members, elected for a four-year term in single-seat constituencies. The presidential election of Ghana is won by having more than fifty percent (50%) of valid votes cast while the parliamentary election is won by simple majority with the both elections held on 7th December at the same time (Electoral Commission Ghana, 2020).

2.1 Voters Registration Process

Voter's registration is made public and takes place before elections. The registration process is a process of enabling an eligible voter to have his or her name entered into a document (that is, the voter Register) with the aim of offering the person the opportunity to exercise his/her franchise on the appointed day of voting. Ghana laws peg an eligible voter as one who is 18 years of age or above. During the registration process the following biographic information are collected; the name, age, sex, picture and residential address. The voter is then issued a voter's ID card which must be produced on the day of the election. Currently, biometric data, specifically thump print data is taken and used as the bases of verification and identification of voter during the election day.

The voter register is considered provisional so that changes may be made not until it is pushed during the Voter register exhibition stage. In that session, measures are put in place to ensure that there is unique voter registration number and safeguarded against any possibility of double registration, forged registration forms and most of all to ensure the validity and integrity of the register (Ofori-Dwumfuo and Paatey, 2011).

2.2 The Voting Process

This stage defines the moment where the casting of ballots actually takes place. Voting takes place only on the stipulated day of election starting from 7am to 5pm. All potential voters who show up after 5pm are disallowed to vote. However, all who are present at the pollen station before 5pm are allowed to go through the voting exercise.

As a voter, one is required to check his/her name in the reference list, that is voter's register, to identify him/her 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 (Electoral Commission Ghana, 2020).

When all one is successful across the above checks. The finger is then dipped into indelible ink. The dipping of finger into the ink is done to prevent a comeback that may lead into double voting. On the other side, the voter must ensure that the ballot paper is not stained with that finger since a soiled ballot paper would be rejected.

After receiving a ballot paper, the voter checks whether it has the Electoral Commissioners (EC) official stamp on before casting a ballot.

Voting is done in two (2) ways; presidential and parliamentary. After receiving the presidential ballot, the voter proceeds to a voting booth where an ink is made available for voter to dip the thumb into and then carefully vote in the space provided for your candidate of choice. The ballot is to be folded and placed into the ballot box after fingers well cleaned.

Voters after voting for the presidential candidate of choice, continues to the next desk for the parliamentary ballot paper and also follow the same procedure as the presidential but to select parliamentary candidate of choice. and drop the ballot paper in the parliamentary ballot box.

3. RELATED RESEARCH WORK

There are several research works done by some researchers in the area of e-voting security and trust issues. In the research of Tornos et al (2014), they proposed an e-voting system based on ring signatures. The system is divided into modules. A key generation module for creation of voter's keys to be used in identifying a voter. The second server module which is the voting administration module, verifies the validity of the voter, determines the number of voting rounds to reach a minimum consensus using a linking tag that links together the votes from the same user choosing the last vote as the valid. Finally, casted ballot is sent to a ballot box. This approach adopted by the researchers is deficient of a robust representation of voter's record. Also, using on two(2) physical servers could make easily susceptible to hacks leading to a complete shutdown of the voting process.

Arthur and Adu-Manu (2014) proposed a 2-tier architecture that handles the e-voting application and the server-side database. In their framework, a connection was established from the client to the server to ensure that before voting commences, the database's voters vote count is set to zero(0). The database is further encrypted and isolated before the voting process begins. In their proposed system, voters were to vote using their voter's ID card, finger prints and a unique number attached to their vote after which the system offers a receipt to voter to be placed in a ballot box. Result was said to be saved in nine (9) redundant servers database housed at each regions headquarters. The results of the vote count are displayed on giant screens at the pollen station whiles the voting process is ongoing. The shortcoming of this system is the overly reliance on the nine (9) physical servers. Although is robust but the voters vote record is not well secured,

Agarwal and Pandey (2013), proposed an e-voting system using cloud. In his research, a unique Aadhaar ID was used to identify voters. On Election Day, e-voting website residing on cloud server was opened till the closing time of election for everyone to vote irrespective of their location. The voters are allowed to authenticate using their ID and finger print and a password is automatically generated. With their proposed system, the voter's finger print is compared with the fingerprints in the clouds database of the Electoral Commission and if valid, the voter is allowed access to the system to vote. After voting, the district's server database in the cloud and cloud database of Election commission of India again verifies the authenticity of the voter using the finger print and if matched, the vote is then saved to the above servers. The results are cross checked and finally released automatically by the cloud server after the voting exercise. The proposed framework does not secure votes before transmitting it to the cloud server. This can give room for a

man- in-the-middle attack to be easily done where an attacker can steal data in plain text.

Anandakumar (2014) proposed a future polling system using cloud computing in support with remote client. In their proposed system, voter's finger print was used for authentication (Biometric). A min-min average algorithm for cloud workflow was used to improve the communication overhead between the local cloud servers to the main server. The cloud database was used to provide service for voting to all authenticated user and users were to vote via internet or using a remote client for those without network connection. A local database was also used in storing candidate's data and data updated instantly to a cloud server when there is internet connection. Their research never considered insider threats to votes where votes stored for later transmission when internet connection is available can give insiders the opportunity to modify data.

4. THE INFORMATION DISPERSAL ALGORITHM (IDA)

The IDA provides a methodology for storing information in pieces (dispersed) across multiple locations, so that redundancy protects the information in the event of a location outage, but unauthorized access at any single location does not provide usable information. Only the originator or a user with a list of the latest pointers with the original dispersal algorithm can properly assemble the complete information (Rabin, 1990).

The IDA breaks a file F of length $L = |F|$ into n pieces $F_i, 1 \leq i \leq n$, each of length $|F_i| = {}^{L}/_{m}$, so that every m pieces suffice for reconstructing F. Dispersal and reconstruction are computationally efficient. The sum of lengths $|F_i|$ is $\left(\frac{n}{m}\right).L$. Since nlm can be chosen to be close to 1, the IDA is space efficient.

Let $F = b_1, b_2, \ldots, b_N$ be a :file, i.e., a string of characters. Assume that we want to disperse *F,* either for storage or for transmission, under the given condition that with overwhelming probability no more than *k* pieces will be lost through node or communication-path failures.

The characters bi may be considered as integers taken from a certain range [0...B]. For example, if the b_i are eight-bit bytes, then $0 \leq b_i \leq 255$. Take a prime $B <$ p. For bytes, p = 257 will suffice; but we may wish to choose a prime larger than the smallest $B <$ p. Note that with p = 257 there is an excess of one bit per byte, we shall see later how to implement IDA in fields $GF(2^8), s = 8$ *GF(2'),s* = 8 for bytes, without any excess bits. Now *F* is a string of residues *mod* p, i.e. a string of elements in the finite field Z_p.

Choose an appropriate integer m, so that $m = m + k$ satisfies ${}^{n}/_{m} \leq 1 + \epsilon$ for a specified $\epsilon >$ o. Choose n vectors $a_i = \{a_{i1}, \ldots, a_{im}\} \in Z_p^m, 1 \leq i \leq n$, such that every subset of m vectors in $\{a_1, \ldots, a_n\}$ is linearly independent. We shall see later on how to satisfy each of these conditions.

The: file *F* is segmented into sequences of length m. Thus;

$$F = (b_1, \ldots, b_{mn}), (b_{m+1}, \ldots, b_{2m}) \ldots$$

Denote $S_i = (b_i, \ldots, b_m)$, etc. For i=1,…,n,

$$F_i = c_{i1}, c_{i2}, \ldots, c_{i}{}^{N}/_{m}$$

where

$$c_{ik} = a_i.S_k = a_{i1}.b_{(k-1)m+1} + \cdots + a_{i.m}.b_{k.m}$$

5. THE PROPOSED FRAMEWORK

5.1 Voters Registration Phase

During this phase, voters are registered and a password with a voter's ID is generated and given to them for the purpose of authentication. The password is used as one of the variables to verify the authenticity of the voter. The registration is administered using the Registration client machine and further validated using the Registration server as shown in Figure 1.

5.2 Voting Phase

At this stage the voter is set to vote. Before the voter votes, voters record is authenticated into the system using their ID and passwords. After a successful login the user has the chance to vote by selecting the candidate of choice. Once the user clicks on submit button upon completion of voting, the voters vote record is encrypted wrapped in the keys of the party representatives as explained in section 5.5. Furthermore, the IDA is applied as explained in section 5.4 and illustrated in Figure 2; where the voters encrypted vote records are split and randomly transmitted to a defined set of virtual cloud servers. Once a voter casts his/her ballot, the system interface is disabled shortly for a time period of 10seconds. This mechanism is put in place to prevent malicious voters from having time and space of exploiting the system after voting.

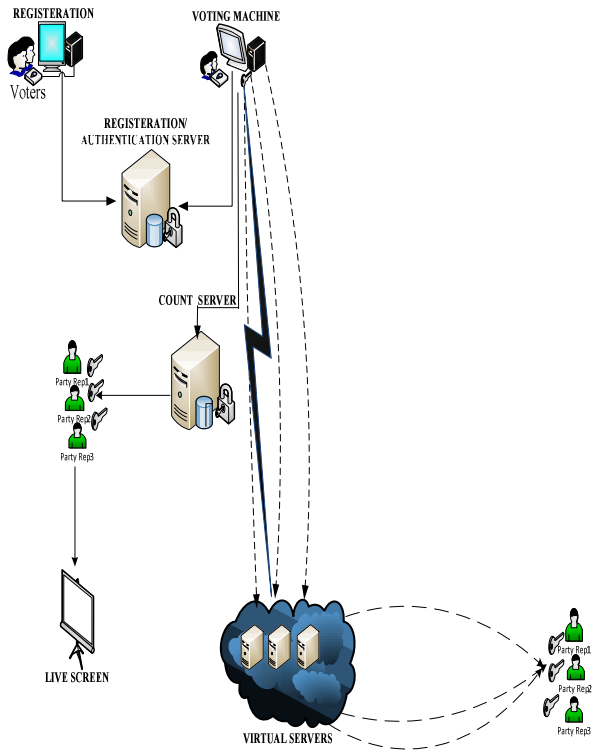

Figure 1: The proposed framework for secured cloud-based e-voting system

5.3 Counting and Tallying of Votes Phase

Once a voter votes, his/her voter's ID is hashed and together encrypted with count as administered by the Count server as shown in fig. 1. At the intermediary server, the encrypted votes are shared to the various severs using the IDA. At the end of voting, only party representatives assigned cryptographic keys append their keys to decrypt votes before results are display.

With the proposed system, the servers can be two or more but cannot be one. The server is updated during voting period

until the voting period is expired. During reconstruction of the votes, each party representative that has a key is required to append their keys before votes are parsed to an array at runtime, decrypted and result displayed at runtime. Result is also saved to the local database from the cloud servers at runtime with the result updated once the keys are appended again.

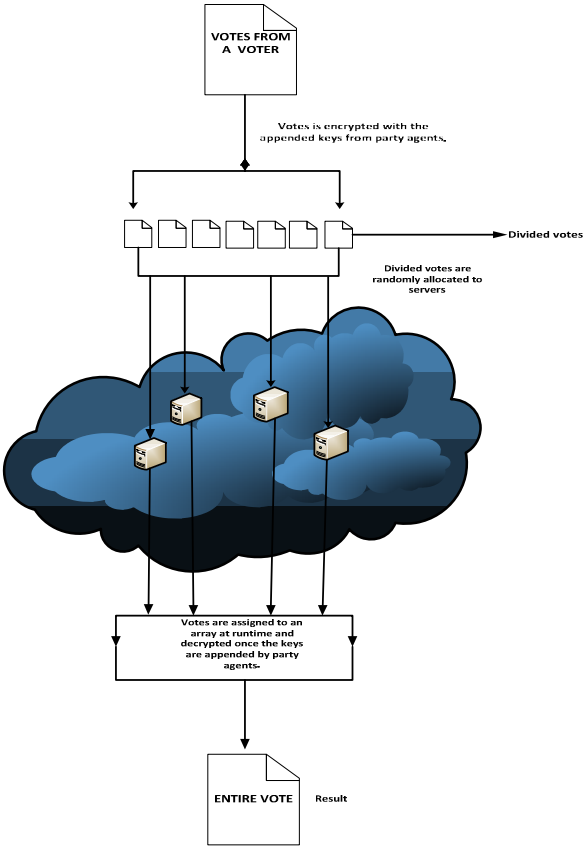

Figure 2: Inside the cloud

5.4 The Application of IDA in the proposed framework

Distributing of votes across servers

Let's Z denote a voter's vote record
Let's X denote a voter's ID
Let's Y denote a Candidate's ID

Here we use Server A

Where h is hash function, eK is the encryption key
Let z=xy1, xy2, …. xyn
H(z)=(h(xy1), h(xy2), ….h(xyn)) ek(h(z)) = eK(h(xy1), h(xy2),…h(xyn))
Here we will split eK(h(z)) randomly to servers A and B
A=h(h(x), eK(h(xy1)))
B=(h(x), eK(xy2)))

Reconstruction of vote record

Let P_k be the party representative's key
$K= P_1k_1+ P_2k_2+ \dots P_nk_n$
And arrVotes=the array that holds the combined votes of all votes of all voters from server A and B
For i=0 to length(arrVotes)-1 // loops through the array to get all ID's that are the same
Let v_i=arrVotes[i] //holds all votes
For j=0 to length(arrCandidate)-1// Array that holds all candidates in a constituency
R=executeQuery(select voter_id from registration
where h(voter_id)=vi[h(x)])// checks for valid voters
if(vi[h(xy)]==h(R, arrCandidate[y])
$n(y_j)$+=1 //increment the count for the candidate
End for
End for

$P_1k_1+ P_2k_2+ \dots P_n$ decrypt n(y)+=1

5.5 Algorithm for Party Representatives to append signature

START

STEP 1: Assuming the party reps where 2 and k is key

P1→ K1

P2→ K2

STEP 2: To encrypt ek1 + ek2 →ek(h(x)(yi))where ek is encrypt key

STEP 3: Append P1 + P2→d(ek(h(x)(yi))) where d is decrypt

STOP

6. SYSTEM IMPLEMENTATION

The system is developed using HTML5, bootstrap, PHP, MySQL. The HTML5 and the bootstrap were used to build the graphical user interface. MySQL was used to construct the database as shown in Figure 3.

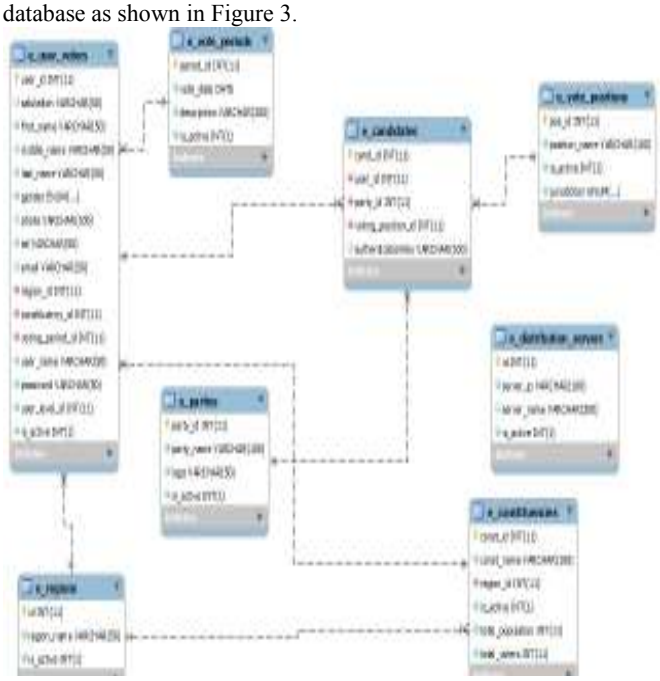

Figure 3: The database design

The database is made up of eight relational tables namely, e_user_voters, e_vote_periods, e_candidates, e_vote_positions, e_parties, e_distribution_servers, e_regions, and e_constituencies. The e_user_voters table contains information about legible registered voters. It takes instances such as first name, last name, gender, etc as shown figure 3 above. The e_vote_periods table contains records voting period which shall be used to used to automatically control the active time frame of voting. The e_candidates table houses information about legitimate candidates vying for positions. Information such as candidateID, user_id and voting position are handled in this table. The e_vote_positions table contains data pertaining to the available positions for candidates. From

this table positions vied for may be made active or inactive. Such that, if a position for example, presidential is not to be voted for in this particular voting period, at the code level this property can be disabled. The e_parties table contains data about the registered political parties and their representatives. Data such as party id, party name, and status are provided. The status could be active or inactive based on the fact that, the party is allowed to contest or not in that particular voting year. The e_distribution_servers table houses data on virtual servers and the related data split that are sent to help in the reconstruction of the voter's vote record. The e_regions and e_constituencies tables contains data about the regions and and constituencies respectively. These are to help validate all vote that will be submitted to the Count Server, as illustrated in Figure 1. All vote records that do not have attribute of the designated areas for voting are rejected.

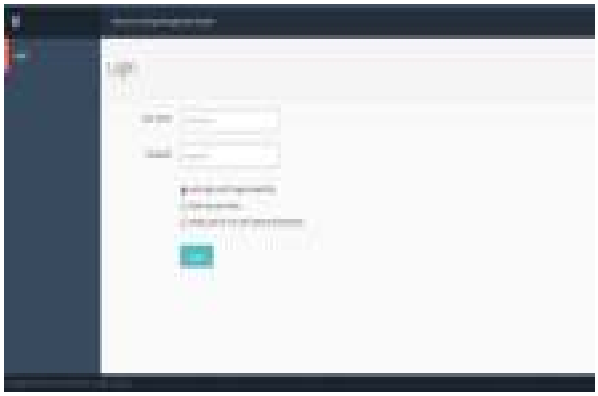

Figure 4: Voters login page

The Login page as shown in Figure 4 allows all users that have an account with the system to login to perform allowable tasks.

Figure 5: The system administrator page

Figure 5 indicate the system administrators page where the the system admin is given privilege in making adding, deleting, updating and viewing records.

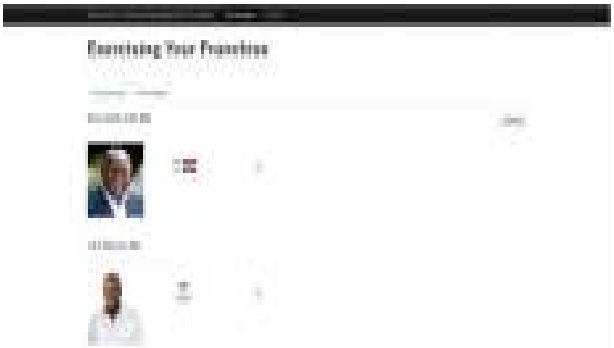

Figure 6: Presidential Voting page

Figure 6 shows the page where the voter gets to vote for the presidential candidate of choice. Radio buttons are deployed to help make just one choice at a time. The submit button is visibly placed to transport vote record and handled by the IDA behind the button.

Figure 7: Candidate page

Figure 7 shows the information related to the registered candidates including the candidate names, party, position, region, constituency and status.

7. CONCLUSION AND RECOMMENDATION FOR FURTHER WORK

E-voting systems help to makes the work of Electoral Commissions easy and much transparent. However, it is prone some insecurities of hacks and fraud to engineered by hackers and political powers that be. Therefore, this research presents a comprehensive secured framework for electronic voting relying on the principle of the Information Dispersal Algorithm. The proposed system represents the voters vote record in a secured manner that could not be easily accessed by hacks and exploitation while the voting process is on going. Transparency and trust is improved by given opportunity to the party representatives invoke a key before and after voting process which imply the voting process only starts when all parties are satisfied with all contingencies of the software. To further this work, an Intrusion Detection System would be explored in the system to help identify and thwart possible intrusions.

8. REFERENCES

[1] Tornos, J. L., Salazar, J. L., Piles, J. J., Saldana, J., Casadesus, L., Ruíz-Mas, J., & Fernández-Navajas, J. 2014. An eVoting System Based on Ring Signatures. *Netw. Protoc. Algorithms*, *6*(2), 38-54.

[2] Arthur, J. K., & Adu-Manu, K. S. (2014). A trustworthy architectural framework for the administration of e-voting: the case of Ghana. *International Journal of Computer Science Issues (IJCSI)*, *11*(3), 97.

[3] Malviya, P.K., 2014. E-voting system using cloud in Indian scenario. *International Journal of Engineering Science & Advanced Technology [IJESAT], ISSN*, pp.2250-3670.

[4] Anandakumar, K., 2014. FUTURE POLLING SYSTEM USING CLOUD COMPUTING IN SUPPORT WITH REMOTE CLIENT.

[5] Electoral Commisision Ghana.2020. Voting. Retrieved from https://ec.gov.gh/voting/ on 7th August 2020.

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

[7] Jones, D.W. 2011. Evaluating voting Technology. Testimony Before the United States Civil Rights Commission. Retrieved from http://homepage.divms.uiowa.edu/~jones/voting/uscrc.html on 7th August 2020

[8] Agarwal, H. and Pandey, G.N., 2013, November. Online voting system for India based on AADHAAR ID. In *2013 Eleventh International Conference on ICT and Knowledge Engineering* (pp. 1-4). IEEE.

[9] Rabin, M.O., 1990. The information dispersal algorithm and its applications. In *Sequences* (pp. 406-419). Springer, New York, NY.

[10] Bestavros, A., 1994. An adaptive information dispersal algorithm for time-critical reliable communication. In *Network Management and Control* (pp. 423-438). Springer, Boston, MA.

[11] Anderson, R.E., Frey, R.L. and Lewis, J.R., General Electric Co, 1981. *Electronic voting system*. U.S. Patent 4,290,141.