Earthline Journal of Mathematical Sciences
E-ISSN: 2581-8147
Volume 14, Number 4, 2024, Pages 631-653
https://doi.org/10.34198/ejms.14424.631653

Improving Security on Election Results Data Transmission via Cloud Using Hybrid Homomorphic Encryption

Arnold Mashud Abukari[1,*], Iddrisu Zulfawu[2], Edem Kwedzo Bankas[3] and Issah Gibrilla[1]

[1] Department of Computer Science, Tamale Technical University, Ghana

[2] Department of Operations, Africa Research Center for Information Security (ARCIS), Ghana

[3] Department of Business Computing, C. K. Tedam University of Technology and Applied Sciences, Ghana

Abstract

Elections in recent years have become topical issues and characterized by violence and conflicts leading to loss of lives and properties. The integrity and confidentiality of the declared collated results have been questioned by individuals and organisations with keen interest in the outcomes of every election. Different countries have adopted different Election Results Management Systems (RMS) to help present a credible, fair and transparent election results. These systems adopted are not without criticisms and suspicions. This research paper has presented various factors that need to be considered when selecting a Results Management System (RMS) for elections. A cloud-based using a Hybrid homomorphic encryption approach is proposed in managing the election results data security and transmission. The proposed scheme has demonstrated effectiveness in handling data integrity, data confidentiality, data privacy and access control. The proposed scheme presented has enhanced the security of election results data against Chosen Ciphetext Attacks (CCA) and Denial of Service (DoS) as well as other cyber related attacks. The time required for the entire election data encryption, transmission, decryption, upload time and download time has been greatly enhanced with the proposed system. The proposed system workflow algorithm, key generation algorithm, encryption algorithm and decryption have been presented in this research paper. The outcome of the research work indicates that only 0.00078 seconds is required to generate keys for about 100 users. About 0.705 seconds and 0.863 seconds is required for the encryption and decryption of a 500MB election results data. It was observed that the overall election results data transmission time is about 51.779 seconds which is less than one minute (60

Received: February 27, 2024; Accepted: April 12, 2024; Published: April 29, 2024

2020 Mathematics Subject Classification: 68-XX.

Keywords and phrases: election, encryption, results management system (RMS), system architecture, cloud computing.

*Corresponding author

seconds) for about 500MB data size of the election results data. This paper makes a case for the adoption and implementation of the proposed system since it performs better in terms of securing the election results data and transmission time in the cloud environment.

Introduction

Countries all over the world have adopted democracy and made electoral processes of determining their leadership a major activity. Political parties and voters turns to be vigilant in these electoral processes leading to the elections of their leaders. Some of these electoral processes often lead to protracted conflicts and violence by dissatisfied parties of the elections. It is often said that "Elections are won at the polling stations" but another school of thoughts also believe that "it is not who votes that count, it's who counts the votes". These have highlighted the crucial nature of the need to effectively manage elections results in the overall electoral process. Individuals across the globe are very particular and interested in the electoral process even though they may not be politicians especially the election results management. It is common for individuals and organisations to believe that the integrity of the elections is greatly affected by the management of the results in the electoral process. The slightest error or mismanagement of the elections results in the electoral process has great potential of throwing a nation into chaos. In Ghana and most countries in the world, the election results management starts at the point votes are counted at the polling stations or designated counting centers. Irrespective of the level of Technology adopted, the electoral process results need to be captured, stored, transmitted, processed and published either physically or technologically. This research work adopted the hybrid homomorphic encryption approach presented by Abukari et al. [22].

Election Results Management System (RMS)

Results management System (RMS) is a term used to describe how election results are captured, stored, transmitted, processed and published. According to literature, there are three (3) forms of Results Management Systems (RMSs) namely All-paper RMS, Hybrid RMS and Fully-Automated RMS. The focus of security requirements on Results Management System (RMS) is different from the other electoral processes. The security focus of Results Management Systems (RMS) is largely on Integrity and availability of the elections data or results but not on confidentiality since results are declared publicly at the various polling stations after counting publicly. What happens after the counting at the polling station is crucial.

Results Management Scenario

The electoral Commission of Ghana and most countries have implemented the Multi-level tabulation of Election results in the Presidential and parliamentary elections. The official results are largely based on paper results on a completed form called Declaration Results Form at the Constituency and Regional level of every recognized or designated polling station. The tabulated and consolidation of the election results on Declaration Results Form has a provision for representatives of political parties or candidates to sign in order to authenticate the results at the constituency and Regional level.

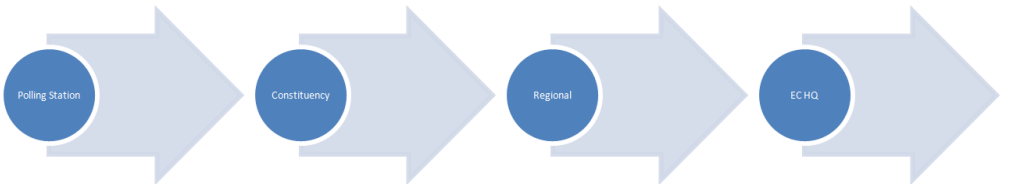

Figure 1: Multi-level Scenario.

Factors for RMS Selection

This research paper explored the various factors that should be considered for the selection of an effective results management System (RMS) for elections in Ghana. The focus of this paper is not to delve into the factors but to explore how they are connected to the effective and efficient elections data sharing or transmission. This research work identified the following as the key factors that requires consideration when selecting a Results Management System (RMS):

1) Political Environment
2) Legal provisions
3) Cultural Considerations
4) Transparency
5) Credibility
6) Complaint Addressing Feature/System
7) Stakeholders involvement and Expectation management
8) Nature of the elections

9) Technology and It's security considerations
10) Costs
11) Risks
12) Infrastructure
13) Physical Security
14) Sustainability
15) Capacity
16) Timing

Results Management System Models

The Results Management System (RMS) implementation is quite a complex operation with so much tension amidst expectations of interested individuals and political parties. This complex operation requires high-level dedication by all stakeholders of the RMS to ensure credibility of the overall electioneering process. The failure of the RMS damages the credibility of the entire electioneering process. Financial, Human and material resources play key role in selecting the model of the Results Management System (RMS). According to Cobos-Flores et al. [21], it is advisable to introduce Information Communication Technology (ICT) gradually by experimenting with pilot projects. This according to UNDP [21] will provide great opportunity to test the performance of the model to be adopted as well as get feedbacks from stakeholders in order to implement more credible model over a period of time. Every RMS consists of three (3) broad components that work collaboratively to ensure credibility of the election results. These are Aggregation, Verification and Publication. How the data is transmitted across the all components is essential and deserves special attention and this is the focus of this research paper. The categorization of the Results Management System (RMS) as presented by Cobos-Flores et al (2015) is based on the incorporation of Technology and these models are:

1) **Manual Systems**: The Manual System Model uses paper, calculators and spreadsheets in managing the results of the entire electioneering process. In the Manual System, the Aggregation, Transmission and Verification are all done manually.

2) **Hybrid Systems**: The Hybrid model adopts both the manual and automated elements. Some processes may be done manually whiles others are automated. The automated component of the Hybrid model may include processes that are related to data aggregation, transmission or creation of database among other processes.

3) **Fully Automated Systems**: The key focus of fully automated systems includes aggregation, verifying and transmission of results without any human interaction or influence.

Election Results Transmission

The approach adopted in the transmission of election results play a very important role in the electioneering process and it is one of the determining factors to ensuring integrity and credibility of the election results data. The implementation of a system to transmit election results data must demonstrate all the following characteristics:

1) High Availability
2) Auditability
3) Effective Network reliability
4) Efficient Network Management
5) High Output
6) Security

The redundancy and continuity of all services connected to the transmission chain must be guaranteed as well as an effective supervised management and monitoring of the network and data assured. The Network capacity used for the transmission must have the required high volumes for the transmission of a lot of data simultaneously without any challenge.

Election Results Data Transmission Using Fax

The Electoral Commission of Ghana has adopted the use of the Fascimile Technology also known as Fax for its election results data transmission for the Presidential category. Constituency and Regional collated results are faxed to the Chairperson of the Electoral Commission of Ghana who then shows the faxed document

to all party agents in the "Strong Room". According to Cavoukian [18], Fax is the production of the exact copy of a printed or written document by scanning and transmitting the data using a telephone line with a connected Fax Machine. The election result declaration sheet is placed in the document feeder of the fax machine and the destination telephone number which is expected to be the fax machine of the Chairperson of the Electoral Commissioner dialed. A replica of the election result declaration form is received by the destination fax machine in a short time. Cavoukian [18] argues that Fax machines represent an imperfect form of communication since sometimes some faxes do not reach their destination which could be attributed to human error or due to technical glitch.

Challenges With Using Fax For Election Results Data Transmission

The usage of the fax machine in today's digital era is widely regarded as an archaic or outmoded technology. However, some organisations across the world including the Electoral Commission of Ghana still rely on the Fax Technology for the transmission of very sensitive data like the Election results declaration sheet. Some researchers have argued that the fax technology is one of the secured technologies for the transmission of documents. According to a report by Perschau [19], advocated for a secured mode of fax transmission for users after identifying some security flaws in the usage of fax machines. Originally, fax machines were design for non-sensitive nature of documents like the sales information and news bulletin among other non-sensitive documents (Perschau [19]). Sensitive data that needs to be transmitted using fax technology needs to be given adequate security attention since the documents can be intercepted during transmission (Perschau [19]). Beside the concern of the data being intercepted during transmission, there is another additional concern of a challenge in authentication of the sender and the receiver as argued by Perschau [19]. In 1993, the National Communications System report NCS TIB 93-16 proposed cryptosystems private keys and public keys in providing a secure data transmission for group 3 and group 4 fax machines. The Group 1 and Group 2 fax machines protocols were developed for analog signal transmission and this created no room for the integration of cryptosystems. The interception of a transmitted data is one of the key challenges identified by Perschau [19] as he states that the intercepted facsimile data can be displayed and/or changed without both the sender and recipient knowing that the data has been stolen or modified or both. Another key challenge identified with the use of Fax machines for transmitting very sensitive data like election

results is Authentication. Fax machines have a challenge in identify the source of a document and the recipient of the intended document. The identification of the sender, the identification of the sender's telephone number, the identification of the recipient and the telephone number of the recipient are all concerns that needs to be addressed in the data transmission using facsimile technology. According to Rydell [20], the speed of faxing can be influenced by a number of factors and notably among them are the speed of the internet, the condition of the fax machine, the transmission speed of the fax machine and the type of document to be faxed. In faxing a document, it is first converted into digital data and transmitted to the recipient's fax machine. The speed is determined by the speed of the internet at the time of the transmission (Rydell [20]). The transmission speed of the fax machine is also another significant determining factor and it is the rate at which the fax machine can send and receive data. The transmission rate of the fax machine is measured in Bits Per Second (bps). A lower transmission rate means the longer it takes to send and receive documents. As stated by Rydell [20], the transmission rate of the fax machine may depend on the model and age of the fax machine. The time used for data transmission using Fax machine is usually between one (1) minute to five (5) minutes and this means between 60 seconds to 300 seconds (Rydell [20]). This research will use the average transmission time of 180 seconds presented by Rydell [20] for the comparative analysis of the proposed system presented in this paper

Proposed System

The research paper presents a proposed system for Elections data sharing in the cloud environment for the purposes of ensuring security based on privacy, integrity and confidentiality. The proposed system is modeled based on a hybrid homomorphic encryption scheme that utilizes the advantages of both AES and RSA.

Proposed System Architecture

The proposed system when implemented seeks to provide confidentiality, privacy and integrity of the transmission of election results data by the electoral commission of Ghana through the cloud environment. The proposed architecture presented in this research work has three entities and each entity is designed to have its own functionalities. The three entities that make up the proposed system are Cloud Storage (CS), Trusted Third Party-Homomorphic Encryption Server (TTP-HES) and Data Users (DUs).

Cloud Storage (CS): The cloud Storage (CS) entity as a component of the proposed system is designed to provide spacious and reliable storage facilities concerning the elections data that needs to be protected against privacy, confidentiality and integrity violations. The Cloud Storage entity is responsible for uploading and downloading of the elections data.

Trusted Third Party-Homomorphic Encryption Server (TTP-HES): The proposed inclusion of a Trusted Third Party-Homomorphic Encryption Server (TTP-HES) is to serve as a trusted source among all stakeholders in the electioneering process as well as provide security and reliability of the election results data transmitted and hosted in the cloud. The TTP-HES is responsible for all the security operations with so much focus on integrity, election results data confidentiality, encryption and decryption keys, Access Control Management (ACM) and digital signatures.

Data Users (DUs): The Data Users (DU) component of the proposed system consist of all relevant stakeholders who have the right to access the election results data in the Results Management System (RMS) process. The Data User (DU) must be known and have the approved permission from the Trusted Third Party-Homomorphic Encryption Server (TTP-HES).

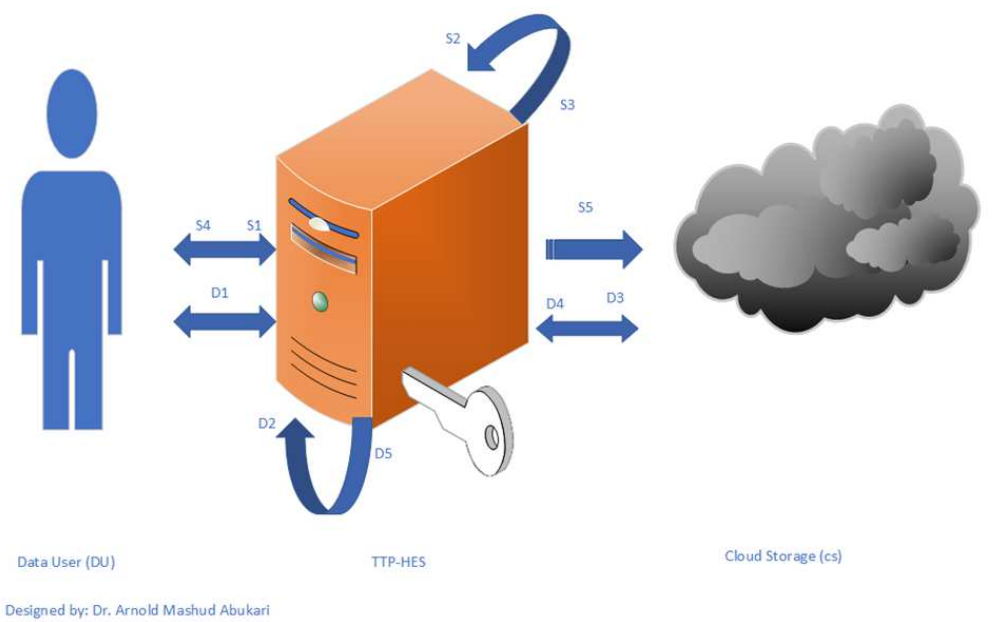

Figure 2: Proposed System Architecture.

Proposed System Algorithm

The research work developed notations purposely for this research paper. Table 1 shows the list of notations adopted in this research work. The definitions for the various notations adopted are also presented in Table 1.

Table 1: Proposed System Notations and Definitions

Notation	**Definition**
R_d	Original Election Results Data
S_kEC	Electoral Commission Private Key
S_kNDC	Private Key for Political Party 1 (NDC)
S_kNPP	Private Key for Political Party 2 (NPP)
S_kCPP	Private Key for Political Party 3 (CPP)
S_kO	Private Key for Election Observer
P_k	Public Key
R_{ID}	Record ID
U_L	User List
K_{AES}	Encryption Key using AES Encryption (Second layer Encryption)
CK_{AES}	AES Decryption Keys
C_{AES}	Cipher-Text of the AES Encryption

Algorithm 1: Proposed System Work Flow

S1: Submission of R_d with U_L to TTP-HES

S2: TTP-HES generates S_kEC, S_kNDC, S_kNPP, S_kCPP, S_kO, K_{AES}

S3: Encryption of R_d (Raw Data) and it's ciphertext to get CK_{AES} and C_{AES}

S4: Retrieves the private keys

S5: Stores the encrypted Election results data in the cloud

D1: A Data User sends request with record identifier R_{ID}

D2: Request verification to authenticate the R_{ID} and source of the request

D3: Sends download request

D4: Receive the encrypted Election results data

D5: Decrypt the encrypted election results data using the private keys of the stakeholders.

This research adopted the RSA and the AES encryption schemes to ensure double layer encryption that will add more security to the election results data transmitted via the cloud in order to prevent Chosen-Ciphertext Attacks (CCA). The Key Generation Algorithm is presented in Algorithm 2

Algorithm 2: Key Generation

1) **Input**: *Pwd, RSA*
2) Generate *EncPwd*
3) Use RSA to generate Public Key P_k and private key S_kEC
4) Divide the S_kEC to all the stakeholders S_kNDC, S_kNPP, S_kCPP, S_kO using XOR
5) Keep the P_k, S_kEC and *EncPwd* for the Data User (DU) in TTP-HES
6) Transmit the private keys to the Data Users (DU)
7) **Output**: *EncPwd*, P_k, S_kNDC, S_kNPP, S_kCPP, S_kO

After the generation of the keys in Algorithm 2, the encryption phase is presented in Algorithm 3 and it uses the generated keys to encrypt the election results data.

Algorithm 3: Encryption Phase

1) **Input**: *Rd, RSA, AES, Access Control List (ACL)*
2) ***For*** each Election record **do**

Use AES to generate K_{AES};

$C_{AES} = (R_d, K_{AES})$;

Calculate Digital Signature;

For each *DU* in the *ACL**do***

CK_{AES} = RSA (K_{AES}, Pk);

End For

Upload C_{AES} to the Cloud;

End For

3) ***Output***: C_{AES}, CK_{AES}, P_k, S_kNDC, S_kNPP, S_kCPP, S_kO

The encryption phase is one of the most essential elements in the proposed system. The security, integrity, confidentiality and reliability of the election results data is heavily dependent on the encryption processes and methods adopted especially when the data is being sent via the cloud. The decryption phase is presented in Algorithm 4.

Algorithm 4: Decryption Phase

1) **Input**: C_{AES}, *RSA, AES, Access Control List (ACL)*
2) Obtain the various private keys from stakeholders S_kNDC, S_kNPP, S_kCPP, S_kO
3) Obtain C_{AES} from the Cloud (CS)
4) Obtain CK_{AES} from the TTP-HES
5) **If** private key (S_kNDC, S_kNPP, S_kCPP, S_kO) doesn't exist in *ACL* then

   'Resend denial access message to the DU';

Else

S_kEC = concatenate (S_kNDC, S_kNPP, S_kCPP, S_kO);

$K_{AES} = RSA\ (CK_{AES}, S_kEC)$;

$Rd = AES\ (C_{AES}, K_{AES})$;

Transmit Rd to the Data user(s);

End if

6) Remove S_kEC and K_{AES};
7) **Output**: R_d (Election Results Data)

The election results data uses both symmetric and asymmetric encryption for its transmission to the cloud and from the cloud. This research adopted a combination of both RSA and AES to enhance the security performance of the Election results data transmission. The proposed system presented in this research paper requires all key stakeholders who are mandated to have access to the system to have login details created by the TTP-HES of the proposed system.

Election Results Data Stored in Cloud

The uploading of the election results data transmits the encryption demand and process to the TTP-HES. The request is submitted and attached to the Election results data (Rd) along with the User List (UL). The Access Control List (ACL) is generated with the respective privileges. Some privileges may be just read only or both read and write permissions depending the user's role in the election results transmission section of the Results Management System (RMS). The election result data is encrypted as shown in algorithm 3 and sent to the cloud. The cloud performs operations on the encrypted election result data.

Key Generation Time

Table 2 presents information on the key generation time for stakeholders of the election results data. This research work considered the number of stakeholders to be in multiples of 10. According to the results presented in a summarized form in Table 2, the proposed system will be more efficient in granting access to election results data compared to the current form being adopted by the electoral commission of Ghana. The key generation time is one of the key important parameters in determining how long it will take the enter transmission and retrieval cycle of the election results data in the cloud taking the encryption time and decryption into consideration.

Table 2: Key generation time for users.

Number of Users (Cloud)	**Key Generation Time**
10	0.000642
20	0.000647
30	0.00065

40	0.000659
50	0.00066
60	0.00067
70	0.00069
80	0.000714
90	0.000744
100	0.00078

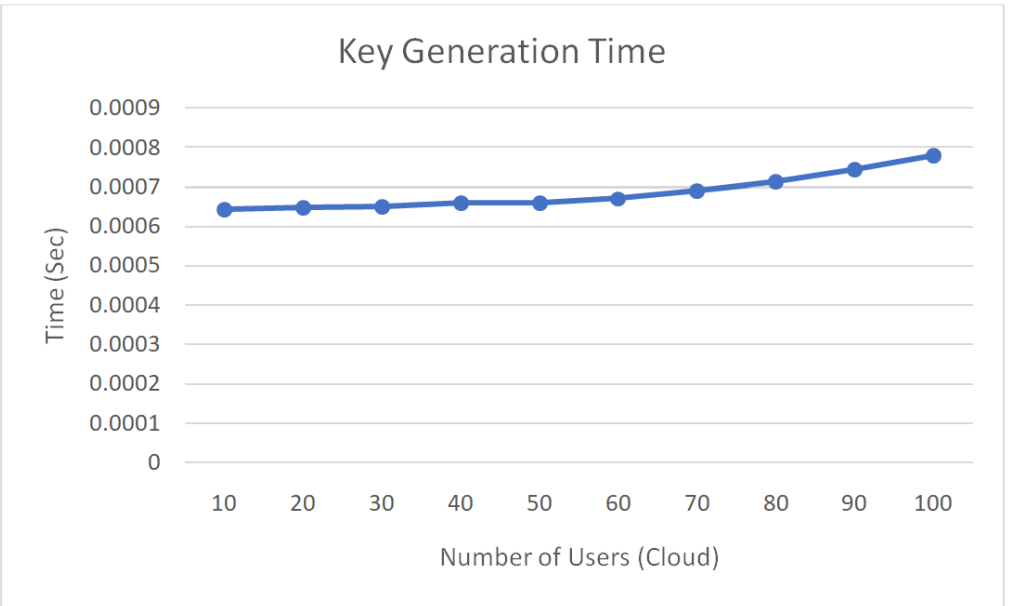

Figure 3: Key generation time.

Figure 3 presented in this research paper indicates the time needed for the generation of the asymmetric key increases as the number of data users (DUs) increases and this is expected. It is also observed that the number of time spent on generating the keys is not entirely uniformly proportional to the number of data users (DUs) as revealed by the research. From the research work, it took 0.000642 seconds to generate keys for 10 data users (DUs) but 0.00066 seconds to generate keys for 50 data users (DUs) confirming that the number of data users (DUs) is not entirely uniformly proportional to the time

needed to generate the keys. The time for key generation does not increase based on a rate similar to that of the data users (DUs) simply because the data users are independent of each other.

Election Results Data Encryption And Decryption Time

In this research paper, the proposed system uses the TTP-HES component to handle the encryption process homomorphically. The encryption time is based on the encryption time set at the TTP-HES and is set according to the data users (DUs) encryption request. In the quest of this research to determine the encryption and decryption times, different file sizes were adopted to determine the encryption and decryption times on each of the data files. The sizes of data files used for the purposes of this research were 1MB, 10MB, 50MB, 100MB, 500MB.

Table 3: Encryption and decryption time.

Data Size	**Encryption Time (Sec)**	**Decryption Time (Sec)**
1MB	0.08	0.067
10MB	0.135	0.243
50MB	0.253	0.544
100MB	0.645	0.788
500MB	0.705	0.863

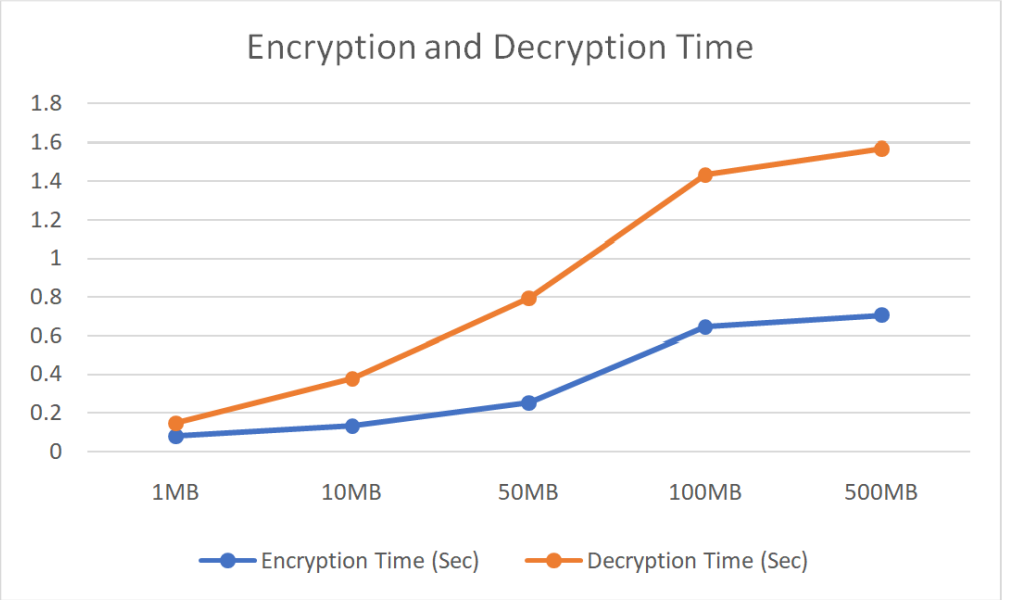

Figure 4: Encryption and decryption time analysis.

As indicated in Table 3, the encryption times have been consistently lower than the decryption time and this is largely attributed to the fact that at the decryption phase stakeholders are involved in the decryption process since they are also part of the Access Control List (ACL).

Election Results Data Upload Time

The research work also considered the times required to upload the election results data onto the cloud. Different data sizes were used for the upload. The data sizes used are 1MB, 10MB, 50MB, 100MB, 500MB. For the purposes of this research work, the upload time is the time needed to transmit or transfer the election results data from the TPP-HES to the cloud. The upload time is observed to be independent of the size of election results data uploaded since it increases proportionality according to the size of the election results data. It is further observed that the time required to calculate the encryption keys to be applied in the cloud remains relatively stable and independent of the election results data size to be uploaded. The encryption of the election results data also contributes to the overall time needed to transmit the election data results and this increases as the size of the election results data increases.

Table 4: Election results data upload.

Election Results Data Size (MB)	**Upload Time (Sec)**
1MB	0.708
10MB	1.34325
50MB	4.18968
100MB	11.25525
500MB	27.3399

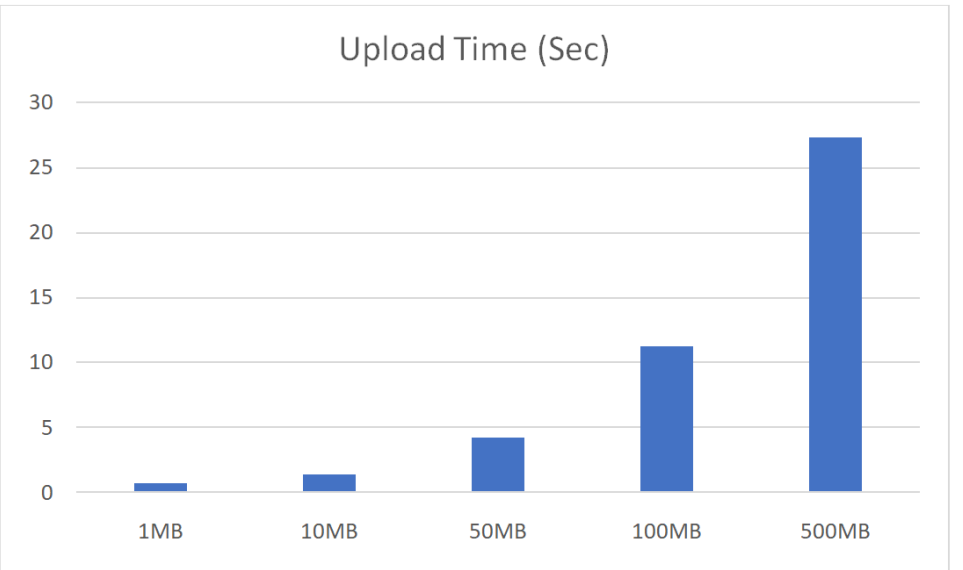

Figure 5: Upload time for election results data.

The research reveals that the encryption time also play significant role in the overall upload time for the election results data. Table 4 indicates the upload time for various election data sizes considered for this research work in an unreliable network environment or a network that has noise. The research work also simulated a perfect network environment without noise and the outcome compared and presented in Figure 6. The outcome of the comparison indicates that, it will take the Electoral Commission of Ghana less than 30 seconds to transmit election results data from various parts of the country even if the network is not very reliable.

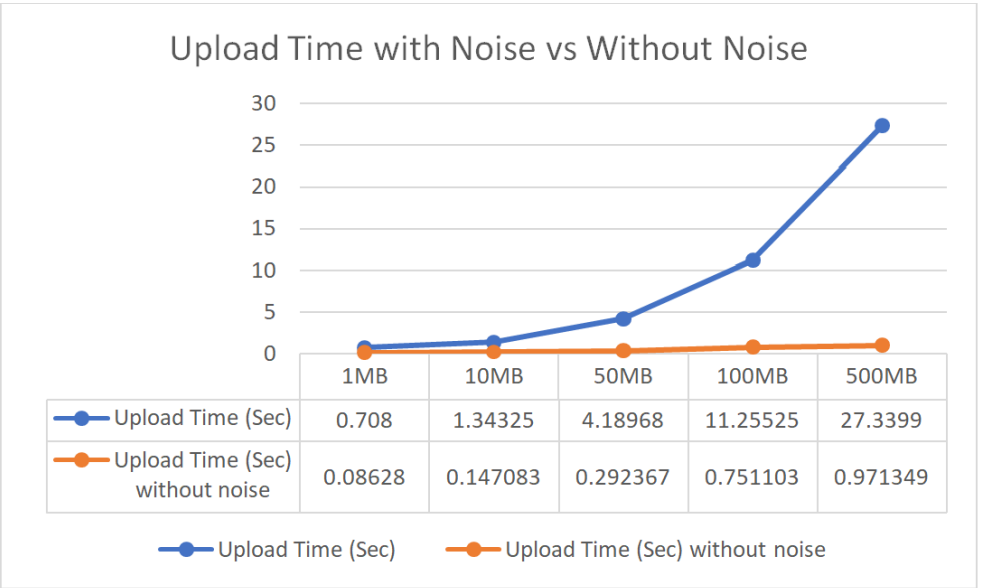

Figure 6: Upload time with noise and without noise.

Election Results Data Download Time

The downloading of the uploaded election results data to be done at the Election Commissioner's headquarters with the consent of stakeholders is essential in the Results Management System processes. Despite the decryption process being relatively high compared to the encryption as presented at Table 3, the download time for the election results data is relatively lower compared to the upload time due to the need for multiple processing of the keys from the stakeholders whose encryption keys are needed for the decryption stage. It is observed that for a data size of 500MB, the download time is 22.87 seconds if all stakeholders with keys are entered at the same time in a noisy network environment. The decryption time also forms part of the overall download time from the cloud.

Table 5: Election results data download.

Election Results Data Size (MB)	**Download Time (Sec)**
1MB	0.655
10MB	1.054
50MB	3.751
100MB	10.045
500MB	22.870

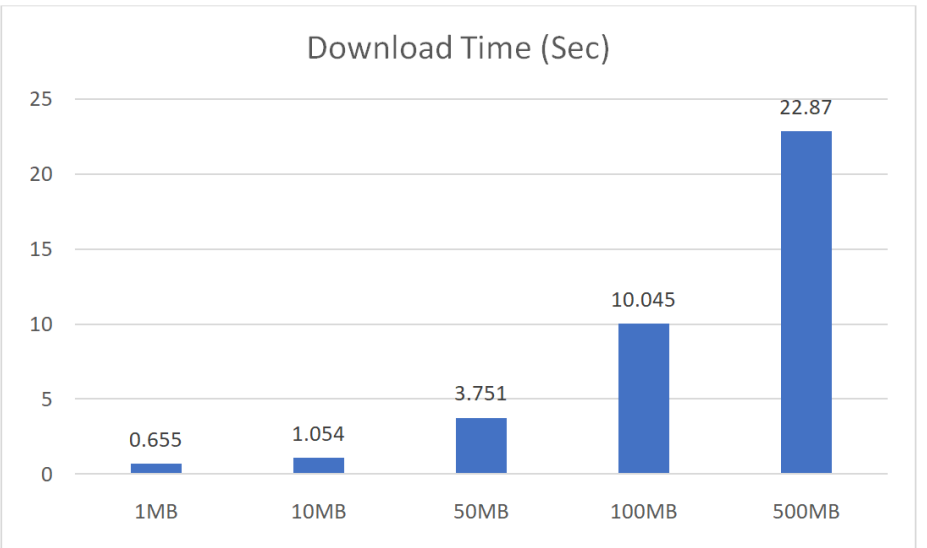

Figure 7: Election results data download time.

Election Results Data Transmission Time

This research work considered all the times used in the entire proposed Results Management System transmission processes and these are the Key Generation Time, encryption time, decryption time, upload time and download time. For the comparison purposes, the research considered 100 users and the election results data size of 500MB. As presented in Table 6 and Figure 8, the upload time (500MB) is the time item that has the highest time in determining the overall election results data transmission whiles the

Key Generation time for 100 users considered is the lowest time recorded in the overall data transmission process. The overall election results data transmission time according to the outcome of this research is about 51.779 seconds which is less than one minute (60 seconds) for about 500MB data size of the election results data.

Table 6: Election results data transmission.

Time Item	**Time (Sec)**
Key Generation Time (100 users)	0.00078
Encryption Time (500MB)	0.705
Decryption Time (500MB)	0.863
Upload Time (500MB) - Noisy	27.3399
Download Time (500MB) - Noisy	22.870

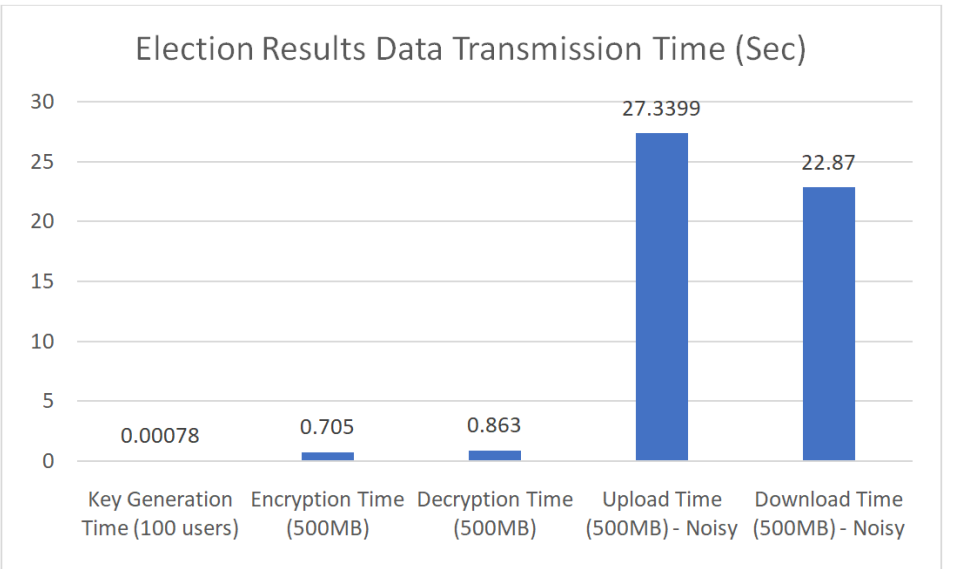

Figure 8: Election results data transmission comparison.

A comparative analysis of the proposed system and the Electoral Commission (EC) transmission systems are presented in Figure 9. The average document transmission time of 180 seconds presented by Rydell [20] is compared with the overall election result data transmission using the proposed system.

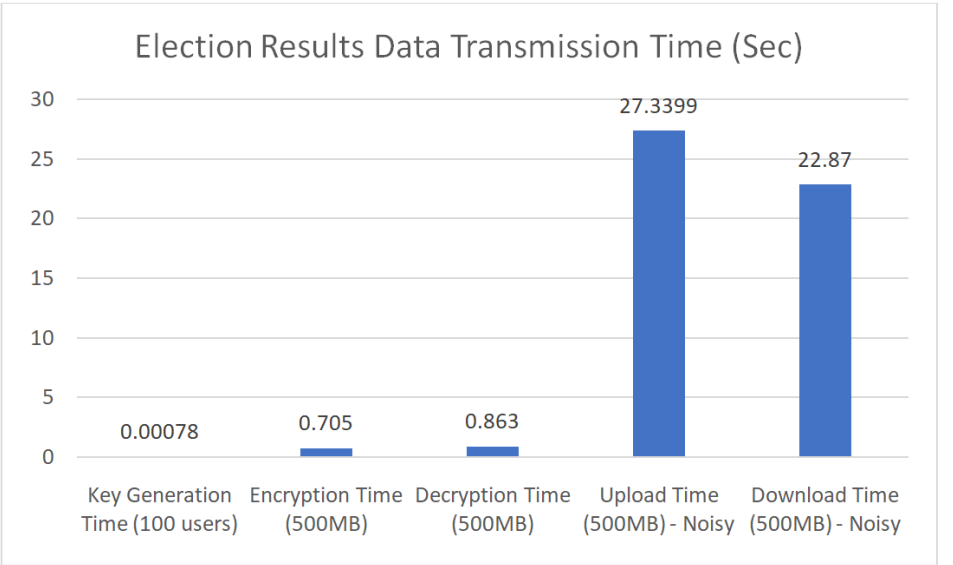

Figure 9: Comparative analysis of proposed system and EC system transmission times.

Security Enhancement with the Proposed System

The proposed system presented in this research work improves the security of election results data significantly. The adoption of a hybrid encryption scheme involving RSA and AES is adding layers of security since different encryption and decryption keys are needed for the encryption and decryption phases. The double layer encryption involving the RSA and AES is also protecting the elections results data against Chosen-Cipher Text Attacks (CCA). The concept of Homomorphism applied in this scheme is to allow the cloud to perform operations on the encrypted data without revealing the content of the election results data. This protects the election results data from Cloud Service Providers (CSP) and other unauthorized users. The private key in the proposed scheme is divided into several other segments according to the parties involved and stored for decryption. The encrypted election results data can only be decrypted by concatenating the various keys from the authorized parties' keys to ensure data integrity and confidentiality. This research work ensures and verifies that no unauthorized person knowingly or unknowingly can alter the election results data. Some of the key data security elements effectively addressed by the proposed scheme are key encryption, encryption, hybrid encryption, privacy, authentication, integrity, access control and non-repudiation as well as data confidentiality. This makes the proposed system presented in

this research work has demonstrated superiority in securing the election results data as compared to how the Electoral Commission of Ghana is currently handling the transmission process.

Conclusion

Digital Security is a major concern when election results are transmitted online or through a digital medium. A threat assessment must be conducted on the infrastructure, software, devices (Biometric Verification Devices), procedures and data. The main goal of this research work was to propose a new, secured and effective way of transmitting election results data during elections in Ghana and beyond in order to ensure efficient access control, integrity of the data, confidentiality and data privacy. This paper presents a cloud-based homomorphic encryption approach to secure and transmit election results based on symmetric and asymmetric encryption. The proposed system adopted the RSA and AES encryption schemes to secure the election results. The research work also considered the time consumed for the entire encryption, transmission, decryption, upload time and download time and the outcome indicates the proposed system performs better compared to the EC's system and can reliably and effectively transmit election results data. For future work, the research recommends addressing situations where a party refuse to consent for the decryption of the election result data since the party's key will be needed and the integration of this proposed system into the blockchain technology requires further research.

References

[1] Hansen, J., Sato, M., & Kharecha, P. (2023). Good news for young people about climate change and a thank you. *Climate Science, Awareness and Solutions, CSAS Columbia*.

[2] Ali, M., Dhamotharan, R., Khan, E., Khan, S. U., Vasilakos, A. V., Li, K., & Zomaya, A. Y. (2017). SeDaSC: Secure data sharing in clouds. *IEEE Systems Journal*, *11*(2), 395-404. https://doi.org/10.1109/jsyst.2014.2379646

[3] Al-Issa, Y., Ottom, M. A., & Tamrawi, A. (2019). eHealth cloud security challenges: A survey. *Journal of Healthcare Engineering*, 2019, Article ID 7516035. https://doi.org/10.1155/2019/7516035

[4] Babitha, M., & Babu, K. R. (2016). Secure cloud storage using AES encryption. In *2016 International Conference on Automatic Control and Dynamic Optimization Techniques* (*ICACDOT*), (pp. 859-864). IEEE. https://doi.org/10.1109/ICACDOT.2016.7877709

[5] Babrahem, A. S., & Monowar, M. M. (2021). Preserving confidentiality and privacy of the patient's EHR using the OrBAC and AES in cloud environment. *International Journal of Computers and Applications*, *43*(1), 50-61. https://doi.org/10.1080/1206212X.2018.1505025

[6] Bentajer, A., Hedabou, M., Abouelmehdi, K., Igarramen, Z., & El Fezazi, S. (2019). An IBE-based design for assured deletion in cloud storage. *Cryptologia*, *43*(3), 254-265. https://doi.org/10.1080/01611194.2018.1549123

[7] Boumezbeur, I., & Zarour, K. (2022a). Privacy-preserving and access control for sharing electronic health record using blockchain technology. *Acta Informatica Pragensia*, *11*(1), 105-122. https://doi.org/10.18267/j.aip.176

[8] Boumezbeur, I., & Zarour, K. (2022b). EMR sharing with privacy preservation using blockchain technology. In *Proceedings of the 1st national Conference on Information and Communication* (*CICT*) (pp. 41-43). Tamanrasset.

[9] Jana, B., Poray, J., Mandal. T., & Kule, M. (2017). A multilevel encryption technique in cloud security. In 2017 *7th International Conference on Communication Systems and Network Technologies* (*CSNT*) (pp. 220-224). IEEE. https://doi.org/10.1109/CSNT.2017.8418541

[10] Khan, A. N., Kiah, M. L. M., Madani, S. A., Ali, M., Khan, A. ur R., & Shamshirband, S. (2013). Incremental proxy reencryption scheme for mobile cloud computing environment. *The Journal of Supercomputing*, *68*(2), 624-651. https://doi.org/10.1007/s11227-013-1055-z

[11] Mahalle, V. S., & Shahade, A. K. (2014). Enhancing the data security in cloud by implementing hybrid (Rsa & Aes) encryption algorithm. In *2014 International Conference on Power, Automation and Communication* (*INPAC*) (pp. 146-149). IEEE. https://doi.org/10.1109/INPAC.2014.6981152

[12] Michalas, A., Bakas, A., Dang, H. V., & Zalitko, A. (2019). MicroSCOPE: Enabling access control in searchable encryption with the use of attribute-based encryption and SGX. In *Nordic Conference on Secure IT Systems* (pp. 254-270). Springer. https://doi.org/10.1007/978-3-030-35055-0_16

[13] Rajakumar, M., Ramya, J., Sonia, R., & Uma Maheswari, B. (2021). A novel scheme for encryption and decryption of 3D point and mesh cloud data in cloud computing. *Journal of Control Engineering and Applied Informatics*, *23*(1), 93-102

[14] Seo, S.-H., Nabeel, M., Ding, X., & Bertino, E. (2014). An efficient certificateless encryption for secure data sharing in public clouds. *IEEE Transactions on Knowledge and Data Engineering*, *26*(9), 2107-2119. https://doi.org/10.1109/tkde.2013.138

[15] Singh, N., & Singh, A. K. (2017). Data privacy protection mechanisms in cloud. *Data Science and Engineering*, *3*(1), 24-39. https://doi.org/10.1007/s41019-017-0046-0

[16] Yang, Y., Zheng, X., Guo, W., Liu, X., & Chang, V. (2019). Privacy-preserving smart IoT-based healthcare big data storage and self-adaptive access control system. *Information Sciences*, *479*, 567-592. https://doi.org/10.1016/j.ins.2018.02.005

[17] Zhang, L., Wu, Q., Mu, Y., & Zhang, J. (2016). Privacy-preserving and secure sharing of PHR in the cloud. *Journal of Medical Systems*, *40*(12). https://doi.org/10.1007/s10916-016-0595-1

[18] Cavoukian, A. (2003). Guidelines on Facsimile Transmission Security [Review of the book *Guidelines on Facsimile Transmission Security*]. In *Information and Privacy Commissioner of Ontario*. https://www.ipc.on.ca/

[19] Perschau, S. (1995). Security and Facsimile [Review of the book *Security and Facsimile*]. In Delta Information Systems, Inc. HORSHAM PA. https://apps.dtic.mil/sti/pdfs/ADA319870.pdf

[20] Rydell, P. (2023, April 22). How Long Does It Take To Fax Something? [Review of the book *How Long Does It Take To Fax Something*?]. https://www.faxburner.com/blog/how-long-does-it-take-to-fax-something/

[21] Cobos-Flores, F., McDermott, R., Catozzi, G., Rico-Bernabe, R., & Patel, A. (2015). Electoral Results Management Systems: Catalogue of Options [Review of Electoral Results Management Systems: Catalogue of Options]. In Jeff Hoover (ed.), www.undp.org. UNDP. https://www.undp.org/sites/g/files/zskgke326/files/publications/Electoral_Results_Management_Systems_Catalogue.pdf

[22] Abukari, A. M., Bankas, E. K., & Iddrisu, M. M. (2021). A hybrid of two homomorphic encryption schemes for cloud enterprise resource planning (ERP) data. *International Journal of Computer Applications*, *183*(38), 1-7. https://doi.org/10.5120/ijca2021921789