International Journal of
Statistics and Applied Mathematics

**ISSN:** 2456-1452
Maths 2023; 8(5): 31-39
© 2023 Stats & Maths
https://www.mathsjournal.com
Received: 01-05-2023
Accepted: 06-06-2023

**Arnold Mashud Abukari**
Department of Computer Science, Tamale Technical University, Ghana

**Edem Kwedzo Bankas**
Department of Business Computing, C. K. Tedam University of Technology and Applied Sciences, Ghana

**Alhassan Abukari**
Department of Statistics, University for Development Studies, Ghana

**Mohammed Muniru Iddrisu**
Department of Mathematics, University for Development Studies, Ghana

**Corresponding Author:**
**Arnold Mashud Abukari**
Department of Computer Science, Tamale Technical University, Ghana

# A statistical performance analysis of three double-layer homomorphic encryption schemes for cloud enterprise resource planning (ERP) data

**Arnold Mashud Abukari, Edem Kwedzo Bankas, Alhassan Abukari and Mohammed Muniru Iddrisu**

**DOI:** https://dx.doi.org/10.22271/maths.2023.v8.i5a.1195

## Abstract

This study presented a statistical performance analysis of three double-layer homomorphic encryption schemes for cloud Enterprise Resource Planning (ERP) data. In this study, Abukari *et al*. (2021) proposed a hybrid of two homomorphic encryption scheme and compared with the state-of-the-art Usha (2018) and Bellafqira *et al*. (2017) double layer homomorphic encryption schemes using the combination of the RSA cryptographic algorithm and the modified Paillier cryptosystem in a hybrid approach. The Multivariate Analysis of Variance (MANOVA) was used to test whether the mean encryption times of the three schemes differ significantly across the data sizes as well as determine which encryption times among the three schemes have the largest difference for each of the data sizes. Preliminary analysis revealed that our new proposed scheme Abukari *et al*. (2021) has the lowest mean mean encryption times of 5.4150, 10.6570 and 39.9770 across the different data sizes of 7MB, 14MB and 200MB compared to the existing state-of-the-art Bellafqira *et al*. (2017) and Usha (2018). The MANOVA test revealed that there is a statistically significant difference in encryption times of the various schemes across the different data sizes, F (6, 52) = 8.827, p<0.005; Pillai's trace = 1.009. The partial $\eta^2 = 0.505$ indicating that approximately 51% of multivariate variance of the mean encryption times of the three schemes is associated with the different data sizes.From the analysis, the proposed homomorphic encryption scheme which combined the RSA algorithm and a modified Paillier cryptosystem outperformed the other two double layer homomorphic encryption schemes investigated.

**Keywords:** Homomorphic, Encryption, RSA, paillier, double layer schemes, cryptography, RSA, paillier, proxy re-encryption, homomorphism, mean, encryption, multivariate analysis, tests of between subjects effects, grand mean estimates, data size estimates

## Introduction

The use of computing devices and technological advancement continues to grow astronomically across the globe. This significant growth comes with challenges that require attention from researchers, manufacturers and the end-users. Notably among the challenges is cyber security. Data confidentiality and data privacy has taken center stage in the quest of researchers to find solutions to the cyber security challenges presented by computing devices and cyber criminals. In a research conducted by Abukari *et al*. (2021) [1], it was made clear that the increase in data globally coupled with data processing, data input and data security are still problematic and requires serious attention. Researchers across the world have proposed several encryption schemes geared towards solving the challenges of cyber security, data confidentiality, data privacy and data security. Single-layer encryption schemes have been proposed over the years but they are still not been able to adequately deal with the increasing cyber security and data security challenges (Abukari, Bankas & Iddrisu, 2021) [1]. The researchers Abukari, Bankas and Iddrisu (2021) [1] believes that encryption schemes that are single-layer in nature are prone to Chosen Ciphertext Attacks (CCA). In an attempt to address the challenges of the single-layer encryption schemes and the Chosen Ciphertext Attacks, double-layer encryption schemes and proxy re-encryption schemes have been proposed. This research work seek to analyse the performance of three double-layer homomorphic encryption schemes by applying statistical analysis.

### Homomorphic Encryption

According to Rocha and Lopez (2019) [11], Homomorphic encryption is the process of performing a mathematical operations on encrypted data (ciphertext) without having access to the actual data itself (plaintext). The operations are conducted on the ciphertext without revealing the content or identity of the plaintext. Decryptions are performed to obtain the desired output. The Homomorphic concept of encryption has contributed significantly in addressing data security concerns in computing devices especially in the area of cloud computing security. As stated by Li *et al* (2018), the concept of homomorphic encryption has contributed greatly in the processing of medical data, outsourcing of financial transactions, preservation of patients records and anonymous database queries among several others. The homomorphic encryption comes in three forms namely Somewhat Homomorphic Encryption, Partially Homomorphic Encryption and Fully Homomorphic Encryption Schemes (Rocha, 2019) [11].

$$Enc(m_1) * Enc(m_2) = Enc(m_1 * m_2)\ \forall m_1, m_2 \in M \ (1)$$

Where *Enc* is the algorithm for the encryption and *M* is the plaintext. The Homomorphic encryption operates on four parameters namely KeyGen, Enc, Dec and Eval. The KeyGen is responsible for the generation of public keys and private keys for the encryption scheme. The *KeyGen*, *Enc* and *Dec* functions are largely applied to most encryption schemes but the *Eval* function is Homomorphic Encryption (HE), specific function. The *Eval* function takes in the ciphertext as input and perform operations on it to output the desired result.

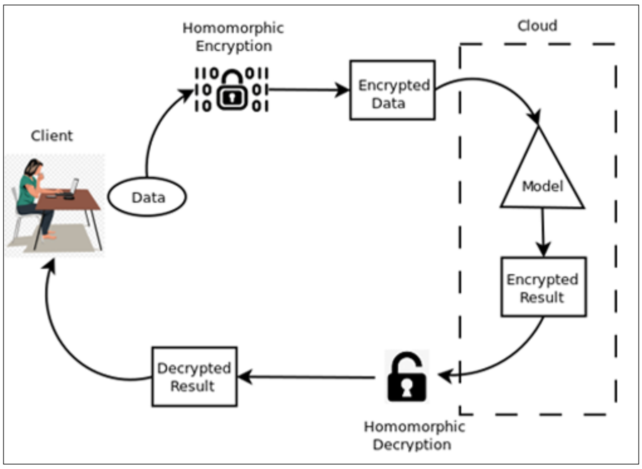

**Fig 1:** Homomorphic Encryption

### Somewhat homomorphic encryption

The Somewhat Homomorphic Encryption scheme is a type of homomorphic encryption scheme that supports mathematical operations on only addition and multiplication (Rocha, 2019) [11]. Researchers have demonstrated that the Somewhat Homomorphic encryption has limited operations largely attributed to the buildup of noise in the data. The buildup of noise from the ciphertext causes more computational overheads and thereby makes the execution of the Somewhat Homomorphic encryption scheme very slow. The Somewhat Homomorphic Encryption (SHE) undergoes through series of steps. An asymmetric public and private keys are generated based on a polynomial function as indicated in equation 2 below:

$$f(x) = x^n + 1 \qquad (2)$$

Where the parameter *n* has a power of 2. The Public Key ($P_k$) and the Private key ($S_k$) are generated using equation 2 and equation 3 respectively:

$$c = Enc(m) = g^m h^r \ mod\ n\ Enc(m) \qquad (3)$$

is the ciphertext of the encryption, *g* and *h* are generated by the *KeyGen* algorithm and *r* is a set of random numbers (0,1,2,…,n-1) whiles *m* is the message to be encrypted.

$$m = Dec(c) = \log_{g^{s_k}}(g^m h^r)^{s_k} \qquad (4)$$

### Double-layer encryption

The dangers associated with computing devices and online presence of information systems needs an additional layer of security to ensure the protection of these information systems online and computing devices of individuals and organizations. The encryption scheme that adds extra layer security is termed as Double-layer Encryption. In the Double-layer encryption scheme, two different encryption schemes could be combined at different layers to ensure a more secured system or data security without compromising on computational speed. One encryption scheme may also be applied twice in two different layers to also enhance the security of the information system or data protection. The double-layer encryption schemes have some advantages when implemented. Some of the advantages presented by Double-layer encryption schemes according to researchers are enhanced security, protection against keylogging, protection against cyber-attacks and improved security in general. The implementation of the double-layer encryption scheme ensures data protection for the data-owner in the cloud (Usha, 2018) [13]. As stated by Usha (2018) [13], the double layer encryption is designed with the aggregation of key generation encryption approach.

### Bellafqira *Et al*. (2017) [5]

The Paillier cryptosystem is one of the popular encryption algorithms that has caught the attention of researchers interested in cyber security, data security and cryptography. The need for a secured cloud environment using a double layer encryption scheme saw Bellafqira *et al.* (2017) [5] proposing a double layer encryption scheme built from the application of the Paillier cryptographic Scheme. The concept of the Bellafqira *et al.* (2017) [5] proxy re-encryption scheme or double layer encryption scheme do not require a user to re-upload a data shared by another user. The researchers in Bellafqira *et al.* (2017) [5] used the help of a Secure Linear Congruential Generator (SLCG) to perform the computations in the cloud which serves as the proxy. The public key and private key of the Paillier cryptographic algorithm be (g, $p_k$) and $p_s$ such that:

$$p_k = pq \qquad (5)$$

Where p and q are two large prime integers. The Private key $p_s$ is also determined using equation 2 below:

$$p_s = (p-1)(q-1) \qquad (5)$$

The value of *g* is selected by the application of the multiplicative inverses modulo $p_k$. The Paillier cryptographic system is used to encrypt the message using equation 7 below:

$$c = Enc\ [m, r] = g^m r^{p_k}\ mod\ p_k^2 \qquad (7)$$

The value *r* is a random integer that is associated with *m*. To decrypt this encrypted data using the private key $p_s$, the following equation is applied:

$$m = Dec\ [p_s, p_k] = (c^{p_s} - 1)p_s^{-1} mod p_k^2 p_k mod p_k \qquad (8)$$

Bellafqira *et al.* (2017) [5] applied the Paillier cryptosystem twice to encrypt the data and the decryption was also done twice. Despite the double layer encryption achieved by Bellafqira *et al.* (2017) [5], a study conducted by Abukari *et al.* (2021) [1] revealed that the encrypted data using Paillier Cryptosystem are sent to the cloud through the internet which could be intercepted by hackers or unauthorised user. Using the same random value to encrypt the ciphertext was also considered problematic by Abukari *et al.* (2021) [1]. It was also revealed that the cloud was trusted to host the proxy re-encryption generator. These challenges identified by Abukari *et al.* (2021) [1] led to the proposed Hybrid of two Homomorphic Encryption Scheme presented by Abukari *et al.* (2021) [1].

**USHA (2018)** [13]

The Usha (2018) [13] proposed double-layer homomorphic encryption used the RSA (Rivest, Shamir and Adleman) encryption algorithm for the encryption of both of the two layers. The RSA Algorithm is one of the widely used cryptographic schemes in the world and it uses public key for encryption and a secret or private key for decryption. The security of the RSA Cryptographic algorithm is based on the complexities in factoring huge integers in the decryption process. The implementation of the RSA Cryptographic algorithm involves three steps namely Key generation, encryption and decryption. The Key generation algorithm is presented in Algorithm 1 below:

| **Algorithm 1: Key Generation Phase** |
|---|
| 1) Choose two different prime numbers, *p* and *q* |
| 2) Find *t* such that *t = pq* |
| 3) Calculate *f(t) = (p-1)(q-1)* |
| 4) Choose e such that *1<e<f(t)* and such that *e* and *f(t)* are relatively prime |
| 5) Use modular arithmetic to determine d = 1 (mod f(t)) |
| 6) Public key = (e, t) |
| 7) Private key = (d, t) |

The key generation phase uses two prime numbers such that their product will generate the value of *t* and the values of *e* and *d* are calculated to determine the public key and private key for the encryption to be carried out. The encryption phase of the Usha (2018) [13] double layer homomorphic encryption scheme is presented in algorithm 2 below:

| **Algorithm 2: Encryption Phase** |
|---|
| 1) Data owner transmits public key to user |
| 2) Data owner converts message (m) into an integer using reversible protocol known as padding scheme such that *0 < m < n* |
| 3) The ciphertext (c) is calculated using $c = m^e$ *(mod n)* |
| 4) The data owner uploads the encrypted data c to the cloud. |

The data owner first converts the message to be sent in to an integer using the reversible padding scheme. The ciphertext is then calculated and upload in the cloud for the user to access it. The user having the public key perform computations on the encrypted data to decrypt as indicated in the algorithm 3.

| **Algorithm 3: Decryption Phase** |
|---|
| 1) User recovers the message using m = $c^d$ (mod n) |
| 2) A reverse padding scheme is conducted to fully recover the message |

The decryption phase performs two operations to in order to reveal the original message of the plaintext. The first layer decryption converts the second layered encrypted data to the ciphertext of the first encryption and another operation converts the first encrypted data to the plaintext.

**Abukari *et al.* (2021)** [1]

Abukari *et al.* (2021) [1] proposed a Hybrid of two homomorphic encryption scheme using two different homomorphic encryption schemes, the RSA cryptographic algorithm and the Paillier cytptosystem. Abukari *et al.* (2021) [1] applied the Paillier Cryptosystem for the first layer encryption. To ensure the first layer encryption, a public key $p_k$ and private key $p_s$ is calculated using the below equations:

$$p_k = pq \qquad (9)$$

$$p_s = (p-1)(q-1) \qquad (10)$$

The first layer ciphertext is computed using equation 11 below:

$$c = Enc\ [m, r] = \ g^m r^{p_k} \ mod\ p_k^2 \qquad (11)$$

Abukari *et al.* (2021) [1] presented a faster version of the Paillier Cryptosystem by introducing a new parameter by letting $g_f = r_g + g$ and modified the Paillier cryptosystem as presented in equation 12.

$$c = Enc\ [m, r] = (1 + mp_k)r^{p_k} \ mod\ p_k^2 \qquad (12)$$

Applying the new parameter $g_f$ proposed, the encryption of the first layer was done using equation 13 below to get the first ciphertext $c_1$:

$$c_1 = Enc\ [m, r] = (1 + mg_f)r^{g_f} \ mod\ p_k^2 \qquad (13)$$

The $c_1$ serves as a plaintext that is passed to the second layer for another encryption process using the RSA cryptographic algorithm. Another set of public and private keys to be used for the second layer encryption are determined using the RSA algorithm. The second layer encryption is calculated using equation 14.

$$c_2 = \ c_1^r . e mod p_k^* \qquad (14)$$

C1 and c2 are ciphertext of the first and second layers encryption respectively and $p_k^*$ is the private key calculated using the RSA cryptographic algorithm. The decryption phase to get back c1 and m uses equation 15 and equation 16 respectively.

$$c_1 = \ c_2 * (n)^* mod p_k^* \qquad (15)$$

$$m = L\left(c_1^{pk} mod p_k^2\right) L\left(g_f^{pk} mod p_k^2\right) mod p_k \qquad (16)$$

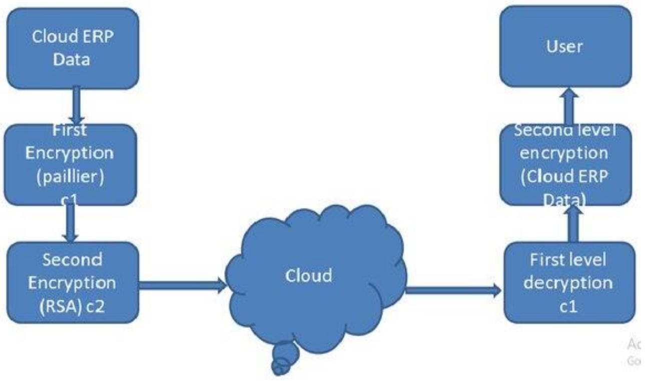
Cloud ERP Data
First Encryption (paillier) c1
Second Encryption (RSA) c2
Cloud
First level decryption c1
Second level encryption (Cloud ERP Data)
User

**Fig 2:** Abukari *et al.* (2021) [1] proposed Double-layer Encryption Scheme

## Multivariate analysis of variance (MANOVA)

The Multivariate analysis of variance (MANOVA) procedure provides regression analysis and analysis of variance for multiple dependent variables by one or more factor variables or covariates. The factor variables divide the population into groups. Using this general linear model procedure, you can test null hypotheses about the effects of factor variables on the means of various groupings of a joint distribution of dependent variables. If more than one dependent variable is specified, the MANOVA using Pillai's trace, Wilks' lambda, Hotelling's trace, and Roy's largest root criterion with approximate F statistic are provided as well as the univariate analysis of variance for each dependent variable. In addition to testing hypotheses, MANOVA produces estimates of parameters.

Fundamentally, MANOVA has basic assumptions of normality, equality of variance covariance and Linearity.

## Data

In MANOVA, the dependent variables should be quantitative. Factors are categorical and can have numeric values or string values. The data under consideration was the simulated encryption times of three different schemes measured across different data sizes. Our dependent variable was the encryption times of the schemes: Abukari *et al* (2021), Usha (2018) [13] and Bellafqira *et al.* (2017) [5]. The independent variable was the data sizes which was categorized as: 1. Small data size (7MB), 2. Medium Data size (14MB) 3. Large data size (20MB).

## Results and Discussions

### Preliminary Analysis

The table below shows the summary measures of the various encryption times of the schemes across the different data sizes.

**Table 1:** Mean and Standard deviation table across different data sizes.

| Data size | Encription scheme | Mean | Standard deviation |
|---|---|---|---|
| Small (7MB) | Abukari *et al.* (2021) [1] | 5.4150 | 0.01269 |
| | Usha (2018) [13] | 5.7110 | 0.02685 |
| | Bellafqira *et al.* (2017) [5] | 6.9040 | 0.02221 |
| Medium(14MB) | Abukari *et al.* (2021) [1] | 10.6570 | 0.06897 |
| | Usha (2018) [13] | 11.4060 | 0.05758 |
| | Bellafqira *et al.* (2017) [5] | 13.7900 | 0.07379 |
| Large (200MB) | Abukari *et al.* (2021) [1] | 39.9770 | 1.31526 |
| | Usha (2018) [13] | 45.8700 | 5.59160 |
| | Bellafqira *et al.* (2017) [5] | 65.0590 | 18.34942 |

It is observed from the above table 1 that Abukari *et al.* (2021) [1] scheme has the lowest means of 5.4150, 10.6570 and 39.9770 across the different data sizes of 7MB, 14MB and 200MB compared to Bellafqira *et al.* (2017) [5] and Usha (2018) [13] as well as the lowest standard deviation. These indicates that Abukari *et al.* (2021) [1] scheme is efficient compared to Bellafqira *et al.* (2017) [5] and Usha (2018) [13].

Figure 3, further demonstrated a steady increase in the encryption times over the schemes as the data sizes increases. As stated in literature, the larger the data the longer it takes for both encryption and decryption. Despite this, Abukari *et al.* (2021) [1] still maintained a better performance compared to Usha (2018) and Bellafqira *et al.* (2017) [5] across the different data sizes.

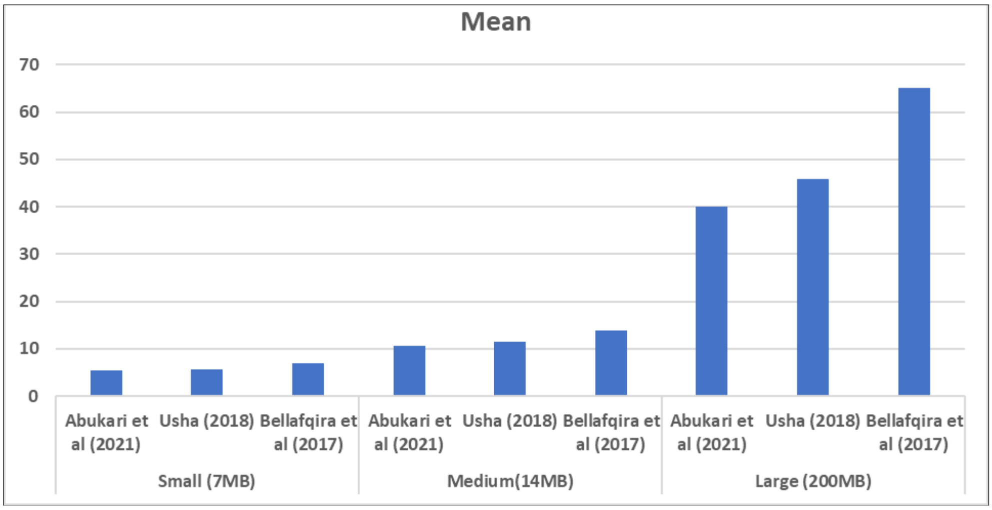

**Fig 3:** Data Sizes and Mean Encryption Time

## Grand Mean Estimates

The study also considered the grand mean estimates of Abukari *et al*. (2021) [1] encryption scheme, Usha (2018) encryption scheme and Bellafqira (2017) [5] encryption scheme. The results are presented in table 2.

**Table 2:** Grand mean estimates

| Dependent variable (Encription scheme) | Mean | Standard error |
|---|---|---|
| Abukari *et al*. (2021) [1] | 18.683 | 0.139 |
| Usha (2018) [13] | 20.996 | 0.589 |
| Bellafqira *et al*. (2017) [5] | 28.584 | 1.934 |

Table 2 indicates Abukari *et al*. (2021) [1] scheme has the lowest grand mean of 18.683 and a standard error of +/-0.139 which further supports that Abukari *et al*. (2021) [1] scheme is efficient compared to Bellafqira *et al*. (2017) [5] and Usha (2018) [13] at 95% confidence interval.

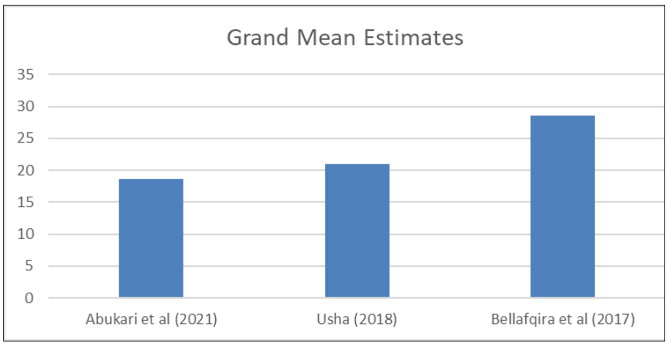

**Fig 4:** Grand Mean Estimates.

## Data Sizes Estimates

The data sizes used in the simulation of the three different proposed encryption schemes are presented with their various means and standard errors table 3.

**Table 3:** Data sizes estimates

| Dependent variable(scheme) | Data size | Mean | Standard error |
|---|---|---|---|
| Abukari *et al*. (2021) [1] encryption scheme | Small (7 MB) | 5.415 | 0.240 |
| | Medium (14 MB) | 10.657 | 0.240 |
| | Large (200 MB) | 39.977 | 0.240 |
| Usha (2018) [13] encryption scheme | Small (7 MB) | 5.711 | 1.021 |
| | Medium (14 MB) | 11.406 | 1.021 |
| | Large (200 MB) | 45.870 | 1.021 |
| Bellafqira *et al*. (2017) [5] encryption scheme | Small (7 MB) | 6.904 | 3.350 |
| | Medium (14 MB) | 13.790 | 3.350 |
| | Large (200 MB) | 65.059 | 3.350 |

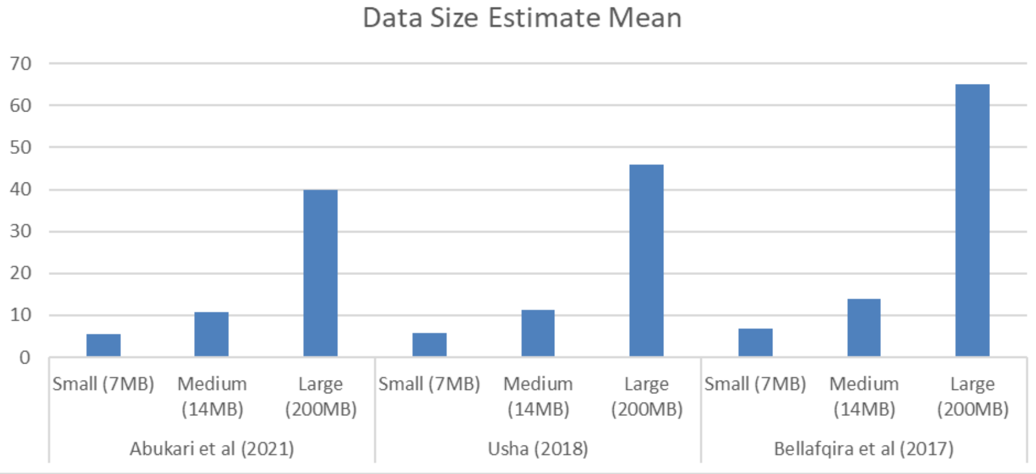

**Fig 5:** Data Sizes Estimates

## Further analysis

We further subjected the data to further analysis by conducting MANOVA to test whether the mean encryption times of the three schemes differ significantly across the data sizes as well as determine which encryption times among the three schemes have the largest difference for each of the data sizes. Then we assess the differences between the groupings (data sizes) and finally examine the univariate results of the individual encryption times of the three schemes.

We investigated the normality assumption of the encryption times of the three schemes by using the Box M test with the Hypothesis that their variance-covariances are the same. The analysis indicated that their covariances are not equal with a *p* value of 0.000 which is less than 0.05. See table 1 below. This indicates a violation of the assumption, hence we used the Pillai's trace criterion because it is more robust to departures from assumptions (Tabachnick, Fidell, & Ullman, 2007) [12].

**Table 4:** Box's Test of Equality of Covariance Matrices

| | |
|---|---|
| Box's M | 443.159 |
| F | 30.877 |
| df1 | 12 |
| df2 | 3532.846 |
| Sig. | .000 |

## Normality Test

The normality test was conducted by generating Normal Q-Q plot of all the encryption times of the three schemes thus: Abukari *et al*., Usha and Bellafqira *et al*. The output of the analysis in the Normal Q-Q plot for all the encryption times of the three schemes indicates a general straight line in all the figures exhibiting a fairly normal distribution in the encryption times of the three schemes.

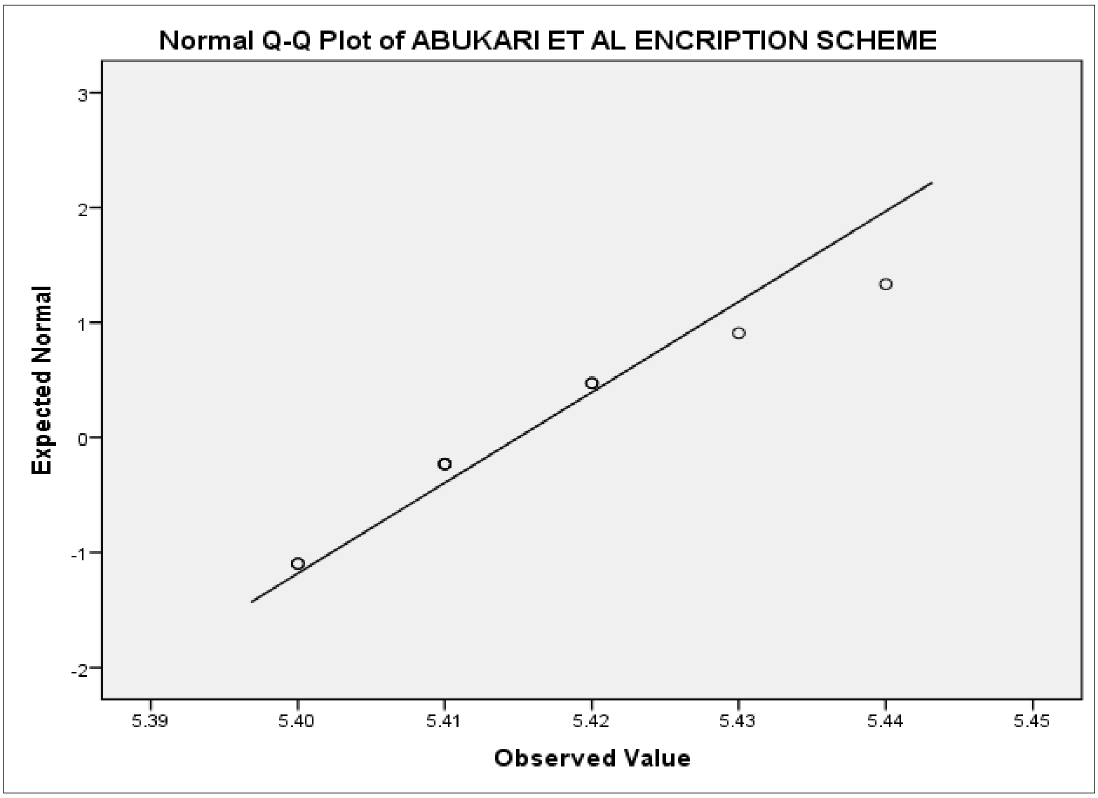

**Fig 6:** Abukari *et al*. normality test.

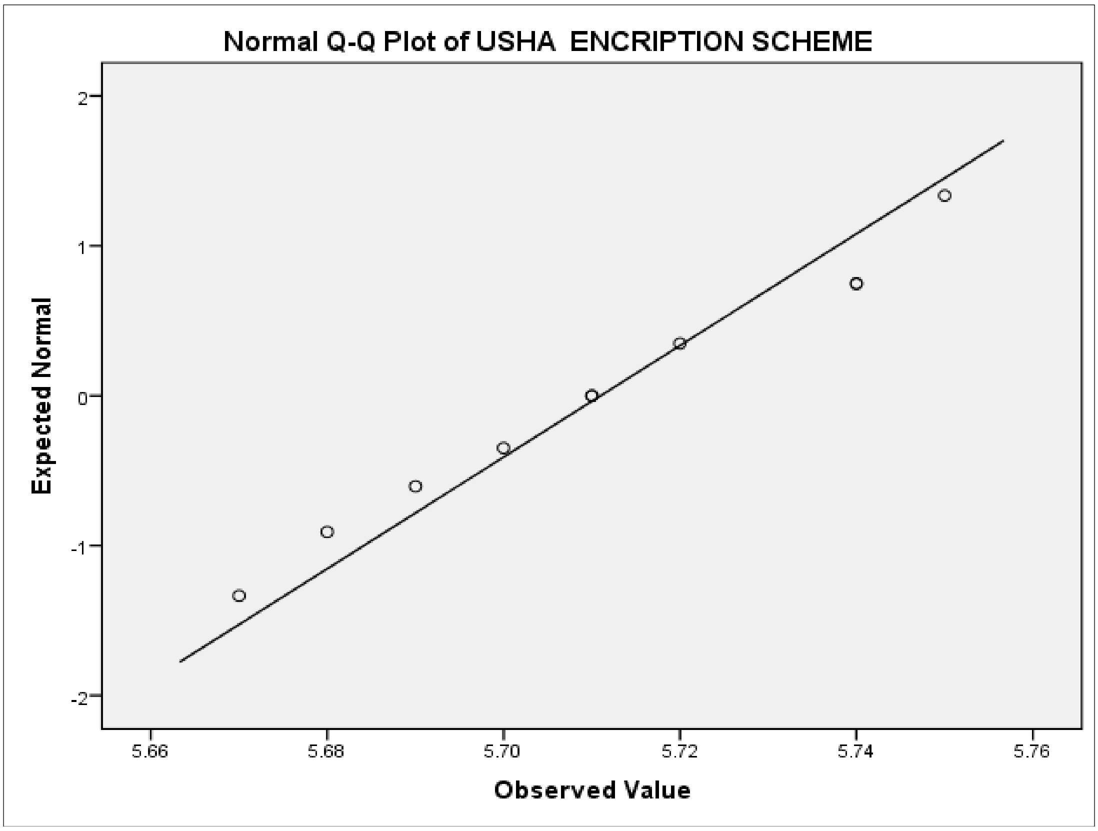

**Fig 7:** Usha normality test

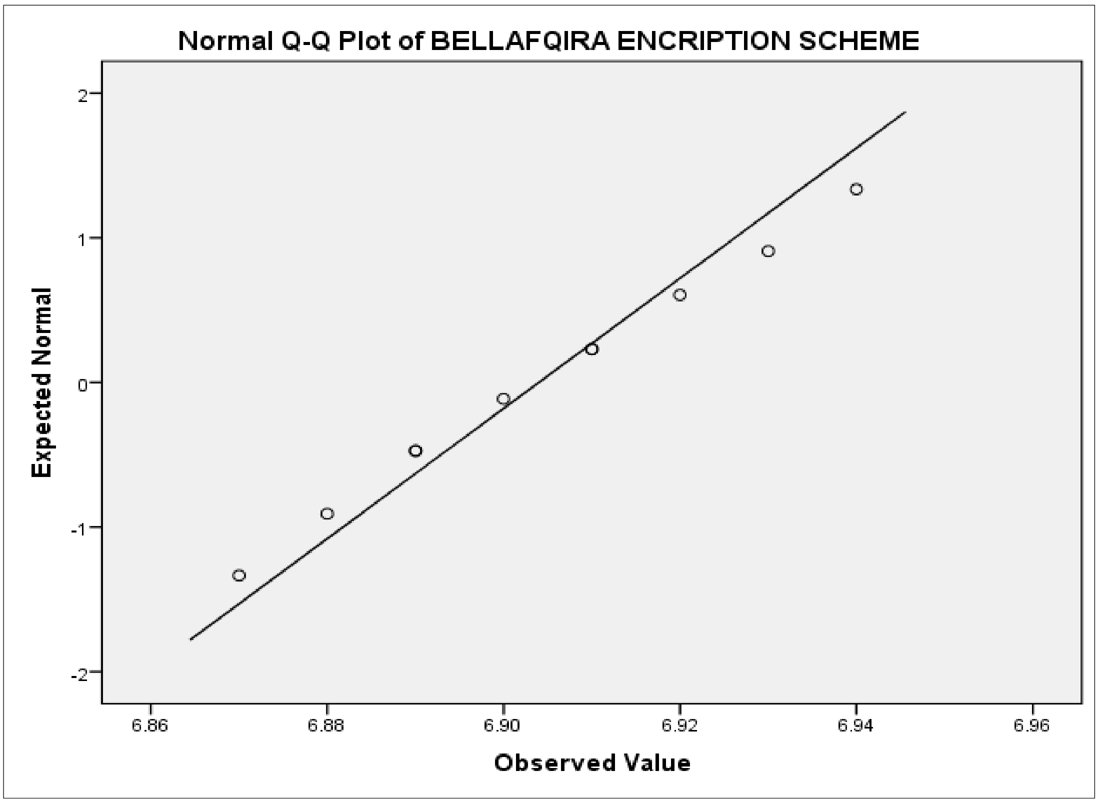

**Fig 8:** Bellafqira *et al.* Normality test

### Multivariate test

This test examined the relationship between the variables by testing whether the mean encryption times of the three schemes differ significantly across the data size. It can be observed from table 4 below that there is a statistically significant difference in encryption times of the various schemes across the different data sizes, F (6, 52) = 8.827, p < 0.005; Pillai's trace = 1.009. The partial $\eta^2 = 0.505$ indicates that approximately 51% of multivariate variance of the mean encryption times of the three schemes is associated with the different data sizes.

**Table 5:** Multivariate Tests

| | Value | F | Hypothesis df | Error df | Sig. | Partial Eta Squared | Noncent. Parameter | Observed Power[c] |
|---|---|---|---|---|---|---|---|---|
| Pillai's trace | 1.009 | 8.827 | 6.000 | 52.000 | .000 | .505 | 52.962 | 1.000 |
| Wilks' lambda | .002 | 179.048[a] | 6.000 | 50.000 | .000 | .956 | 1074.291 | 1.000 |
| Hotelling's trace | 498.979 | 1995.916 | 6.000 | 48.000 | .000 | .996 | 11975.495 | 1.000 |
| Roy's largest root | 498.968 | 4324.387[b] | 3.000 | 26.000 | .000 | .998 | 12973.160 | 1.000 |

### Tests of between-subjects effects

We examined the univariate results of the individual encryption times of the three schemes across the three data sizes which is a follow-up univariate ANOVAs (shown below in table 6).The results indicated that the encryption times of all the three schemes were significantly different for each of the data types with different data sizes F(2, 27) = 5999.645, $p < 0.05$, partial $\eta^2 = 0.998$, F(2, 27) = 452.981, $p < 0.05$, partial $\eta^2 = 0.971$ and F(2, 27) = 89.958, $p < 0.05$, partial $\eta^2 = 0.870$ respectively.

It is clearly seen that Abukari *et al.* (2021) [1] scheme is strongly associated with the data types than Bellafqira *et al.* (2017) [5] scheme and Usha (2018) [13] scheme.

**Table 6:** Tests of Between-Subjects Effects

| Source | Dependent variable | Type iii sum of squares | Df | Mean square | F | Sig. | Partial eta squared | Observed power |
|---|---|---|---|---|---|---|---|---|
| Corrected model | Abukari *et al.* (2021) [1] | 6938.909 | 2 | 3469.455 | 5999.645 | 0.000 | 0.998 | 1.000 |
| | Usha (2018) [13] | 9443.152 | 2 | 4721.576 | 452.981 | 0.000 | 0.971 | 1.000 |
| | Bellafqira *et al.* (2017) | 20193.105 | 2 | 10096.552 | 89.958 | 0.000 | 0.870 | 1.000 |
| Intercept | Abukari *et al.* (2021) [1] | 10471.635 | 1 | 10471.635 | 18108.347 | 0.000 | 0.999 | 1.000 |
| | Usha (2018) [13] | 13224.541 | 1 | 13221.541 | 1268.742 | 0.000 | 0.979 | 1.000 |
| | Bellafqira *et al.* (2017) [5] | 24511.923 | 1 | 24511.923 | 218.397 | 0.000 | 0.890 | 1.000 |
| Datasize | Abukari *et al.* (2021) [1] | 6938.909 | 2 | 3469.455 | 5999.645 | 0.000 | 0.998 | 1.000 |
| | Usha (2018) [13] | 9443.152 | 2 | 4721.576 | 452.981 | 0.000 | 0.971 | 1 |
| | Bellafqira *et al* (2017) [5] | 20193.105 | 2 | 10096.552 | 89.958 | 0.000 | 0.870 | 1 |
| **Error** | Abukari *et al.* (2021) [1] | 15.613 | 27 | 0.578 | | | | |
| | Usha (2018) [13] | 281.431 | 27 | 10.423 | | | | |
| | Bellafqira *et al.* (2017) [5] | 3030.366 | 27 | 112.236 | | | | |

### Pairwise comparisons of encryption schemes

Since the MANOVA test was significant, we followed up with a pairwise multiple comparison test to determine which of the data sizes are significantly different for each of the encryption schemes. We used the Bonferroni approach in order to control for Type I error across the pairwise comparisons (for the three encryption schemes)

It can be observed that, for Abukari *et al*. (2021) [1] encryption scheme, there is a significant pairwise difference in the encryption time between and amongst all the data sizes. Likewise, Usha (2018) [13] encryption scheme.

However, for Bellafqira *et al.* (2017) [5] encryption scheme, there is a significant pairwise difference in the encryption time between small data size and medium data size. This could be attributed to the Cloud service provider hosting the Secure Linear Congrential Generator (SLCG) thereby introducing some latency to the entire encryption process. Bellafqira *et al.* (2017) [5] also used the Pailier Cryptography for the double layer encryption which is adjudged to be under performing in terms of time against RSA schemes.

**Table 7:** Pairwise Comparisons of Encryption Schemes Based on the Data Sizes.

| Dependent variable(Scheme) | Data Size(I) | Data Size(J) | Mean Difference(I-J) | Standard Error | Sig. |
|---|---|---|---|---|---|
| Abukari *et al*. (2021) [1] encryption scheme | Small | Medium | -5.242 | 0.340 | 0.000 |
| | | Large | -34.562 | 0.340 | 0.000 |
| | Medium | Small | 5.242 | 0.340 | 0.000 |
| | | Large | -29.320 | 0.340 | 0.000 |
| | Large | Small | 34.562 | 0.340 | 0.000 |
| | | Medium | 29.320 | 0.340 | 0.000 |
| Usha (2018) [13] encryption scheme | Small | Medium | -5.695 | 1.444 | 0.001 |
| | | Large | -40.159 | 1.444 | 0.000 |
| | Medium | Small | 5.695 | 1.444 | 0.001 |
| | | Large | -34.464 | 1.444 | 0.000 |
| | Large | Small | 40.156 | 1.444 | 0.000 |
| | | Medium | 34.464 | 1.444 | 0.000 |
| Bellafqira *et al*. (2017) [5] encryption scheme | Small | Medium | -6.886 | 4.738 | 0.158 |
| | | Large | -58.155 | 4.738 | 0.000 |
| | Medium | Small | 6.886 | 4.738 | 0.158 |
| | | Large | -51.269 | 4.738 | 0.000 |
| | Large | Small | 58.155 | 4.738 | 0.000 |
| | | Medium | 51.269 | 4.738 | 0.000 |

### Conclusion

This study presented a statistical performance analysis of three double-layer homomorphic encryption schemes for cloud Enterprise Resource Planning (ERP) data. In this study Abukari *et al*. (2021) [1] proposed a hybrid of two homomorphic encryption scheme and compared with the state-of-the-art Usha (2018) [13] and Bellafqira *et al*. (2017) [5] double layer homomorphic encryption schemes using the combination of the RSA cryptographic algorithm and the modified Paillier cryptosystem in a hybrid approach.

The data used was the simulated encryption times of the three different schemes measured across different data sizes. Our dependent variable was the encryption times of the three schemes: Abukari *et al*. (2021) [1], Usha (2018) [13] and Bellafqira *et al*. (2017). [5] The independent variable was the data size which was categorized as: (1) Small data size (7MB) (2) Medium Data size (14MB) (3) Large data size (20MB). The Multivariate Analysis of Variance (MANOVA) was used to test whether the mean encryption times of the three schemes differ significantly across the data sizes as well as determine which encryption times among the three schemes have the largest difference for each of the data sizes.

Preliminary analysis revealed that our new proposed scheme Abukari *et al*. (2021) [1] has the lowest means of 5.4150, 10.6570 and 39.9770 across the different data sizes of 7MB, 14MB and 200MB compared to the existing state-of-the-art Bellafqira *et al*. (2017) [5] and Usha (2018) [13].

The MANOVA test showed that there is statistically significant difference ($p$< 0.05) in the encryption times of the three schemes across the different data sizes. The univariate results of the individual encryption times of the three schemes across the three data sizes produced a very large effect size for Abukari *et al*. (2021) [1] scheme (partial $\eta^2$ = 0.998) indicating a strong association with the data sizes as compared to Bellafqira *et al.* (2017) [5] scheme (partial $\eta^2$ = 0.971) and Usha (2018) [13] scheme ($\eta^2$ = 0.870).

**A pairwise multiple comparison test of the three encryption schemes revealed** a significant pairwise difference in the encryption time between and amongst all the data sizes for Abukari *et al.* (2021) [1] and Usha (2018) [13] encryption scheme. However, for Bellafqira *et al.* (2017) [5] encryption scheme, there is no significant pairwise difference in the encryption time between small data size and medium data size. Conclusively, the analysis consistently showed that our new scheme Abukari *et al.* (2021) [1] performed better as compared to the state of the art.

### References

1. Abukari AM, Bankas EK, Iddrisu MM. A Hybrid of two Homomorphic Encryption Schemes for Cloud Enterprise Resource Planning (ERP) Data. International Journal of Computer Applications; c2021. p. 1–7. DOI: 10.5120/ijca2021921789
2. Abukari AM, Bankas EK, Iddrisu MM. A Secured Video Conferencing System Architecture using A Hybrid of Two Homomorphic Encryption Schemes: A Case of Zoom. International Journal of Engineering and Technical Research. 2020;9:237.
3. Ateniese G, Fu K, Green M, Hohenberger S. Improved proxy re-encryption schemes with applications to secure distributed storage, ACM Transactions on Information and System Security (TISSEC). 2006;9(1):1?30.
4. Baek J, Safavi-Naini R, Susilo W. Certificateless public key encryption without pairing," in International

Conference on Information Security. Springer; c2005. p. 134?148.

5. Bellafqira R, Coatrieux G, Bouslimi D, Quellec G, Cozic, M. Sharing Data Homomorphically Encryptedwith Different Encryption Keys. 2017;arXiv:1706.01756v1 [cs.CR].
6. Blaze M, Bleumer G, Strauss M. Divertible protocols and atomic proxy cryptography, in International Conference on the Theory and Applications of Cryptographic Techniques. Springer; c1998. p. 127?144.
7. Deng RH, Weng J, Liu S, Chen K. Chosen ciphertext secure proxy re-encryption without pairings, in International Conference on Cryptology and Network Security. Springer; c2008. p.1?17.
8. Gantz J, Reinsel D. Extracting value from chaos. Framingham, MA: International Data Corporation; c2011. Retrieved from www.emc.com/collateral/analyst.../idc-extracting-value-from- chaos-ar.pdf (Archived by WebCite®athttp://www.webcitation.org/6bZoomByo)
9. Green M, Ateniese G. Identity-based proxy re-encryption, in Applied cryptography and network security. Springer; c2007. p. 288?306.
10. Li T, Huang Z, Li P, Liu Z, Jia C. Outsourced privacy-preserving classification service over encrypted data. Journal of Network and Computer Applications. 2018;106:100-110.
11. Rocha VF, Lopez J. An Overview of Homomorphic Encryption Algorithms. State University of Capinas. Technical Report IC-PFG-18-28; c2019. p. 1-24.
12. Tabachnick BG, Fidell LS, Ullman JB. Using Multivariate Statistics; c2007. p. 5.
13. Boston MA, Pearson Usha D, Subbulakshmi M. Double Layer En-cryption Algorithm Key Cryptography for Secure Data Sharingin Cloud. International Journal of Scientific and Engineering Research; c2018. p. 9(5).
14. Subramaniyaswamy V, Jagadeeswari V, Indragandhi V, Rutvij H, Jhaveri V, Ketan V, *et al*. Somewhat Homomorphic Encryption: Ring Learning with Error Algorithm for Faster Encryption of IoT Sensor Signal-Based Edge Devices. Security and Communication Networks. 2022;10:2022. Article ID 2793998, https://doi.org/10.1155/2022/2793998