ENHANCING RIVEST SHAMIR ADLEMAN ENCRYPTION ALGORITHM WITH SIMPLE SYMMETRIC KEY FOR CLOUD DATA SECURITY

O.O. Kolawole[1*], N.D. Nwiabu[2*], E.O Bennett[3*]

Department of Computer Science, Rivers State University, Port Harcourt, Nigeria

Abstract *- Although cloud is the future, but its security is of utmost important. With serious security issues and breaches recorded all over the world daily and yearly, there is need to review and see where improvement can be made to the current security system. For this reason modifying or remodeling of the current system will be of great gain for all cloud users. This work presents an improved security approach for cloud data using constructive research methodology. The researcher provided an enhanced RSA encryption algorithm with SSK in the enhancement of cloud data security after a comprehensive study of the Original RSA encryption Algorithm. An Object oriented software development (OOSD) which incorporates object oriented analysis and object oriented design plan was similarly embraced to help indicate the relationship between an object and its class. This research is focus on the implementation of the proposed enhanced RSA Encryption algorithm in a Cloud Based System. PHP programming language, HTML and Java, JavaScript, MySQL database system, Xampp server were used to test-run the system during the development process. Experimental result shows that the use of enhanced RSA algorithm plus SSK as the security parameters to secure cloud data was able to optimize security of data in the cloud.*

Keywords *– Cloud Computing, Data Security, Encryption, Decryption, Cryptography,*

I. INTRODUCTION

Cloud refers to an internet. Cloud Computing is defined as a model which enables convenient and cheap access to shared resources easily managed with minimal effort [19]. Cloud can save an Organization's money and time, but trusting the system itself is more important because the asset of an organisation is the data which they share in cloud to use the needed services by putting it in data base through an application. If security measures are not provided adequately for data operations and transmissions, then data will be at high risk. To avoid risk, it is necessary to secure databases and also the data that involves transit or process [18]. Data Security is the main element of services in cloud computing. Security is an act that requires the deployment of "proportionate defenses". The deployed defenses implemented should be proportionate to the threat. The travelling of data over the internet, also makes it to make data secure [11]. Challenges are the most significant of security and privacy is ensuring authorized access to user data and both Cloud Provider and its Customer should share responsibility for privacy and security [18]. Encryption is a method of protecting secret data on communication network by cryptographic algorithms. A strong cryptographic can be achieved by Asymmetric-key which make use of two keys one for encryption and the other for decryption such as Ravest

Shamir-Adleman (RSA). [22] discussed the encryption of RSA algorithm for the sensitive data that are to be stored in the cloud. When the authorized user requests the data for usage then the data is decrypted and provided to the user. This research proposed an efficient RSA encryption algorithm for cloud data security. The performance of the cryptographic is measured on throughput and response time. This method keeps data safe from adversary.

This academic research is organized into six chapters, as follows: **1** contains the background to the study; it provides the basic understanding of data security in cloud and way of protecting data from adversary, the research problem

with respect to data security, the goal of research and highlights ways of accomplishing task. **II** contains theoretical and empirical review of related literature on data security in cloud. **III** presents the methodology and the use case diagram of the system. **IV** contains the architectural and steps taken to enhance cloud security. V describes the result and discussion of the system are presented. IV concludes the research work.

II. RELATED WORKS

[15] proposed secure file storage in cloud through the use of a hybrid encryption algorithm. They have used symmetric key cryptography algorithm and steganography which combines four algorithms (blowfish, AES, BRA, and RC6) for efficient security of data in the cloud and used the LSB steganography technique to secure key information. [16] proposed three steps security approaches for cloud based on steganography and RSA techniques. They have applied cryptography and steganography to secure information in the cloud for data storing and sharing. The first step of security is the use of cryptography technique to secure the data. RSA algorithm is for key generation, decryption and encryption process. The second step is for image data hiding of steganography to hide encrypted data. The algorithm used in the paper for strong security in cloud and web. [10] enhanced the cloud security as per cloud customer's requirement and to eliminate the concerns related with data privacy. Their system uses combination of two security algorithms such DES & RSA, for encryption and decryption of user uploaded text files in cloud. [12] proposed encryption technique for cloud applications. The techniques used are RC5 and AES algorithms. The level of security and performance in the system was more flexible and also provide the privacy and integrity to the users' identities. [2] proposed comparison and evaluation of security on cloud. The work implemented some crypto algorithms in the cloud and concludes that the algorithms implemented are more reliable than using them on just one system. [14] proposed Homomrphic encryption for data auditing to verify the correctness of shared Patient Hospital Records (PHRs). Also [21] implemented mechanism for control of data access to PHRs in semi-structured servers using a homomrphic encryption technique. [19] proposed enhancement of data storage security in cloud through steganography. They used steganography technique to unauthorized data access from the cloud. This enhanced steganography method is used to store data at cloud data and retrieves data from the data center when it is needed. The drawback is that the scheme only solve limited number of security threats. [20] proposed hybrid encryption for an improved security in cloud. The plain text contains the text that needs to be encrypted and the content of the plain text to be converted to whitened text. They provided better security in the cloud. To the message, the encryption is in the form of the hash function. This scheme is used to prevent insider attacks. [7] proposed security of data in the cloud. They provided security of data in cloud computing using a triple algorithm like Data Encryption Standard (DES), DSA, and Steganography. DSA was used for verification and authentication of data in the cloud. DSA assure the privacy and originality of data. DES is symmetric key encryption algorithm and is used for encrypting data. [5] proposed a model that preserve multi keyword search over encrypted cloud files. The Basic concept of the system is coordinate matching. The matching is used for obtaining similar traits between data documents and query search. The Multi-Keyword Ranked Search (MRS) is also used to describe inner product similarity of the encrypted cloud data. The features of this method are, privacy-preserving, multi-keyword ranked search, and high efficiency which eliminate unwanted traffic and also improve search potency. This model does not support single keyword search with ranking, and not also suitable for large scale data, it is developed as crypto primitives which provides much less semantics.

[3] proposed a Public Key Encryption Technique with keyword search. A method obtained through keyword. PKET uses trapdoor permutations and the Decision Diffie-Hellman Assumption (DDHA) to search encrypted data. This paper implies Identity Based Encryption (IBE), but the main problem was conversing. These construct of PKET is based on recent IBE construct. Two constructions for PKET are Trapdoor Permutation (TP) and Bilinear Diffie Hellman (BDH). The Gateway will learn nothing about the encrypted email.

III. METHODOLOGY

Constructive Research Approach (CRA) and Object-Oriented Design (OOD) was adopted for this study. CR is a problem solving oriented approach that enables the purposeful creation of tools, techniques, methods, and modules that have applicability well beyond the case study that motivated their creation [4].

Research methodology is a systematical way of solving the research problem. Research methods may be understood as all those techniques used for the conduction of research. It is the learning of how a specific research is completed utilizing certain strategies[17]. The resultant collective vision for trans-disciplinary innovation that has resulted offers new approaches to maintaining individual wellness within communities across their entire lifespan on earth

and in space. The main idea of Constructive Research is that building, based on the existing or present knowledge is used in a fresh or new way, with possibly adding a few missing links[8].

The technique is the combination of an enhanced RSA asymmetric key algorithm techniques in terms of ***n*** and Simple Symmetric Key algorithm (SSK). This protocols uses the potential advantages of private cryptography in term of strength and public cryptography in term of speed. This propose enhancement to RSA comes with crucial security ability that affect the speed and security of the algorithm. The increased length of the modulos ***n*** invokes complexity of decomposing such into factors, and therefore increasing the length of the private key, which will in turn make it difficult to dictate the key.

Simple Symmetric key (SSK) algorithm is implemented either as a block cipher or stream cipher. Block as the name imply transforms fixed length block of plaintext into a block of cipher text of the same length. User information consist of Alphabets and numbers ranging from A-Z, 0-9 and other characters.
In a bid to address the weakness of factorization in RSA algorithm computation, this research will involve the use of "***N***" distinct prime numbers. The private and the public will comprise of one components, of which is ***n,*** the product of 5 randomly selected prime numbers ***i, j, k, q*** and ***w*** The public key will be made up of ***"x*** and ***h"***, ***x*** is randomly selected number. This, together with factoring *"**N**"* adds complexity to the key generation function of the scheme. Out of these values, ***N*** is the only value that is both private and public key, we also employ crt for decryption of data.

IV. SYSTEM ARCHITECHURAL DESIGN

System design is the design of solution for the creation of a new system. The proposed system is based on the enhancement of RSA and SSK encryption to enhance cloud data security. Figure 3.2 represents proposed system.

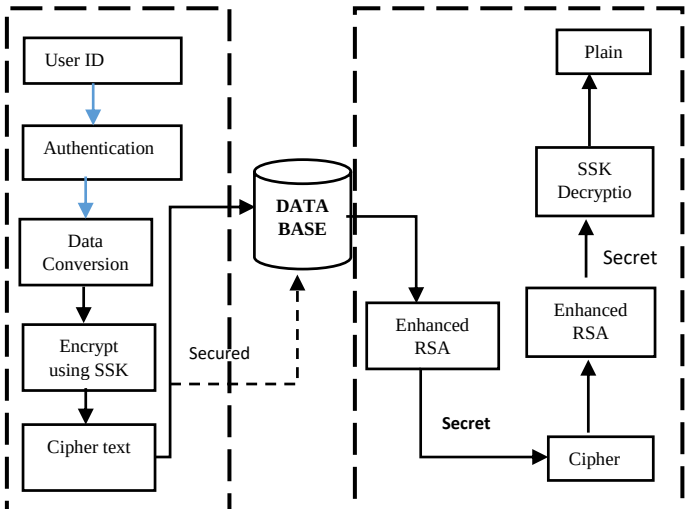

Fig. 1: Proposed System Architecture

The proposed system is a hybrid data security system which concatenates SSK and enhanced RSA encryption algorithms to enhance security of data in cloud. Cloud user sends message and the message undergoes SSK and RSA encryption which produces cipher text to ensure high security on message and prevent unauthorized user or receiver accessing the message.

4.2 UNIFIED MODELLING LANGUAGE

Unified Modelling Language (UML) is a tool for the creation of activity, domain and system class diagrams. UML creates a conceptual model of data security system. For easy understanding, visualization and planning of the project.

4.2.1 USE-CASE DIAGRAM

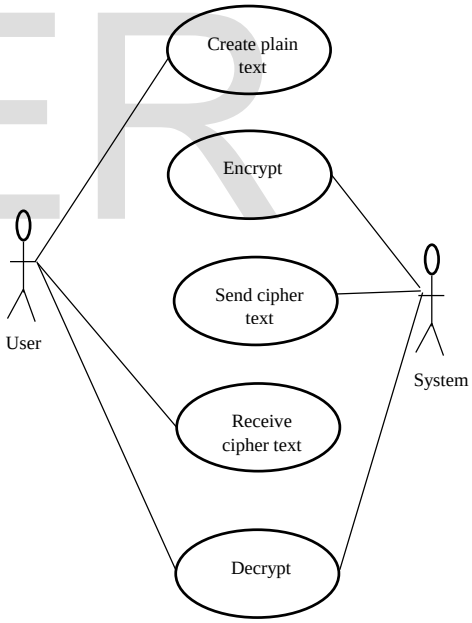

Fig. 2: Use-case Diagram

A. Simple Symmetric key algorithm

1) Key Generation
(i) Choose ***n*** // a number
(ii) Compute Inverse of n mod 37(key1) say k.
(iii) n1 // Negative number chosen for secure key
(iv) mod 37(key2) say k1. // Inverse of negative number

2) Encryption method
(i) Synthetic value for user information

(ii) SV * ***n*** // Synthetic value multiply with selected number
(iii) Compute with mod 37
(iv) Multiply with -v number
(v) Calculate $CT = (PT \times n \times n1) mod 37$

3) Decryption method

(i) key1 × key2 // Multiply with text
(ii) Compute with mod 37
(iii) Decrypt $PT = (CT \times n^{-1} \times n1^{-1}) mod 37$

B. RSA Asymmetric Key Algorithm

Algorithm for Enhanced RSA

1. Choose five prime numbers ***(N): i, j, k, q*** *and* ***w.***
2. Compute the value of ***N = i*j*k*q*w.***
3. Calculate ***phi*** = ***(i-1)*(j-1)*(k-1)*(q-1)*(w-1)***
4. Choose e such that ***1<x<phi*** // ***x*** is greater than 1 but less than phi.
5. Choose d such that ***x*d*** mod ***phi*** = 1
6. Compute ***C= M^x mod N*** //Encryption: Cipher text
7. Generate public key ////Public key ***(x, n)***
8. Generate private key //Private Key ***(h, n)***
9. Decrypt cipher using ***CRT*** //Decryption: Plain text

Algorithm for Hybrid enhanced RSA and SSK

1. SSK_ke y= concat(SSK_key, Random ***n***.);
2. // Generate key
3. S = stringToBiginteger(SSK_key)
4. //convert number to big integer
5. S is publish as secret key
6. Choose five prime numbers (N): *i, j, k, q* and *w*.
7. Compute the value of N = *i*j*k*q*w*.
8. Calculate phi = *(i-1)*(j-1)*(k-1)*(q-1)*(w-1)*
9. Choose ***e*** such: ***1<x<phi*** *// **x** is greater than 1 but less than **phi**.*
10. Choose Private key ***h*** such that ***x*d mod phi = 1***
11. Compute ***C= M^x mod N*** //Encryptn: Cipher text
12. Generate public key ////Public key *(x, n)*
13. Generate private key ////Private Key *(h, n)*
14. Compute ***M= C^h mod N*** //Decryption: Plain text
15. Decrypt cipher using ***CRT*** //Decryption: Plain text

V. RESULT AND DISCUSSION

The result for the simulation of the proposed algorithm and system is presented below. The results shows the simulation of enhanced RSA in JAVA. The enhanced RSA shows improvement in the strength of *n* and reduction in decryption time. The ERSA + SSK is implemented in a cloud webpage. A user register and the record encrypted in the database, with key generation for the decryption of dashboard information. The system authenticate a user whose information is already encrypted on the database. This records are generated on the dashboard in an encrypted format which can only be decrypted by the use of the key.
The GUI is show in the appendix B of the main work.

A. Response Time of System

Table 1: Response Time of Encryption and Decryption

PLAIN TEXT	DATA SIZE	DATA SIZE (KB)	DATA SIZE (MB)	SSK+RSA ENCRYP TIME (SECS.)	SSK+RSA DECRYPT ION TIME (SECS.)
martin	6	0.006	$6E^{-6}$	0.0018	0.0027
dimabo	6	0.006	$6E^{-6}$	0.0018	0.0027
male	4	0.004	$4E^{-6}$	0.0012	0.0018
Married	7	0.007	$7E^{-6}$	0.0021	0.0031
YKC, woji, port harcourt	24	0.024	$2.4E^{-5}$	0.0072	0.0108

Table 1 and Figure 3 shows the response time of our system, showing the time required to encrypt and decrypt user's data. It show that an increase in length of the field determine the response time largely due to the large key factor.

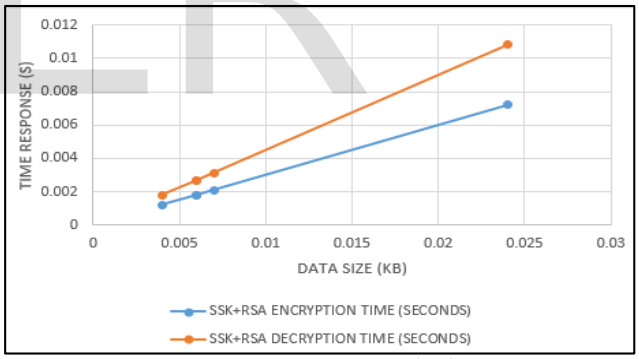

Fig. 3: Response Time (ms)

B. Throughput of System

Throughput is the measure of how many units of information is processed by a system in a given amount of time. Throughput of the system is encrypted Text size in Kilobyte divide by Response time for Encryption in second. Table 2 shows the throughput table of our system.

Encryption Throughput (KB/Sec.) = $\frac{\sum Input\ Files}{EET}$.

Table 2: Throughput Table

DATA SIZE OF ENCRYPTED TEXT (BIT)	DATA SIZE OF ENCRYPTED TEXT (MB)	SSK+ERSA ENCRYPTION TIME (SECS.)	THROUGHPUT (MB/S)
256	$3.2e^{-5}$	0.0018	0.01777
256	$3.2e^{-5}$	0.0018	0.01777
256	$3.2e^{-5}$	0.0012	0.02666
256	$3.2e^{-5}$	0.0021	0.01523
256	$3.2e^{-5}$	0.0072	0.00444
Average THROUGHPUT		0.00282	0.01135

Encryption Throughput (KB/Sec.) = $\frac{\sum 0.032kb}{0.00282sec.}$=

11.35kb/s

C. Comparison Analysis of Result

The proposed system was compared in encryption, decryption and throughput with MD5+RSA and ECC+RSA algorithm as shown in Table 5.5. The encryption time of SSK+ERSA and MD5+RSA was same, but the throughput of SSK+ERSA model is better than the throughput of MD5+RSA and ECC+RSA.

Chidambaram et al., 2016	MD5 +RSA	Strong	No	Yes	2	Variable
Proposed System	SSK+ RSA	Very Strong	Yes	Yes	5	256

Table 3: Comparison of Encryption Response Time and Throughput with existing Algorithms

MODELS	DATA SIZE BEFORE ENCRYPTION (BYTE)	DATA SIZE OF ENCRYPTED TEXT (BIT)	DATA SIZE OF ENCRYPTED TEXT (MB)	ENCRYPTION TIME (SEC.)	THROUGHPUT
MD5+RSA	**7**	32	$4e^{-6}$	0.0021	0.001904
ECC+RSA	7	32	$4e^{-6}$	0.0019	0.002105
SSK +ERSA	7	256	$3.2e^{-5}$	0.0021	0.015231

Table 3: Depict the comparison result of Encryption time and throughput of different models with SSK + ERSA posing the best result because of the encrypted byte size. Table 4 shows the comparison between existing system and proposed system.

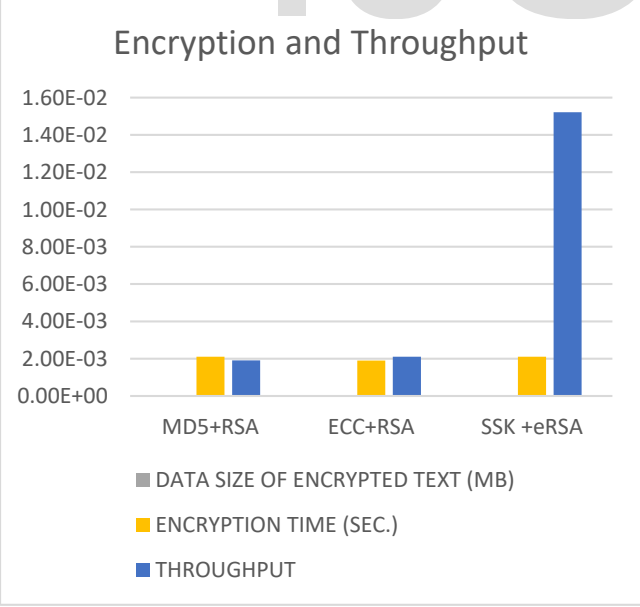

Fig. 4: Encryption time and Throughput of different models

Table 4: Comparison of Existing System

System	Security	Dashboard Encryption	Speed	Key length	Block Size

D. RSA Evaluation

This system and the algorithm used for implementation were evaluated and data recorded as follows. RSA with large key value is less prone to hackers thereby making it more secure.

Table 4: RSA ***n*** Comparison Table

FACTOR	RSA		ERSA	
Key Length	n=p*q		n=i*j*k*q*w	
n	7303		51051	
Phi(n)	7128		23041	
Block Size	variable		256byte	
Bit Size	**8Bits**	**`16Bits**	**8Bits**	**16Bits**
Encryption Time(Sec)	0.000079	0.000061	0.000075	0.000041
Decryption Time(Sec)	0.00021	0.001445	0.000023	0.001415
Speed	Slow		Not Slow	
Security	Least Secure		More Secure	

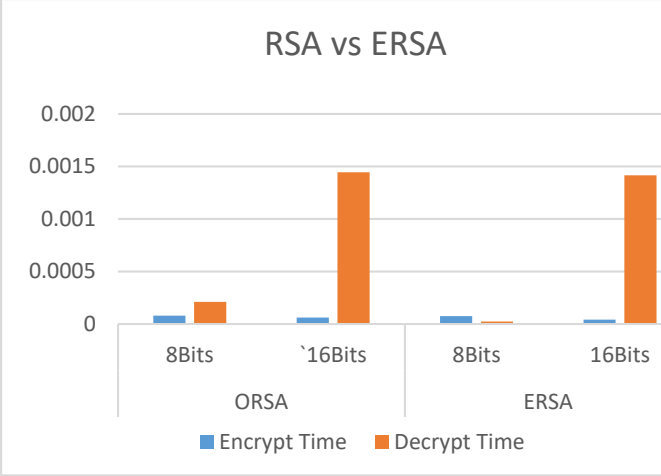

Fig. 5: RSA vs ERSA comparison graph

The measurement of RSA against enhanced RSA is such that with higher increase ***n*** also comes with an increased security. With the time relatively the same.

Fig. 6 shows the online implementation phase of the research work with encrypted dashboard only decrypted with key.

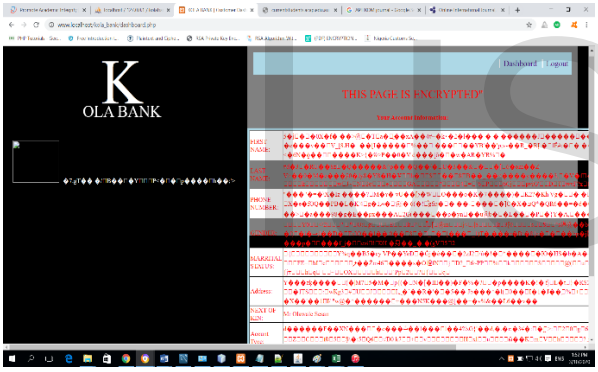

Fig. 6: Cloud GUI Implemented Dashboard Table

E. Hensel's Lemma Attack

Using Hensel's lemma for factoring n, $N = \prod_{i=1}^{u} ri$, integer N can be factor in polynomial time, given a δ fraction of random bits of its prime factors greater than $2\text{-}2^{\frac{1}{u}}$. By definition $E[B] = \frac{(2-\delta)^{u}}{2} < 1$,

$$((2-\delta)^{u} < 1$$

$$2 - \delta < 2^{\frac{1}{u}}$$

$$\delta > 2 - 2^{\frac{1}{u}}$$

$-N = \prod_{i=1}^{2} ri, \delta \geq 0.59(2-2^{\frac{1}{2}} \approx 0.5858)$ needed fraction of bits to factor N.

$-N = \prod_{i=1}^{3} ri, \delta \geq 0.75(2-2^{\frac{1}{3}} \approx 0.7401)$ needed fraction of bits to factor N.

$-N = \prod_{i=1}^{4} ri, \delta \geq 0.81(2-2^{\frac{1}{4}} \approx 0.8108)$ needed fraction of bits to factor N.

$-N = \prod_{i=1}^{5} ri, \delta \geq 0.85(2-2^{\frac{1}{5}} \approx 0.9000)$ needed fraction of bits to factor N.

Therefore if ***u > 2***, to factor N becomes harder. The advantages of using a multi prime modulus ***N*** is that the attacker will need more than $2^{\frac{1}{u}} - 2^{\frac{1}{2}}$ fraction of random bits if a basic modulus ***N*** is used.

VI. CONCLUSION

In this research, a hybrid data security system has been developed, which concatenates Simple Symmetric Key (SSK) and an enhanced Rivest Shamir Adleman (RSA) algorithms to enhance data security in cloud. System user sends message and the message undergoes SSK and enhanced RSA encryption which produces cipher text to ensure high security on message and prevent authorized user or receiver accessing the message. SSK as a block cipher convert a fixed length block of plain-text into a block of cipher text data of the same length. RSA use keys that are related between each other, generating from prime numbers by multiplying the numbers together, thus this is derived via mathematical formula. Object-oriented methodology has been employed to model the interaction of system components; using a use-case and class diagram.

REFERENCES

[1]. Abbas, S. A. and Mohammed, M. Q.(2017). Improved Data Storage Security in Cloud Using RC6 Algorithm. *(IOSR-JCE)*, 19(5), pp. 51-56.

[2]. Arora P, Singh A. and Tyagi H.(2012). Evaluation & Comparison of Security Issues in Cloud Environment. *World of Computer Science and Information Technology Journal*, 2(5), pp. 179-183.

[3]. Boneh, D., Crescenzo, G. D., Ostrovsky, R. and Persiano, G. (2004). Public Key Encryption with Keyword Search. *EUROCRYP, LNCS*, 3027, pp.506-522.

[4]. Blount, M., McGregor, C., James, A., Sow, D., Kamaleswaran, R., Tuuha, S., Percival, J and Percival, N. (2010). On the Integration of an Artifact System and a Real-Time Healthcare Analytics System. In *Proceedings of the 1st ACM International Health Informatics Symposium*, pp. 647–655.

[5]. Cao, N., Wang, C., Li, M., Ren, K. and Lou, W. (2011). Privacy-Preserving Multi-keyword Ranked Search over Encrypted Cloud Data. *INFOCOM, Proceedings IEEE*.

[6]. Chidambaram, N., Pethuru Raj, P., Thenmozhi, K. and Amirtharajan, R. (2016). Enhancing the Security of Customer Data in Cloud Environments Using a Novel Digital Fingerprinting Technique. *International Journal of Digital Multimedia Broadcasting*, http://dx.doi.org/10.1155/2016/8789397

[7]. Garima, S. A, and Naveen, S. H. (2014). Triple Security of Data in Cloud Computing. *International Journal of Computer Science and Information Technologies (IJCSIT)*, 5(4), pp. 5825-5827.

[8]. Jönsson, S and Luka, K. (2007). There and Back Again: Doing Interventionist Research in Management Accounting, in Chapman, C.S., Hopwood, A.G., Shields, H.G. (eds.) *Handbook of Management Accounting Research*, Elsevier, pp (373–397).

[9]. Karun, H. A. and Uma, S. I. (2015). "Data Security in Cloud Computing using Encryption and Steganography". *International Journal of Computer Science and Mobile Computing*, 4(5), pp. 786-791.

[10]. Khan, S. S. and Tuteja, R. R. (2015). Security in Cloud Computing using Cryptographic Algorithms. *International Journal of Innovative Research in Computer and Communication Engineering*, 3(1).

[11]. Khanezaei, N. and Hanapi, Z. M. (2014). A Framework Based on RSA and AES Encryption Algorithms for Cloud Computing Services. *IEEE*, pp. 58-62.

[12]. Khorsheed, N. K., Khorsheed, O. K., Rashad, M. Z. and Hamza, T. T. (2015). Encryption Technique for Cloud Applications. *International Journal of Scientific & Engineering Research*, 6(9).

[13]. Krishna, B. H., Kiran, S., Murali, G. and Reddy, R. P. K. (2016). "Security Issues in Service Model of Cloud Computing Environment", In *Proceedings of the International Conference on Computational Science Procedia Computer Science*, 87, pp.246-251.

[14]. Liang, X., Lu, R., Lin, X. and Shen, X. S. (2010). Patient self-controllable access policy on PHI in e-health care systems. *Proceedings of Advances in Health informatics conference*, pp. 1-5.

[15]. Maitri, P. V. and Verma, A. (2016). Secure File Storage in Cloud Computing Using Hybrid Cryptography Algorithm, *IEEE WiSPNET conference*.

[16]. Pant, V. K., Prakash, J. and Asthana, A. (2015). Three Step Data Security Model for Cloud Computing based on RSA and Steganography techniques. *IEEE*.

[17]. Rahman, M. O., Hossen, M. K., Morsad, G., Roy, A. C. and Chowdhury, S. A. (2018). An Approach for Enhancing Security of Cloud Data using Cryptography and Steganography with E-LSB Encoding Technique. *IJCSNS International Journal of Computer Science*.

[18]. Rani, D. and Ranjan, R. K. (2014). Enhance data security of private cloud using encryption scheme with RBAC. *International journal of Advanced Research in cloud and communication Engineering*, 3(6).

[19]. Sarkar, K. A. and Chatterjee, T. R. (2014). Enhancing Data Storage Security in Cloud Computing Through Steganography. *ACEEE International Journal on Network Security*, 5(1), pp. 234-279.

[20]. Sidhu, A. and Mahajan, R. (2014). Enhancing security in cloud computing structure by hybrid encryption. In *International Journal of Recent Scientific Research*, 5(1), pp. 128-132.

[21]. Soubhagya, B., Venifa, M. G. and Jeya, A. J. (2013). Homomorphic encryption technique for scalable and secure sharing of personal health records in cloud computing. *International Journal of Computer Applications*, 67(11).

[22]. Yellama, P, Narasimham, C. and Sreenivas, V. (2013). Data Security in Cloud using RSA. *IEEE*, 1-6.

Authors Profile

Mr. O.O. Kolawole pursue Bachelor of Science from National Open University, Abuja, Nigeria in 2016. He is currently pursuing Masters of Science from Department of Computer Science, Rivers State University, Nigeria since 2017. His main research work focuses on Enhancing RSA encryption for cloud security. He has 1 year of research experience.

Dr. N. D.Nwiabu pursued Bachelor of Science from Kwame Nkrumah University of Science & Technology, Kumasi, Ghana in 2002, and Master of Science from University of Port Harcourt, Nigeria in 2006. He also obtained PgCert in Research Methods and PhD from Robert Gordon University, Aberdeen, UK in 2009. He is currently working as a lecturer in Department of Computer Science, Rivers State University, Nigeria since 2012. He is a member of IEEE computer society since 2011, a member of NCS since 2005 and CPN since 2005. He has numerous publications and conference papers in reputed international journals including IEEE. His main research work focuses on Situation-aware system, Pipeline monitoring, Decision support system, prediction system, etc. His work won awards in the North Sea, IEEE, MIT, and EIM. His work has also got an application area in sociaology to monitor crime. He has 16 years of teaching experience and over 10 years of Research Experience.

Dr. E.O Bennett pursue Bachelor of Science from Rivers State University, Nigeria. He also obtain PgCert and PhD from the University of Port Harcourt, Nigeria. He is currently working as lecturer in Department of Computer Science, Rivers State University, Nigeria. He is an astute researcher who has publish numerous works in world journals.