World Journal of Engineering Research and Technology
WJERT
www.wjert.org
SJIF Impact Factor: 5.218

ENHANCED DATA SECURITY FRAMEWORK IN CLOUD COMPUTING FOR LOSS OF DATA USING EXTENDED RSA ALGORITHM

Biba Bobai[1], Rabia Khan[2], Rashid Husain*[3] and A. S. Magaji[4]

[1]Research Scholar, Kaduna State University, Nigeria.
[2]MCA, Punjab Technical University, India.
[3]Lecturer, Sule Lamido University, Kafin Hausa, Jigawa, Nigeria.
[4]Lecturer, Kaduna State University, Nigeria.

Article Received on 08/11/2018 Article Revised on 29/11/2018 Article Accepted on 20/12/2018

***Corresponding Author**
Rashid Husain
Lecturer, Sule Lamido University, Kafin Hausa, Jigawa, Nigeria.

ABSTRACT

Cloud computing is the process of utilizing network of remote servers deployed on the internet to manage each and every action on data more willingly than a local server or personal computer. The cloud has provided many advantages/benefit to individuals and organization, but security still exist as a major setback of the cloud as intruders or other users bridged others data privacy. The cloud suffers from loss of data, identity theft, denial of service and lots more. This security concerns includes Data Confidentiality, Integrity and Availability (CIA) etc. This paper presented the security protection of user data in the cloud through a thin novel approach incorporated with a federated cloud to generate cryptographic key pairs using RSA algorithm.

KEYWORDS: Cloud Computing, Cryptography, Data Security, Data Control, Federated cloud, RSA Algorithm.

INTRODUCTION

There has been a tremendous increase in large volume of data storage and computation since the emergence of cloud computing, computation has become very easy and fast. The present modern data storage and computation has brought about a fundamental approach in the

networking, resources storage, security and management of computing resources at ease. Many service providers such as Google Drive, Amazon, Drop Box etc. provide an infrastructure for cloud service users to store their data. Storage and computation of users data on one cloud service provider usually undergo many challenges like service availability, mechanism issues, and management reliability (Peter M., 2011).

Cloud computing is a form utilizing ever-present, less cost, on demand network access to a networked shared pool of configurable computing resources which can be speedily provisioned and released with minimal management effort or service provider interaction (Peter M., 2011).

Data security in cloud computing

Data security is the one of major challenges in cloud computing. Since a third party also shares storage of sensitive and confidential business data, it is never known what is going on with the data (Venkata, *et. al.*, 2011).

Cloud storage federation provides a solution to single cloud service provider's problem through brokerage. Cloud service users employ the cloud storage federation that takes care of the data storage and maintenance at different cloud service providers, rather than using a single storage location, the federation replicates user's data and distributes it to many service providers (Wuchner *et. al.*, 2013).

Despite the sophistication of cloud computing application service, cloud computing is fraught with security risks and the basic security issues are brought to the attention of potential cloud service subscribers such as authentication, auditing, confidentiality, integrity, availability and non-repudiation. The virtualization and cloud computing delivers wide range of dynamic resources, but the security concern is generally perceived as the huge issue in the cloud which makes the users to resist themselves in adopting the technology of cloud computing (Venkata, *et. al.*, 2011).

Three Major Security Issues in Cloud (Yuhong Liu, *et. al.*, 2015)

1. Confidentiality: this ensures that data privacy is not disclosed to unauthorized persons. Confidentiality loss occurs when privacy is breached by any individual who are unauthorized to access a given location (Wood K. *et. al.*, 2010).

2. Integrity: this ensures that the data held in a system is a proper representation of data intended and it has not been modified by an authorized person (Wood K. *et. al.*, 2010).

3. Availability: this ensures that data processing resources are not made unavailable by malicious action. It is a simple idea that when a user tries to access something, it is available to be accessed. This is vital for safety critical systems (Wood K. *et. al.*, 2010).

Related Works

Wunchner *et. al.*, 2013, introduced a Federated cloud to provide improve service availability and reduces vendor lock-in risks of single-provider cloud storage solutions. The Federation therefore distributes and replicates data among different cloud storage providers. Missing controls on data location and distribution however was a major security and compliance issues. These men propose a novel approach of using data-driven usage control to preserve compliance constraints in cloud storage federation. Based on common compliance regulations and laws they provided a brief categorization of compliance problems into spatial, temporal, and qualitative requirements. In addition, they showed how usage control policies can be employed to constrain federation according to these categories.

Shinde *et. al.*, 2015, proposed a work plan to eliminate the concerns regarding data privacy using encryption algorithms to enhance the security in cloud as per different perspective of cloud customers. These engineers made used of the combination of Public and Private key encryption to hide the sensitive data of users, and cipher text retrieval. The paper analyzed the feasibility of applying encryption algorithm for data security and privacy in cloud Storage. They proposed a method that improved on classical encryption technique by integrating substitution cipher and transposition cipher which both uses alphabet for cipher text. Since the user has no control over the data after his session is logged out, the encryption key acts as the primary authentication for the user.

Endalew, 2016, proposed a framework of communication between applications within a payment card system with the integrated security component. The security component contains a combined algorithm (AES, RSA and SHA2) that ensure data confidentiality and integrity at the time of data transfer into the cloud and a selected access control technique which is applied to the databases and library files of a banking sector. In his approach, the cloud environment for the payment card system was simulated using cloud simulator. His

approach provided a stronger security through confidentiality and integrity with respect to card payment system for the banking industries.

Frame work of proposed system

The enhanced security framework is made up of a realistic Federated cloud with an RSA Security Crypto system that can take advantage of a technique of data compliance and encryption in cloud computing. The Cryptosystem make use of RSA algorithm to protect any form of malicious attempt by intruders. These cloud system security model uses RSA Algorithm with a federated cloud computation practice as a technique to preference active securities.

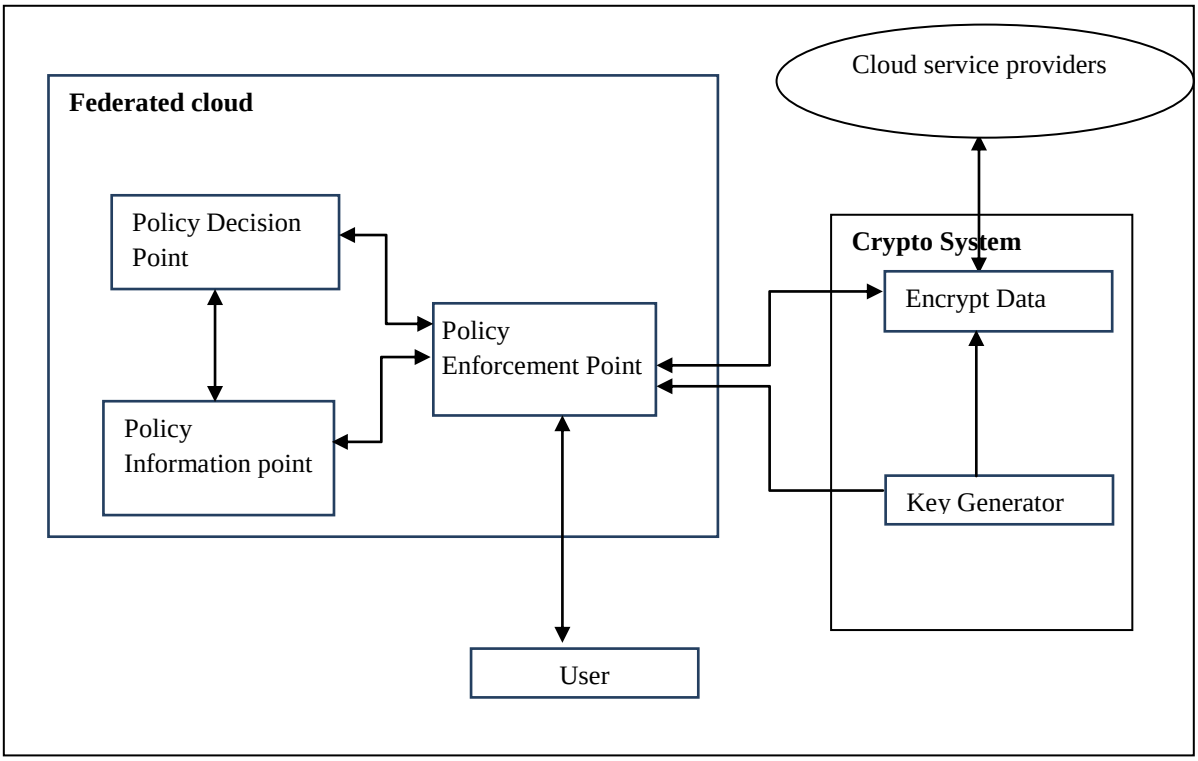


Fig. 1.0: Proposed framework.

User

The user/client is the person who chooses to make use of the cloud services. The client must first create an account with the system before performing any operation.

Policy enforcement point

At this point, all attempts to retrieve, store, or delete data from a cloud storage is been intercepted and further sent/retrieve the data from the crypto system after a series of operations.

Policy decision point

Based on some deployed policies (Spatial, Temporal, Qualitative requirement), the Policy Decision Point decides on execution and modification, by potentially querying the Policy Information Point, which implements a data flow model (virtual distribution of data), for additional context information.

Policy information point

This point implements a data flow model and updates internal state according to the modeled semantics of the intercepted event.

Crypto system

One of the distinguishing techniques employed in public key cryptography is the use of asymmetric keys. In this scheme, one key (public key) is used to encrypt the message while a different key (private key) is used to decrypt it. The keys are related mathematically, but the parameters are chosen so that calculating the private key from the public is either impossible of prohibitively expensive.

The Cloud Service Providers

This are organizations that provides an information technology (IT) paradigm to users, which enables ubiquitous access to shared pools of configurable system_resources and higher-level services that can be rapidly provisioned with minimal management effort, often over the Internet. These organizations include Amazon, Google, Oracle, Microsoft, Cisco, Verizon, Citrix, Ibm.

Computational steps for key generation in proposed system

The computational steps for key generation are;

Step 1: Generate two different primes p_i *and* q_i

Step 2: Generate an even constant$k$**,** such that

$$k < p_i \text{ and } k < q_i,$$

Step 3: Calculate

$$p = (p_i - k)$$

$$q = (q_i - k)$$

Step 4: Calculate the modulus

$$n = (p * q)$$

Step 5: Calculate the totient

$$\emptyset(n) = (p - 1) * (q - 1)$$

Step 6: Select for public exponent an integer e such that

$$1 < e < \emptyset(n) \; and \; gcd(\emptyset(n), e) = 1$$

Step 7: Calculate for the private exponent a value for d such that

$$d = e^{-1} \; mod \; \emptyset(n)$$

Step 8: Public Key $= [e, n]$

Step 9: Private Key $= [d, n]$

- n is known as the modulus.
- e is known as the public exponent or encryption exponent.
- d is known as the secret exponent or decryption exponent

Explaining computational steps for key generation in proposed system

Step 1: Two given prime numbers are generated randomly between the ranges of 100-9000000 which are 602918 in number.

Step 2: An even constant is generated that is less than the two random prime numbers generated in step 1. We decided to choose and even numbers because we want to subtract the even number from each prime number generated and still have a prime number as a reminder.

Step 3: We subtract each the even number from each prime number; we now got p and q.

Step 4: The modulus is the multiplication between the two prime numbers from Step3 p and q.

Step 5: The totient is a function such that the two primes are subtracted by 1 for each respectively and then the result is then multiplied together.

Step 6: And integer e is selected such that it is greater than 1 and less than the totient value obtained from step5, and that integer must satisfy the condition that the greatest common divisor of the integer and the totient is equal to 1. This integer is known as the public exponent.

Step 7: We calculated d as the private exponent by taking the inverse of the integer e in step6 mod the value of our totient in step 5.

Step8: The public key is [e,n].

Step9: The private key is [d,n].

Performance Test

After the login session, the user uploads his/her data; this data is encrypted before been stored at the service provider by the system. The time interval between the upload and encryption is recorded, and the procedure is repeated with different sizes of data 250 times for each size of data and the corresponding time is recorded. Using Z test to know whether to either accept or reject a null hypotheses.

Let X_1, X_2, $X_3 \ldots X_n$ be the time interval.

The Average Time

$$\bar{x} = \sum_{i=1}^{n} \frac{x_i}{n}$$

The Standard Deviation

$$\sigma\bar{x} = \sqrt{\sum_{i=1}^{n} \frac{(x_i - \bar{x})^2}{(n-1)}}$$

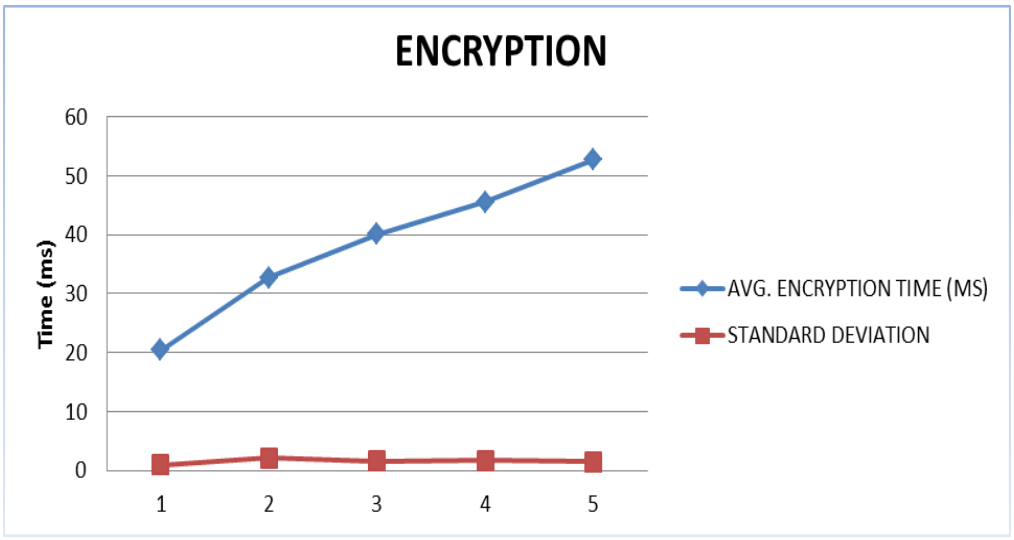
Performance of the proposed system

The table below shows a random set of data that was stored to the cloud using the enhanced data security framework simulated, the following Encryption/Decryption time where obtained after 250 times testing on each file size and the average Encryption/Decryption time are;

Table 1.0: Performance result obtained

File Name	Size (KB)	Avg. Encryption Time (MS)	Standard Deviation	Avg. Decryption Time (MS)	Standard Deviation
.txt	1	20.436	0.907126174	8.865	0.674002186
.txt	2	32.6715	2.079785604	9.86	0.668950474
.txt	3	40.056	1.56317964	12.801	0.863724493
.txt	4	45.5545	1.644529928	14.0315	0.812677673
.txt	5	52.74	1.450335714	17.3915	0.737187222

The table shows that as the size of data increases the corresponding time of encryption increases. This is illustrated below using a chart.



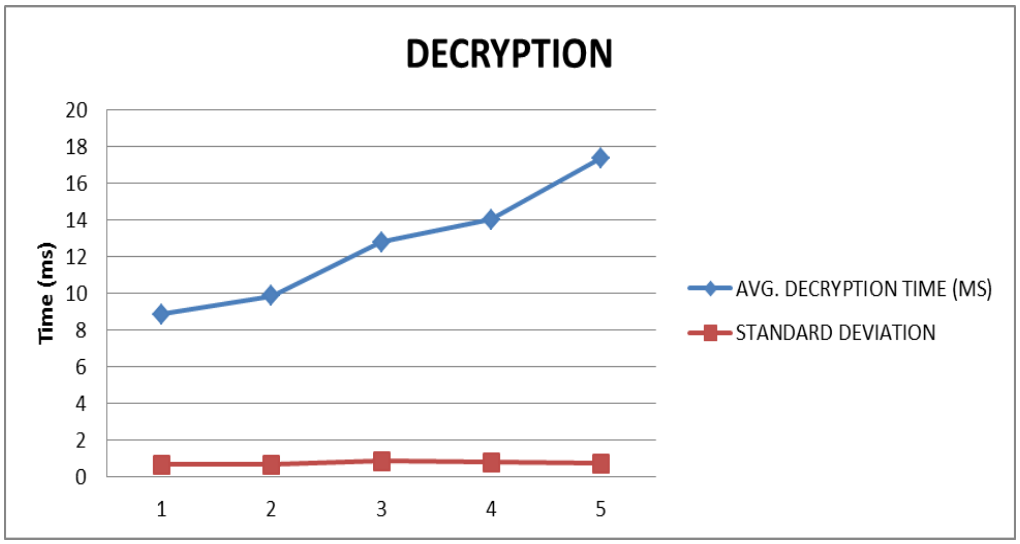


Fig. 1.2 & 1.3: Chart Illustration.

Complexity of proposed algorithm

Time Complexity: Time complexity is usually computed by counting the total operations performed by system where each operation takes a fixed amount of time. An algorithm performance time may vary with respect to the size of the input, in this case computed the time complexity by varying the length in bits of the key and finding the required execution time. A summary of the different sizes of key length and their execution time is given in milliseconds as shown below.

Table 1.1: Time Complexity of RSA algorithm.

Private Key Length (Bit)	Time Complexity (ms)
64	86.00
128	91.33
256	110.33
512	142.64
1024	363.67
2048	2748.67

Space Complexity: Apart from Time complexity, space complexity is also an important metric of evaluating the performance of an algorithm. It is the amount of memory which the algorithm needs for performing its computations. The way in which the amount of storage space required by an algorithm varies with the size of the problem it is solving. We analyzed the space complexity between key length and run time memory consumed by the system. The key length varies with respect to the prime numbers generated and the even constant.

Table 1.2: Space Complexity of RSA algorithm.

Private Key Length (Bit)	Space Complexity (ms)
64	86.00
128	91.33
256	110.33
512	142.64
1024	363.67
2048	2748.67

CONCLUSION

The need for a more secured security framework should not be neglected as this system was particularly designed to advance the form of security lapses encountered while using other existing security methods to keep data safety in the cloud. The problem was best handled by the newly introduced framework as it is fast in encrypting/decrypting of information as well as exhibit high reliability in terms of security. Also is its swift in retrieving and storing data

and also utilizes the cloud, which aids data/information integrity and safety, as it is not prone to misplacement or disaster.

Hence the Enhanced security framework has improved the standard of cloud data security as well as given users the opportunity to embrace the use of the cloud to store their information with no doubt or fear of compromise.

REFERENCES

1. Endalew, E., "Cloud Data Security Framework for Payment Card System: the case of Ethiopia", *Thesis Submitted to the Department of Computer Science in Partial Fulfillment for the Degree of Master of Science in Computer Science Addis Ababa, Ethiopia*, 2016.
2. Manisha R. Shinde & Rahul D. Taur, "Encryption Algorithm for Data Security and Privacy in Cloud Storage", *American Journal of Computer Science and Engineering Survey, AJCSES,* 2015; 3(1): 034-039.
3. Peter Mell, & Tim Grance, "The NIST Definition of Cloud Computing", 2011; [online], Available: http://www.wheresmyserver.co.nz/storage/media/faq-files/cloud-def-v15.pdf.
4. Venkata, S. & Shivashanker, R., "Security Techniques for Protecting Data in Cloud Computing", *School of computing, BlekingeInstitute of Technology Swenden*, 2011; 36-38.
5. Wood, K. & Pereira, E., "An investigation into Cloud Configuration and Security", *International Conference for Internet Technology and Secured Transaction*, 2010; 1-6.
6. Wuchner, T., Muller, S., & Fischer, R., "Compliance-preserving Cloud Storage Federationbased on Data-driven Usage Control", *Karlsruhe Institute of Technology, Germany*, 2013.
7. Yuhong Liu, Yan Lindsay Sun, Athanasios V. Vasilakos, JungwooRyoo and Syed Rizvi, "A Survey of Security and Privacy Challenges in Cloud Computing: Solutions and Future Directions", *Journal of Computing Science and Engineering JCSE*, 2015; 9(3): 119-133.