IJSGS

ISSN: 2488-9229
FEDERAL UNIVERSITY
GUSAU-NIGERIA

INTERNATIONAL JOURNAL OF SCIENCE FOR GLOBAL SUSTAINABILITY

Experimental Performance Evaluation Of Encryption Algorithms For Securing User Data In Cloud Computing

Jamilu Usman Waziri
MIS/ICT Department, Federal University Gusau, P.M.B 1001, Zamfara State, Nigeria

Corresponding Author's Email & Phone No.: jamiluwaziri@fugusau.edu.ng, +2348060054074

Received on: October, 2020 **Revised and Accepted on:** November, 2020 **Published on:** December, 2020

ABSTRACT

As cloud computing is a new area for research and development and also a utility where services can be remotely purchased and users can store their data in the cloud to enjoy on demand high quality applications and services from a shared pool of configurable computing resources available through which service providers offers customers management functionalities as well as the expensive hardware. Data privacy is the major security determinant and a factor that needs to be given more concern since un- trusted server is dangerous and unsafe for the users. Therefore, this research work gives concern to the security elements in cloud environment and suggests techniques to mitigate the security issues of the cloud by providing flexible access through encryption using the RSA, DES, AES and Blowfish algorithms.

Keywords: Cryptography, Cloud Computing, Data Security, Privacy, Encryption.

1.0 INTRODUCTION

Cloud computing is the ability to access a pool of computing resources owned and maintained by a third party via the internet. It is not a new technology but a way of delivering computing resources based on long existing technologies such as server virtualization. Cloud computing usually involves the transfer, storage, and processing of information on the providers infrastructure, which is not included in the customers control policy. However, Parashar and Arora (2013) described the "cloud" as a composition of hardware, storage, networks interfaces, and services that provide the means through which users can access the infrastructures, computing power, applications, and services on demand which are independent of locations. The concept cloud computing is linked closely with those of information as a service (IaaS), platform as a Service (PaaS), Software as a service (SaaS) all of which means a service-oriented architecture. As there is no need to store data at users end because it is already at some other location. So instead of buying the whole infrastructure required to run the processes and save bulk of data which you are just renting the assets according to your requirements. Also, Hossain *et al.* (2016) discuss Cloud Computing as a set of IT Services such as network, storage, hardware, software, resources and these services are provided to a customer over a network. Benefits of cloud storage are easy access means access to your knowledge anyplace, anytime, anyhow, availability, cost efficiency, and high reliability of the data. For these benefits, each and every organization is transferring its data to the cloud. For this reason, there is a need to protect that data against unauthorized access, alteration or interchanging. Security is considered as one of the most critical feature for cloud computing due to sensitively and importance of data stored on the cloud.

The similar idea behind all cloud networks discussed by Ayushi (2012) which uses remote services through a network using various resources. It is basically meant to give maximum with the minimum resources i.e. the user end is having the minimum hardware requirement but is using the maximum capability of computing. This is possible only through this technology which requires and utilizes its resources in the best way. The advantage of cloud computing over traditional computing include: agility, lower entry cost, device independence, location independence and

scalability by Sahu and Kushwaha (2014). In order to solve the problem of data integrity checking, many schemes are proposed under different systems and security models.

Cloud computing is a form of information technology which is being used where lesser investment in efficient software is needed. Cloud computing consists of Access to applications and services is enabled over the network and it also require only access to internet connection. Possibly one can get access of the cloud with the use of an ordinary client simply anywhere and anytime and one needs a certain information facility, without any special software. Cloud computing also facilitates the clients for immediate access to pre-set common but valuable information resources (as access to the network, hardware, storage capacities, software, and special information services) that are eagerly available without a wide agreement making process. In all these works great efforts are made to design solutions that meet various requirements, high scheme efficiency, stateless verification, unbounded use of queries etc. Considering the role of the verifier in the model all the schemes presented before fall into two categories: private auditability and public auditability. Although schemes with private auditability can achieve higher schemes efficiency, public auditability allows anyone not just the client (data owner), to challenge the cloud server for correctness of data storage while keeping no private information.
Cloud computing is the outsourcing of IT communications by the use of the internet and maintaining own hardware and software environment. Cloud computing facilitates computing assets (processor compute time and data storage on demand by the use of a service provider. Comparisons of cloud services are made by their nature and utilize services such as gas or electricity. It is there whenever you need it, as much as you need, and you pay as you go and only for what you use. Now a day's security of data has become a big distress. High levels of data repositioning have off-putting implications for data security and data shield as well as data availability Rani and Gangal (2012). Thus the main worry regarding security of data residing in the cloud is how to make sure the security of data which is at rest. Although, consumers know the dimensions and location of web data high in no data mobility, you can find questions associated with its security of the USB ports. To be sure the cloud computing areas happens to be larger to its broad network access. But reliability regarding a secure and secure environment to the personal data and info on the user is still required.

1.4 Statement of the Problem

With the cloud, physical security is lost because of sharing computing resources with other companies therefore concerns arise when it is not clear to individuals why their personal information is requested or how it will be used or passed on to other parties. Therefore, no knowledge or control of where the resources run and also ensuring the integrity of the data transfer, Storage, and retrieval. That is why some standards encryption algorithms where proposed to ensure data security and integrity are ensured.

1.5 Scope and limitation of the Study

The research concentrates on data security of cloud computing using four encryption algorithms to eliminate the concerns regarding data loss, segregation and privacy while accessing applications on cloud and also a comparative study among them have been presented through the use of technology in the form of encryption and decryption. A limitation to these studies is the usage of an elaborated categorization scheme and also not providing well secured authentication technique, that is why We propose that further study in Cloud computing is required to understand why some of these requirements are least researched and also recommend some encryption algorithms that will be used as a one key symmetric authentication. They also said further study should follow another structure to describe Cloud Computing security requirements like we proposed in our research which might help in identifying requirements missed in their study.

1.6 Significance of the Study

The findings of this study will redound to the benefit of security algorithms considering that cryptography plays an important role in security algorithms of cloud computing. The greater demand for cloud services and its security justifies the need for more effective, life changing encryption approaches. Thus, cloud service providers that apply the recommended technique

derived from the results of this study will be able to solve several major issues and concerns, such as data security, trust, expectations, regulations and performance issues. This will uncover critical security areas in the cryptography processes that many researchers were not able to explore.

From these studies it can be clearly understood that there are no security standards defined, even after a few researchers trying to formulate them. It can also be understood that even though few organizations and researchers tried to formulate strategies to handle security issues in cloud, there are still many companies that are reluctant to join the group of Cloud Computing users. Their major concern is still security in cloud computing. This research tries to identify every possible challenge cloud faces and their solutions from literature, then pick the challenge that has no proper practices and proposed the encryption algorithms to mitigate the challenge. This study will help both organizations and academics to identify the extent of research. It also will help to identify a set of solutions and guidelines to harness the power of Cloud Computing securely. This study will also include benefits of using the encryption and Decryption algorithms techniques listed out, which can help organizations to choose a solution that fit their requirements.

1.7 Motivation

Many Researchers of Cloud storage security are giving more focus on how to make data more secure and giving less attention towards degradation of Cloud performance due to not selecting proper encryption algorithms because security is considered as one of the most critical aspects in everyday computing and it is not different for cloud computing due to sensitivity and importance of data stored on the cloud So, if users are paying awareness in selection of proper encryption technique then it can achieve confidentiality without losing performance of Cloud. Sahu and Kushwaha (2014) presented the best method or technique for achieving high performance and secured user data by selecting a proper modern symmetric encryption algorithm.

This research aimed at Evaluating encryption algorithms for securing user data in cloud computing.

Few scholars have worked on secure data in cloud computing using encryption algorithms and also the ones that shows experimental, characteristics and comparisons between those encryption algorithms were overviewed, some of the important considerations in Symmetric and asymmetric key algorithm, hybrid encryption and security architecture considered by the previous research are identified.

Data security in cloud computing is rising trust area in research work. It was concluded in Seth and Mishra (2014) that AES is faster and more efficient cryptographic algorithms. When the data transmission is considered there is insignificant difference in performance of different symmetric key schemes. While in Kaur and Bhardwaj (2012) concern were shown on security element in cloud computing and suggested a technique to enhance the security of cloud database. The techniques provides the flexible multilevel and hybrid security which uses RSA, Triple DES and Random Number Generation algorithms as an encryption tool. The encryption algorithm applicability provides the flexibility in range and sequence to the user's choice because from the three of the encryption methods a user can apply all or omit any in any order. So also Shete and Hipparkar (2013) proposed an encryption algorithm in order to make cloud data secured, vulnerable and gave major concern to security issues, challenges and performed comparison between AES, DES and RSA algorithms.

Jayant *et al.* (2015) shows the mathematical model for calculating the trust of the user, the model gives the uploading rights to the user when it is recommended by the Administrator, and when user exceeds the specified experience and trust threshold value the RSA and AES algorithm for encryption and decryption of data with role based access control model are used to provide access according to the role played by user. Shukla *et al.* (2012) discussed that in order to facilitate rapid deployment of cloud data storage service and regain security assurances with outsourced data dependability, efficient methods that enable on demand data correctness and verification on behalf of cloud data owners have been designed, this is to explore the possibilities to develop an effective audit and Authentication algorithms for cloud users

and also monitor their services. Parashar and Arora (2013) have also discussed about cloud computing security issues, mechanism and challenges that cloud service provider face during cloud engineering. The work presented the metaphoric study of various security algorithms and proposed encryption algorithms to make cloud data secure and vulnerable. More so, Archana and Sikri (2015) discussed cryptography as a techniques which ensures the secrecy and authentication of the information where an appropriate cryptographic algorithm needs to be selected and used based on security and performance attributes. Two asymmetric-key algorithms i.e. RSA and Elliptic-Curve Cryptography (ECC) were studied and a comparative analysis of both the algorithms was done on the basis of results obtained. The analysis showed that ECC takes less time for encryption and decryption and also provides key of smaller size as compared to RSA. Inukollu *et al.* (2014) comes up with some approaches in providing security system that can scale to handle a large number of sites and also be able to process large and massive amounts of data.

2.0 MATERIALS AND METHODS

Different security algorithms were proposed to eliminate the concerns regarding data loss, segregation and privacy while accessing web applications on cloud. Algorithms like: RSA, DES, AES, Blowfish have been used and comparative study among them have also been presented to ensure the security of data on cloud. DES, AES, Blowfish are symmetric key algorithms, in which a single key is used for both encryption and decryption of messages whereas DES was developed in early 1970s by IBM. Blowfish was designed by Bruce Schneier in 1993, expressly for use in performance constrained environments such as embedded system. AES was designed by NIST in 2001. RSA is a public key algorithm invented by Rivest, Shamir and Adleman in 1978 and also called as Asymmetric key Algorithm that uses different keys for encryption and decryption purposes. The key sizes of all the algorithms are different from each other. The key length of DES algorithm is 56 bits. The key size of AES algorithm is 128,192,256 bits. The key size of Blowfish algorithm is 128-448 bits. The key size of RSA algorithm is 1024 bits.

Therefore, in this experimental performance analysis of the given algorithms Netbeans IDE 8.2 and Java Run Time Environment was used to implement the idea in the form of encryption and decryption algorithms which have been discussed earlier, and also Microsoft excel was used to plot graphs considering line based and column based representation, this is to make comparison between them on the basis of their characteristics.

3.0 RESULTS

The proposed encryption algorithms are implemented using Netbeans 8.2 IDE with different key size for different data types and file size. The comparative experimental summary results are shown in table-1, AES, DES, BLOWFISH, and RSA are presented in to four factors which are Algorithms, Contributor, Key Length and Block Size. The key sizes of all the algorithms are different from each other. The key length of DES algorithm is 56 bits, AES algorithm is 128, 192, 256 bits, Blowfish algorithm is 128-448 bits while RSA algorithm is 1024 bits.

Table-1: Characteristics of Encryption Algorithms

Algorithm Scheme	Algorithm Type	Contributor	Key length	Block Size
AES	Symmetric	Rijindael	128,192,256	128bits
DES	Symmetric	IBM 75	56Bits	64bits
BLOWFISH	Symmetric	Bruce Schneier 93	128-448bits	64bits
RSA	Asymmetric	Rivest, Shamir, Adleman 77	1024bits	Minimum 512bits

Experimental result for encryption algorithm AES, BLOWFISH, DES, and RSA are shown in table-2 which has been implemented several input file sizes: 329 bytes, 778 bytes and 2048 bytes. The Key size of each algorithm that is used in this experiment is also mentioned in table-2. All the results are obtained with due care, for achieving higher accuracy, several samples of total execution time were taken then an average of the samples were taken for the measurement and comparative analysis among algorithms and for the graph plotting as well. Encryption and Decryption time

is calculated in millisecond and the input size is taken in kilobytes. All the respective observation readings and graph are shown for all the analyzed algorithms on single system.

Table-2: Performance Evaluation of Different Algorithms

S/No.	Algorithm	Key Size (Bit)	File Size(Kb)	Running Time(3 Rounds)	Encryption Time(Millisecond)	Decryption Time(Millisecond)
					287	293
1	AES	256	329	11	299	304
			778	13	300	297
			2048	14	293	290
2	DES	56	329	15	284	317
			778	17	292	286
			2048	18	303	280
					282	292
3	RSA	1024	329	17	541	499
			778	19	488	491
			2048	14	450	485
					491	450
5	BLOWFISH	128	329	13	287	278
			778	15	283	279
			2048	14	284	280
					292	282

Figure- 1 and 2 represent the encryption time on line and column based while Figure-3 and 4 also show the decryption time line and column based respectively both of the symmetric algorithms (AES, BLOWFISH, and DES) and the asymmetric algorithm (RSA). Generally, from the below figures we can see that the symmetric encryption/decryption techniques are faster than the asymmetric encryption/decryption techniques. Moreover, all algorithms in both categories (symmetric and asymmetric) enjoy the proportion relation between the running time and input file size, except the DES and RSA algorithms. The DES and RSA running time changes slightly with input file size increase. By analyzing Figure-10 the key size and time taken by RSA algorithm for both encryption and decryption process is much higher compare to key size and the time taken by AES, BLOWFISH, and DES algorithms

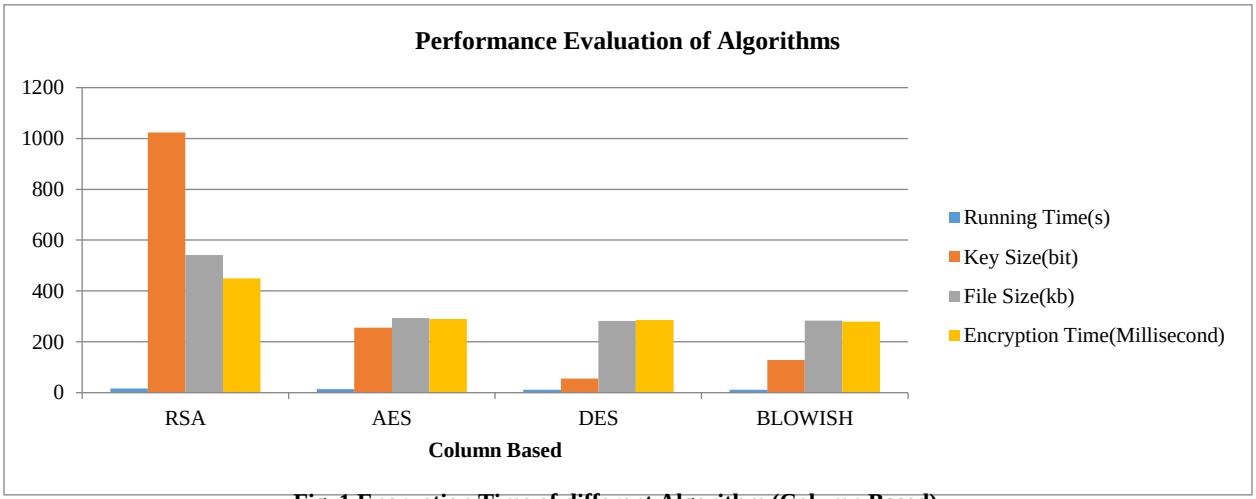

Fig. 1 Encryption Time of different Algorithm (Column Based)

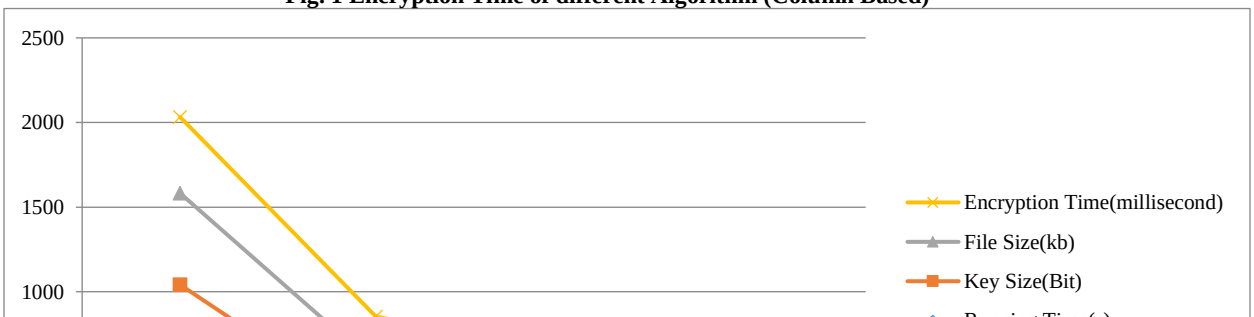

Fig. 2 Encryption Time of different Algorithm (Line Based)

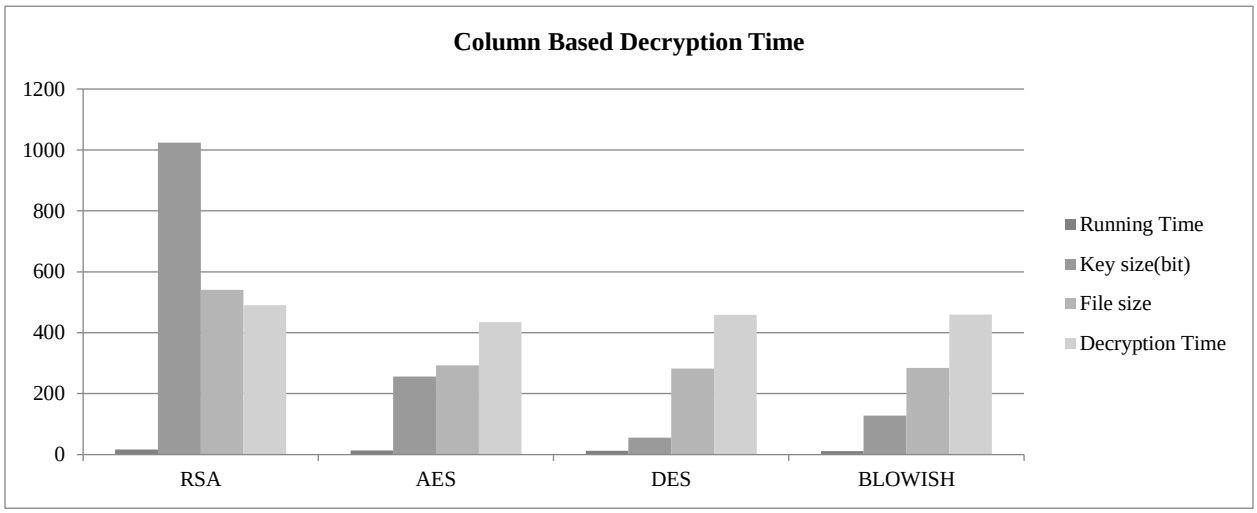

Fig. 3 Decryption Time of Different Algorithm (Column Based)

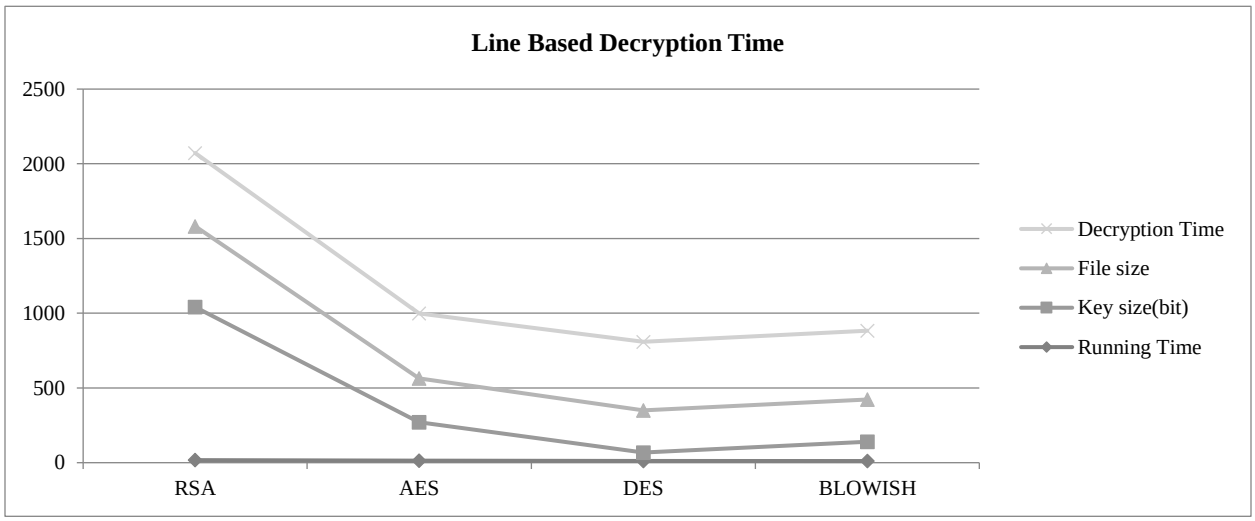

Fig. 4 Decryption Time of Different Algorithm (Line Based)

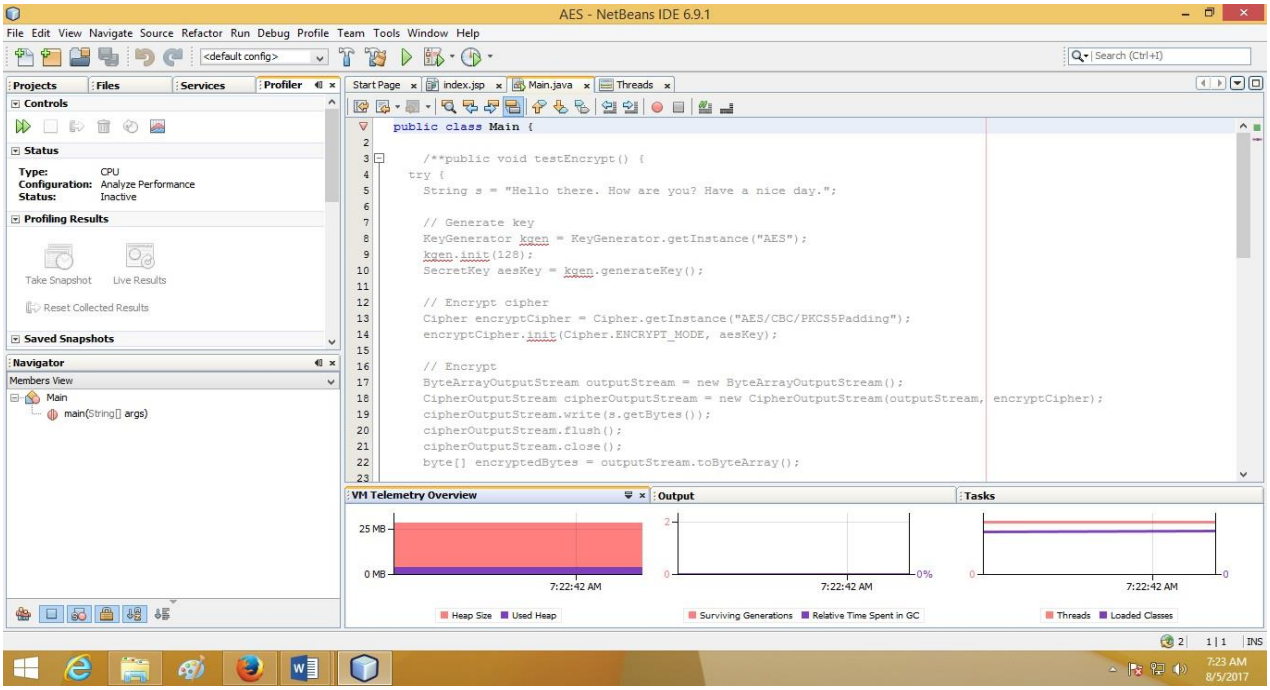

Fig. 5 CPU Utilization of Encryption Algorithms

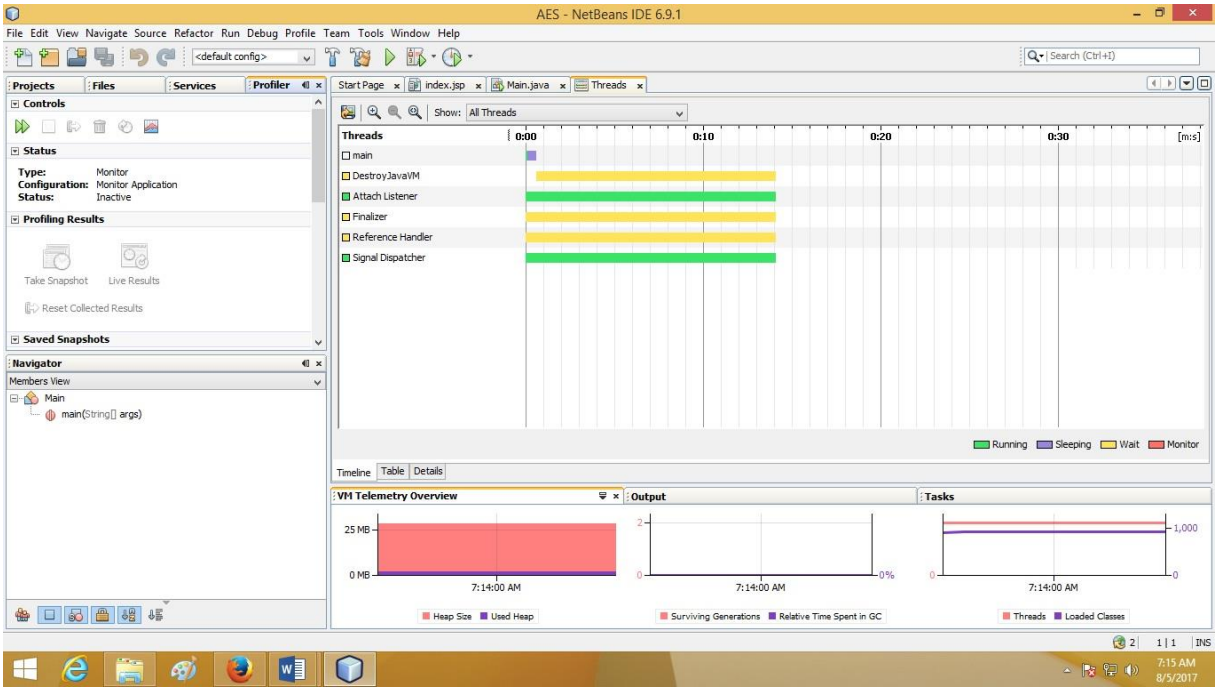

Fig. 6 Memory Utilization of Encryption Algorithms

4.0 DISCUSSION OF RESULTS

By implementing all the algorithms the desired output for the data on cloud computing has been achieved because the encryption algorithms play an important role in data security on cloud and by comparison of different parameters such as Key size, Scalability and Initial Vector size, Memory Usage, the platform it operate on, which shows some variation continuously. It has been found that AES algorithm uses least time to execute cloud data. DES algorithm consumes least encryption time. RSA consumes longest key and memory size and encryption time while blowfish secure both providers and user/client side and has less execution time.

In today's era demand of cloud is increasing so the security of the cloud and user is on top concern. Hence, proposed algorithms are helpful for today's requirement. In future several comparisons with different approaches and results show effectiveness of proposed implementation can be provided.

When migration of data to the chosen CSP (Cloud Service Provider) happens and in future whenever an application uploads any data on cloud, the data will first be encrypted using any of the algorithms and then the admin sent an email containing the encrypted key to the user who is demanding the stored data from the cloud. Data can be access in the cloud and the user can perform any request to read the data after it is decrypted on the users end. This encryption solution is transparent to the application and can be integrated quickly and easily without any changes to the application. This encryption protects data and keys and guarantees that they remain under users control and will never be exposed in storage or in transit.

5.0 CONCLUSION

Encryption algorithm keeps very important contribution in cloud computing security. This research work showed the performance of widely used encryption techniques like AES, DES and RSA algorithms. Based on the text files used and the experimental result, it was seen that AES algorithm consumes least encryption and RSA consume longest encryption time. We also showed that decryption of AES algorithm is better than other algorithms. From the analytical result, we can say that AES algorithm is much better than DES and RSA algorithm. In future, image and audio data as input next we will compared and analysed existing cryptographic algorithm like AES, DES and RSA and focus will be to improve encryption time and decryption time. In this way we can conclude that encryption algorithms are the best techniques that enhance security in cloud computing.

6.0 RECOMMENDATION

In today's world the internet is used for the secure communication on cloud. Therefore, strong algorithms are required to provide the security to the data it is recommended to take an option from cloud encryption security because data owners have more concern about sensitivity of the data and performance required for the chosen encryption algorithm, therefore based on the evaluation performed on these algorithms one can decide to use the highest performed technique as the best algorithm for use.

REFERENCES

Ahmed, E. A. & Sa'eed, R. A. (2014). A Survey of Big Data Cloud Computing Security. International Journal of Computer Science and Software Engineering. 3(4), 2409-4285.

Archana, K. & Sikri, V. (2015). Comparative Analysis of RSA and ECC. International Journal of Innovative Research in Computer and Communication Engineering. 3(7), 2320-9801.

AlMorsy, M., Grundy, J. & Muller, I. (2010). An analysis of the cloud computing security problem on the Asia Pacific Cloud Workshop, Collocated with APSEC2010, Australia, 42 – 69.

Ayushi D. (2012), A Symmetric Key Cryptographic Algorithm. International Journal of Computer Applications.

Elminaam, D. S., Kader, H. M. & Hadhoud, M. M. (2010). Evaluating the performance of symmetric encryption algorithms. International Journal of Network Security. 10(3) 216-222.

Himani, H. & Monisha, S. (2010). Implementation and analysis of various symmetric cryptosystems. Indian Journal of Sceince and Technology. 3(1), 0974 – 6846.

Hossain, M. A., Hossain, M. B., Uddin, M. S. & Imtiaz, M. S. (2016). Performance Analysis of Different Cryptography Algorithms. International Journal of Advanced Research in Computer Science and Software Engineering. 6(3), 2277-128X.

Inukollu, V. N., Arsi, S. & Ravuri, S. R. (2014). Security Issues Associated with Big Data in Cloud Computing. International Journal of Network Security & Its Applications.3,

Jayant, D. B., Swapnaja, U. A., Subhash, P.V. & Kailash, K. J. (2015). Developing Secure Cloud Storage System by Applying AES and RSA Cryptography Algorithms with Role based Access Control Model. International Journal of Computer Applications.118 (12), 0975-8887.

Kaur, A. & Bhardwaj, M. (2012). Hybrid Encryption for Cloud Database Security. International Journal of Engineering Science and Advanced Technology. 2(3), 737-741.

Kumar, P., Suthar, K., Gupta, H. & Patel, H. (2012). Analytical Comparison of Symmetric Encryption and Encoding Techniques for Cloud Environment. International Journal of Computer Applications. 60(19) 0975 – 8887.

Manisha, B. Sarbjeet, S. & Makhan, S. (2011). Implementation of Single Sign on and Delegation Mechanisms for Alchemi.NET Based Grid Computing Framework. International Journal of Information Technology and Knowledge Management. 4, 289-292.

Monika, A. (2012), A Comparative Survey on Symmetric Key Encryption Techniques. International Journal on Computer Science and Engineering 4(5).

Nadeem, A. (2006), A Performance Comparison of data Encryption Algorithms. IEEE Information and Communication Technologies.

Nidhi, S. & Raina, J. (2011). Comparative Analysis of AES and RC4 Algorithms for Better Utilization. International Journal of Computer Trends and Technology. Pp. 177. 181, (2319-7242).

Patill, A. & Goudar, R. (2013). Sensitive Data Storage in Wireless Device Using AES Algorithm. International Journal of Engineering and Computer Science. 2 (2231-2180).

Penchalaiah, N & Seshadri R. (2010). Effective comparison and Evaluation of DES and Rijindael Algorithm (AES). International Journal of computer Science and Engineering. 2 1641-1645

Parashar, A. & Arora, R. (2013). Secure User Data in Cloud Computing Using Encryption Algorithms. International Journal of Engineering Research and Applications. 3(4), 1922-1926.

Rani, S. & Gangal, A. (2012). Cloud Security with Encryption using Hybrid Algorithm and Secured Endpoints.International Journal of Computer Science and Information T echnologies. 3(3), 4302 – 4304.

Rachana, S. C. & Guruprasad, H. S. (2014) Emerging Security Issues and Challenges in Cloud Computing. International Journal of Engineering Science and Innovative Technology, 3.

Sahu, S. K. & Kushwaha, A. (2014). Performance Analysis of Symmetric Encryption Algorithms for Mobile ad hoc Network. International Journal of Emerging Technology and Advanced Engineering. 4. 2250-2459.

Schneier, B. (1996), Applied Cryptography Wiley & Sons, p. 399.

Seth, K & Mishra, S. (2011). Performance Analysis of Symmetric key cryptography algorithms: DES AES and BLOWFISH. International Journal of Engineering science. 4, 28-37.

Shukla, K., Trivedi, H. & Shah, P. (2012). Architecture for Securing Virtual Instances in Cloud. International Journal of Computer Science and Information Technologies. 3(3), 4279-4282.

Shete, M. M. & Hipparkar, P. D. (2013) Data Secure in Cloud Computing Using Encryption Algorithms. International Journal of Science and Research. 2319-7064.

Shashi, M. S. & Rajan, M. (2011) Comparative Analysis of Encryption Algorithms for Data Communication. International Journal of Computer Science and Technology. 2.

Singh, S. P. & Raman, M. (2011) Comparison of Data Encryption Algorithms. International Journal of computer Science and Communication. 2(1), 125-127.

Subashini, K. & Srivaishnavi, K. (2015) Big Data on Cloud Computing- Security Issues International Journal of Innovative Research in Science, Engineering and Technology. 4.

TanzimKhorshed, M., Almutairi, A. Sarfraz, M., Basalamah, S., Aref, W. & Ghafoor, A. (2015). Distributed Access Control Architecture for Cloud Computing Software. 44 -51.

Tamimi, A. Al (2008). Performance Analysis of data Encryption Algorithms. IEEE