INTERNATIONAL JOUNAL OF: SCIENCE RESEARCH AND TECHNOLOGY

TIMBOU-AFRICA ACADEMIC PUBLICATIONS
INTERNATIONAL JOURNAL, MAY, 2021 EDITIONS
VOL. 5 NO. 9 ISSN: 2623-7861

CLOUD-BASED DATA MANAGEMENT SECURITY MODELS

***SHEHU ABDULWAHAB; **KABIRU IBRAHIM MUSA (PhD); & ***AHMADU MAIDORAWA**

**Department of Information Technology, Modibbo Adama University of Technology, Yola, Nigeria. **Department of Management and Information Technology, Abubakar Tafawa Balewa University Bauchi, Nigeria. ***Department of Computer Science, Federal Polytechnic Bauchi, Nigeria*

ABSTRACT

The advents of Computing have led to the evolutions of large data. However, the availability of these large data can no longer be effectively stored and analyzed with traditional data management techniques. This brought about the emergence of Cloud Based computing that are used to process large-scale data management tasks efficiently with least cost. Despite this

INTRODUCTION

Cloud Computing (CC), as an emerging technology of the next generation of computing has become extremely popular and has received significant interest from big data users. Cloud Computing evolved from other technologies like distributed computing, grid computing, virtualization, etc., and supports the theme of one application and many users. This was brought about due to rapid development of processing and storage intensive technologies. And with the success of the Internet, computing resources have become cheaper, more powerful and more ubiquitously available than ever before [1]. These resources: CPU and storage are provided as general utilities that can be leased and released by users through the Internet in an on-demand fashion. The emergence of cloud computing has made a tremendous impact on the Information Technology (IT) industry over the

past few years, where large companies such as Google, Amazon and Microsoft strive to provide more powerful, reliable and cost-efficient cloud platforms, such that sectors and industries seek to reshape their business models to gain benefit from this new paradigm. Indeed, cloud computing provides several compelling features that make it attractive to sectors, industries and Governments.

The main usage of cloud computing is data storage and computing [2].Governments, Industries and organizations are outsourcing their private and confidential data over the cloud which makes the Cloud users, and the data vulnerable to cyber threats [3] [4] [5]. The nature of cloud computing raises serious security issues regarding user Authentication, data/information Availability, integrity and confidentiality (AAIC), while transferring, storing and accessing the data from and to data centers with efficient performances issues [6] [7] [8].

development security and privacy are issues of concern. This Study explores a cloud based data Management security models that maintain both data and user privacy using File Encryption/Decryption using AES algorithm and Role based access control respectively. The study adopts a Model Design and Simulation-based approach using Java API 8.2 and CloudSim 3.0 respectively to implement the security components: where Response time, latency and throughput were determined. The experiment values reached demonstrates a fast performance Role based Access control and AES File Encryption technique. General analysis shows that the models exhibit highly secured approach for organizations to overcome large data management and computing benefits of cloud computing. Testing the performance of the framework with more complicated data, security threats, and bandwidth/memory were recommended for further studies.

Keywords: *Cloud Computing, Role-Based Access Control and Advanced Encryption Scheme (AES).*

Most of the prevailing Cloud security uses Cryptographic encryption schemes [9][6]. The schemes are tightly coupled to the host-based Internet architecture that requires users to interact with numerous servers for authentication, license acquisition and retrieval of the protected content [7]. However, Organizations across industries are seeking more effective ways to protect their data, infrastructure, people and reputations [10], in order to have full control of their own data [7][12], and restrict the Cloud providers/third party from sharing, updating, and querying a dataset [13].

In order to implement a system that optimizes the organizational security and privacy, the techniques needs to optimize speed and resistivity coupled with high level of performance [14] [15]. [9] Opines the need for a solution between user applications and database servers in the cloud initiated by the Organization to secure its Accessibility and data with guarantees they remain under Administrative control and are never exposed in storage or in transit.

It is in light of these challenges that this study proposes models, which envisaged a well-Managed and secured cloud based data computing with the capability to prevent some critical issues such as abuse of permissions, unauthorized access, loss of data and data modification in motion (AAIC).

CLOUD CONCEPT AND SECURITY ISSUES

Cloud Computing Defined

The concept of cloud computing emerged around 2006, and has been embraced by businesses and governments as a new way to deliver IT services over the Internet [16]. A number of computing experts, researchers and practitioners have attempted to define Clouds in different perspectives.[17] have argued that despite the numerous Cloud Computing definitions some writers have criticized the whole idea as just the rebranding of same old IT packaged in a new bottle and doubt if it is really new concept. The variability of technologies and these hypes around Cloud Computing further confused the concept [17] [18]. However the most accepted definition of cloud computing was according to the U.S National Institute of Standards and Technology

(NIST); Cloud Computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or cloud provider interaction [19].

Data Security Issues in the Cloud

Security emphases in the Cloud should be in two perspectives: from the User, the Cloud Service provider (CSP) or both the user and the CSP in order to describe the possible threats and shall be addressed based on the security requirements presented [20] [21].

***Confidentiality*:** This is where the Cloud system must assure that data is accessible only to authorized users and that all hosted data, information and knowledge will be kept undisclosed in all circumstances to third parties. Confidentiality loss occurs when data can be read or observed through third parties who are not authorized to access it [21].

Data Integrity: In the Cloud system data integrity must be ensured, so that data held in a system is a proper depiction of the data intended and that it has not been modified/tempered by unauthorized party (i.e. not lost or altered), either on transit or at rest by encryption and decryption techniques [21].

Availability: This ensures that cloud system and data processing resources are not made inaccessible or unavailable respectively by malicious action. It is the basic idea that when a user tries to access something, it should be available to be accessed at any given time [21].

Authentication: This is a process by which one entity verifies the identity of another entity and could be a person or program. A user is authenticated in the server when the correct login credentials are provided and, are not permitted to access private files or non-public files uploaded by other users. Users are segregated based on administrative rights in the cloud service for data management purpose [21].

Cloud Security Solution Schemes

The actual implementation of security goals needs some techniques. Two techniques are prevalent today: one is very general (cryptography) and one is specific (steganography) [20].

Cryptography protect data transmission over network and is a science of making data and messages secure and immune to attacks by converting the data to be sent (plaintext) into non-readable form (Cipher text) using encryption and then performing decryption which is reverting back to the original plaintext using a key system to keep the data secret, digitally sign documents, access control and so forth [22]. While steganography means, concealing the message itself by covering it with something else (e.g. pictures, video or in audio music).

Cryptography is categorized into three algorithms. These algorithms are Symmetric-key algorithms, Asymmetric-key algorithms, and Hashing [23].

-Symmetric Key Cryptography/Algorithms

Symmetric key cryptography sometimes also called a secret key cryptography or private key cryptography is the most important type of the encryption. Symmetric-key algorithms are those algorithms which use single same key for both encryption and decryption; hence the key is kept secret. The sender uses this key and an encryption algorithm to encrypt data and the receiver uses the same key with the corresponding decryption algorithm to decrypt the data. Some popular Symmetric-key algorithms used in cloud computing includes: Data Encryption Standard (DES), Triple-DES, and Advanced Encryption Standard (AES).

-Asymmetric Key Cryptography/Algorithms

In Asymmetric key or public-key cryptography, there are two keys involved for encryption and decryption: a private key and a public key. The Public key is used by the sender for encryption and the private key is used for decryption of data by the receiver. In cloud computing asymmetric-key algorithms are used to generate keys for encryption. The most common asymmetric-key algorithms for cloud are: RSA, IKE, and Diffie-Helman Key Exchange etc.

-Hashing Functions/Algorithm

A cryptographic hash function takes a message of arbitrary length and creates a message digest of fixed length. All cryptographic hash

functions need to create a fixed-size digest out of a variable-size message. Creating such a function is best accomplished using iteration. Instead of using a hash function with variable-size input, a function with fixed-size input is created and is used a necessary number of times. The fixed-size input function is referred to as a compression function. It compresses an *n*-bit string to create an *m*-bit string where *n* is normally greater than *m*. The scheme is referred to as an iterated cryptographic hash function. Examples include: MD5, and SHA etc.

Related Works, Models/Frameworks

A lot of researches were conducted on cloud security, and specific ones related to this study were studied. A research area that is related to this work is an integrated data intensive framework for managing sensor data uncertainty using cloud computing [24]. Where a comprehensive framework for managing continuously changing data objects(CCDOs) was studied, with insights into the spatiotemporal uncertainty problem and presents an original parallel-processing solution for efficiently managing the uncertainty using the map-reduce platform of cloud computing.

[25] Also proposed a data control access protecting cloud computing for controlled disclosure of personal data to third parties using a preeminent technology called Attribute-based Encryption (ABE) as a cryptographic primitive, which establishes the decryption ability on the basis of a user's attributes. [4] Proposed a new Role Based Encryption System with access control in the cloud dwelling on practical implementation with architecture description and analyze the results in terms of encryption and decryption time. Thus, others dwell on general cloud security, algorithms and frameworks approach [5] [7] [2]. Finally [26] have presented various security algorithms in cloud computing that aim to keep the authentication, privacy and reliability levels of data.

The works of these researchers have placed the fundamentals for more research to be conducted in the area.

Experimental Methodology

Design and Setup

The study used Simulation-based approach that allows the services/models to be tested in repeatable and controllable

environment. The design, running and observation of the simulation stages follow an iterative approach in order to ensure the appropriateness of the result.

In order to achieve the objectives of the study, all designs were implemented using Microsoft Visio and simulations were conducted using java program (Java API version 8.2) and Cloudsim (Version 3.0). Three sets of simulations were conducted: to assess the performance of Role based access control, AES algorithms and file transfer between authorized users in the Cloud to provide good quality service in terms of response time, encryption/decryption time, and file transfer latency of a given task. The aim of the first simulation is to see the impact of change on the response time on specified number of users, were the number of users were varied from 10 to 10000. The second simulation is aimed to see the impact of change on the AES encryption and decryption algorithm on specific file sizes, were the file sizes were varied from 5kb to 100000kb. The third simulation is aimed to determine the latency in sending the encrypted files by varying the file sizes with overall execution time of successful cloudlets using Time Shared Vm Scheduler.

Parameters and Performance Matrices

In order to evaluate the performance of Role based access control algorithm, the parameters to determine the performance are response time speed to number of users, and for the Encryption/Decryption the chosen factor here to determine the performance is the algorithm's speed to encrypt/decrypt data blocks of various sizes. To measure the file transfer latency, the execution time of file transferred and various encrypted/unencrypted data blocks were used.

The Performance Matrices for the simulation were *throughput* —the total amount of work done in a given time. *low latency*-the time between sending the encrypted file and receiving the file between authorized users, *response time* —the time between the start and the completion of an event— also referred to as *execution time*.[4][21].

PROPOSED MODELS

The proposed Models are designed to ensure user authentication, data confidentiality, integrity and availability.

Role based Access Control Model

In a role-based access control model, users are assigned roles, and roles are assigned access privileges to protected resources in the cloud. The model is shown in Figure 1 below.

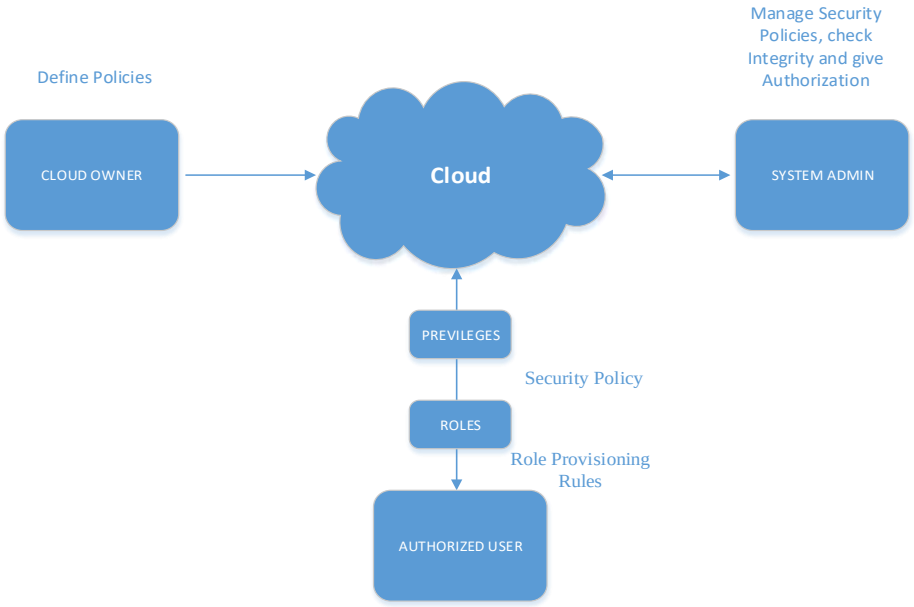

Figure 1: Role based Access Control Model

The System Admin is the core functionality that can perform all the tasks of data owner efficiently and will manage all security policies, check integrity and give authorization to users. The Admin is responsible for generating and computing parameters for the users. The Role is based on privileges and its provision rules define the position of a user in the role hierarchy. Admin is allowed to update parameters in the cloud if necessary. The User is the entities that upload/downloads data to and from the cloud upon successful authentication by the system admin. The Authorized user is then able to encrypt /decrypt that data with the help of a generated secret key. In this scheme, admin performs various tasks as the cloud owner only provides Storage and computation platform.

Data Encryption Flow Model

The authorized user is the user who has successfully been registered and has been assigned a role with the cloud system. After registering the user can access the cloud system by login to the cloud system to access the

services provided by the cloud based on the assigned task, hence can upload and download file on the system. While uploading the content of the file (plaintext) is encrypted using the AES algorithm and is saved on cloud system as Ciphertext. If the Administrative user /any co authorized user who is also registered with that cloud system wants to access/download the content of the file (Ciphertext) assigned to him can perform decryption to plaintext using the same key which is used for the encryption, so that the Data file remains secure both on transit and at rest. The model is shown in Figure 2 below.

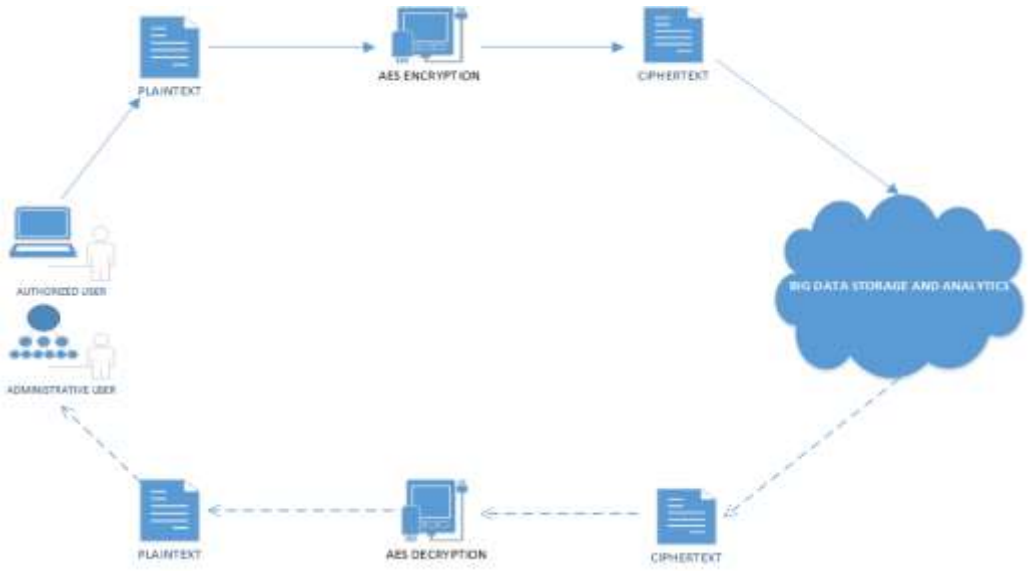

Figure 2: Data Encryption Flow Model

RESULTS AND DISCUSSION

The prototype has three parts. The first one is simulating an organizational Role Based Access Control algorithm that will be applied to the User When logged in, the second is encryption applied to data before transfer from user to cloud storage and decryption applied to data after download from cloud storage to the user through the simulation tools, and lastly the simulation of File transfer from users to the cloud server. Sample for both simulated components results were presented in tables and graphs, and discussed based on the corresponding results. The results were obtained from running the simulation programs several times in order to have relatively fair and accurate results. Response time for Access control,

encryption/decryption time for files, Latency for sending and receiving files were observed to determine throughput. The Throughputs were calculated to determine the speed and performance of the modified components.

Role Based Access Control Response time

The results presented in table I were obtained from running the simulation program and observing the response time against specified number of users as compared between an open accessed (no role based access control) and a closed accessed (with role based access control). Multiple numbers of users ranging from 10 to 10,000 have been used to determine the average Response time in seconds. The comparison between the open and closed accessed controls responds time are presented and plotted in figure 3.

Table 1: Role based Access Control Response Time

Number of Users	10	50	100	200	500	1000	2000	5000	10000	Average Time(s)
Closed Accessed (Seconds)	0.217	0.232	0.253	0.272	0.293	0.315	0.322	0.346	0.382	**0.286**
Open Accessed (Seconds)	0.391	0.418	0.455	0.489	0.528	0.567	0.579	0.633	0.688	**0.528**

TIJSRAT
ISSN: 2623-7861

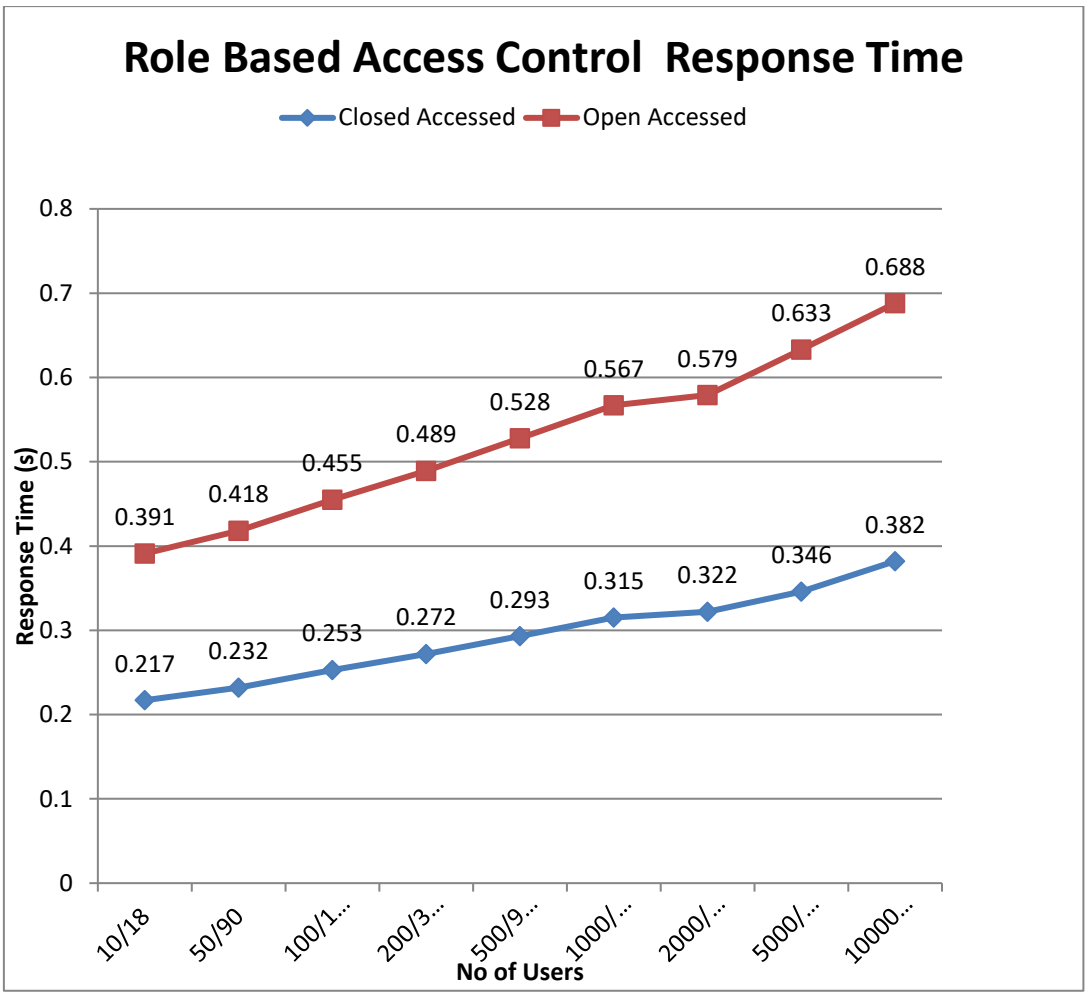

Figure 3: Role based Access Control Response Time

The above graph, shows the performance of Role based access control, where the closed accessed have lower response time due to specific and limited no of users that accessed the system. Unlike an open accessed system that requires higher response time due to its public access provision that drive the system to have growing demands of accessibility, searches, internal and external attacks on the need to get more information. The closed accessed system is compared using Symantec Internet Security Threat Report, (2017 P. 33) which states that "*organizations experience some form of web attack in every seven minutes and the level of the attacks are increasing exponentially almost daily*". Meanwhile service performance is characterized by the response time speed, availability, and security [14]. As seen above the average open

accessed response time (0.528s) is higher than the Closed Accessed Response Time (0.286s) and these results to lower speed, and degrade the performance of the server applications caused by unauthorized use of resources, space, bandwidth and network connections instigated by the public users.

Performance Results of Encryption

The results presented in table 2 were obtained from running the simulation program and observing the average Encryption time of AES and DES. Multiple Text files of different size (5kb to 100,000kb) have been used to determine the encryption time. The time is in seconds while File loads are in Kilobytes and the results shows the impact of varying the data file sizes on the encryption as compared with DES encryption scheme of [27]. The throughputs were calculated to determine the performance of AES Encryption algorithm in kb/s. The results were presented and plotted in figure 4.

Table 2: Performance Result for Encryption

S/N	File Input Size (Kb)	Encryption Time (S)	
		Advance Encryption Standard(AES)	**Data Encryption Standard (DES)**
1	5	0.75	0.79
2	10	0.76	0.82
3	50	0.80	0.94
4	100	0.81	1.06
5	200	0.84	1.25
6	500	0.93	1.87
7	1,000	1.03	5.98
8	2,000	1.29	9.70
9	5,000	2.33	18.70
10	10,000	3.19	37.40
11	20,000	5.16	74.80
12	50,000	11.88	187.00
13	100,000	23.94	374.00

Total	**188,865**	**53.71**	**714.31**
	Throughput(Kb/S)	**3516.82**	**264.40**

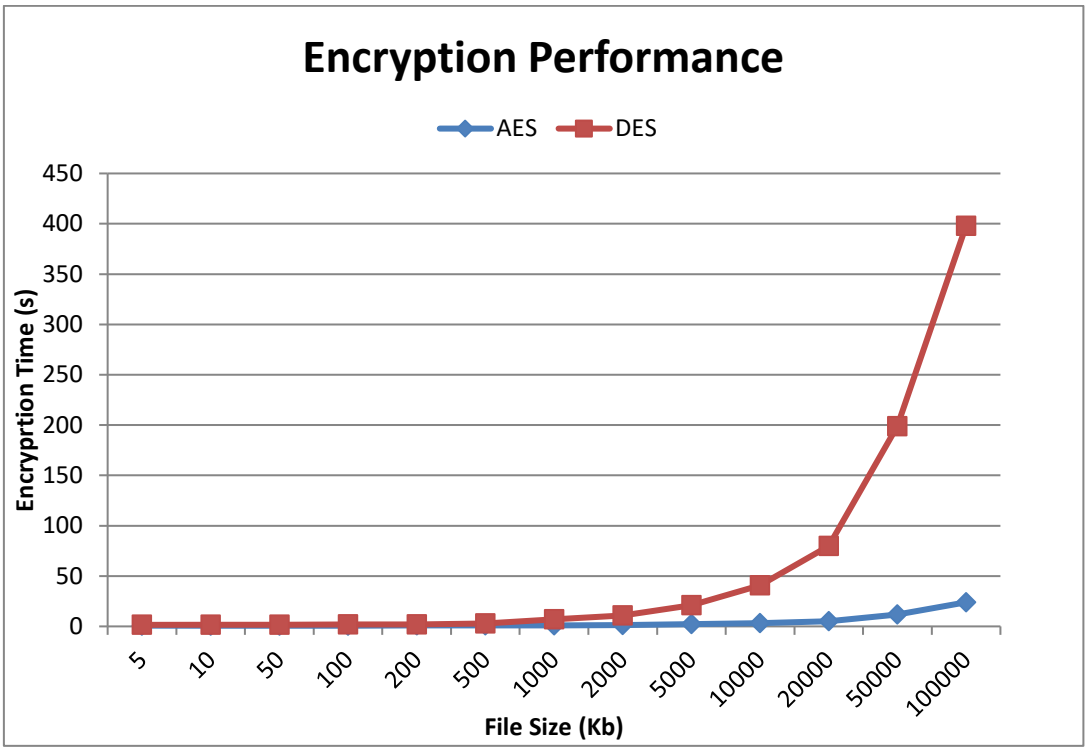

Figure 4: Encryption Performance

As seen from the above result the encryption time of both algorithms increases as the file size increases. The AES encryption incurs a minimum time as compared to the DES encryption time, and the throughput values of 3516.82kb/s(AES) and 264.40kb/s(DES) signifies AES encryption as a lightweight solution with high speed encryption throughput that enhance the system performance. Conclusively this signifies that there is a direct relationship between the encryption time and the size of the input file. Such that, the increase of the input file size (plainfile) led to slight increase of the encryption time, hence as the file becomes larger there is a significant larger increase in the encryption time.

Performance Results of Decryption

The results presented in table 3 were obtained from running the simulation program and observing the average decryption time of AES.

Multiple Text files of different size (5kb to 100,000kb) have been used to determine the decryption time. The time is in seconds while File loads are in Kilobytes and the results shows the impact of varying the data file sizes on the decryption as compared with DES scheme of [27]. The throughputs were calculated to determine the performance of AES Decryption algorithm in kb/sec. The results were further plotted in a figure 5.

Table 3: Performance Result for Decryption

S/N	File Input Size (Kb)	Decryption Time (S)	
		Advance Encryption Standard(AES)	**Data Encryption Standard (DES)**
1	5	0.67	0.79
2	10	0.67	0.82
3	50	0.67	0.94
4	100	0.69	1.06
5	200	0.72	1.25
6	500	0.84	1.87
7	1,000	0.92	5.98
8	2,000	1.19	9.70
9	5,000	1.19	18.70
10	10,000	3.19	37.40
11	20,000	5.88	74.80
12	50,000	12.33	187.00
13	100,000	24.52	374.00
Total	**188,865**	**54.28**	**714.31**
	Throughput(Kb/S)	**3479.76**	**264.40**

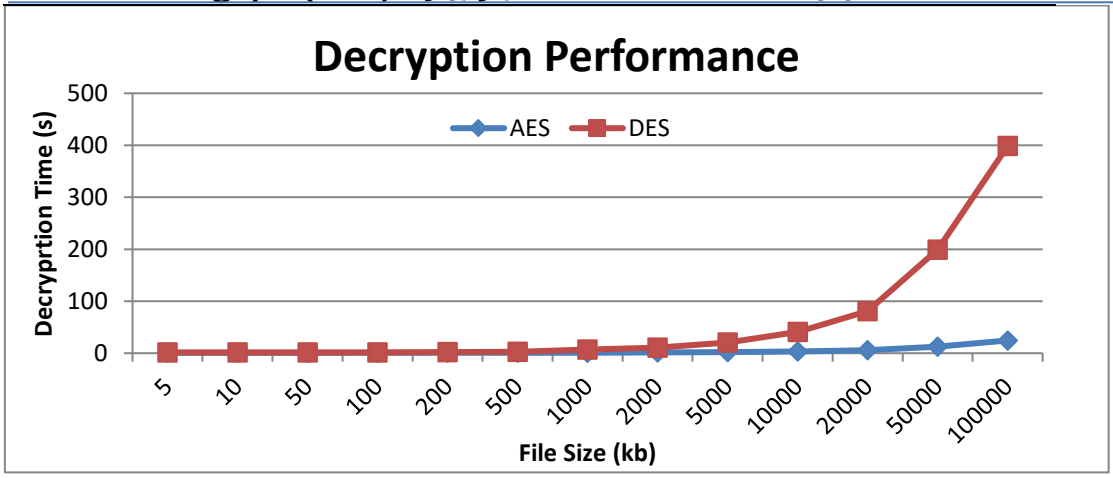

Figure 5: Decryption Performance

As seen from the above results the decryption time of both algorithms increases as the file size increases. The AES decryption incurs a minimum time as compared to the DES encryption time, and the throughput values 3479.76kb/s (AES) and 264.40kb/s (DES) signifies AES decryption as a lightweight solution with high speed decryption throughput that enhance the system performance. Conclusively this signifies that there is a direct relationship between the decryption time and the size of the input file. Such that, the increase of the output file size (cipherfile) led to slight increase of the decryption time, hence as the file becomes larger there is a significant larger increase in the decryption time.

File Transfer Latency

The results presented in table 4 were obtained from running the simulation program and observing the latency against specified number of files sent. The total time of uploading files were recorded in two cases for comparison where multiple encrypted and unencrypted files of sizes ranging from 5kb to 100000kb have been used to determine the average latency in seconds and are further plotted in figure 6.

Table 4: File Transfer Latency

S/N	File Input Size (Kb)	Average File Transfer Latency(seconds)	
		Encrypted File	**Unencrypted File**
1	5	0.015	0.015
2	10	0.016	0.016
3	50	0.016	0.016
4	100	0.016	0.016
5	200	0.016	0.016
6	500	0.021	0.021
7	1,000	0.032	0.032
8	2,000	0.032	0.032
9	5,000	0.042	0.042

10	10,000	0.078	0.078
11	20,000	0.187	0.187
12	50,000	0.682	0.682
13	100,000	1.344	1.344
Total	**188,865**	**2.31**	**2.31**
	Throughput(Kb/s)	**81759.74**	**81759.74**

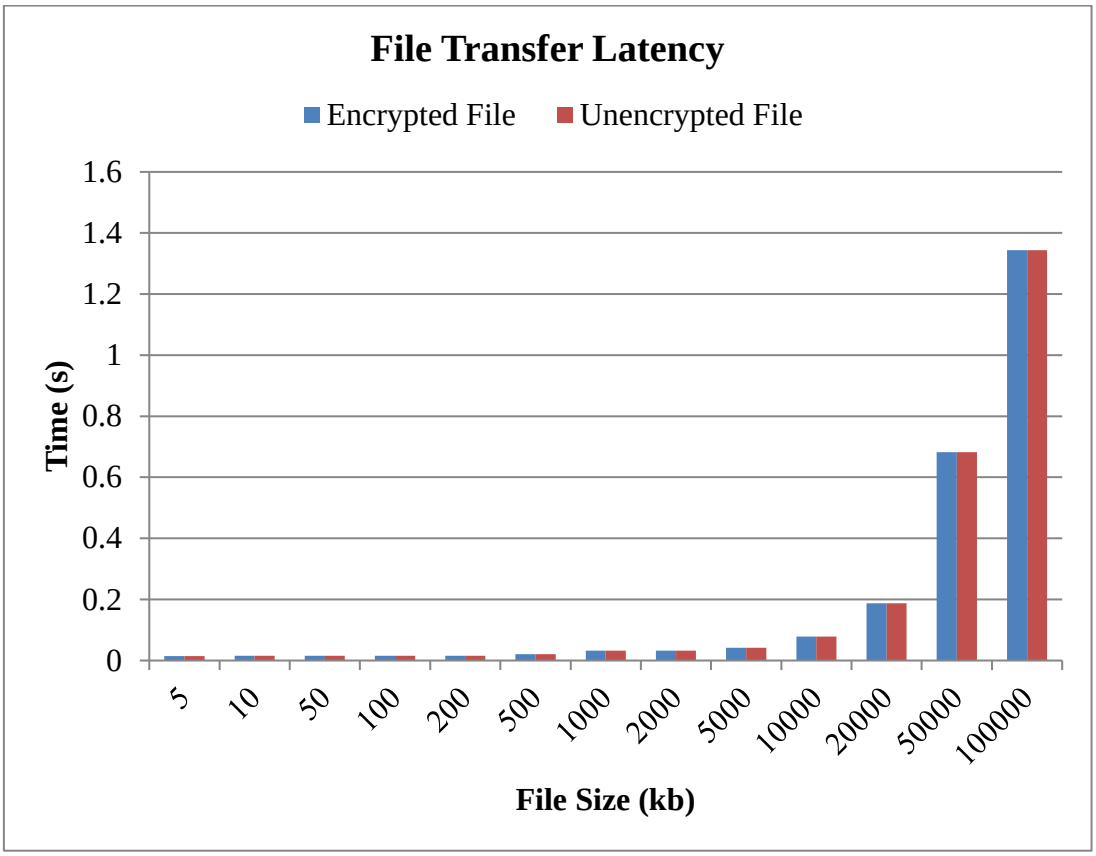

Figure 6: File Transfer Latency

The above graph shows a gradual increase in file transfer time as the size of file increases. It is observed that both encrypted and unencrypted file from 5kb to 100000 kb has the same transfer time. Thus, result to low latency signifying high speed and performance. The service performance is characterized by the low latency and security [14] while the impact of traffic load to system performance is measured by the uploading speed [3]. Both Conditions of low latency i.e. speed and security have been achieved by the encrypted file unlike the unencrypted file that have no

security with high vulnerability of breaching data confidentiality and integrity. Conclusively, the result shows that there is a reasonable direct relationship between the latency and size of file to a certain level, but as the file sizes tends to be larger, there is a constant average latency. Such that, the increase in file size led to increase in latency.

Throughput

There is need to determine the performance of the above parameters and this is done by calculating each parameter throughput. The Encryption time and decryption time are all used to calculate the throughput of an encryption scheme, and decryption scheme respectively. In a communication systems throughput is the rate of successful data transfer via an eventful communication channel, usually measured in bits per second/ packets per second. It indicates the speed of a scheme, calculated as the total plaintext in bytes encrypted divided by the encryption time high and the Higher the throughput higher is the efficiency of the system [6] [28]. Here the throughput of the algorithm is calculated by dividing the total data in bytes by encryption time in seconds. From Table 3 and 4, the throughput value of AES seems to be reasonably high signifying higher speed and performance. There is an inverse relationship between the throughput value and Speed/performance. Such that, the lower the time value the higher the speed of a scheme, thus optimized performance.

CONCLUSION

The key consideration dealt in this study is the provision of user control and encryption schema to secure data privacy by making it unintelligible for all except the authorized users. The presented simulation results of low latency and high throughput showed that the secured cloud Framework can be implemented for data management because it is relatively fast, reliable, scalable, secured and coupled with good performance. Implementing Role based and AES for security over user and data respectively provides benefits of insignificant computation time. The violation of security constitutes a risk of data loss, unauthorized modification, denial of service attack and also the level of

performance could weaken because of limited bandwidth, disk space, memory, and the CPU cycle and data transmission latency. The impact of the level of security by the cloud user (high-level security) led to raise in the level of performance of the cloud service, where the security level depends on external factors which includes security risks, confidentiality of data, and physical security (Access Control).

The main feature in this solution is that the security operations are performed at the organizational client side, and therefore the organization does not need to render all trust to cloud servers. The only elements that make it possible to access the stored data are based on roles and corresponding keys, and thus file sharing between users can only happen by exchanging keys managed by the organization. If an intruder (unauthorized user) tries to get the access data directly from the cloud, he must have to decrypt the data at each level which is a very difficult task. It may be expected that this will provide more security for Cloud Storage and computation than with no/single level encryption.

RECOMMENDATIONS

The application of lightweight user Authentication (Role based access control) and data security (AES encryption of data) proposed within the framework in data management, envisaged a more secured framework with high speed that enhanced cloud based data management computing. In order to achieve this, it should take into consideration the fact that cloud computing is still at a developing stage and continuously changing and may need to be enhanced in the future.

This will provide a good contribution to the area of big data security on the cloud. Thus there are still several issues regarding User and data security on the cloud computing environment that warrant further research in the future and integrated in the above framework for a better output. The following are the recommended future works:

I. Firstly is to expand the current benchmarks to further explore the performance of the Framework with other more complicated data types such as Audio and Video.
II. Testing with different security threats at the time of data transfer and on the stored data for a better endorsement.

III. Measuring the performance of the encryption solution through various parameters such as bandwidth and memory required.

IMPLICATIONS OF THE STUDY

The proposed models make data sharing more secured in accordance with any data Management policy (optimized data quality and security. The Study will contribute to the body of existing knowledge in the fields of Cloud computing as related to the use of user control (Role based access control) and data privacy (AES algorithm for data encryption/decryption) in Data Management.

REFERENCES

Zhang, Q., Cheng, L., & Boutaba, R. (2010). Cloud Computing: State-of-the-Art and Research Challenges. Journal of Internet Services & Applications, 1(1), 7-18.

Ghosh, P., Thakor, V. & Bhathawala, P. (2017). Data Security and Privacy in Cloud Computing Using Different Encryption Algorithms, International Journal of Advanced Research in Computer Science and Software Engineering, 7(5),469-471.

Wei, L., Zhu, H., Cao, Z., Dong, X., Jia, W., Chen, Y. (2014). Security and Privacy for Storage and Computation in Cloud Computing, Journal of Information Sciences, 258, 371–386.

Bandewar, G. V & Borhade, R. H. (2016). Role Based Encryption with Efficient Access Control in Cloud Storage. International Journal of Science and Research (IJSR), 5(2), 560-564.

Nisha & Dhillon, N. S. (2016). A Novel Approach to Enhance the Security in Cloud Computing using AES Algorithm, International Journal on Emerging Technologie,s (Special Issue) 7(1): 76-79.

Pharkkavi, D. & Maruthanayagam, D. (2017). The Implementation and Comparative Analysis for Security Algorithms in Cloud Environment. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 2(6), 635-642.

Singh, N. K. (2017).Advanced Security Model for Ensuring Complete Security in Cloud Architecture, International Journal of Computational Intelligence Research, 13(5), 663-672.

Sudha, M., & Monica, M. (2012). Enhanced Security Framework to Ensure Data Security in Cloud Computing Using Cryptography. Advances in Computer Science and its Applications, 1(1), 32-37.

Sachdev, A. & Bhansali, M. (2013). Enhancing Cloud Computing Security using AES Algorithm. International Journal of Computer Applications, 67(9), 19-23.

Ganesh & Asha. (2017). Security Capabilities of Fine Grained Two Factor Access Control In Web Based Cloud Computing Services. International Research Journal of Engineering and Technology, 4 (5), 894-899.

Singh, S. K, Manjhi, P. K. & Tiwari, R. K. (2016). An Approach towards Data Security in the Cloud Computing Using AES, International Journal of Advanced Research in Computer and Communication Engineering. 5(6),22-29.

Abdulla, N. & Ercelebi, E. (2017). Identify Cloud Security Weakness related to Authentication and Identity Management (IAM) using Openstack Keystone Model. Proceeding of International Conference on Engineering and Technology, Computer, Basics and Applied Sciences, 3 (42),1-5.

Zanoon, N. (2015). Toward Cloud Computing: Security and Performance, International Journal on Cloud Computing: Services and Architecture (IJCCSA) ,Vol. 5(5/6),17-26.

Semwal, P. & Sharma, M. K. (2017). Comparative Study of Different Cryptographic Algorithms for Data Security in Cloud Computing. International Journal on Emerging Technologies (Special Issue), 8(1), 746-750.

Zhao, L., Zhang, L. J, & Liu, T. (2014). Research Gaps and Trends In Cloud Computing: A Systematic Mapping Study. International Journal of Cloud, 2(4), 1-11.

Geelan. J., (2008).Twenty one experts define Cloud Computing. [Electronic Version] Virtualization Electronic Magazine. Retrieved December, 14, 2017 from: http://virtualization.sys-con.com/node/612375.

Milojicic, D. (2008).Cloud computing: Interview with Russ Daniels and Franco Travostino. IEEE Internet Computing, 5, 7-9.

Mell, P., & Grance, T. (2011). The NIST Definition of Cloud Computing. Retrieved December 12, 2016; from: http://docs.ismgcorp.com/fi-les/external/Draft-SP-800-145_cloud-definition.pdf

Gupta, G., Hemrajani, N. & Kumar, A. (2017). Data Integrity Verification in Cloud Computing. Journal of Computer Engineering), 19(3), 23-27.

Bhardwaj, A., Subrahmanyam, G. V., Avasthi, V. & Sastry, H.(2016). Security Algorithms for Cloud Computing. International Conference on Computational Modeling and Security, Procedia Computer Science 85,535-542.

Bansal, S. & Jagdev, G.(2017). Analyzing Working of DES and AES Algorithms in Cloud Security. International Journal of Research Studies in Computer Science and Engineering (IJRSCSE), 4(3), 1-9.

Nigoti, R., Jhuria, M., & Singh, S. (2013). A Survey of Cryptographic Algorithms for Cloud Computing. International Journal of Emerging Technologies in Computational and Applied Sciences, 4(2), 141-146.

Yu, B., Sen, R., Jeong, D. H. (2013). An integrated framework for managing sensor data uncertainty using cloud computing, Journal of Information Systems, 38(8), 1252-1268.

Sookhak, M., Yu, F. R., Khurram Khan, M., Xiang, Y. & Buyya, R. (2016). Attribute-based Data Access Control in Mobile Cloud Computing: Taxonomy and open issues, Future Generation Computer Systems.72(C), 273-287.

Ramaporkalai, T. (2017). Security Algorithms in Cloud Computing. International Journal of Computer Science Trends and Technology, 5(2), 500-503.

Jasim, O. K, Abbas, S., El-Horbaty, M. E. & Salem, A. M.(2013). Efficiency of Modern Encryption Algorithms in Cloud Computing. International Journal of Emerging Trends & Technology in Computer Science (IJETTCS). 2(6), 270-274.

Abdul El minaam, D. S., AbdulKader, H. M., & Hadhoud, M. M. (2009).Performance Evaluation of Symmetric Encryption Algorithms, Communications of the International Business Information Management Association. 8, 58-64.