JCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-6, Issue-10, Oct 2018 E-ISSN: 2347-2693

Comparative Study of Hybrid Attribute Based Encryption for Cloud Computing System

G. Narmadhai[1*], S. Vijay Bhanu[2]

[1]Dept. of Computer Science, Annamalai University, Annamalai Nagar – 608 002
[2]Dept. of Computer Science & Engineering, Annamalai University, Annamalai Nagar – 608 002

[*]*Corresponding Author: narmadhaiphd@gmail.com*

Available online at: www.ijcseonline.org

Accepted: 16/Oct/2018, Published: 31/Oct/2018

Abstract— Due to reliability, there are million and millions of the uses and users of the cloud storages. So clouds are heavily developing field for various purposes. Many cloud hosts are providing services to different clients for their data storage. Due to disaster management cloud can be used as secured storage mechanism. For such cloud storages encryption is done many a ways for securing cloud data. The hybrid attribute based encryption i.e hybrid H-HABE is the method to encrypt the contents. This paper discusses the hybrid H-HABE encryption method for the cloud storages. The technique is also used to hide identity of the user that means the anonymous authentication can be implemented only by use of attributes. Our research work also analyses the importance of the data security in the cloud. Reason for choosing symmetric encryption algorithms are efficient to handle encryption and decryption for large amount of data, and effective speed of storing data and accessing the data in the cloud system. For implementation purpose here are considered the type of file as document file(doc), text file(txt) which can be enhance to sound file(.avi), video file, image file with different formats(BMP,JPG,GIFF,PNG).

Keywords— Cryptography,Security,Cloud Computing System; hybrid H-HABE

I. INTRODUCTION

The cloud is the storage mechanism for various electronic data such as Databases, Softwares, Platforms, Communication Services, Commercial Data Storages etc. The security is also a veery big issues for the contents in the storage at clouds. Various encryption mechanisms are used to protect the data from unauthorized access as well as from the losses, attacks, hacks etc. There are methods used such as public key infrastructure, Identity based encryption(IBE) as well as fuzzy identity based encryption method. The attribute based encryption(ABE) is also a method to encrypt the contents by using attributes only. This paper contents few of these methods to secure cloud storage by using hybrid attribute based authentication. Many sensitive and Important data can be secured by using this mechanism. For the same things, here it may achieve the anonymous authentication.

II. RELATED WORK

The necessary resources like authentication and access control for computation of cloud control and integration management. The practical solutions were not suggested by Role-Based Access Control (RBAC) and context aware RBAC to the clients, which was based on dynamic access control. The new model, ontology based access model control (Onto-ACM), was used to address the limitations of cloud computing suggested by Choi et al. [19]. A process such as resource virtualization, global replication, and migration assured quality of service by the computing paradigm. The cloud storage data had cloud users hopeful, but the clear computing results were not obtained.

The computation auditing secure protocol was proposed by Wei et al. [20] to secure storage and the process was completed with the batch verification, the signature verified by the designator, and sampling technique through this size was optimized and cost was minimized. The effectiveness and efficiency were clearly obtained from the experimental results.

The novel patient-centric framework had been proposed by Li et al. [21] to store personal records and access the data. The personal health record (PHR) a Health Centre files of each patient had been encrypted. Through this, clear and scalable data had been obtained, but it will be differed from the outsourcing of secure data by attribute-based encryption(ABE) techniques. The multiple security domains degrade the complexity of key management due to the PHR system division by the scenario of multiple data. The security, scalability, and efficiency were enabled by break glass and access policy.

Subashini and Kavitha [22] presented a detailed survey regarding security issues in service delivery models in cloud computing and they discussed each method, along with their pros and cons.

In this proposed research work, hybrid hierarchical attributes based encryption (H-HABE) algorithm is developed for securing the data stored in the cloud storage system. An attribute encryption scheme with more authority is more suitable for data access control cloud storage systems, because the user can be held by multiple institutions to manage property, and access to policy data owners to use the property that may be defined in different institutions. In addition, a single authority solution requires a completely honest authorized body; it is difficult to meet the security requirements of cloud computing environments. Weighted Attribute-Based Encryption(WABE) is hybridized with the Hybridized Hierarchical Attributes Based Encryption (H-HABE) for encryption purposes. Encryption, key generation, and decryption are ensured with the AES and blowfish algorithm. A key contribution in this research paper is summarized as follows:

- Here the propose a novel data collaboration scheme for secure read and write operations in cloud computing that allows a symmetric encryption algorithm for effective key management to reduce computational overhead. A full delegation approach-based hybridized encryption (H-HABE) that is employed for the outsourced data should be secure.

- Here, provide a verification method for the outsourced encryption and decryption. If the cloud returns incorrect results, users can notice it immediately by running the corresponding verification algorithm. Therefore, the user can access the data anywhere and anytime using any device. The computational cost is low, which is introduced by ABE in the user side.

Here, provide a security and performance analysis of our scheme, which shows that our scheme is both secure and highly efficient.

III. EXPERIMENTAL SETUP

The algorithms are implemented using the Java (Eclipse Platform Version: 3.3.1.1) Experiments are performed Intel Core i3 4150 and 8 GB of memory. Here it is used different size of text files.Images, Audio, Video, Different Platforms and Different Browsers in our experiments.

A. Experimental Result

All of these systems not only provide data security, but also accomplish the access control of encrypted data on a cloud network. While comparing the data collaboration schemes of ABE [15] and HABE [16], the proposed H-HABE attains partial signing, and full delegation, with less workload (data user and WAA) and also accomplish the lightweight key management in a large-scale consumer.

In the proposed scheme, various input files of different sizes (in GB) are encrypted and decrypted by hybrid of H-HABE algorithm. Key generation and weight generation are also done by our proposed algorithm. This algorithm is generated for security purpose and also it yields less execution timings for "encryption and decryption process" for Text files, Images, Audio and Video files. The security aspect of our encryption approach has been enhanced. The final outcome of the proposed scheme is illustrated below. The time taken for encryption and decryption process by the proposed H-HABE is compared with the conventional HABE scheme by considering the performance metrics.

The performance metrics are calculated based on the following tasks:

- o Calculate the encryption and decryption time for each algorithm using different sizes of input files.
- The effect of changing the file size on encryption / decryption time in Cloud.
- Compute the power consumption for each algorithm in Mb/Sec.
- A study is performed on the effect of changing packet size during throughput for each selected cryptography algorithm.
- A study is performed on the effect of changing data types such as text or document, audio file, and video file, Platforms, Browsers for each cryptography selected algorithm.

B. Throughput

Throughput is the amount of work that can be performed or the amount of output that is produced by a system or component in a given period of time. In a computer context, throughput is the amount of work that a computer can do in a given period of time. The work can be measured in terms of amount of data processed or transferred from one client to given cloud web link. The data transfer rates for disk drives and networks are commonly measured in terms of kilobits per second (kbps), megabits per second (Mbps) or gigabits per second (Gbps). The throughput of the encryption scheme is calculated as in equation (1).

$$\text{Throughput of encryption} = \frac{\text{Et Second}}{\text{Tp MByte}} \quad (1)$$

where

Tp: total plain text (Mbytes)

Et: encryption time (second)

Table 1. Experimental results of execution time of encryption/decryption, throughput for ABE, BH-WABE and H-HABE.

Text file Size in KB	Experimental results of execution time of encryption/decryption					
	ABE		BH-WABE		H-HABE	
	Encryption Time in sec	Decryption Time in sec	Encryption Time in sec	Decryption Time in sec	Encryption Time in sec	Decryption Time in sec
18186.24	960	900	840	921	810	800
8739.626	2060	2120	2036	2135	1998	2078
8949377.024	3040	3100	3051	3158	3012	3008
Total Time	6060	6120	5927	6214	5820	5886
Average Time	2020	2040	1975.667	2071.333	1940	1962
Throughput	4443.71	4400.15	4543.42	4333.59	4626.96	4575.07

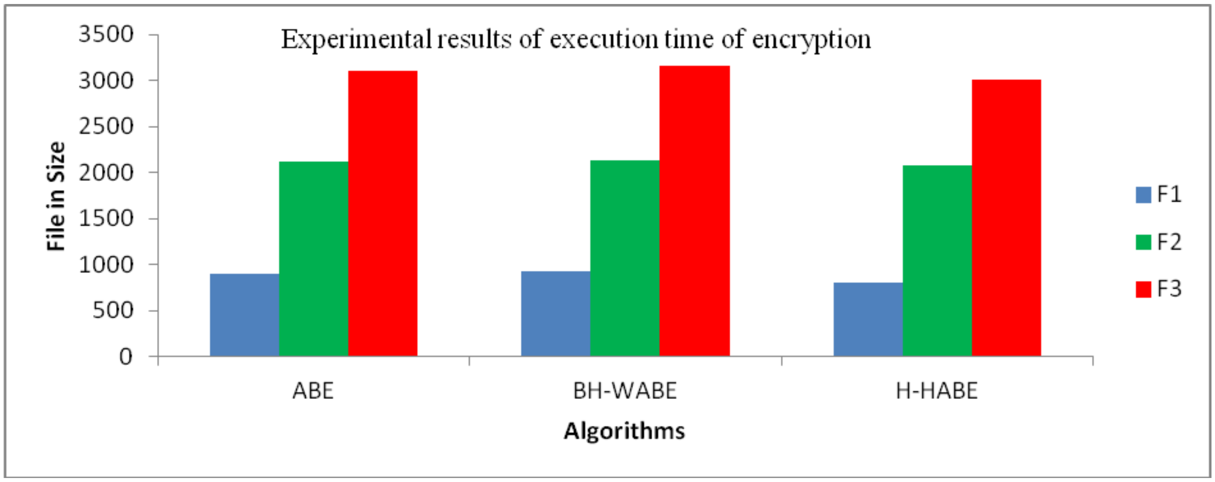

Figure 1: Experimental results of execution time of encryption

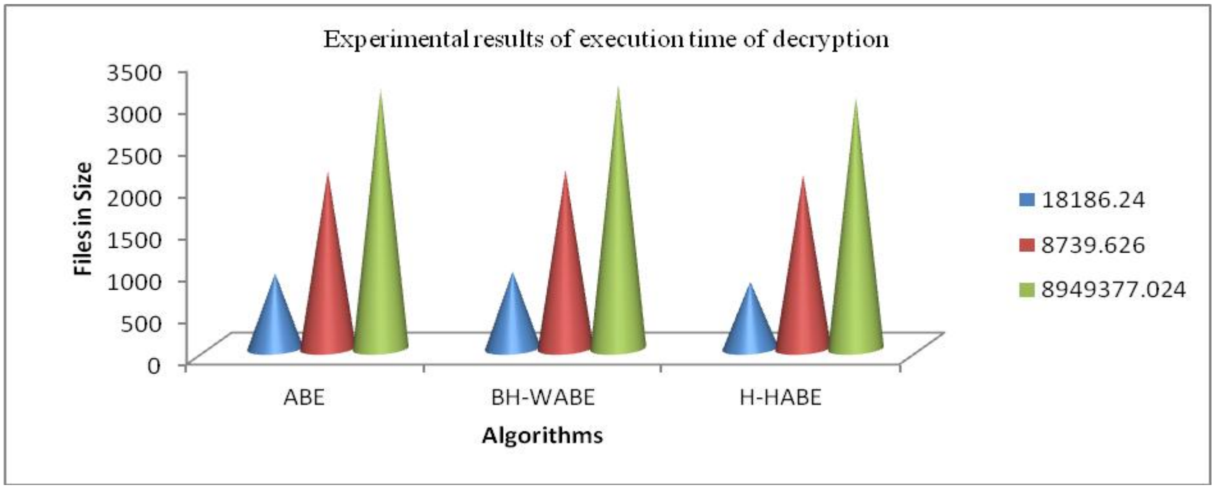

Figure 2: Experimental results of execution time of decryption

Experimental results for this compassion point are shown Figure 1 at encryption stage. The results show the superiority of proposed algorithm(H-HABE) over other algorithms in terms of the processing time. Another point can be noticed here; that BH-WABE requires less time than all algorithms except proposed algorithm. A third point can be noticed here; that H-HABE has an advantage over other ABE and BH-WABE in terms of time consumption and throughput.

C. Decryption of Different Packet Size

Experimental results for this compassion point are shown Figure 2 decryption stage. Here it can find in decryption that proposed algorithm(H-HABE) is the better than other algorithms in throughput and power consumption. The second point should be noticed here that H-HABE requires less time than all algorithms except our proposed algorithm.

D. Encryption of Different Audio Files Encryption Throughput

In the previous section, the comparison between attribute based encryption algorithms has been conducted at text files. Now here it make a comparison between other types of data (Audio files) to check which one can perform better in this case. Experimental results for audio files in the format (.avi) are shown Figure 3 at encryption.

Table:2 Time consumption to Encrypt Different Audio File Sizes

Audio File size	H-HABE	BH-WABE	ABE
F10(2409994k byte)	1404	2402	1957
F9(2409880kbyte)	1695	1886	1935
F8(2408880 k byte)	1547	1885	1855
F7(2407844 k byte)	1453	1756	1840
F6(2406844 k byte)	1460	1615	1675

A first point can be noticed here; that H-HABE has an advantage over other ABE and H-WABE in terms of time consumption and throughput especially in big size file.

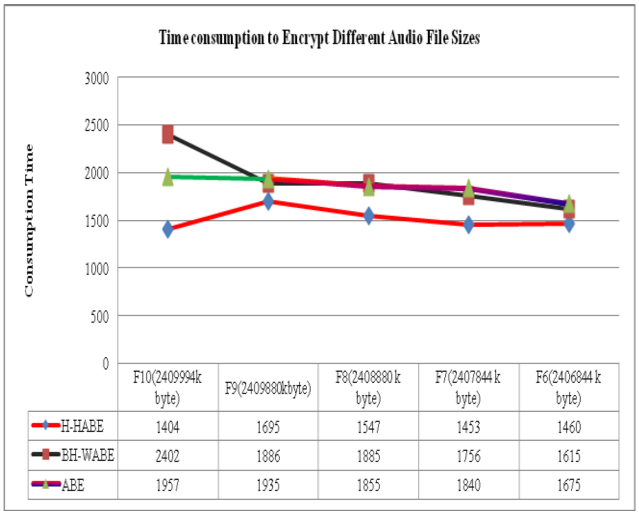

Figure:3 Shows Time consumption to Encrypt Different Audio File Sizes

A second point can be noticed here; that ABE has low performance in terms of Time consumption and throughput when compared with H-WABE. It always requires more time than H-HABE.

E.Encryption of different video files (different sizes)

Table 3 Encryption time with different sizes for video files

K bytes of data used	H-HABE	H-WABE	ABE
F1(64,006 k byte)	4230	4249	4243
F2(64,415 k byte)	4234	4261	4249
F3(65,013 k byte)	4270	4295	4275
Total Time	12734	12805	12767
Average Time	4244.667	4268.333	4255.667

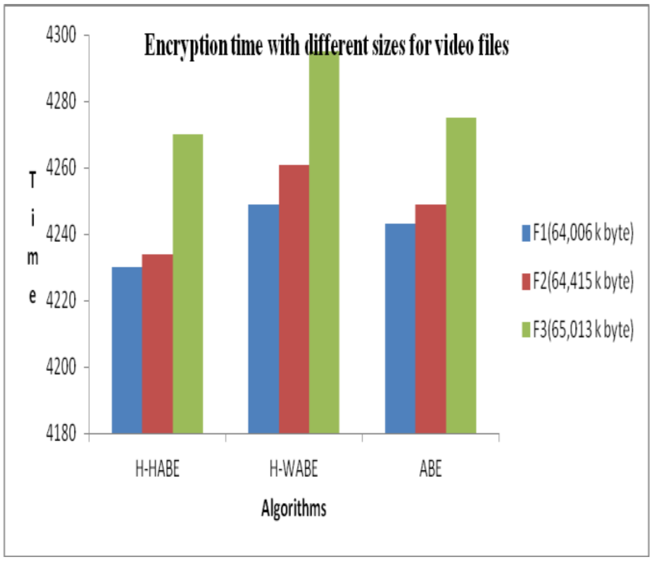

Figure:4 Encryption time with different sizes for video files

F. Encryption Throughput

Now here it will make a comparison between other types of data(video files) to check which one can perform better in this case. Experimental results for video data type are shown Figure:4 at encryption.

G. CPU Work Load

In Figure 4, we show the performance of cryptography algorithms in terms of sharing the CPU load. With a different audio block size. The results show the superiority of proposed algorithm over other algorithms in terms of the processing time and throughput as the same as in Audio files. Another point can be noticed here; that ABE still requires less time has throughput greater than all algorithms except proposed algorithm.

H. Depends on the operating system installed in the computer

The front end tools are installed in all three laptops and three platforms installed. Here it is encrypt 40 text files, Images, Audio and video files of size 20GB. First we tabulated their encryption time in ms(milli seconds) and then calculated their mean execution speed in MB/sec (MegaBytes per second) .

Table 4: Encryption Speed (in MB/sec) of Algorithms on different OS for text data

OS / Encryption	Windows XP	Windows Vista	Windows 7
ABE	2884.56	2784.15	2678.24
BH-WABE	2571.25	2455.35	2510.65
H-HABE	2150.50	2095.10	1940.55

H-HABE has an advantage over other ABE and BH-WABE in terms of throughput especially in large size files.

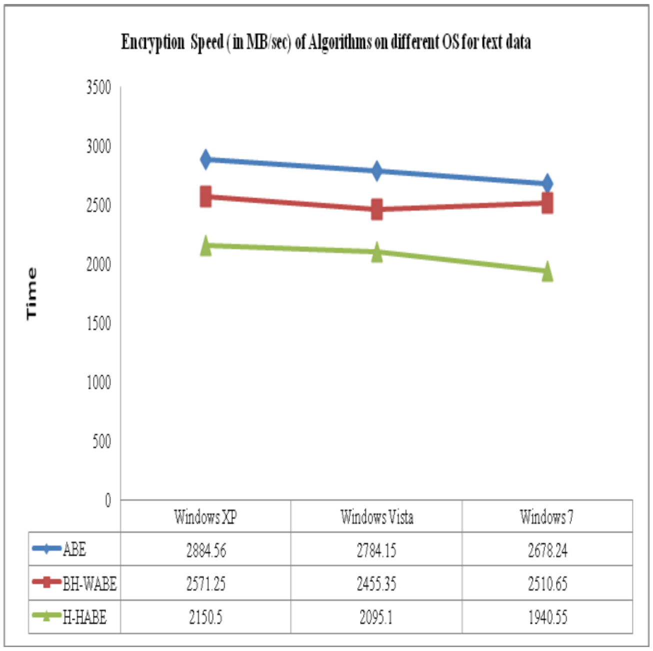

Figure:5 Encryption Speed (in MB/sec) of Algorithms on different OS for text data

The different platforms encrypt the files results show the superiority of H-HABE algorithm over other algorithms in terms of throuhput.

I. Comparison of Web Browser Speed Test

It is tend to find that different browsers have different strong advantages and disadvantages over one another for storage of cloud data, but as with a lot of things in life; one of the key characteristics of a good browser is pure unadulterated speed. Different latest versions of web browsers are used in this cloud based research.

The following factors affect the response time and speed of web browsers:

1.Depends on Web Browser
2. Depends on the operating system installed in the computer
3. Depends on the Computer configuration

The first test focuses on how long it takes for each browser to launch from the time the user decides to open it until it appears on public display, ready for action. The test has been slightly changed from previous versions, and is only timed up until it is ready for user communication. The graphics show that Chrome is unquestionably faster with Internet Explorer (in second place) followed by Opera and finally Firefox which lagged behind by approximately some seconds.

There are lot of web browsers that are available in the market, but these five are known to be the most popular among the top. They are Internet Explorer(IE), Mozilla Firefox, Opera, Netscape Navigator and Google Chrome.

Figure 6: Different popular Web Browsers available in the Software Market

Table 5: Encryption and Decryption of Different popular Web Browsers

File Size	ABE					BH-WABE					H-HABE				
	Encryption					Encryption					Encryption				
	IE	Chrome	Opera	FireBox	Netsc	IE	Chrome	Opera	FireBox	Netsc	IE	Chrome	Opera	FireBox	Netsc
18186.24	960	936	990	1024	950	955	932	912	954	935	924	902	905	900	914
8739.626	2060	2004	2095	2150	2045	2100	1998	2100	2014	2010	1997	1932	1997	1845	1997
8949377.024	3040	2998	3120	3225	3005	3250	3122	3210	3015	3025	2985	2910	2898	2850	2942
Total Time	6060	6045	6124	6185	6050	6120	6320	6124	6015	6010	5596	5874	5845	5750	5885
Average Time	2020	1979.33	2068.33	2133	2000	2101.66	2017.33	2074	1994.33	1990	1968.67	1914.66	1933.33	1865	1951
Throughput	740.61	749.08	728.06	713.31	744.92	722.43	725.53	727.06	748.14	749.27	780.41	772.62	770.82	791.2123	764.7217

The outcome of the testing will project the response time i.e. the encryption process and the time taken by the five web browsers, namely, Internet Explorer(IE), Mozilla Firefox, Opera and Netscape Navigator and Google Chrome after performing the encrypting scripts timed in millisecond onto the computer screen.

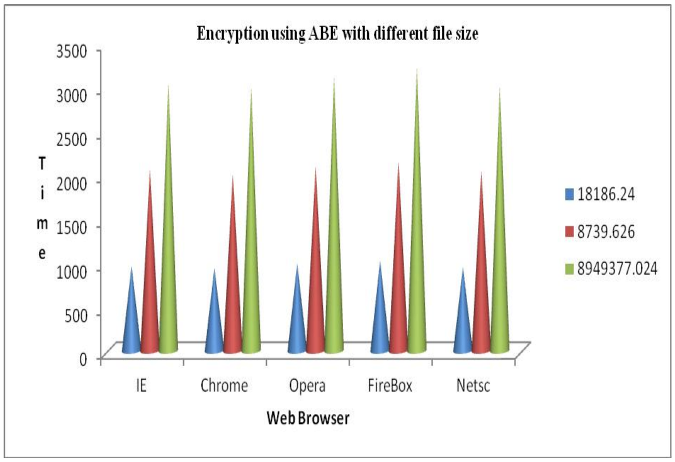

Figure:7 Encryption using ABE with different file size

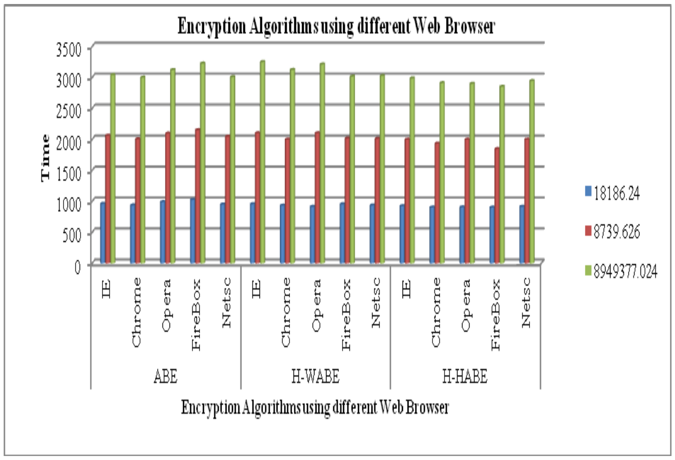

Figure:8 Encryption Algorithms using different Web Browser

IV. ADVANTAGES OF PROPOSED SYSTEM

- One Ciphertext can be decrypted by several rounds keys.
- Both precise level description and user attribute should be supported in the access structure of our new scheme /method.
- The keys in the authentication center have to the same hierarchical structure just as the structure of users privilege levels.

V. RESULTS AND CONCLUSION

In this paper proposed and implemented a hybrid attribute based encryption algorithm to encrypt data at client side before uploading it to a cloud storage service. The main aim of this paper was to propose and implement an algorithm, so that data can be encrypted at client side before it is uploaded to a cloud storage service, because it provides an extra layer of security, minimises data theft in transit, minimises data intrusion and spying when data in moving within data centres of the service provider and also solves the problem of lack of standardisation,where some service providers guarantee end-to-end security. But in reality their services are not secure. Hackers often trick a cloud into treating their illegal activity as a valid activity, and gain unauthorized access to the information stored in the cloud. This algorithm has been currently tested for text files, image file, Audio and Video file and even larger files could be encrypted at client side before uploading to the cloud.

REFERENCE

[1]Rajadeep Bhanot, Rahul Hans, “A review and Comparative Analysis of various Encryption Algorithms”, International Journal of Security and its Applications, vol. 9,Issue 4,2015.

[2]Zaran Hercigonja, Durga gimnazija Varazdin and Croatia, ”Comparative Analysis of Cryptographic Algorithms”, International Journal of Digital Technology and Economy, Vol 1, issue 2, 2016.

[3]Faiqa Maqsood, Muhammad Ahmad, Muhammad Mumtaz Ali, Munam Ali hah,” Cryptography: A Comparative Analysis for

Modern Techniques", International journal of Advanced Computer Science and Applications, vol 8, issue 6,2017.

[4] Shraddha D. "Performance Analysis of AES and DES Cryptographic Algorithms on Windows & Ubuntu using Java", International Journal of Computer Trends and Technology. 2016;35(4):179-183.

[5] Pooja B.,"Optimization of Cryptography Algorithms in Cloud Computing", International Journal of Computer Trends and Technology. 2017;46(2):67-72.

[6] Cloud Computing Challenges Businesses are Facing These Days an article by Mona Lebied in Business Intelligence , January 2017.

[7]"An Overview of Cryptography" an article by Gary C. Kessler, Embry-Riddle Aeronautical University - Daytona Beach, March 2016 .

[8] Managing Data Encryption, an article available at https://cloud.google.com/storage/docs/encryption#rotating-keys , January 2017

[9] What are the 12 biggest cloud computing security threats? , an article by Matthew Wilson available at https://www.ibm.com/blogs/cloud-computing/2016/04/12-biggest-cloud-computing-security-threats/ , April 2016.

[10] Encryption At Rest In Google Cloud Platform, an article available at https://cloud.google.com/security/encryption-at-rest/default-encryption/ , April 2017.

[11] Pereira, G. C., et al.,(2017). "Performance Evaluation of Cryptographic Algorithms over IoT Platforms and Operating Systems", Security and Communication Networks, 2017.

[12]. Sharma, S., et al., (2017). "Study on Cryptography and Techniques", International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 2(1).

[13]. Wu, Jiehong et al.,. "A study on the power consumption of using cryptography algorithms in mobile devices." Software Engineering and Service Science (ICSESS), 2016 7th IEEE International Conference on. IEEE, 2016.

[14]. Bhandari, Akshitaet al.,"Secure algorithm for cloud computing and its applications.", Cloud System and Big Data Engineering (Confluence), 2016 6th International Conference. IEEE, 2016.

[15]. Jakimoski, Kire, "Security Techniques for Data Protection in Cloud Computing" International Journal of Grid and Distributed Computing Vol.9. No1 (2016):PP.49-56.

[16]. Waleed, AL-Museelem, and Li Chunlin. "User Privacy and Security in Cloud Computing." International Journal of Security and Its Applications Vol.10 No.2 (2016): Pp.341-352.

[17]. Alotaibi, Mutlaq B. "Antecedents of software-as-a-service (SaaS) adoption: a structural equation model." International Journal of Advanced Computer Research Vol.6 No.25 (2016): PP.114.

[18] Li, J.; Huang, X.; Chen, X.; Xiang, Y. Securely outsourcing attribute-based encryption with checkability. IEEE Trans. Parallel Distrib. Syst. 2014, 25, 2201–2210.

[19] Choi, C.; Choi, J.; Kim, P. Ontology-based access control model for security policy reasoning in cloud computing. J. Supercomput. 2014, 67, 711–722.

[20] Wei, L.; Zhu, H.; Cao, Z.; Dong, X.; Jia, W.; Chen, Y.; Vasilakos, A.V. Security and privacy for storage and computation in cloud computing. Inf. Sci. 2014, 258, 371–386.

[21]Li, M.; Yu, S.; Zheng, Y.; Ren, K.; Lou, W. Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption. IEEE Trans. Parallel Distrib. Syst. 2013, 24, 131–143.

[22]Subashini, S.; Kavitha, K. A survey on security issues in service delivery models of cloud computing. J. Netw. Comput. Appl. 2011, 34, 1–11.