Cloud Data Security Using Modified Version of AES with Character Replacement –A Framework

Zaibunnisa Malik[1], Sabir Sayed[2], Ayesha Niyaz Malik[3]

[1]*Principal and HOD, Comp. Dept, M.H.Saboo Siddik Polytechnic, Mumbai, India*
[2]*Director, AI's Computer Center, Research Scholar Mumbai University, Mumbai, India*
[3]*Diploma in Computer Engineering, M.H.Saboo Siddik Polytechnic, Mumbai, India*

***Abstract*---In cloud computing, the data is stored in storage areas provided by the service providers. The clients might have certain confidential information for which no one other than the party for which the data is intended can be trusted. As the cloud has no explicit boundaries and the client's data can be dispersed across multiple servers on the globe, data security in cloud has become a major issue of concern. Hence, to overcome these serious issues regarding user authentication and data confidentiality, there is a need to implement a data protection framework which can perform authentication, verification and encrypted data transfer, thus maintaining data confidentiality. AES (Advanced Encryption Standard) has not been cracked by the attackers yet but research says that the algorithm is vulnerable to the brute force attack and hence there is a need to enhance the algorithm to make it more secure and robust. The proposed model, an enhancement to the AES-256 bit algorithm, is a tailor-made security framework with character replacement technique. The modified algorithm can be used to encrypt the client's data before it can be stored onto the cloud. This would ensure security of data as well as augment client-provider trust and relationships.**

Keywords: **Data Security, Modified AES, Encryption, Decryption, Cloud Computing.**

I.INTRODUCTION

Cloud computing has become a hot topic in the global technology industry. Cloud computing also faces the data security, privacy and confidentiality challenges. As the data owners store their data on external servers, there have been reportedly increasing demands and concerns for data confidentiality, authentication and access control. In addition to confidentiality and privacy breaks, the external servers could also use part or whole of the data for their financial gain. Therefore, ruining the data owners market or even bringing economic loss to the data owners. These concerns start off from the fact that cloud servers are usually operated by commercial providers which are probably from outside of the trusted domain of users [1].

Organizations today are increasingly looking towards Cloud Computing as a new revolutionary technology promising to cut the cost of development and maintenance and still achieve highly reliable and elastic services. The Cloud technology is a growing trend and is still undergoing lots of experiments. Cloud promises huge cost benefits, agility and scalability to the business [2].

Several trends are opening the era of Cloud Computing, which is an Internet-based development and use of computer technology. The ever cheaper and more powerful processors, together with the Software as a Service (SaaS) computing architecture, are transforming data centers into pools of computing service on a huge scale. The increasing network bandwidth and reliable yet flexible network connections make it even possible that users can now subscribe high quality services from data and software that reside solely on remote data centers.

Moving data into the cloud offers great convenience to users since they don't have to care about the complexities of direct hardware management. The pioneer of Cloud Computing vendors, Amazon Simple Storage Service (S3) and Amazon Elastic Compute Cloud (EC2) are both well-known examples. While these Internet-based on-line services do provide huge amounts of storage space and customizable computing resources, this computing platform shift, however, is eliminating the responsibility of local machines for data maintenance at the same time. As a result, users are at the mercy of their cloud service providers for the availability and integrity of their data. Recent downtime of Amazon's S3 is such an example [3].

Today's world is moving expeditiously towards virtualization and cloud; and since there are security issues associated with them, it becomes very consequential for the organizations to encrypt the critical data. This application provides this facility by enhancing the AES algorithm by integrating custom encryption settings in the algorithm. Since AES has been attacked by attackers in the past, we propose a configurable algorithm that allows the users to modify the algorithm each time they encrypt the text. The algorithm uses AES and integrates some custom configurable steps in the system where the user may modify the encryption process as needed. In this framework, more steps of encryption are integrated in order to make the data less liable to be deciphered by the attackers.

The enhancement in technology has led to increment in demand for sundry standard security measures to forfend data. Two types of cryptographic methods developed to

achieve this are: (1) Symmetric, secret key and (2) Asymmetric, public key. Symmetric cryptography includes: Data Encryption Standard (DES), 3DES, and Advanced Encryption Standard (AES).It is our attempt to make AES more secure by extending it, the extended version being called as Modified Advanced Encryption Standard with character replacement. The framework will not only support the AES algorithm but additionally the supplemental feature of replacement of units.

The AES encryption algorithm is a block cipher that uses an encryption key that is same for both the sender and receiver and has several rounds of encryption. It has proved to be better than DES as 56-bit key was not enough to secure data from various attacks. AES uses 128,196,256 key for encryption process and in addition, includes several rounds with respect to size of plaintext 128-bit 10 rounds, 192-bit 12 rounds, 256-bit 14 rounds respectively, resulting in the cipher text. The rounds include various techniques such as substitution, rearrangement and transformation encoding techniques. The key expansion method was adopted to double the number of iterations for increasing the immunity of algorithm against various types of attacks, example the brute force attack.

Recently, the importance of ensuring the remote data integrity has been highlighted by various research works. These techniques, while can be useful to ensure the storage correctness without having users possessing data, the cloud data storage is not addressing all the security threats, since they are all focusing on single server scenario and most of them do not consider dynamic data operations. As a complementary approach, researchers have also proposed distributed protocols for ensuring storage correctness across multiple servers or peers. Again, none of these distributed schemes are aware of dynamic data operations. As a result, their applicability in cloud data storage can be drastically limited.

II. LITERATURE REVIEW

Yang and Liu [6], describes that in this network friendly environment, cloud computing involves services related to the internet that are provided in order to augment the use of delivery models, often associated with the internet to aid in finding effortless scalable resources. They analysed a new algorithm of data mining model using web fuzzy clustering.

Li et al. [7], states that one of the most efficient opportunities for data processing, storage, and distribution is cloud computing. It enables on demand, scalable, pay-as-you-go computing and storage capacity.

Dev et al. [8], enunciates that cloud computing has transformed and reformed the ways computing and software services are sent to the customers in demand. The services empower the customers with the capability to connect to computing resources and contact IT handle services with simplicity and ease. The proposed system provides security against mining based attacks. The analysis may have to access data from multiple locations.

Stefania [9], explains how data Mining is used in Cloud Campus for acquiring likely useful information from basic unfinished data.

Naskar and Mishra [1], describes that currently the most challenging and demanding research in cloud computing is about data security and access control because of the customers delivering their sensitive personal data to the cloud providers in order to attain their services. This will allow the providers to access the information of the client without any authorization. However, this power of acquiring client information without any permission proves to be rather risky because of the fear of sensitive personal information being leaked and the method is apparently expensive as well.

Gruschka and Jensen[12], introduces the step to classifying security issues hence developing their analysis and making them more stable for use.

Ahmed et al. [15], states that as the promising cloud computing model sustained by virtualization is on rise, it still accounts for many security and trust mechanisms. They inspect the facts of cloud computing security challenges and aims to investigate and develop a protected base for the Information Owner (INO) to converse with the Cloud Service Provider (CSP).

III.RELATED WORK

The proliferation of web-based applications and information systems has led to increase in research work being carried out corresponding to data security.

Numerous algorithms & techniques are being proposed for providing high level of security.

Encryption is a technique in which the plain text is converted into cipher text by using various encryption algorithms like RSA, DES, 3DES, AES etc. In the year 2000, the NIST introduced Advanced Encryption Standard (AES) as a refinement over the previously expounded cryptography algorithms. AES is a cipher based encryption technique which uses a key and involves processing of the data over several rounds through which data and the key are encrypted. Before applying the algorithm, we must determine the size of the data and the cipher key. AES supports block sizes of 128,192,224,256 bits for data and 128,192,256 bits for cipher key. It is more efficient than other cryptographic algorithms due to its cryptanalysis, soundness of its mathematical basis, randomness of the algorithm output and relative security as compared to others. Cost was the second important area of evaluation that encompassed licensing requirements, computational efficiency (speed) on various platforms, and memory requirements. The speed of the algorithm on a variety of platforms needed to be considered. During Round 1, the focus was primarily on the speed associated with 128-bit keys. During Round 2, hardware implementations and the speeds associated with 192 and 256-bit key sizes were addressed.

Memory requirements and software implementation constraints were also important considerations.

Advanced Encryption Standard (AES) – Advanced Encryption Standard (AES) algorithm is not only good for security but withal for great celerity. Both hardware and software implementation is more expeditious. It is the encryption standard that is recommended by NIST to replace DES. It encrypts data blocks of 128 bits in 10, 12 and 14 round depending on key size. It can be implemented on various platforms especially in small devices. AES is conscientiously tested for many security applications.

IV. PROPOSED WORK

MAES (Modified Advanced Encryption Standard) algorithm provides a facility to upload the file, accept password (which is the key) and then this key will be appended with the file name. Hence, until and unless the password as well as identically tantamount file is provided the decryption process will not take place.

The first level of security is replacement of characters, like, alphabets can be replaced with alphabets, numeric values or any special characters; for instance, A is replaced with $ and the final level of encryption is AES. Rounds of AES include Sub-Byte Substitution, Row shifting, Mix column and Add Round key.

A. Block Diagram of MAES

Fig.1 shows the block diagram of MAES with character replacement.

1. User - It is a required entity that performs the task.
2. File - The file required to be encrypted.
3. Key – A customized, symmetric key used in AES algorithm.
4. Replacement – First level of encryption, stored in database.
5. Encrypt – Second level of encryption (AES 256 bit)
6. Decrypt – Deciphering the encrypted text.
7. Download – Output File can be downloaded.

B. Algorithm:

1. Start
2. Enter password (required key)
   Byte Key: =Textbox1.text
3. Click on encryption button or decryption button
4. If encryption is selected then follow steps 5 through 9, else follow step 11
5. Upload the file
6. Replace the characters with desired characters
7. Store the original characters and replaced ones in the database
8. Click on Encrypt button
9. Download the encrypted file
10. Upload the file with .enc as the extension
11. Click on Decrypt button
12. Download the decrypted file

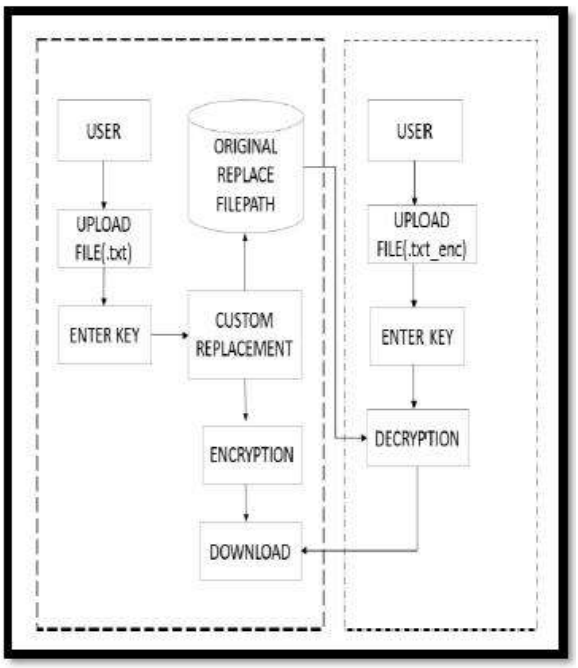

Fig.1 Block Diagram of MAES

C. Flowchart:

Fig. 2 shows the flowchart of MAES, which will explicate how the file is encrypted or decrypted on the website that is present on the cloud.

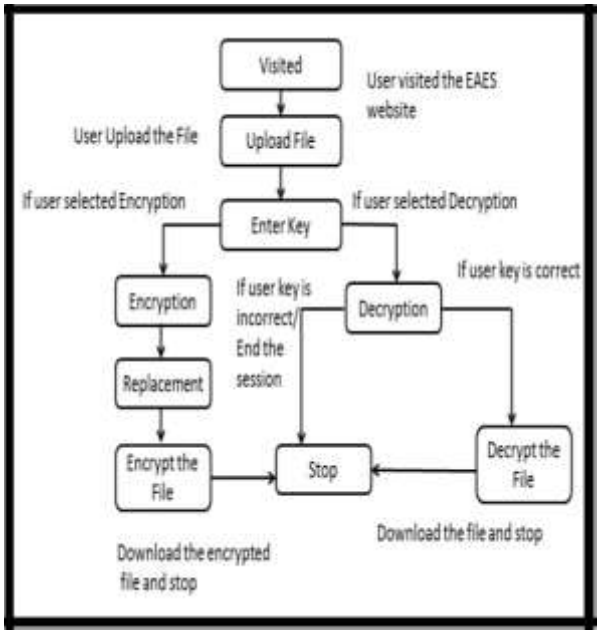

Fig.2 Flowchart of MAES

V. IMPLEMENTATION OF THE PROPOSED MODEL

The Proposed model is divided into two categories - Phase 1 and Phase 2.

Phase 1: Encryption

1.1 Login to the website by entering the password, here the website password is utilized as the key for encryption

Fig 3. Homepage of MAES

1.2 Send the selected file which is to be encrypted from local machine to the website

Fig. 4 File Encryption

1.3 Now, select the replacement characters, for the encryption algorithm.

Fig.5 Save Page of MAES

1.4 Now press the Encrypt button, which will encrypt the file and it is saved. After custom replacement encryption is done on the data and the encrypted file get downloaded by the user.

Fig.6 Encrypted File

Phase 2: Decryption

1.1 User will upload the file which user want to decrypt is selected and get in decrypted file in plain format.

Fig.7 Upload the file for Decrypt

1.2 Click on Decrypt button and get the decrypted file.

Fig. 8 Save Decrypted File

1.3 Download the file after decryption.

Fig. 9 Decrypted File

VI. RESULT ANALYSIS

The result analysis of implementation of the proposed system is given in the subsequent section. The categories of files include: image file, text file, video file and audio file.

We observed that the time taken for the encryption process of various files is approximately same as the time taken for the decryption process. Hence, to eliminate redundancy, the graphical representations of the result analysis have been given only for the encryption process.

TABLE I. SIZE AND TIME FOR IMAGE FILES

SIZE OF IMAGE FILE	TIME REQUIRED (Min:Sec:MiliSec)
100KB	00:01:22
500KB	00:01:10
1000KB	00:02:06

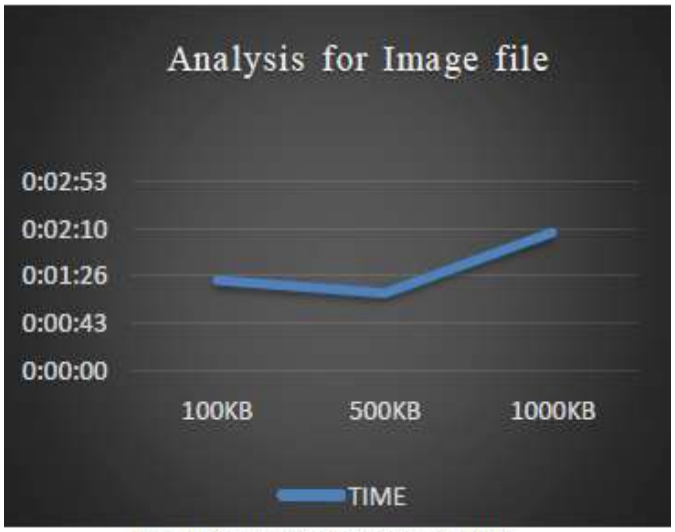

Fig. 10 Analysis for Image file

Fig. 10 represents the result analysis for different sizes of image files. For file size of 100KB, the time required is 00:01:22, for file size of 500KB, time required is 00:01:10. Hence, we observe that the difference in time between the two file sizes is almost negligible.

TABLE II. SIZE AND TIME FOR TEXT FILES

SIZE OF TEXT FILE	TIME REQUIRED (Min:Sec:MiliSec)
100KB	00:01:05
500KB	00:01:30
1000KB	00:01:90

Fig.11depicts the result analysis for different sizes of text files. We find that for file size of 100KB, the time required is 00:01:05, for file size 500KB time required is 00:01:30 and for file size of 1000KB, the time required to encrypt is 00:01:90.

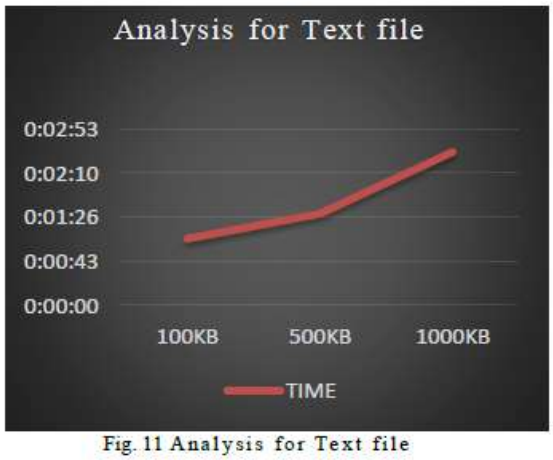

Fig. 11 Analysis for Text file

TABLE III. SIZE AND TIME FOR IMAGE FILES

SIZE OF VIDEO FILE	TIME REQUIRED (Min:Sec:MiliSec)
1MB	00:01:51
2MB	00:02:14

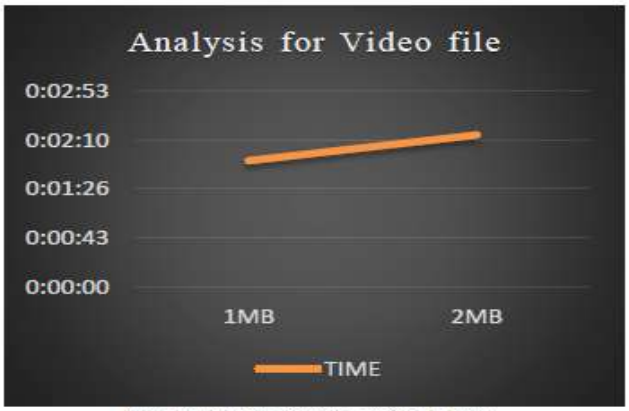

Fig. 12 Analysis for Video file

Fig.12 depicts the result analysis for different sizes of video files. For 1MB, the time required is 00:01:51, for 2MB, the time required is 00:02:14.

TABLE IV. SIZE AND TIME FOR IMAGE FILES

SIZE OF AUDIO FILE	TIME REQUIRED (Min:Sec:MiliSec)
100KB	00:01:04
500KB	00:01:05
1000KB	00:01:09

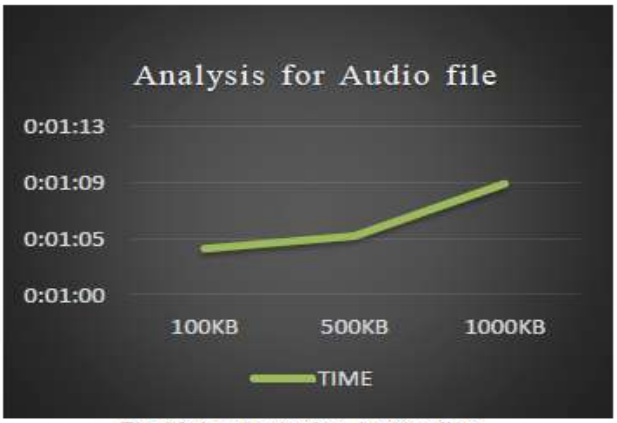

Fig. 13 Analysis for Audio file

Fig.13 represents the result analysis for different sizes of audio files. For 100KB, the time required is 0:01:04, for 500KB time required is 00:01:05 and for 1000KB, time required is 00:01:09. Hence, we observe that the difference in time for encryption between the files is almost negligible.

VII. CONCLUSION

In this paper, we presented the findings of the literature survey that was conducted on the security challenges faced by cloud computing and proposed a framework, that is the modified AES algorithm. This framework ascertains that the clients can store their data onto the cloud without any hesitation or trepidation of breach of confidentiality or integrity of their critical data. The proposed framework also enhances trust between the client and the cloud service provider.

The framework that has been implemented is not only an enhancement to the security provided by AES algorithm, but additionally does the encryption and decryption of data in efficient time, contrary to a framework that would provide enhanced security but not in efficient time or vice versa. Hence, we can conclude that the proposed system is reliable and efficient to be used for security of data on cloud. One can believe that more efforts should be exerted by both, the cloud vendors as well as the cloud service users, to provide a highly forfended and safe cloud computing environment.

VIII. FUTURE SCOPE

The system that we have implemented does not fortify encryption and decryption of video files above 2MB. Hence, the future scope is the implementation of such a system that could fortify more colossal file sizes.

REFERENCES

[1]. Naskar Ankita, Mishra Monika R.,"Using cloud computing to provide data mining services", International Journal Of Engineering And Computer Science March 2013.
[2]. Prashant Srivastava, Satyam Singh, Ashwin Alfred Pinto, ShvetankVerma, Vijay K. Chaurasiya, Rahul Gupta, "An architecture based on proactive model for security in cloud computing" in IEEE-InternationalConference on Recent Trends in Information Technology, June 2011.
[3]. N. Gohring, By Nancy Gohring, "Amazon's S3 down for several hours,"http://www.pcworld.com/article /142549/ article.html.Accessed on 25-04-2013.
[4]. PriyankaArora, Arun Singh Himanshu Tyagi, "Evaluation and Comparison of Security Issues on Cloud Computing Environment", World of Computer Science and Information Technology Journal (WCSIT) ISSN: 2221-0741 Vol. 2, No. 5, 179-183, 2012.
[5]. Mandeep Kaur and Manish Mahajan, VSRD International Journal of Computer Science & Information Technology, Vol. 2 No. 10 October 2012 / 831.ISSN No. 2231-2471 (Online), 2319-2224 (Print) © VSRD International Journals.
[6]. Xianfeng Yang, Pengfei Liu, "A New Algorithm of the Data Mining Model In Cloud Computing Based On Web Fuzzy Clustering Analysis", Journal of Theoretical and Applied Information Technology 10thMarch 2013, Vol. 49 No. 1 China.
[7]. Juan Li, Pallavi Roy, Samee U. Khan, Lizhe Wang, Yan bai, "Data Mining Using Clouds: An Experimental Implementation of Apriori over MapReduce".
[8]. Himel Dev, TanmoySen, Madhusudan Basak and Mohammed Eunus Ali, "An Approach to Protect the Privacy of Cloud Data From Data Mining Based Attacks".
[9]. Ruxandra-StefaniaPetre, "Data mining In Cloud Computing", Database systems Journal Vol. III, No. 3/2012.
[10]. Jing Ding, Shanlin Yang, "Classification Rules Mining Model With Genetic Algorithm in Cloud Computing", Internal Journal of Computer Application (0975-888) Volume 48-No.18, June 2012.
[11]. Kaikala Anjani Sravanthi, Yalamarthi Madhavi Lata, "Web Mining Using Cloud Computing", Internal Journal Of Emerging Technology And Advanced Engineering (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 3, Issue 4, April 2013). Systems workshops.
[12]. Meiko Jensen, JorgSchwenk, Nils Gruschka, Luigi Lo Iacono, "On Technical Security Issues in Cloud Computing 2009 IEEE International Conference On Cloud Computing.
[13]. Bhaskar Prasad Rimal, Eunmi Choi, Ian Lumb, "A Taxonomy and Survey of Cloud Computing Systems", 2009 Fifth International Joint Conference on INC, IMS and IDC.
[14]. Nils Gruschka, Meiko Jensen, "Attack Surfaces: A Taxonomy For Attacks on Cloud Services", 2010 IEEE 3rd International Conference on Cloud Computing.
[15]. Mahbub Ahmed, Yang Xiang, Shawkat Ali, "Above the Trust and Security in Cloud Computing: A Nation towads Innovation", 2010 IEEE/IFIP International Conference on Embedded and Ubiquitous Computing.