International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 08 Issue: 03 | March - 2024 Impact Factor: 8.176 ISSN: 2582-3930

A Dual Encryption Scheme for Network Security

Meenu Yadav[1]

Dr. Vinod Kumar[2]

1Ph.D. Research Scholar, Department of Computer Science and Application, BMU Rohtak

2Professor, Ph.D. Research Scholar, Department of Computer Science and Application, BMU Rohtak

---

Abstract - Cloud computing is an emergent part in the arena of IT. Nowadays, a good amount of fast, advanced and challenging technologies are available in cloud computing for accessing, sharing, and transmitting large data over the network. Along with this growth, the existence of data hackers and attackers has also increased. Every organization always seeks error free and secured data transmission over the cloud. Moreover, the users also expect their data, stored on to the cloud should be more secured, confidential, and authorized. The server stores the encrypted data and it is decrypted at client side. In this article, we proposed cryptographic mechanisms that verify the uniqueness of data stored at cloud is same as original data put by the client. Additionally, we have also explored the existing encryption procedures, namely, AES and Blowfish for the evaluation. Performance evaluation of the algorithms based on the parameters memory requirement, time complexity for dissimilar documents formats like Text, Images, Pdfs. Word documents and Movie clips etc. at different configurations for individual users is done.

Key Words: Information Technology, Cloud Computing, Cryptography, Cloud Security, AES, Blowfish

1. INTRODUCTION

Cloud computing is a model which is universal, easy and as per requirement network access to a common pool of computing resources which could be configured, thus, enabling a quick plan and release involving limited management effort or interaction with the service provider. These computing resources could be networks, servers, applications, storage and affiliated services which are a part of virtual environmentreading a simulated setting on an present host to ride use's preferred package, deprived of interfering with any of the supplementary facilities providing by the host platform to further consumers is well-known as virtualization. Hence, cloud computing facilitates the idea of virtualization that carry segregated data and the remote applications in virtual machines. So cloud service providers create a platform for users that ensures the secured data transmission and storage. For securing critical data in corporate IT environment that is no longer in your control can be protected by cryptography in cloud .Cryptography as technique use encryption methods that prevent unauthorized data access and provide confidentiality. So for this cloud clients have to have a very enhanced and robust encryption of data before it is transmitted to cloud [1]. Also, the cloud server has strong and enhanced encryption techniques so that data could be retrieved safely. Encryption process involves conversion of a plain text or information from a user into a cipher text or code via a communication channel where again cipher text is converted into original plain text when it reaches the receiver end. Cryptography procedures can be categorized into Symmetric and Asymmetric key cryptography.

Symmetric key also known as secret key encryption use single key, shared key, and one key to encrypt and decrypt cipher text. Decryption of data is easy if a weak key is used in algorithm. The size of the key is determining factor for the encryption of symmetric key. Two methods for encryption are used in Symmetric algorithms: a) block cipher and b) stream cipher. Block cipher encrypts data in block of text or data in groups. Examples are AES (Advanced Encryption Standard), Blowfish. Whereas, Stream ciphers works on a single bit one at a time. Examples are Data Encryption Standard (DES), RC4.

In Asymmetric key encryption two keys i) public and ii) private are used. Key generation protocol is used by cryptographic algorithms to generate key pair. This key generation protocol is a mathematical function. Combination of two functions is used in this algorithm. a) Encryption function b) Decryption function. Here, open key is castoff for encryption and reserved key is cast-off for decryption. Examples of asymmetric encryption – RSA (Rivest-Shamir-Adleman) , Diffie-Hellman.

Symmetric key techniques are preferred by researchers for creating Message Authentication Code (MAC) in Wireless Sensor Network which further helps in securing storage i.e. databases hosted by the cloud provider. This is why symmetric key techniques are more efficient than asymmetric techniques.

1.1 Basic Terms

Plain Text – Any human readable or text message that is sent by a user for communication with the other user, before encryption and after decryption is well-defined as Ordinary Text. User X intends to send "Good Morning!!" message to user Y. So, here "Good Morning!!'' is a simple text message.

Cipher Text – A meaningless message that cannot be assumed by someone is called a Cipher Text.

"YTgre516!@#^8" is a Cipher Text formed for "Good Morning!!"

Encryption – It is a process which converts plain text into Cipher text. It requires an encryption algorithm which uses a technique and a key. Encryption happens at the sender's end.

Decryption – It is reverse of Encryption. It converts cipher text into Plain text. It uses the decryption procedure. In most cases, encryption and decryption procedures are similar.

Key – It is a numeric or alpha numeric typescript or can be a distinctive character. It is castoff on the simple typescript at the stage of Encryption and on the Cryptogram text at the time of Decryption. For example if the plain text on laptop is "Hello!" then the corresponding cipher text formed will be "Sqwuhylghz" [2.]

1.2 Purpose of Cryptography

- Authentication: The information at the user end is secured with a secret key that is used while encrypting and decrypting the data and is known to user as well as the receiver of information, maintaining the authenticity.
- Confidentiality: All the information stays confidential and thus maintaining the identity of the user and resulting in a successful communication between user, server and the party with whom the data is to be shared.
- Integrity: Modification on any transmitted information can be made only by authorized Parties i.e. the user; nothing can be changed by the parties who receive the information.
- Non–repudiation: Once the information generated at user end is stored on server the user cannot deny its authenticity.
- Access Control: It is in the hands of user with whom the information generated is to be shared.

1.3. Evaluation Parameters

Randomness of cipher, vulnerability to known attack, performance with different types of data are some factors which need to be pondered upon before we go into the details of cryptography. So some of the parameters which determine Strength or weakness of any given algorithm are discussed below:

Encryption time: It is dependent on the length of data contained in a particular block and the length of the secret key generated. It is measured in milliseconds. It has direct influence on encryption algorithm performance. Fast encryption time is indicative of advanced algorithmic performance.

Decryption time: It is also measured in milliseconds. It is the time period in which original text is regained from cipher text. Here also the quick decryption time is indicative of advanced algorithmic performance.

Memory used: To make system cost effective a low usage of memory is aimed

Throughput: It is the number of output bits in a particular time. It should never be confused with execution time (end time-start time).If the throughput cost increases, power consumption decreases.

2. RELATED WORK

Yahia Alemami, et al., (2019) [3] Security plays a critical role for placing the secured and private information in cloud. Many encryption strategies are accessible for the protecting the records during communication or storage in cloud. The encryption algorithm approaches vary in parameters like CPU utilization, memory, cipher and decipher time (speed), throughput utilization. The researcher tried to create more secured and safe methods by using appropriate factors which are frequently used in cryptography algorithms.

S.V.N.Srivall, et al., (2019) [4] the two phase approaches one cryptography for distorting the message and second steganography for concealing the message's existence is used. It helps to reduce the security risk of the text files. The system divide the original text file into two equal sub parts and each sub part will go through Blowfish and AES encryption and then again merging of these subparts and uploading into the cloud server. By using the LSB steganography method the keys used to encrypt the sub parts of the text file are hidden behind the cover image and then to respective user mails the stegno image is sent. The results provide more secured and protected text files are uploaded and stored into the cloud.

Shilpi Harnal et al., (2019) [5] A proposed hybrid cryptography algorithm supported by end-to-end encryption (E2EE) technique is designed for the safety, truthfulness and privacy of mass media records in cloud environs. The hybrid procedure is verified and matched in contradiction of the other suggested and present procedures. The performance analysis is based upon the testing and comparison of algorithms using various parameters like confidentially, speed, data integrity, memory usage in footings of tables and charts. The compared result for existing and proposed algorithms for stored media files is satisfactory

Shafi'i Muhammad, et al., (2018) [6] The Microsoft Azure cloud server stored the encrypted data using blowfish algorithm. The data is encrypted at user end and gets a unique identification from the cloud storage to retrieve encrypted data. The two parties cannot have same exclusive Id and all users must have the exclusive Id top-secret sideways with the top-secret key chosen by the user. The consumer can access the stored data with the help of unique Id and decryption can be done at retrieval. The designed system functioning is to send the encrypted content at cloud server, it enables decryption at retrieval. Single user can encode typescript memo formerly directing to the cloud setting. This is the easiest technique for documents storing and encryption techniques of the warehoused data.

G. Sathish Kumar, et al., (2018) [7] Many encryption procedures are available for gotten information

stockpiling and partaking in cloud. Key escrow and declaration renouncement is dealing with issue in the personality based encryption. The proposed structure, for information encryption utilizes blowfish and for key encoding utilizes RSA. The information holder encodes his/her mysterious key for using the information. The data holder encodes the mysterious key twice to outline a middle of the road key. This encoded data will send and widely appealing keys to the cloud. The cloud will unscramble the widely appealing key to some extent and send the generally decoded key and mixed data to the arranged recipient. The customer will unravel again the fairly decoded data which is sent by the cloud and the customer will get the necessary key for deciphering with the objective that the customer can translate it completely. The data holder can send comparable data to various clients with most minimal cost.

Ako Muhamad Abdullah (2017) [8] Advanced Encryption Standard (AES) calculation is one on the most well-known and broadly symmetric square code calculation utilized in around the world. This calculation has an own specific design to scramble and unscramble touchy information and is applied in equipment and programming everywhere on the world. It is incredibly hard to programmers to get the genuine information while encoding by AES calculation. Till date isn't any proof to crake this calculation. AES can manage three distinctive key sizes, for example, AES 128, 192 and 256 digits and every one of these codes has 128 cycle block size. This paper clarifies various significant highlights of AES calculation and presents some past explores that have done on it to assess the presentation of AES to encode information under various boundaries. As indicated by the outcome acquired from investigates shows that AES can give substantially more security contrasted with different calculations like DES, 3DES and so forth.

Neha, et al., (2016) [9] the primary objective behind the plan of encryption calculation should be protection from unapproved assaults. Encryption calculation is a lot of secure however delayed in execution. To accomplish security, different cryptographic calculations are utilized to scramble and decode the information.. The three procedures AES, Blowfish and Twofish are broke down. Twofish will give preferred execution over blowfish. Twofish is a lot quicker; its key arrangement is however quick as 1.5 encryptions while Blowfish seems to be delayed in setting up a key, taking up to 521 encryptions. Blowfish isn't appropriate for smartcards where Twofish is productive for smartcards. In Twofish, S-Boxes are developed cautiously to ensure that all S-Boxes are solid. Twofish has no frail keys though Blowfish has powerless keys. This paper shows correlation based on encryption/unscrambling time and mixture of AES and Twofish sets aside less effort to encode and decode the record when contrasted with AES and Blowfish.

3. PROPOSED WORK

In the initial phase of the research process, the focus was to explore the wide range of published literature. This was to understand the different cloud services. Through this way, the collection and evaluation of data about various services provided by cloud provider's was done. For this search strategy, systematic literature reviews, market study, user reviews, social media postings was done. In addition, industry survey and questionnaire based approach was also performed. Based on these a framework was designed using security techniques for the measurement of the performance of the cloud services.

The selection of cloud service usage and quality assessment of the cloud resource supplier, up to the customer satisfaction enhanced the small organizations to adopt cloud computing. Past credentials and current survey approach sum-up that load time, reliability and data integrity parameters are best for managing services of cloud providers. Through fog we have compute the values of three parameters load time for service, Integrity for each provider and reliability and calculate trust factor. Then selection of the service and uploading of file is done on the basis of cluster which offers the different services to the set of nodes.

The security mechanism are applied to maintained the safety, integrity and correctness of data in cloud .The sever stores the encrypted data and it is decrypted at client side. This will assure the user that his data is secured in cloud server and third party cannot access his data.. If the data stored on cloud may be transformed without the awareness of client then key generation mechanism verifies the uniqueness of data. This verifies the data has been is same as the original data put in storage by the client. It supports all kind of documents i.e. Text, Images, Pdfs, Word documents and Movie clips etc.

Oracle Virtual Box which executes as a Virtual Machine and Fog is be used for protected access and facility agreed platform. Ruby centered cloud collection in Fog permits setting up an authorization folder to link various facility sources and function similarly for creating on-demand provision as necessary.

The Proposed work consists of three scenarios:

1) The encoded documents are saved over the cloud using AES technique at client side.

2) The encoded documents are saved over the cloud using Blowfish with error control encryption.

3) The encoded documents are saved over the cloud using Blowfish without error control encryption.

Encryption algorithms are written into Python scripting language. The experimental setup helps in performance evaluation. Ubuntu 18.04 on Oracle VM Virtual Box 6.1.2 assessed the outcomes centered on time consumption considerations.

4. RESULTS AND DISCUSSION

Following graphs shows the encryption based results and comparison show in bar graph format as performance measurement of time analysis and utilization of storage space of different type of data on cloud. The proposed work has implemented the secured approach of data storage while transmitting the files on cloud.

Text, Images, Pdfs, Word document, Movie clips etc.

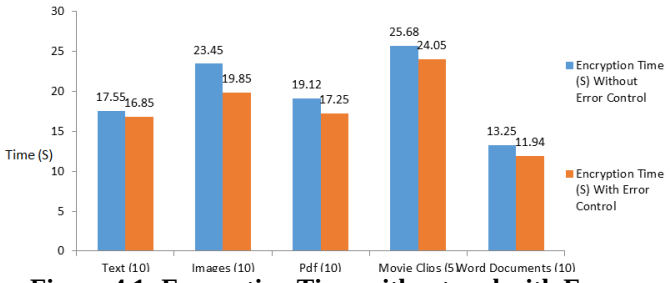

Figure 4.1: Encryption Time without and with Error Control

Figure 4.1 represents the data of encryption stage has been considered on different files by means of the above approach. Encryption time estimate the speed of the system. It can be seen from the above chart that the encryption time (s) without error control is more show more time along with less speed of communication. The performance of encryption time (s) with error control is better as the less time show high speed of communication between user and cloud server.

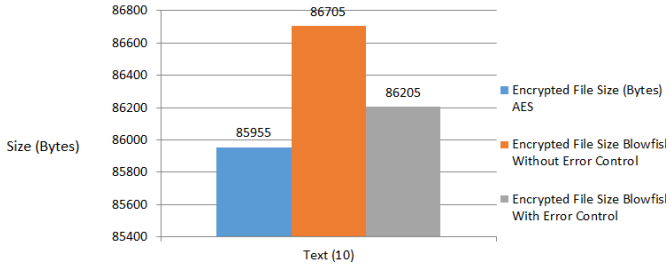

Figure 4.2: Encrypted File size (Text) AES vs. Blowfish

Figure 4.2 represents the data on ten text files and their encrypted file size has been calculated. It can be seen from the above graph that the encrypted file size with AES is 85955 bytes are found as memory space is less as compared to encrypted file size without and with error control of blowfish.

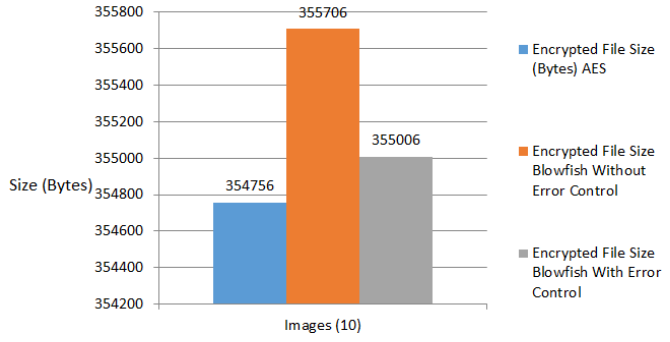

Figure 4.3: Encrypted File size (Image) AES vs. Blowfish

Figure 4.3 represents the data on ten image files and their encrypted file size has been calculated. It can be seen from the above graph that the encrypted image file size with AES are found as less data storage as compared to encrypted file size without and with error control of blowfish.

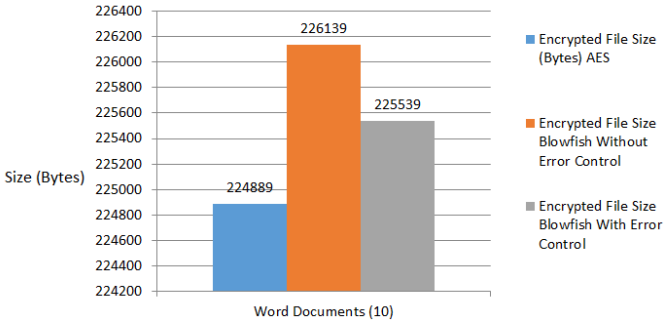

Figure 4.4: Encrypted File size (Word Documents) AES vs. Blowfish

Figure 4.4 represents the data on ten word documents files and their encrypted file size has been calculated. It can be seen from the above graph that the encrypted file size with AES are found as less memory utilization as compared to encrypted file size without and with error control of blowfish

CONCLUSIONS

In the prevalent systems there are several security and privacy issues for data transmission from cloud and data storage on cloud. A secure two tier way for file storage in cloud computing involving both client and server side must be placed. Encryption efforts have been done for the data stored in the cloud must be secured Client side encryption with AES technique is apply on various text file send by user. Server receives and checks the encrypted file by using technique blowfish with and without error control before storing the data in cloud. Blowfish with error control results are best for data transfer with faster speed in cloud.

REFERENCES

[1] M. U., Shallal, Q. M., and Tamandani,Y. K. Bokhari, "Security and privacy issues in cloud computing," in Computing for Sustainable Global Development (INDIACom),3rd International Conference on IEEE, 2016.

[2] Sonia Kuwelkar Chaitali Haldankar, "IMPLEMENTATION OF AES AND BLOWFISH ALGORITHM," International Journal of Research in Engineering and Technology (IJRET) , vol. 3, no. 3, pp. 143-146, May 2014.

[3] Yahia Alemami, "Research on Various Cryptography Techniques,"Mohamad Afendee Mohamed, Saleh Atiewi International Journal of Recent Technology and Engineering (IJRTE), vol. 8, no. 2S3, pp. 395-405, July 2019.

[4] Ben SwarupMedikonda S.V.N.Srivalli, "Development of a Cloud-based Secure Text File Application using Hybrid Cryptography and Steganography," International

Journal of Recent Technology and Engineering (IJRTE), vol. 8, no. 1, pp. 3267-3271, May 2019.
[5] R.K. Chauhan Shilpi Harnal, "Hybrid Cryptography based E2EE for Integrity & Confidentiality in Multimedia Cloud Computing ," International Journal of Innovative Technology and Exploring Engineering (IJITEE), vol. 8, no. 10, pp. 918-924, August 2019.
[6] Nafisat Abubakar Sadiq, Mohammed Abdullahi, Nadim Rana, Haruna Chiroma, and Dada Emmanuel Gbenga Shafi'i Muhammad Abdulhamid, "Development of Blowfish Encryption Scheme for Secure Data Storage in Public and Commercial Cloud Computing Environment," in 2nd International Conference on Information and Communication Technology and Its Applications (ICTA), Federal University of Technology, Minna, Nigeria, September 5 – 6, 2018, pp. 231-237.
[7] K. Premalatha, N. Aravindhraj, M. Nivaashini, M. Karthiga G. Sathish Kumar, "Secured Cryptosystem using Blowfish and RSA Algorithm for The Data in Public Cloud," International Journal of Recent Technology and Engineering (IJRTE), vol. 7, no. 4S, pp. 45-49, November 2018.
[8] Cryptography and Network Security, "Advanced Encryption Standard (AES) Algorithm to Encrypt and Decrypt Data," Cryptography and Network Security, pp. 1-13, June 2017.
[9] Mandeep Kaur Neha, "Enhanced Security using Hybrid Encryption Algorithm," International Journal of Innovative Research in Computer and Communication Engineering, vol. 4, no. 7, pp. 13001-13007, July 2016.
[10] Mandeep Kaur Neha, "Enhanced Security using Hybrid Encryption Algorithm," International Journal of Innovative Research in Computer and Communication Engineering, vol. 4 , no. 7, pp. 13001-130007, July 2016.
[11] Abdel-Karim Al Tamim. https://www.cse.wustl. edu /~jain/cse567-06/ftp/encryption_perf/