RESEARCHERID
THOMSON REUTERS

[Jothy * *et al.*, 7(2): February, 2018]
IC™ Value: 3.00

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

ENHANCING THE SECURITY OF THE CLOUD COMPUTING WITH TRIPLE AES, PGP OVER SSL ALGORITHMS

K Arul Jothy[*1], K Sivakumar [2] & Delsey M J[3]

[*1]Final Year CSE, Department of Computer Science and Engineering, JCT College of Engineering and Technology, Coimbatore, Indi

[2&3]Assistant Professor, Department of Computer Science and Engineering, JCT College of Engineering and Technology, Coimbatore, India

DOI: 10.5281/zenodo.1165634

ABSTRACT

The cloud computing is indispensable to the business world today. It provides keen business insights. Cloud technology makes it possible to store this data and ensure that it is easily accessible. It is like storage space available virtually to the user and the emergence of the cloud computing which made it easier to provide the best of technology in the most cost-effective package. The cloud computing are used in the variety of filed like education, business etc. The cloud computing uses the service models like SaaS, PaaS, and IaaS an organization achieves their business goal with minimum effort as compared to traditional computing environment. So the security is the major concern that must be provided to these sectors to have reliable and secure communication over the internet and to maintain the privacy of the data. So the security become the major issues in the cloud computing and it seems like the attackers are restless, and they keep inventing new ways to find the entry points in the system. Cryptography provides various symmetric and asymmetric algorithms to secure the data. This paper presents the symmetric cryptographic algorithm named as TRIPLE AES (Advanced Encryption Standard) for data at rest and PGP (Pretty Good Privacy) along with SSL (Secure Socket Layer) provide security for the data at motion.

KEYWORDS: Cryptography; Security; Cloud Computing; Advanced Encryption Standard; Pretty Good Privacy; Secure Socket Layer.

I. INTRODUCTION

The cloud computing has been emerged from the earlier technology called grid computing. Cloud computing has the tremendous growth in the internet and the increasing demand for the e-commerce transaction and it all has been carried out widely around the world. So these improvements cause the large companies to adopt this technology to create huge data centers, to handle with the movement taking place all over the Internet [1]. The greatest benefit of this technology is that it provides the internet service to the companies without the need of purchasing the additional hardware, and also helps in reducing the cost. This causes that cloud computing is being seen as:"cloud computing is rapidly emerging as a technology trend almost every industry that provides or consumes software, hardware and infrastructure can leverage" [1].The cloud is used to satisfy the user demand whenever it require and at all points. And the cloud computing will provide the demand to the hardware and the software resources with minimal management efforts. . The full functionality is been provided by the considering it as an infrastructure to provide certain functionality by using some physical component. These components are the processors, databases, network hardware or operating system. These definitions are the extension of concepts such as SaaS (Software as a System), PaaS (Platform as a system) and IaaS (Infrastructure as a system) [6]. These concepts are also treated as cloud layers, where each of them fulfills a different role or provides services to individual users. In addition to these layers, there is another dSaaS (Data Storage as a Service), which provides a place to store files. As the central data storage is the key facility of the cloud computing it is of prominent importance to provide the security [6].And there is a problem in providing the security to the operation that occur inside the cloud computing. Cryptography was introduced to solve this problem. Cryptography is an art and the science of creating the secret code. There are three main security goals

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

they are: Availability, Confidentiality, and Integrity. The cryptography is the group of two types of algorithm used they are I) Symmetric-key algorithms II) Asymmetric-key algorithms. These two algorithms are used to perform the encryption and the decryption operation with the key called as a secret key. The symmetric algorithm performs the encryption and the decryption operation with same set of key for both operations. This is termed as secret key. With the same key messages are encrypted by the sender and decrypted by the receiver. It contains algorithms like Data Encryption Standard (DES), Advanced Encryption Standard (AES), Ron's Code (RCn), Triple DES and Blowfish etc [12]. The asymmetric algorithm uses the two different keys for encryption and the decryption. The two keys used among them are named as the public key and the private key. The public key is used in the encryption operation and the private key is used in the decryption. Public key is known to public and private key is known to the user. It comprises various algorithms like Rivest, Shamir, and Adleman (RSA), Digital Signature Algorithm (DSA), Elliptic Curve (EC), Diffi-Hillman (DH), El Gamal etc [12].Here we make use of the symmetric key cryptosystem as a solution to solve the security issues in the cloud computing and this method has the speed and computational efficiency to handle encryption of large volumes of data .In symmetric cryptosystems, the longer the key length, the stronger the encryption. AES is most frequently used encryption algorithm today this algorithm is based on several substitutions, permutations and linear transformations, each executed on data blocks of 16 byte. As of today, no practicable attack against AES exists. Therefore, AES remains the preferred encryption standard for governments, banks and high security systems to store data in the cloud server around the world [12]. So the triple AES is stronger and more efficient method to provide more security to the information. So we use the triple AES to provide more secure communication. So we need to provide the security for the data that travel from to sever to the user thought the network from the serve and vice versa. To improve the open network security we use the PGP (Pretty Good Privacy). So the security is provided to the data that in rest and in the motion. But sometimes if the hacker attacks the data in the transmission there may be a chance of attaining the original information after some logical sequence. In order to avoid this situation we use SSL along with the PGP in order to avoid that critical situation. SSL is the kind of algorithm in which it converts the code into another form in which user not able to understand that code. SSL will convert the data of one form to another form in which hacker not able to understand the form and the type of the code or the information.

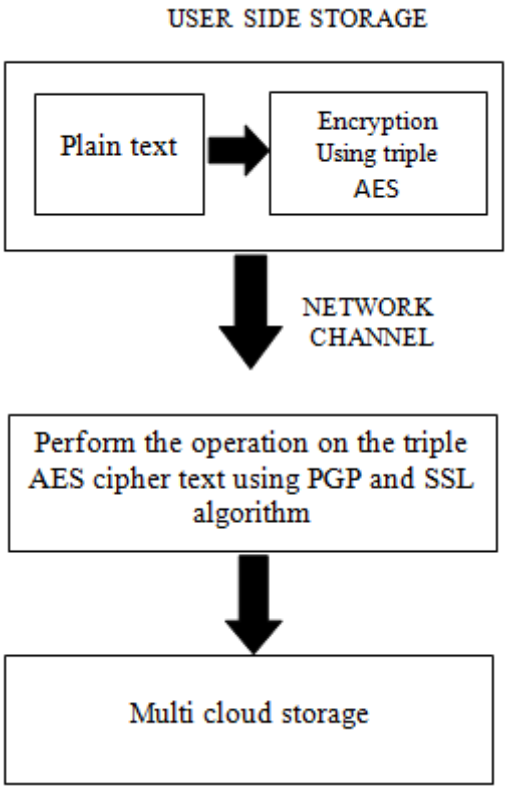

Figure1. Encryption operation

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

II. LITERATURE REVIEW

The process of providing the security feature to the cloud storage can be provided with the Triple AES, PGP, and SSL algorithm. And the more secure communication can be established by using these three algorithms.
AES is a symmetric block cipher that is intended to replace DES as the approved standard for a wide range of applications. Compared to public-key ciphers such as RSA, the structure of AES and most symmetric ciphers is quite complex and cannot be explained as easily as many other cryptographic algorithms [13].

AES data encryption is more scientifically capable and graceful cryptographic algorithm, but its main force rests in the key length. The time necessary to break an encryption algorithm is straight related to the length of the key used to secure the communication. AES allows choosing a various type of bits like 128-bit, 192-bit or 256-bit key, making it exponentially stronger than the 56-bit key of DES [12]. So here we are using triple AES algorithm in which the same operation is been performed thrice here to establish more complex secret code.

PGP (Pretty Good Privacy) is an operation mode that is used to provide security for data in network channel .when using PGP will have binary data to send (encrypted message etc.) .PGP must encode raw binary data into printable ASCII characters [13]. It uses radix-64 algorithm (aka "ASCII Armour"). And it maps 3 bytes to 4 printable chars (it's the Base64 of MIME). Then it also appends a 24-bit CRC .PGP also segments messages if too big. It needs a session key for each message of varying sizes: 56bit DES, 128-bit CAST or IDEA, 168-bit Triple-DES. It is generated using ANSI X12.17 mode. And uses random inputs taken from previous uses and from keystroke timing of user .Since many public/private keys may be in use (by one user), need to identify which is actually used to encrypt session key in a message and it could send full public-key with every message . Secure Socket Layer it provides a secure transport connection between applications (e.g., a web server and a browser) SSL was developed by Netscape. SSL version 3.0 has been implemented in many web browsers (e.g., Netscape Navigator and MS Internet Explorer) and web servers and widely used on the Internet .SSL v3.0 was specified in an Internet Draft (1996). It evolved into RFC 2246 and was renamed to TLS (Transport Layer Security). TLS can be viewed as SSL v3.1

It is described a new architecture for security of data storage in multicloud data travel through the network to and from cloud. Three mechanisms-data encryption and file splitting are used. When user uploads a file, it is encrypted using AES encryption algorithm and again data is encrypted using PGP algorithm and SSL algorithm and travel through the channel. Then that encrypted file is divided into equal parts according to the number of clouds and stored into multicloud. This proposed system enhances the data security in multicloud and in network channel.

III. IMPLEMENTATION OF ALGORITHM

Cipher text by using AES algorithm and the cipher text of AES is given as input to the PGP algorithm in the network and PGP provides the second cipher text of given plain text. Then the cipher text from the PGP is travelled through the network and it is stored in multicloud.

- So usage of PGP in the channel makes the data more secure and more confidential.
- Then during the decryption process the vice versa process take place.

A. AES OPERATION STEPS

AES is based on ‘substitution–permutation network’. It comprises of a series of linked operations, some of which involve replacing inputs by specific outputs (substitutions) and others involve shuffling bits around (permutations).

STEP I:

1. Add Round Key

STEP II: (The following four functions are periodically repeated)

1. SubByte
2. ShiftRow

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

3. MixColumn
4. AddRoundKey

STEP III:

1. SubByte
2. ShiftRow
3. AddRoundKey

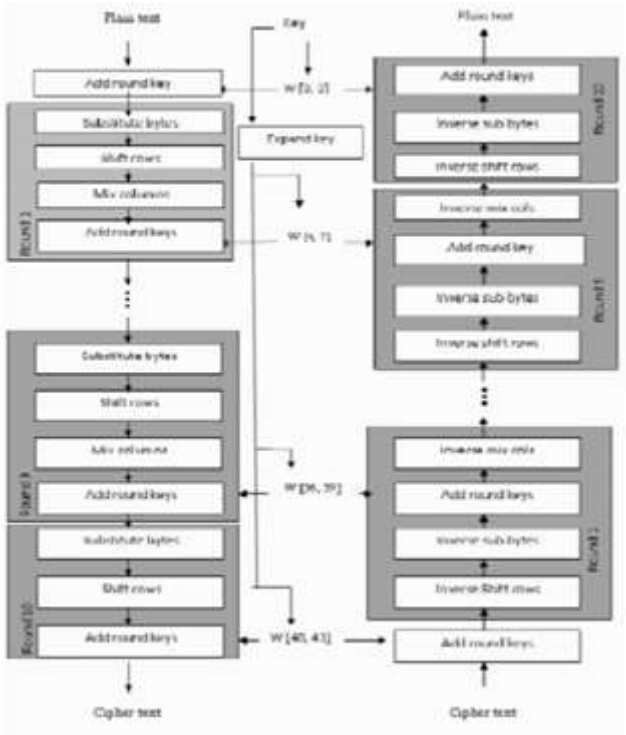

Figure2. Encryption and decryption in AES

STEP IV: Byte Substitution (Sub Bytes)

The 16 input bytes are substituted by looking up a fixed table (S-box) given in design. The result is in a matrix of four rows and four columns

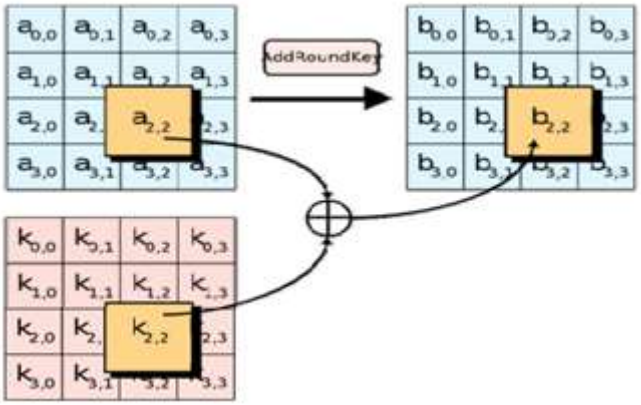

Figure 3. Byte Substitution (Sub Bytes)

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

STEP V: Shift Rows

Each of the four rows of the matrix is shifted to the left. Any entries that 'fall off' are re-inserted on the right side of row. Shift is carried out as follows First row is not shifted. Second row is shifted one (byte) position to the left. Third row is shifted two positions to the left. Fourth row is shifted three positions to the left. The result is a new matrix consisting of the same 16 bytes but shifted with respect to each other

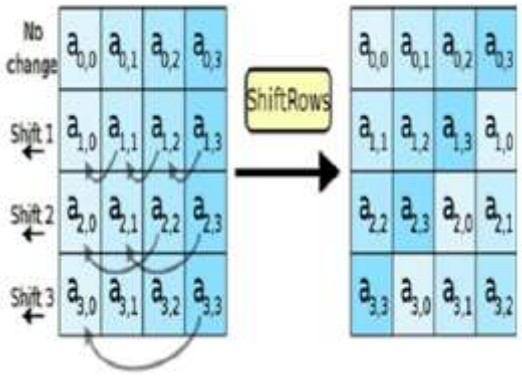

Fig.Shift Rows

STEP VI: Mix Columns

Each column of four bytes is now transformed using a special mathematical function. This function takes as input the four bytes of one column and outputs four completely new bytes, which replace the original column. The result is another new matrix consisting of 16 new bytes. It should be noted that this step is not performed in the last round.

2 3 1 1
1 2 3 1
1 1 2 3
3 1 1 2

STEP VII: Add Round Key

The 16 bytes of the matrix are now considered as 128 bits and are XORed to the 128 bits of the round key. If this is the last round then the output is the ciphertext. Otherwise, the resulting 128 bits are interpreted as 16 bytes and we begin another similar round.

B. TRIPLE AES

The triple AES operation is similar to the AES operation but only the difference is that the operation is performed thrice with three different keys. The performance of the operation thrice will result in the more confidential code with more secure feature.

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

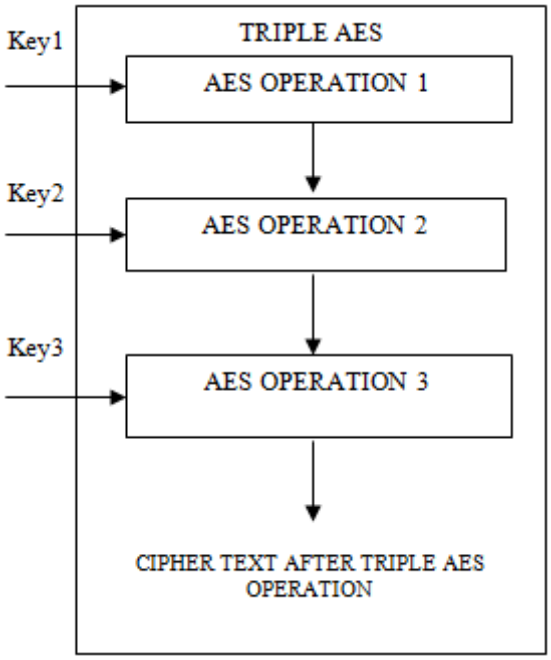

Figure5. TRIPLE AES operation

C. PGP OPERATION STEP

Operational Description PGP consists of the following five services:

1. Authentication
2. Confidentiality
3. Compression
4. E-mail compatibility
5. Segmentation

STEPS:

1. The sender generates a message and a random number to be used as a session key for this message only.
2. The message is encrypted using CAST-128, IDEA or 3DES with the session key.
3. The session key is encrypted with RSA (or another algorithm known as ElGamal) using the recipients public key and is pretended to the message.
4. The receiver uses RSA with its private key to decrypt and recover the session key.
5. The session key is used to decrypt the message

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

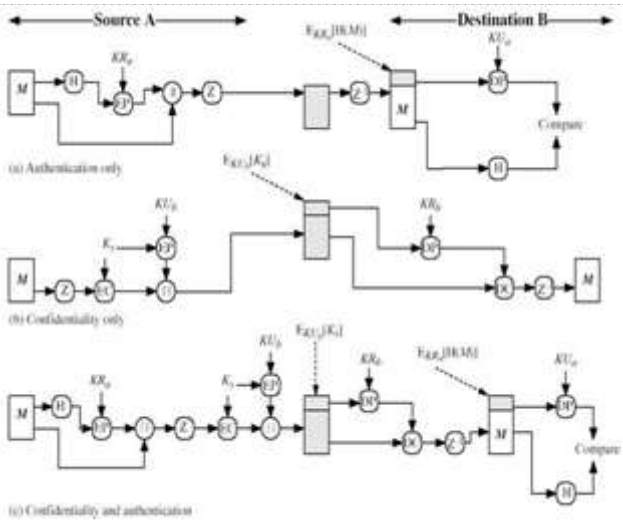

Figure 6. PGP cryptographic functions

D. SECURE SOCKETS LAYER (SSL)

The Secure Sockets Layer (SSL) is a method for providing security for web based applications. It is designed to make use of TCP to provide a reliable end to-end secure service. SSL is not a single protocol but rather two layers of protocols as illustrated in figure 11.1. It can be seen that one layer makes use of TCP directly. This layer is known as the SSL Record Protocol and it provides basic security services to various higher layer protocols. An independent protocol that makes use of the record protocol is the Hypertext Markup Language (HTTP) protocol. Another three higher level protocols that also make use of this layer are part of the SSL stack.

They are used in the management of SSL exchanges and are as follows:

1. Handshake Protocol.
2. Change Cipher Spec Protocol.
3. Alert Protocol.

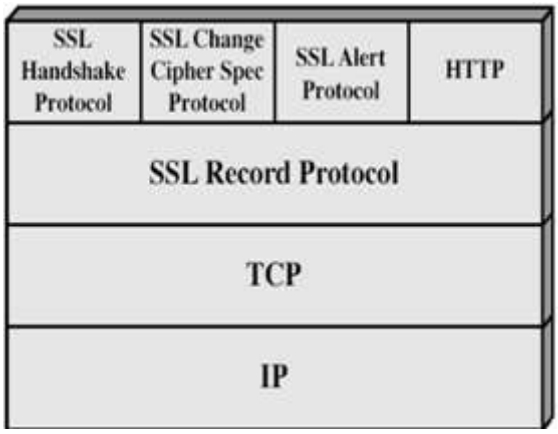

Figure 7.SSL protocol stack

IV. CONCLUSION

The current architecture provides more secure communication over the channel and during the data storage process. It shows resistance against a variety of attacks such as square attack, key attack, key recovery attack and differential attack. Therefore, AES algorithm is a highly secure encryption method. Data can also protect against future attacks such as smash attacks. AES encryption algorithm has minimal storage space and high performance without any weaknesses and limitations while other symmetric algorithms have some weaknesses and differences in performance and storage space [12]. The encryption of PGP over SSL offers is just as strong as that of AES, but it adds the additional security that prevents anyone with just the public key from being able

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

to encrypt and decrypt data being transferred across network. So the combination of AES and PGP over SSL provides more security to the data at rest (cloud server) and in data in motion (network channel). So it provides more security to the confidential data. Even then these processes are more secure the time consumption and the key values required are more. So the future work can be enhanced in reducing the time consumption of the operation and in reducing the number key values used

V. ACKNOWLEDGEMENT

I am thankful to Prof. K. Sivakumar and M J Delsey for them guidance and support to pursue this work.

VI. REFERENCES

[1] AbhaSachdev, MohitBhansali "Enhancing Cloud Computing Security using AES Algorithm" International Journal of Computer Applications (0975 – 8887) Volume 67– No.9, April 2013.
[2] Dr.S.Gunasekaran, M.P.Lavanya "A Review On Enhancing Data Security In Cloud Computing Using RSA and AES Algorithms"(IJAER) 2015, Vol. No. 9, Issue No. IV, April ISSN: 2231-5152.
[3] Rashmi S. Ghavghave, Deepali M. Khatwar "Architecture for Data Security In Multicloud Using AES-256 Encryption Algorithm" International Journal Recent and Innovation Trends in Computing and Communication Volume: 3 Issue: 5 ISSN: 2321-8169.
[4] Mr. Santosh P. Jadhav, Prof. B. R. Nandwalkar "Efficient Cloud Computing with Secure Data Storage using AES"International Journal of Advanced Research in Computer and Communication Engineering Vol. 4, Issue 6, June 2015 ISSN (Online) 2278-1021
[5] Namita N. Pathak, Prof. MeghanaNagori "Enhanced Security for Multi Cloud Storage using AES Algorithm" International Journal of Computer Science and Information Technologies, Vol. 6 (6), 2015 ISSN:0975-9646
[6] R. H. Sakr, F. Omara, O. Nomir "An Optimized Technique for Secure Data Over Cloud OS" International Journal of Emerging Trends & Technology in Computer Science (IJETTCS) Volume 3, Issue 3, May-June 2014 ISSN 2278
[7] Ranjit Kaur, Raminder Pal Singh "Enhanced Cloud Computing Security and Integrity Verification via Novel Encryption Techniques" SSRG International Journal of Mobile Computing & Application (SSRG-IJMCA) – volume 2 Issue 3 May to June
[8] P.V.NITHYABHARATHI, T.KOWSALYA, V.BASKAR "To Enhance Multimedia Security in Cloud Computing Environment Using RSA and AES" International Journal of Science, Engineering and Technology Research (IJSETR), Volume 3, Issue 2, February 2014
[9] T. ShobanaMaheswari, S. Kanagaraj and Shriram K. Vasudevan "Enhancement of Cloud Security Using AES 512 Bits" Research Journal of Applied Sciences, Engineering and Technology ISSN: 2040-7459; e- ISSN: 2040-7467 November 25, 2014
[10] Disha Shah, "Digital Security Using Cryptographic Message Digest algorithm", International Journal of Advance Research in Computer Science and Management Studies, Volume 3, Issue 10, October 2015.
[11] AtulKahate (2009), Cryptography and Network Security, 2nd edition, McGraw-Hill.
[12] Stallings, W. (2006), Cryptography and Network Security 4/E., Pearson Education India.
[13] Behrouz A Fourouzan, DebdeepMukhopadhyay (2010), Cryptography and Network, 2nd edition, McGraw-Hill. [14] Goyal, Kashish, and SupriyaKinger. "Modified Caesar Cipher for Better Security Enhancement." International Journal of Computer Applications (0975–8887) Volume (2013).

CITE AN ARTICLE

Jothy, K. A., Sivakumar, K., & J, D. M. (n.d.). ENHANCING THE SECURITY OF THE CLOUD COMPUTING WITH TRIPLE AES, PGP OVER SSL ALGORITHMS. *INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY*, *7*(2), 75-82.