Efficient Cloud Computing with Secure Data Storage Using AES and PGP Algorithm

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

[*] *Department of Computer Science and Engineering*
JCT College of Engineering and Technology,India.

Abstract- **Cloud computing is usually associated with a set of applications and tools, used by companies to conduct their businesses. However, the possibilities offered by the cloud, and its versatility, causes that its tools and applications can also be used in education and many other fields. And 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 among the data service becomes more concern with the entire factor. It requires a very high degree of privacy and authentication. So the cryptography is the one of the method used to provide the security among these data in the cloud server. Cryptography provides various symmetric and asymmetric algorithms to secure the data. This paper presents the symmetric cryptographic algorithm named as AES (Advanced Encryption Standard) for data at rest and PGP (Pretty Good Privacy) provide security for the data at motion.**

This paper is organized into four section I section is introduction which gives brief information about cloud computing and secret keys and its various algorithms, attacks on cryptography etc. Section II is literature survey which includes related work in corresponding topic. Section III contain proposed algorithm. Section IV conclusion.

Keywords— **Cryptography, Security, Cloud Computing, Advanced Encryption Standard, Pretty Good Privacy**

I. INTRODUTION

Cloud computing has evolved from the earlier technology called grid computing, but has reached the stage of commercialization recently. Cloud computing has risen from a large growth of the Internet and the increasing number of e-commerce transactions, carried out all around the world. This caused, that large technology companies have created huge data centers, to handle with the growing movement taking place all over the Internet [1].

Cloud computing has enabled companies to provide Internet service without the need to purchase additional hardware, also helped to reduce costs, including incurred in connection with the work, they had done at the customer service staff . 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 main task of cloud service providers is the ability to data mass management, and the ability to acquire data at the point whenever user demands it. Also Cloud computing presents a model that provides on demand access to software and hardware resources with minimal management efforts.

And considering Cloud computing as an infrastructure, it refers to the physical components that are required by the system in order to provide the full functionality. 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].

The art and science of concealing the messages to introduce secrecy in information security is recognized as cryptography. Security goals of data cover three points namely: Availability, Confidentiality, and Integrity. Cryptography, in modern days is considered grouping of three types of algorithms. They are

I) Symmetric-key algorithms
II)Asymmetric-key algorithms

Symmetric algorithms use the same key for encryption and decryption. 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),

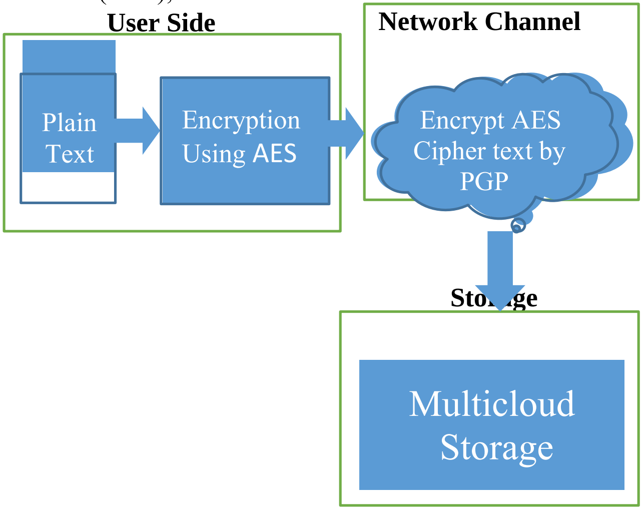


Fig.1 Encryption Process

Advanced Encryption Standard (AES), Ron's Code (RCn), Triple DES and Blowfish etc [12].

Asymmetric algorithms use different keys. One key (public) is used for encryption and other (private key) is used for decryption. This is named as public key. Public key is known to public and private key is known to the user. It comprises various algorithms like Rivest, Shamir, & Adleman (RSA), Digital Signature Algorithm (DSA), Elliptic Curve (EC), Diffi-Hillman (DH), El Gamal etc [12].

We choose symmetric cryptosystem as solution as it 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 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.

II. Literature Review

A privacy-preserving public auditing system for data storage security in cloud computing is intended, although the computational time is increased but the privacy is preserved where data is stored in the cloud by using the most prominent algorithm AES.

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].

PGP (Pretty Good Privacy) is a 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: 56-bit 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 .

It is described a new architecture for security of data storage in multicloud data travel through the network to and from cloud. Two 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 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
3. MixColumn
4. AddRoundKey

STEP III:

1. SubByte
2. ShiftRow
3. AddRoundKey

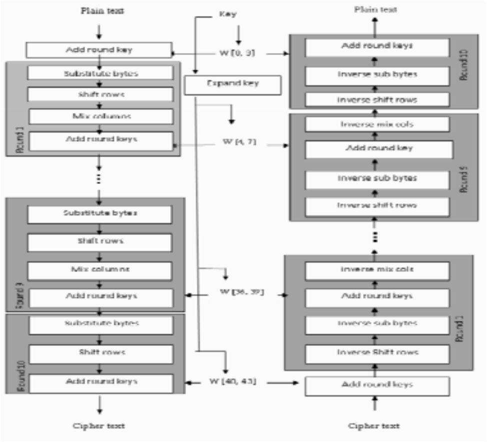


Fig.2 Encryption and decryption in AES

STEP IV: Byte Substitution (SubBytes)

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.

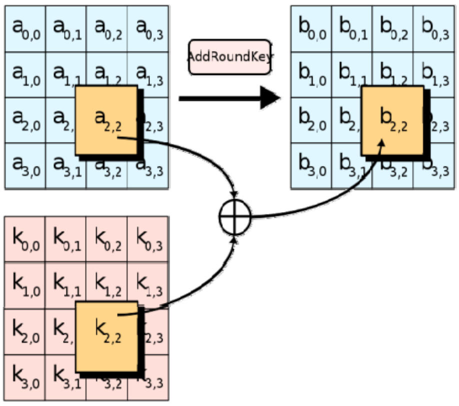

AddRoundKey
$a_{0,0}$ $a_{0,1}$ $a_{0,2}$ $a_{0,3}$
$a_{1,0}$ $a_{1,1}$ $a_{1,2}$ $a_{1,3}$
$a_{2,0}$ $a_{2,1}$ $a_{2,2}$ $a_{2,3}$
$a_{3,0}$ $a_{3,1}$ $a_{3,2}$ $a_{3,3}$
$b_{0,0}$ $b_{0,1}$ $b_{0,2}$ $b_{0,3}$
$b_{1,0}$ $b_{1,1}$ $b_{1,2}$ $b_{1,3}$
$b_{2,0}$ $b_{2,1}$ $b_{2,2}$ $b_{2,3}$
$b_{3,0}$ $b_{3,1}$ $b_{3,2}$ $b_{3,3}$
$k_{0,0}$ $k_{0,1}$ $k_{0,2}$ $k_{0,3}$
$k_{1,0}$ $k_{1,1}$ $k_{1,2}$ $k_{1,3}$
$k_{2,0}$ $k_{2,1}$ $k_{2,2}$ $k_{2,3}$
$k_{3,0}$ $k_{3,1}$ $k_{3,2}$ $k_{3,3}$

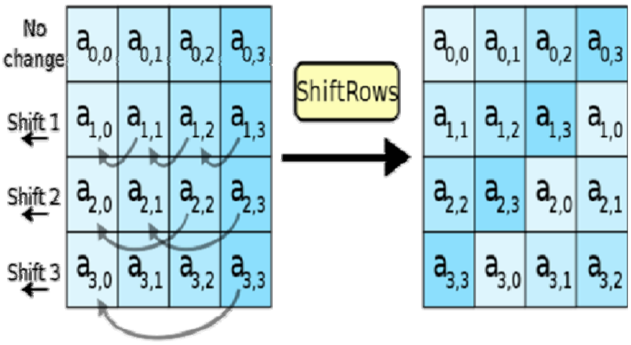
Fig. 3 Byte Substitution (SubBytes)

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.



$a_{0,0}$	$a_{0,1}$	$a_{0,2}$	$a_{0,3}$
$a_{1,0}$	$a_{1,1}$	$a_{1,2}$	$a_{1,3}$
$a_{2,0}$	$a_{2,1}$	$a_{2,2}$	$a_{2,3}$
$a_{3,0}$	$a_{3,1}$	$a_{3,2}$	$a_{3,3}$

$a_{0,0}$	$a_{0,1}$	$a_{0,2}$	$a_{0,3}$
$a_{1,1}$	$a_{1,2}$	$a_{1,3}$	$a_{1,0}$
$a_{2,2}$	$a_{2,3}$	$a_{2,0}$	$a_{2,1}$
$a_{3,3}$	$a_{3,0}$	$a_{3,1}$	$a_{3,2}$

Fig.4 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.

$$\begin{matrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{matrix}$$

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. 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 prepended to the message.

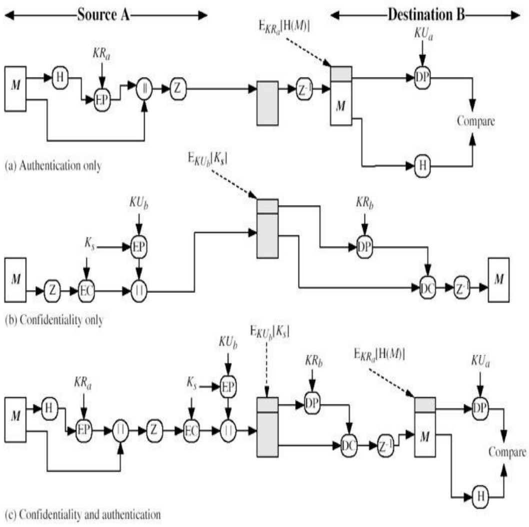


Fig.5 PGP cryptographic functions

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.

C. GENERATION OF SIGNATURE

1. The signature is generated before compression for two reasons:
   (a) It is preferable to sign an uncompressed message so it is free of the need for a compression algorithm for later verification.
   (b) Different versions of PGP produce different compressed forms. Applying the hash function and signature after compression would constrain all PGP implementation to the same version of the compression algorithm.
2. Message encryption is applied after compression to strengthen cryptographic security. Because the

compressed message has less redundancy than the original plaintext, cryptanalysis is more difficult.

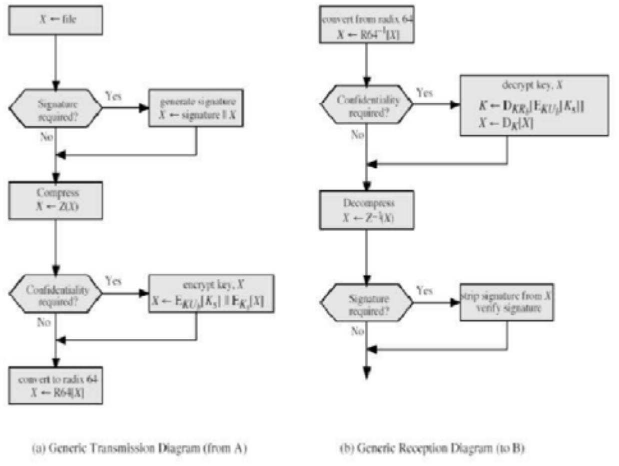

$X \leftarrow$ file
Signature required?
Yes
generate signature $X \leftarrow$ signature $\|$ X
No
Compress $X \leftarrow Z(X)$
Confidentiality required?
Yes
encrypt key, X $X \leftarrow E_{KU_b}[K_s] \| E_{K_s}[X]$
No
convert to radix 64 $X \leftarrow R64[X]$
(a) Generic Transmission Diagram (from A)
convert from radix 64 $X \leftarrow R64^{-1}[X]$
Confidentiality required?
Yes
decrypt key, X $K \leftarrow D_{KR_b}[E_{KU_b}[K_s]]$ $X \leftarrow D_K[X]$
No
Decompress $X \leftarrow Z^{-1}(X)$
Signature required?
Yes
strip signature from X verify signature
No
(b) Generic Reception Diagram (to B)

Fig.6 Transmission and Reception of PGP messages

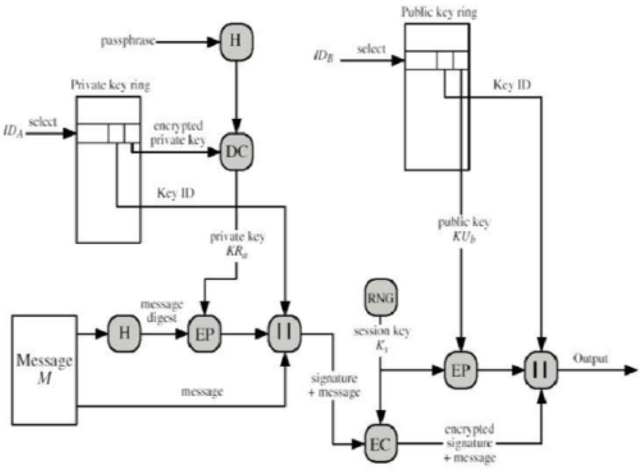


Fig.7 PGP Message generation (from User to storage; no compression or radix64 conversion)

CONCLUSION

- AES is a symmetric key encryption algorithm which essentially means that same key is used for the encryption and decryption of the data.AES is the good method to protect sensitive data stored in large databases [12].

On the other hand, the required memory for AES algorithm is less than the Blowfish algorithm. AES algorithm has a very high security level because the 128, 192 or 256-bit key are used in this algorithm [12].

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 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 to encrypt and decrypt data being transferred across network.

So the combination of AES and PGP 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.

ACKNOWLEDGEMENT

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

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 on 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 2278-6856

[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 2015

[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).