American Journal of Engineering Research (AJER)
e-ISSN: 2320-0847 p-ISSN : 2320-0936
Volume-6, Issue-10, pp-334-337
www.ajer.org
Research Paper Open Access

Using Cryptography Algorithms to Secure Cloud Computing Data and Services

Eng. Hashem H. Ramadan, Moussa Adamou Djamilou
[1]*Master in Computer Science Indian Academy Degree College, Bangalore*
[2]*Master in Computer Science Indian Academy Degree College, Bangalore*

ABSTRACT: *These days regrading to the high demand on usingthe cloud computing services for storing and processing data, there is awareness about the information security and cloud computing. This paper present and take you to see an overview about the cryptography algorithm to detect the best cryptography algorithms for protecting and securing data on cloud computing. In this paper, we are reviewing the asymmetric and symmetric key cryptography with concentration on the symmetric key cryptography with consideration on the best algorithm to use for cloud application and services that require data security.*
Keywords: *Cloud, Cloud Computing, Cryptography, Encryption, Decryption, Security, Symmetric-Key, Asymmetric Key, etc.*

Date of Submission: 13-10-2017 Date of acceptance: 31-10-2017

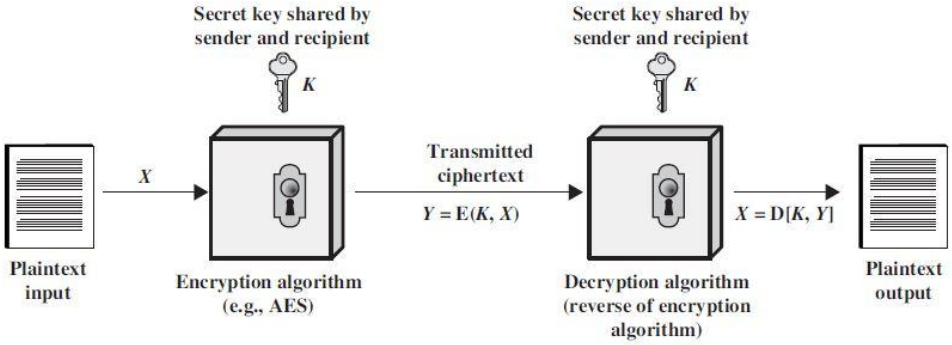
I. INTRODUCTION

Cloud Computing is the process of providing cloud services on the internet. Cloud services allows the organizations and individuals to use the software that managed by cloud services provider. Cloud computing model allow accessing the services and information remotely. Because of moving data to cloud services, organizations are looking for protecting their data against unauthorized access. Securing the cloud means secure the calculation, storage and applications. Security goals located into three points: confidentiality, integrity and availability. Cryptography is caring about the confidentiality of data in the cloud. Cryptography these days is a combination of three algorithms types: (1) Symmetric Key Algorithms (2) Asymmetric Key Algorithms and (3) hashing.

Data cryptography is encoding the content of the data like text and media to make it not understandable, meaningless and invisible during transmission and storage, this term known as encryption. The opposite process of retrieving the original data from encrypted data known as decryption. To encrypt data on cloud storage both symmetric key and asymmetric key can be used, but according to the huge size of the database and data stored in cloud storage using of symmetric key algorithm is faster than asymmetric key.

II. SYMMETRIC KEY CRYPTOGRAPHY

Private Key cryptography is also known as symmetric key cryptography; a secret key may be held by one person or exchanged between the sender and receiver of a message. If private key cryptography used to send secret message between two parties, both the sender and receiver must have a copy of the secret key. However, the key may be compromised during transit. If you know the party you are exchanging messages with, you can give them the key in advance. However, if you need to send an encrypted message to someone, you have never met; you will need to figure out a way to exchange keys in a secure way. One method is to send it via another secure channel [1].



Model of Private Key Encryption

Private Key Encryption Ingredients:

Plain Text Input, This is data and information as the input that will sent to encryption algorithm. It is the original readable message. **Encryption algorithm,** Symmetric encryption algorithms may use stream ciphers or clock ciphers, Steam ciphers encrypt digits once at a time, Block ciphers take number of bits and encrypt them as a single unit. Common unit size is 64 bits, **A**dvanced **E**ncryption **S**tandard **(AES)** is an algorithms used for encrypting 64 bit block. **Secret Key,** it is also an input to the algorithm and it is independent value from plain text and algorithm. The algorithm is generating a new output depending on the secret key provided and known by the sender and receiver.**Cipher Text,** The output of the encryption algorithm. For each different keys, it will produce different cipher text according to the secret key. The cipher text is unintelligible. **Decryption algorithm,** as there is some algorithms for encrypting the data there must be also an algorithm for decrypting the data, this algorithm is commonly will be the reverse of the encryption algorithm. The output must be the plain text input; else, the decryption algorithm is not working correctly [2].

Comparison between DES, TRIPLE DES, AES:

Data Encryption Standard**(DES)** takes 64-bit as plain text and 56-bit as secret key as input and its use 64-bit cipher text as an output. DES strength lies in two factors: first when using 56 bit as a key there are 256 possible keys, second the nature of the algorithm, the cryptanalyst can perform cryptanalysis by exploiting the characteristics of DES algorithm but it is hard to succeed the weakness. DES weakness points locating on if we are using two inputs to an S-box can create the same output;also,the purpose of initial and final permutation is not clear.**3DES**algorithm is an extension of DES algorithm; we are applying the DES algorithm three time with three different keys. Which means that the key length will be three time of the DES key, the length will be (3*56) which will be 168-bit length. The weakness point of 3DES algorithms detected during using three weak keys [3].**AES** (Advanced Encryption Standard) is an encryption algorithms used for protecting data in commercial transaction. It consists of three block ciphers: AES-128, AES-192 and AES-256. Each of these ciphers are 128-bit block size and 128, 192 and 256-bit key size respectively.**AES** is not caring only about the security, even it also improving the performance of setting like hardware implementation. It is faster and stronger than **3DES**. **Rijndael** is an AES-256 algorithm and it is the strongest algorithms because of the key size is stronger than other algorithms [4].

III. ASYMMETRIC KEY CRYPTOGRAPHY

The public key cryptography is a cryptography technique used two different keys, first one for encryption (public key) and the other one for decryption (private key). The public key known to everyone and private key only known by the owner. The public key cryptography has a very good system of verification, such that even a single character change will cause verification to fail.

The Asymmetric encryption do not have key distribution problem but slow compare to the symmetric encryption because they use huge amount of power for their process [5].

Different asymmetric algorithms used like RAS, Diffie Hellman (DH), Elliptic Curve Cryptosystem (ECC), Digital Signature Algorithm (DSA) and El Gamal. The best algorithms in asymmetric are RSA and Diffie Hellman.The most common public key algorithm is RSA, it named for its inventors (Rivest, Shamir, and Adleman) [5]. The algorithm is a one way function, RSA(n,e,x) = x^e mod n where the case of interest is that n is the product of two large primes p and q and gcd(e, ϕ(n)) = 1 [6]. For RSA algorithm n and e together form the public key while d is the private key that is why to compute d is very crucial. RSA is the most widely used asymmetric encryption algorithm and it used for SSL/TLS.

RSA Algorithm:
The RSA algorithm is a cipher in which the plaintext and cipher text are integers between zero and n-1 for some n. It make use of an exponentials, plaintext encrypted in blocks by: $C = M^e \bmod n$ where C is the cipher text and M the plaintext. In the same way the plaintext is obtain by $M = Cd \bmod n$, where d is the private key.

Process of RSA

- Chose two large prime number p and q then calculate n = p*q.
- Select the public key (e), encryption key such that it is not a factor of (p - 1) and (q – 1).
- Select the private key d (decryption key) such that the following equation is true: (d*e)mod(p – 1)(q – 1) = 1.
- For encryption, calculate the cipher text (CT) from the plaintext (PT), $CT = (PT)^e \bmod n$. Send CT to the receiver.
- For decryption: $PT = (CT)^d \bmod n$.

Comparison between RSA and Diffie Hellman

The strength points of **RSA** lies in that algorithm can be applicable for encryption/decryption, digital signature and for key exchange. Itis the most widely used asymmetric encryption algorithm. When you encrypt with a private key, the cipher text can only decrypted with the public key. It used for SSL/TLS (secure sockets layer/transport layer security), for protecting information, you transmit and receive over the Internet, for instance, when you do your online banking or simply log into a website. The biggest obstacle RSA algorithm is once d is determine the cipher text can easily be decrypted.

Diffie Hellman algorithm designed to generate a shared secret key for exchanging information confidentially.DH is one of the earliest, practical examples of public key exchange implemented within the field of cryptography and provides the basis for a variety of authenticated protocols. For example: DH is used to provide perfect forward secrecy in Transport Layer Security's ephemeral modes (referred to as EDH or DHE depending on the cipher suite) [7].The algorithm make used of exponentials module calculation to generate key, which make key secured [6].

IV. PROPOSED SYSTEM

To ensure that data on cloud computing services is secure, one algorithms is not sufficient for encrypting and decrypting data because it is common for hackers. Cryptography of multilevel better than using one algorithm. According to the file size, we need to use combination of algorithms that are compatible to each other. For that, we are going to use a combination of both symmetric and asymmetric algorithms. These algorithms are AES and RSA. First step to encrypt data using the AES algorithm then encrypt using the RSA algorithm after that send the file to the cloud service. We need to ensure also to encrypt the keys used to encrypt the data.

Proposed System Design:

The proposed system designed to provide security to the databases and data uploaded to the cloud storage. This proposed system used AES-256 and RSA encryption algorithms to generate encryption to data before uploading it to the cloud, and it generate decryption to the data before downloading it from cloud. The proposed system design focuses in the following objectives:

1- For encryption of data:

a. Load the data needed to secure to the system.
b. Implement the AES encryption algorithm to generate first level of encryption.
c. Implement the RSA encryption algorithm to generate second level of encryption.
d. Save cipher output from two levels and upload it to cloud storage.

2- For decryption of data:

a. Download the ciphered uploaded data from cloud storage.
b. Implement RSA decryption algorithm to generate first level of decryption.
c. Implement AES decryption algorithm to generate second level of decryption.
d. Read the data after decryption levels.

V. CONCLUSION

Cloud computing is defined as a set of services provided by the cloud service provider to be accessed over the internet. Most of the organization are shifting their data over the cloud, which means that they are using the storage service provided by cloud service providers. Therefore, there is a need to secure the data uploaded over the cloud storage. To ensure about the security of the data over the cloud storage, we are using the cryptography term to secure the data. For that purpose, we are embedding two algorithms from different

cryptography ways to encrypt and decrypt our data. In this paper, we are using the most security algorithms, which are compatible with each other AES and RSA algorithms. The proposed system that we are designing to use multilevel cryptography, first we are encrypting the data using the AES algorithms and then we are encrypting the output from the first level using RSA algorithms then uploading it over the cloud storage.

REFERENCE

[1] Ajit Singh, Rimple Gilhotra, "Data Security Using Private Key Encryption System Based in Arithmetic Coding",International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.3, May 2011.
[2] Book: William Stallings,"Cryptography and Network Security Principles and Practice", Prentice Hall, 2011
[3] http://www.careerride.com/Networking-DES-weakness-and-strength.aspx
[4] http://www.electronicsbus.com/advanced-encryption-standard-aes-encryption-algorithm/
[5] Aman Kumar,Dr.Sudesh Jakhar, Mr Sunil Makka, "Comparative Analysis between DES and RSA Algorithm's", International Journal of Advanced Research in Computer Science and Software Engineering , Vol.2 Issue.7, July- 2012.
[6] Book: William Stalling, "Cryptography and Network Security", 6th Ed.
[7] https://crypto.stackexchange.com/tags/diffie-hellman/info

Eng. Hashem H. Ramadan. "Using Cryptography Algorithms to Secure Cloud Computing Data and Services ." American Journal of Engineering Research (AJER), vol. 6, no. 10, 2017, pp. 334–337.