Journal for Research | Volume 03| Issue 01 | March 2017
ISSN: 2395-7549

Security Based Issues in View of Cloud Based Storage System

Grusha Chouhan
Department of Computer Science & Engineering
Acropolis Technical Campus, Indore, India

Ankit Upadhyay
Department of Computer Science & Engineering
Acropolis Technical Campus, Indore, India

Anuradha Deolase
Department of Computer Science & Engineering
Acropolis Technical Campus, Indore, India

Prashant Lakkadwala
Department of Computer Science & Engineering
Acropolis Technical Campus, Indore, India

Abstract

With growing awareness and concerns regarding to cloud computing and information security, there is a growing awareness and usage of security algorithms into data systems and processes. Confidentiality means the data is understandable to the receiver only for all others it would be waste; it helps in preventing the unauthorized disclosure of sensitive information. Integrity means data received by receiver should be in the same form, the sender sends it; integrity helps in preventing modification from unauthorized user. Availability refers to assurance that user has access to information anytime and to any network. In the cloud confidentiality is obtained by cryptography. Cryptography is technique of converting data into unreadable form during storage and transmission, so that it appears waste to intruders. In the cloud integrity can be checked using a message authentication code (MAC) algorithm. Also by the help of calculating the hashing value. But both methods are not practically possible for large amount of data. Here symmetric algorithms (like IDEA, Blowfish, and DES) and asymmetric algorithms (like RSA, Homomorphic) are used for cloud based services that require data encryption. While sending data and during storage data is under threat because any unauthorized user can access it, modify it, so there is need to secure data. Any data is secure, if it fulfills three conditions i.e., Confidentiality, Integrity and Availability. There is a need to find a way to check data integrity while saving bandwidth and computation power. Remote data auditing, by which the data integrity or correctness of remotely stored data is investigated, has been given more attention recently.

Keywords: Cloud Computing, Information Security, Security Based Issues

---

I. INTRODUCTION

Cloud computing is mainly used for data storage. Here the data is stored on multiple third-party servers [2]. The user sees a virtual server; it appears as if the data is stored in a particular place with a specific name, when storing the data. This doesn't exist in reality. It's just used to reference the virtual space of the cloud. In reality, the user's data could be stored on any one or more of the computers used to create the cloud. Three important conditions for the data security over the cloud are (i) Confidentiality [8], (ii) Integrity [4], (iii) Availability [5][8]. Understanding cloud security risks is related to understanding the relationships and dependencies between cloud computing models and how they are deployed. IaaS[5][9] forms the foundation of the service model architecture, PaaS builds upon IaaS, and SaaS[5][9] in turn builds upon PaaS[5][9]; and information security issues and risks are inherited just as capabilities are.

Cloud allows users to achieve the power of computing which beats their own physical domain. It leads to many security problems. The cloud service provider for cloud makes sure that the customer does not face any problem such as loss of data or data theft. Cloud computing infrastructures use new technologies and services, most of which haven't been fully evaluated with respect to security [9].

Cryptography can be seen as a method of storing and disguising confidential data in a cryptic form so that only those for whom it is intended can read it and are able to communicate information in the presence of an adversary and the security algorithms mitigate security issues by use of cryptography, authentication and distributing keys securely. Cryptography is thus the science of making data and messages secure by converting the end user data to be sent into cryptic non-readable form and encrypting or scrambling the plaintext by taking user data or that referred to as clear text and converting it into cipher text and then performing decryption which is reverting back to the original plain text. Cryptography is used for providing the following security:

- Data Integrity: information has value only if it is correct, this refers to maintaining and assuring the accuracy and consistency of data, its implementation for computer systems that store use data, processes, or retrieve that data [4].
- Authentication for determining whether someone or something is, in fact, who or what it is declared to be [3].
- Non Repudiation: is the assurance that a party, contract or someone cannot deny the authenticity of their signature and sending a message that they originated [2].

– Confidentiality: relates to loss of privacy, unauthorized access to information and identity theft [8].

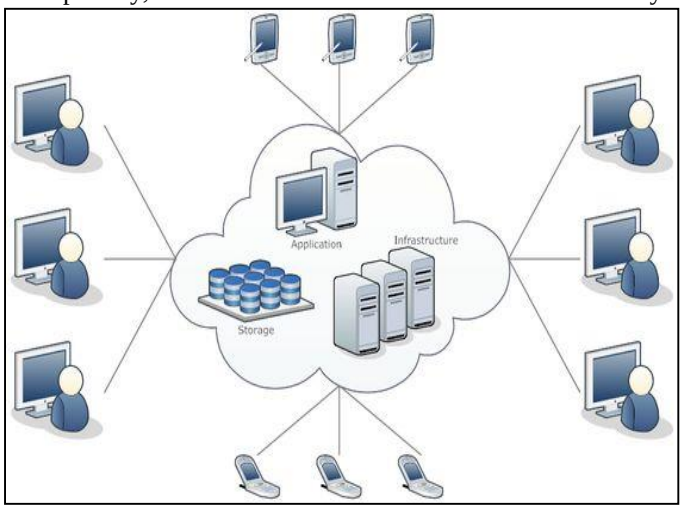

Fig. 1: Cloud Computing Solutions

II. SECURITY CONCERNS

The security concerns are end user data security, network traffic, file systems [7], and host machine security which cryptography can resolve to some extent and thus helps organizations in their reluctant acceptance of Cloud Computing [7]. There are various security issues that arise in the Cloud:

– Ensuring Secure Data Transfer: In a Cloud environment, the physical location and reach are not under end user control of where the resources are hosted [8].
– Ensuring Secure Interface: integrity of information during transfer, storage and retrieval needs to be ensured over the unsecure internet [8].
– Have Separation of data: privacy issues arise when personal data is accessed by Cloud providers or boundaries between personal and corporate data do not have clearly defined policies.
– Secure Stored Data: question mark on controlling the encryption and decryption by either the end user or the Cloud Service provider.
– User Access Control: for web based transactions (PCI DSS), web data logs need to be provided to compliance auditors and security managers [8].

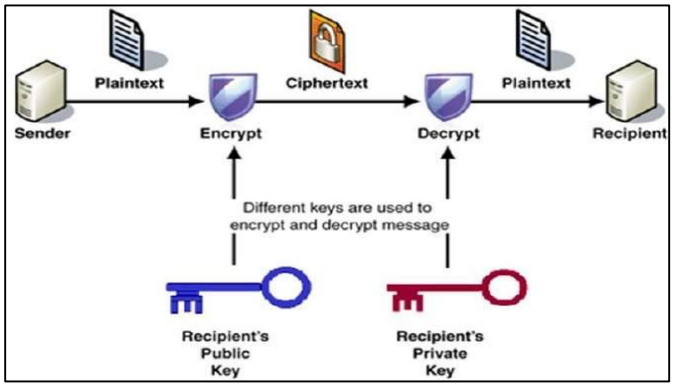

Fig. 2: Asymmetric encryption-decryption for communication

III. SECURITY ALGORITHMS

Security algorithms which are used for cryptography [1][10] are classified in three categories:

– Hash key algorithms: Compress data for signing to standard fixed size. Examples include: MD5, SHA
– Private Key / Symmetric Algorithms: Use single secret key for encrypting large amount of data and have fast processing speed. These algorithms use a single secret key that is known to the sender and receiver. RC6, 3DES, Blowfish, AES are some examples of this algorithms [6][7].
– Public Key [8] / Asymmetric Algorithms: Use a key pair for cryptographic process, with public key for encryption and private for decryption. These algorithms have a high computational cost and thus slow speed if compared to the single key symmetric algorithms. RSA and Diffie-Hellman are some types of public key algorithms [6][7].

IV. ALGORITHMS

- Data Encryption Standard (DES)
- Triple- DES (TDES)
- Blowfish Algorithm
- IDEA
- Homomorphic Encryption
- RSA
- Diffie- Hellman Key Exchange

A. Data Encryption Standard (DES)

DES is very commonly used symmetric key algorithm.[6] It was developed by IBM in 1974, but now a day's many methods are found that had proven this algorithm unsecured. A block cipher is a method of encryption text (to produce cipher) in which a cryptographic key and algorithm are applied to a block of data (for ex: - 64 contiguous bits) at once as a group rather than to one bit at a time. The main alternative method, used much less frequently is called "Stream Cipher". In DES algorithm block cipher is of 64 bits and key used are 56 out of 64 bits.

1) Algorithm

Step 1:- The 64-bit plain text block is handed over to an INITIAL PERMUTATION (IP) function.
Step 2:- The initial permutation is performed on plain text.
Step 3:-Next, The initial permutation (IP) produces two halves of the permuted block i.e., Left Plain Text (LPT) and Right Plain Text (RPT).
Step 4:-Now, each of LPT and RPT go through 64 rounds of encryption process, each with its own key.
Step 5:-In the end, LPT and RPT are rejoined, and a FINAL PERMUTATION (FP) is performed on the combined block.
Step 6:-The result of this process produces 64-bit cipher text.

B. Triple- DES (TDES)

TDES is enhanced version of DES in TDES the key size is increased to increase i.e. 168 bits the security of data. In TDES only size of key is increased rest of the working is similar to DES. In TDES three different keys are applied on cipher block i.e. k 1, k 2 and k 3. [6][10]

1) Algorithm

Step 1:- Encrypt the plain text with key K1. Thus, we have $E_{k1}(P)$.
Step 2:-Decrypt the output of step1 above with key K2. Thus, we have $D_{k2}(E_{k1}(P))$.
Step 3:-Finally, Encrypt the output of step 2 again with key K1. Thus, we have $E_{k1}(D_{k2(}E_{k1}(P)))$.

C. Blowfish Algorithm

Blowfish Algorithm is a symmetric key algorithm [6] which was developed in 1993 by Bruce Schneier. In DES key size is small and can be decrypted easily but in Blowfish algorithm the size of key is large and it can vary from 32 to 448 bits. In Blowfish algorithm also 64 bits of plain text is divided into two parts of size 32 bits.

1) Algorithm

Step 1:- Divide X into two blocks: XL and XR, of equal sizes. Thus, both XL and XR will consist of 32 bits each.
Step 2:- For i=1 to 16
XL=XL XOR Pi
XR=F (XL) XOR XR
Next i
Step 3:- Swap XL, XR (i.e. undo last swap).
Step 4:- XL=XL XOR P18.
Step 5:- Combine XL and XR back into X.

D. IDEA

International Data Encryption Algorithm was proposed by James Massey and Xuejia Lai in 1991.It is considered as best symmetric key algorithm. It accepts 64 bits plain text and key size is 128 bits.

1) Algorithm

Step 1:-The 64-bit input plain text block is divided into four portions of plain text (each of size 16 bits), P1 to P4.Thus, P1 to P4 are the inputs to the first round of the algorithm. There are eight such rounds. The keys consist of 128 bits.
Step 2:-In each round, six sub keys are generated from the original key. Each of sub keys consists of 16 bits. These six sub keys are applied are applied to the four input blocks P1 to P4. Thus, for the first round, we will have the six keys k1 to k6. For the second round we will have k7 to k12.Finally, for the eight round we will have keys k43 to k48.
Step 3:-The final step consists of an OUTPUT TRANSFORMATION, which uses four sub keys (k49-k52).

Step 4:-The final output produced is the output produced by the output transformation step, which is four blocks of cipher text named C1 to C4 (each consisting of 16 bits).
Step 5:-These are combined to form the final 64-bit cipher-text block.

E. Homomorphic Encryption

Homomorphic encryption uses asymmetric key algorithm in which two different keys are used for encryption and decryption i.e. public key and private key . In mathematics homomorphic means conversion of one data set to another, without losing its relation between them. In homomorpic complex mathematics functions are applied to encrypt the data and similar but reverse operation is applied to decrypt the data.

F. RSA

RSA was invented by Ranold Fivest, Adi Shamir [3] and Leonard Adleman in 1977. RSA is also an asymmetric algorithm. [6][10] Functioning of RSA is based on multiplication of two large numbers. Two large prime numbers are generated and multiplied. After multiplying two numbers, modulus is calculated the number that is generated is used as the public and private key. The two numbers that are used for multiplication-one of them is public other is private.

1) Algorithm

Step 1:-Choose two large numbers P and Q.
Step 2:-Calculate N+P*Q.
Step 3:-Select the public key (i.e. the encryption key) E such that it is not a factor of (P-1) and (Q-1).
Step 4:-Select the private key (i.e. the decryption key) D such that the following equation is true:
(D*E) mod (P-1)*(Q-1)=1
Step 5:-For encryption, calculate the cipher text t CT from the plain text PT as follows:
$CT=PT^E \bmod N$
Step 6:-Send CT as the cipher text to the receiver.
Step 7:-For decryption, calculate the plain text PT from the cipher text CT as follows: $PT=CT^D \bmod N$

G. Diffie- Hellman Key Exchange

Diffie Hellman key exchange algorithm was developed by Whitfield Diffie and Martin Hellman in 1976. Diffie Hellman also required two different keys [6]. In Diffie Hellman Key Exchange, a shared secret key established, that is used that is used for communication over the public network [10].

1) Algorithm

Step 1:-Firstly, Alice and Bob agree on two large prime numbers, n and g. These two integers need not be kept secret. Alice and bob can use an insecure channel to agree on them.
Step 2:-Alice chooses another large random number x, and calculates A such that:
$A=g^x \bmod n$
Step 3:-Alice sends the number A to Bob.
Step4:-Bob independently chooses another large random integer y and calculates B such that:
$B=g^y \bmod n$
Step 5:-Bob sends the number B to Alice.
Step 6:-A now computes the secret key k1 as follows:
$K1=B^x \bmod n$
Step 7:-B now computes the secret key K2 as follows:
$K2=A^y \bmod n$

V. CONCLUSIONS

The system will contribute in the designing and development of a user space cryptographic file system. The design goal will mainly focus on the security of the file system. The system will be very convenient to the user and the independenbility will be achieved with the help of java technology which is highly portable.

REFERENCES

[1] "Cloud Security Algorithms" International Journal of Security and its Applications, Vol. 9, No.10 (2015), pp.353-360
[2] Dr. NEDHAL A. AL-SAIYD, NADA SAIL "Data Integrity in Cloud Computing Security" Journal of Theoretical and Applied Information Technology, Vol. 58 No. 3, December 2013
[3] Mandar Kadam, Stewyn Chaudhary, Bony Carvalho, "Security Approach for Multi-Cloud Data Storage" International Journal of Computer Applications (0975-8887) Volume 126-N0.4, September 2015
[4] "Identifying Data Integrity in the Cloud Storage" International Journal of Computer Science Issues, Vol. 9, Issue 2, No 1, March 2012
[5] "TREM: A New Cloud Security Algorithm" International Journal of Advanced Research in Computer and Communication Engineering Vol. 5, Issue 4, April 2016
[6] Randeep Kaur , Supriya Kinger "Analysis of Security Algorithms in Cloud Computing" International Journal of Application or Innovation in Engineering & Management (IJAIEM) Volume 3, Issue 3, March 2014

[7] S. P. Jaikar, M. V. Nimbalkar, "Verifying Data Integrity in Cloud", International Journal of Applied Information Systems Volume 3– No.1, July2012
[8] Sultan Aldossary, William Allen "Data Security, Privacy, Availability and Integrity in Cloud Computing: Issues and Current Solutions" International Journal of Advanced Computer Science and Applications, Vol. 7, No. 4, 2016
[9] "Security Issues and Security Algorithms in Cloud Computing" International Journal of Advanced Research in Computer Science and Software Engineering Volume 2, Issue 10, October 2012
[10] "Security Algorithms for Cloud Computing" International Conference on Computational Modeling and Security (CMS 2016), Procedia Computer Science 85 (2016) 535 – 542
[11] Upadhyay and P. Lakkadwala, "Secure live migration of VM's in Cloud Computing: A survey," Reliability, Infocom Technologies and Optimization (ICRITO) (Trends and Future Directions), 2014 3rd International Conference on, Noida, 2014, pp.1-4.doi: 10.1109/ICRITO.2014.7014766.
[12] Upadhyay, A.; Lakkadwala, P., "Performance evolution of higher reliability task in cloud computing," 2014 Conference on IT in Business, Industry and Government (CSIBIG), vol., no., pp.1,3, 8-9 March 2014 doi: 10.1109/CSIBIG.2014.7056956.
[13] Palkesh Soni, Ankit Upadhyay, Arvind Maheshwari and Prashant Lakkadwala, "Security Related Issues in Cloud Computing: A Survey", IJIRST – International Journal for Innovative Research in Science & Technology| Volume 2 | Issue 11 | April 2016 ISSN (online): 2349-6010.