Security of Data Storage in Cloud Computing

Tania Gaur
M. Tech (CSE) Student
ITM University

Nisha Kharb
Assistant Professor
ITM University

ABSTRACT
With the advent of Information Technology in day-to-day activities, the need for online services such as storage space, software, platforms etc. is increasing rapidly. This lead to the rise of a new concept, the Cloud Computing. The Internet users rely heavily on the Cloud Computing for various computing resources. The main motive of the Cloud Providers is to provide these services in a virtualized manner. One of the main concern of cloud computing is the security of the Cloud Storage. When it comes to security of the data stored in the Cloud Storage, it is entirely in the hands of the Cloud Providers. The Cloud Providers assures the consumer of the Cloud that the data stored on their servers is safe. The consumer plays no role in securing the data. The various cloud providers claim that they provide highly secure cloud storage. But there have been attacks on hot-shot cloud providing companies such as Google, Salesforce.com and Dropbox[1]. Many cloud providers employee third party companies which has led to consumer losing their trust with these companies. Thus, the encryption techniques and the various security measures employed by the cloud providers should be equally strong. The privacy and security of cloud computing depend primarily on whether the provider has implement adequate and robust security controls as desired by the customer or not. In this paper we analyze the different security issues related to the cloud and different cryptographic algorithms to secure the cloud.

Keywords
Cloud, security, storage, cryptography, security issues.

1. INTRODUCTION
Cloud Computing

Cloud Computing is a new term for an old concept. While using a system, a user can store, retrieve, modify and update the contents of that particular system. But if such activities are performed over the internet, it is known as Cloud Computing.

"Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction[2]."

Cloud computing aims to cut down the operational and capital costs and thereby allowing the IT departments focus on strategic projects instead of working to keep the storage secure and running. Cloud computing comes with these characteristics : *on-demand self-service, broad network access, resource pooling, rapid elasticity and measured Service*

Cryptography

Cryptography is a technique of ensuring a secured communication between a sender (say Alice) and a receiver (say Bob). The message sent from Alice is encrypted with the help of a key and an encryption algorithm. This encrypted text, known as cipher text, is decrypted at the receiving side with the help of the same key (Symmetric key Cryptography), or different key (Asymmetric Key Cryptography) and a decryption algorithm. When a message is being sent from Alice to Bob, the privacy of the message is jeopardized during its transmission. A third party intruder can intercept the message, change the contents of the message, block the message or impersonate someone else and use the message for its own advantage. Cryptographic techniques[3] are used to handle such security issues.

SECURITY GOALS

The cloud computing is deployed as one of the four models:- private cloud, public cloud, community cloud and hybrid cloud. The providers of the cloud provide the cloud services in various forms [4]:- Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS) and Infrastructure-as-a-Service(IaaS). There are many security issues for cloud computing as it embraces various technologies including databases, virtualization, operating systems, networks, resource scheduling, concurrency control, transaction management and memory management. Therefore, security issues for many of these systems and technologies are applicable to cloud computing. The various security concerns relating to cloud computing are given below:-

i. *Confidentiality* - refers to protecting our confidential information. Cloud providers need to guard such information from malicious actions that jeopardize the privacy of the data.

ii. *Message Integrity* - refers to the fact that the contents of a given message can only be altered by an authorized user and through authorized mechanisms.

iii. *Availability* – the data stored in the cloud should be available at all times to the authorized entities. Information is useless if it is not available.

2. SECURITY ISSUES
i. *Abuse and Nefarious Use of Cloud Computing*- the cloud computing provides an illusion of unlimited computing resources to its users. Any user can register and start exploiting the cloud services. This makes it easy for the wrong-doers namely, spammers, malicious insiders and other criminals that can perform their activities within this anonymity of registration.

ii. *Insecure Interfaces and APIs* – the cloud interacts with its customers with the help of APIs. The security and availability of cloud services depends on these APIs. Insecure interfaces may lead to dire consequences.

iii. *Malicious Insiders* – a malicious insider in an organization can lead to its doom. a provider may not reveal how it grants employees access to physical and virtual assets, how it monitors these

employees, or how it analyses and reports on policy agreements. The transparency between cloud provider and cloud customer is therefore a must in this situation.

iv. *Shared Technology Issues* – cloud computing is based on virtualization. A cloud consumer has no clue as to which continent or which physical location his data is stored. Each country could have its own security policy. As a result, attackers focus on how to impact the operations of other cloud customers, and how to gain unauthorized access to data.

v. *Data Loss or Leakage* – loss of an encoding key may lead to loss of essential data, unauthorized parties gaining access to private data and thereby preventing access by the authorized entities, etc. are a few scenarios where data loss or leakage of data may occur.

vi. *Account or Service Hijacking* - Attack methods such as fraud, phishing and exploitation of software vulnerabilities still achieve results. Authorized data and passwords are often reused, which increases the effect of such attacks.

vii. *Unknown Risk Profile* – cloud computing reduces the hardware and software ownerships and maintenance to allow companies to focus on their core business. The security policies should be clearly stated by the cloud provider to its customer.

3. ALGORITHMS

The existing algorithms for data storage security studied in this paper are as follows:

3.1 Symmetric Key Encipherment[6](to Provide for Confidentiality and Integrity of the Message)

This cryptographic technique makes use of two separate algorithms for encryption and decryption respectively, and a key that is shared by the sender and the receiver. The original message is known as plaintext and the encrypted message is known as the ciphertext. Sender uses the encryption algorithm and a "key" to convert a plaintext into a ciphertext and sends through a medium. The receiver converts the ciphertext into a plaintext with the help of a decryption algorithm and the same "key" that was used for encrypting the message.

Encryption: $C=E_k(P)$ Decryption : $P=D_k(C)$

And $D_k(E_k(x))=E_k(D_k(x))=x$

3.1.1 DES

DES is a symmetric key block cipher that is used to ecrypt/decrypt 64 bits of a block data. The encryption process is made up of two permutations known as the intial and the final permutation and sixteen Fiestel rounds. Each round employees a 48-bit round key generated by the Round-key-generator. The initial and final permutations refer to the P-boxes that take a 64-bit input and apply permutation on them according to a predefined rule. Each round of a DES is a Fiestel cipher. Each round has two cipher elements- mixer and swapper. The DES function is the core of the DES. It applies a 48-bit key to the rightmost 32-bits to generate a 32-bit output. DES function consists of- expansion D-box, a whitener, a group of S-boxes and a straight D-box.

3.1.2 AES

AES is also a symmetric-key block cipher that is used to encrypt/decrypt a data block of 128 bits. The size of the key in AES can be 128, 192 or 256 bits, depending on the number of rounds (10, 12 or 14 respectively). It is a non-Fiestel cipher. Each round in AES, except the last round, consists of four transformations that are invertible. The last round has only three transformations. (1) KeyExpansions-round keys are derived from the cipher key using Rijndael's key schedule. AES requires a separate 128-bit round key block for each round plus one more. (2)InitialRound-AddRoundKey—each byte of the state is combined with a block of the round key using bitwise xor. (3)Rounds- (3.1)SubBytes—a non-linear substitution step where each byte is replaced with another according to a lookup table.(3.2)ShiftRows—a transposition step where the last three rows of the state are shifted cyclically a certain number of steps. (3.3)MixColumns—a mixing operation which operates on the columns of the state, combining the four bytes in each column. (3.4)AddRoundKey. (4)Final Round (no MixColumns)- (4.1)SubBytes (4.2)ShiftRows(4.3)AddRoundKey[16].

3.2 Asymmetric Key Encipherment (to Provide for Confidentiality and Integrity of the Message)

This cryptographic technique makes use of two separate algorithms for encryption and decryption respectively, a separate key for encryption and a separate key for decryption. The sender encrypts the message using the public key of the sender. The receiver decrypts the cipher text with the help of a private key.

3.2.1 RSA

RSA[9] is a public key algorithm that uses modular exponentiation for encryption/decryption. It uses two exponents, e and d, where e is public and d is private. To attack it, an intruder needs to calculate $\sqrt[e]{C}$. The general idea of RSA algorithm is given below:

Key Generation

Select p, q	p,q both prime $p \neq q$
Calculate n=pxq	
Calculate $\varphi(n) = (p-1)x(q-1)$	
Select integer e	$gcd(\varphi(n),e)=1; 1<e<\varphi(n)$
Calculate d	
Public key	Kpublic={e,n}
Private key	Kprivate={d,n}

Encryption

Plaintext	M<n
Ciphertext	$C = M^e \pmod n$

Decryption

Ciphertext	C
Plaintext	$M=C^d \pmod n$

3.2.2 Diffie-Helman Key Exchange [7].

In Diffie-Hellman protocol, two parties create a symmetric session key without the need of a Key-Distribution-Center (KDC). Prior to creating a symmetric key, the two parties need to choose two numbers p and g. These two need not be

confidential. They can be public, i.e these can be sent through the Internet. The steps involved in the Diffie-Hellman method are as follows:

SENDER

1. Picks a secret number "a"
2. Calculate "A" using the following

   (values of g and p are predetermined)

   $g^a \bmod p = A$
3. Send "A" to Receiver
4. Receive "B" from Receiver
5. Calculate the shared secret using the following

   $B^a \bmod p = S_{AB}$

RECEIVER

1. Picks a secret number "b"
2. Calculate "B" using the following

   (values of g and p are predetermined)

   $g^b \bmod p = B$
3. Send "B" to Sender
4. Receive "A" from Sender
5. Calculate the shared secret using the following

   $A^b \bmod p = S_{AB}$

3.3 Digital Signature [8](to Prove the Authenticity of the Sender)

RSA Digital Signature is used to provide privacy. The concept of RSA can also be used for signing and verifying a message. The digital signature scheme changes the roles of private and public keys. First, the private and the public keys of the sender, not receiver, are used. Second, the sender uses her own private key to sign the document; the receiver uses the sender's public key to verify it. The general idea of the RSA digital signature scheme is given below:

Key Generation

Select p, q	p,q both prime $p \neq q$
Calculate n=pxq	
Calculate $\varphi(n) = (p-1)x(q-1)$	
Select integer e	$gcd(\varphi(n),e)=1; 1<e<\varphi(n)$
Calculate d	$exd=1 \bmod \varphi(n)$
Public key	Kpublic={e,n}
Private key	Kprivate={d,n}

Signing

Create signature	S=Md mod n; send message and signature to Receiver

Verifying

$M' \equiv M \pmod n \longrightarrow S^e \equiv M \pmod n \longrightarrow M^{dxe} \equiv M \pmod n$

4. CONCLUSION

In today's scenario, Cloud computing is emerging rapidly. More and more organizations as well as users are willing to move towards cloud computing. Thus, the security of the cloud becomes even more important in this situation. This paper points out various issues that need to be addressed when it comes to cloud computing. It also discusses various cryptographic algorithms that are used to secure the cloud storage. DES is the most basic cryptographic algorithm to implement. AES algorithm is the next step beyond DES algorithm. RSA and Diffie-Hellman are the asymmetric algorithms that can be used to ensure confidentiality while sharing data. Digital Signature can be used to prove the authenticity of the sender. Though the cloud providers employ many security measures, still they lack somewhere when it comes to earning the trust of the cloud consumers. A proposal could, thus, be considered to provide basic security features on the client side.

5. REFERENCES

[1] Chou, Te-Shun. "Security Threats On Cloud Computing Vulnerabilities."International Journal of Computer Science & Information Technology (IJCSIT) Vol 5 (2013).

[2] Mell, Peter, and Tim Grance. "The NIST definition of cloud computing."National Institute of Standards and Technology 53.6 (2009): 50.

[3] Khan, Miss Shakeeba S., and Miss Sakshi S. Deshmukh. "Security in Cloud Computing Using Cryptographic Algorithms." (2014).

[4] Hashemi, Sajjad. "DATA STORAGESECURITY CHALLENGESIN CLOUD COMPUTING."

[5] Hubbard, Dan, and Michael Sutton. "Top Threats to Cloud Computing V1. 0."Cloud Security Alliance (2010).

[6] Behrouz, A. Forouzan, and Mukhopadhay Debdeep. "Cryptography and network security." McGramHill, International Edition (2008).

[7] Tirthani, Neha, and R. Ganesan. "Data Security in Cloud Architecture Based on Diffie Hellman and Elliptical Curve Cryptography." IACR Cryptology ePrint Archive 2014 (2014): 49.

[8] Somani, Uma, Kanika Lakhani, and Manish Mundra. "Implementing digital signature with RSA encryption algorithm to enhance the Data Security of cloud in Cloud Computing." Parallel Distributed and Grid Computing (PDGC), 2010 1st International Conference on. IEEE, 2010.

[9] Garg, Preeti, and Vineet Sharma. "An efficient and secure data storage in Mobile Cloud Computing through RSA and Hash function." Issues and Challenges in Intelligent Computing Techniques (ICICT), 2014 International Conference on. IEEE, 2014.

[10] Friedman, Allen A., and M. Darrell. "West. Privacy and security in cloud computing." Issues in Technology Innovation 3.

[11] Ashktorab, Vahid, and Seyed Reza Taghizadeh. "Security Threats and Countermeasures in Cloud Computing." International Journal of application or Innovation in Engineering & Management (IJAIEM) 1.2 (2012): 234-245.

[12] , Ankur, et al. "Cloud Computing Security." International Journal on Recent and Innovation Trends in Computing and Communication 1.1 (2013): 36-39.

[13] Padhy, Rabi Prasad, Manas Ranjan Patra, and Suresh Chandra Satapathy. "Cloud Computing: Security Issues and Research Challenges." International Journal of Computer Science and Information Technology & Security (IJCSITS)1.2 (2011).

[14] Kumar, Arjun, et al. "Secure storage and access of data in cloud computing." ICT Convergence (ICTC), 2012 International Conference on. IEEE, 2012.

[15] Xiao, Zhifeng, and Yang Xiao. "Security and privacy in cloud computing." Communications Surveys & Tutorials, IEEE 15.2 (2013): 843-859.

[16] www.wikipedia.com

[17] Liu, Wentao. "Research on cloud computing security problem and strategy." Consumer Electronics, Communications and Networks (CECNet), 2012 2nd International Conference on. IEEE, 2012.