Data Security in Cloud through Confidentialit and Authentication

MS. Roshani Ishwarlal Patel[1] Rachana S. Oza[2]
[1]M.Tech Student [2]Assistant Professor
[1,2]Department of Information Technology & Computer Engineering
[1,2]CGPIT, Maliba Campus, UTU, Bardoli

Abstract— Cloud computing is new computing paradigm that lays on concept of sharing of recourses rather than having local server or personal devices to handle applications. Current issues in cloud are the data modified by administrator having malicious nature or uploading virus affected file on cloud. There is a possibility of an attack while uploading a file on cloud. Different encryption algorithms are used to secure the data in cloud. To provide more security on data from attacker one can choose authentication technique with encryption algorithm. In this paper, various techniques for protecting data using above discussed method are listed. Amongst all technique application of encryption algorithm with the authentication is giving best results. All the discussed techniques are implemented by a researchers on a cloud like test bad and encrypt the data using AES encryption algorithm and authenticate data using Digital Signature is better in all technique.

Keywords: Cloud Computing, AES algorithm, Digital Signature

I. INTRODUCTION

Cloud computing is a type of computing that allows sharing computing resources rather than having local servers or personal devices to handle applications Cloud provides access via Internet to process power, storage, software or other computing services.

Cloud computing is a significant advancement in the delivery of information technology and services. Cloud computing is referred to a model of network computing where program or application runs on a connected servers rather than on a local computing device. A cloud computing technology is quite often used now a days to store data and compute data as and when required. Cloud computing is a term that describes a broad range of services. There are different types of cloud depending on needs. This includes private cloud, public cloud, community cloud and hybrid cloud. Public cloud can be accessed using internet connection by any subscriber. Google and Microsoft provide public cloud. A private cloud is build for specific group or organization with access limited to that group. Community cloud is shared among organization with similar cloud requirements. Hybrid cloud is a combination of at least any of two cloud type. According to the type of services provided cloud computing is classified into three categories.

- Software as a Service (SAAS)
- Platform as a Service (PAAS)
- Infrastructure as a service (IAAS)

1) SAAS: Users can access a software application hosted by the cloud vendor on pay-per-use basis. SAAS applications are designed for end-users, delivered over the web. It increases security risk as anyone can access from anywhere. In SAAS cloud there are two types of Cloud, which delivers software applications to the users. The first group offers the entire application as a service to the end users. Example is Google office automation service, like Google Document or Google Calendar. The second group provides on-demand web services to the users.
2) PAAS: is a development platform that supports the full "Software Lifecycle" which allows cloud consumers to develop their cloud services and applications directly on the PAAS cloud. This cloud service model requires strong authentication to identify users. Example is Microsoft.
3) IAAS: This could include some kind of storage services (database or disk storage) or virtual servers. This service model manages an applications, data operating system, middleware and runtime. Data encryption is a key requirement. Example is Amazon.

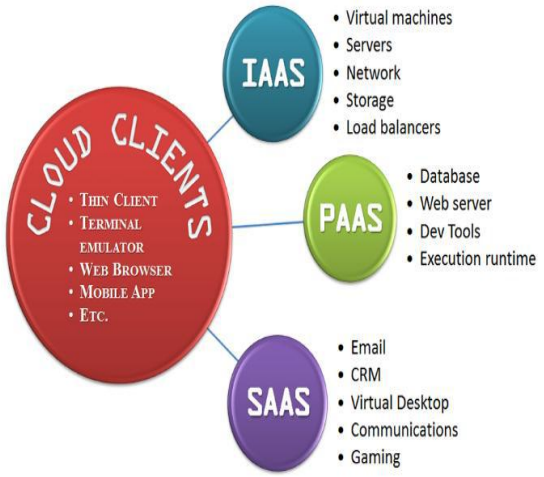

Fig.1: Services Model Of Could Computing

A. Data security Challenges in Cloud:

Storage and uploading of data on cloud is one of the main issues from security point of view. If your data is not encrypted then any one is able to read your files. So security is major concern in cloud. Various types of attack also affect the data file in cloud computing.

1) Insider attack: The attacker having authorized system access carries out the malicious attack.
2) Flooding Attacks: Data transmission between client and server may secure but attacker might choose to attack on cloud directly.
3) Man-In-The-Middle Attacks: This attack is carried out when an attacker places himself between two users. Anytime attackers can place themselves in the communication's path, there is the possibility that they can intercept and modify communications.
4) Authentication Attacks: IAAS offers information protection and data encryption. If the transmitted

data is categorized to high confidential for any enterprise, the cloud computing service based on IAAS architecture will be the most suitable solution for secure data communication.

5) Password Discovery Attacks: Attackers adopt several mechanisms to retrieve passwords stored or transmitted by a computer system to launch this attack.

1) Various Password Attacks Are Following:

- Brute Force Attack: The attacker tries to make all possible combinations of letters and numbers by guessing the probable password.
- Dictionary Attack: Here the attacker tries to guess a password from a pre-computed dictionary of password
- Video Recording Attack: In such type of attack with the help of camera equipped mobile phones attacker captures the password while the victim enters the same.

1) Confidentiality and privacy issue: Confidentiality refers to only authorized parties or systems having the ability to access protected data. Various types of confidentiality are electronic Confidentiality, Software Confidentiality important for overall system Confidentiality. security. Privacy is requiring for protecting personal information. if any personal information are stored at service provider server instead of store at company server then more security is require to protecting information so privacy issue is occur.
2) Integrity issue: Integrity is key aspects of information security. Integrity means data or information are modified by authorize person having malicious nature or unauthorized user. Data Integrity and Software Integrity refers to protecting data from unauthorized deletion, modification.
3) Data loss issue: An important security risk of cloud models In any business area the business data and customer information are stored at cloud. Data in cloud are access by authorized user and external hacker. Authorized user can access data intentionally or accidently but external hacker access data to create some problem.

2) Solution:

If data stored in a cloud are handled by untrusted parties which may cause insecurity of data. In order to solve this problem one have to take measures to make the data secure for that there exist many security measures for the data stored on cloud to secure information on cloud from various types of attack and issues. In cloud before storing data, encrypt the data with various types of encryption algorithms such as DES, Triple DES, AES, RSA etc, and authenticate data using authentication technique such as SHA, SHA512, MD5, Digital Signature etc at server said and decrypt at receiver said then the data is secure in cloud.

II. RELATED WORK

A. Through Encryption & Decryption:

In cloud anyone can uploaded and downloaded data so that more security is require. Many encryption algorithms are used to secure data such as DES, 2DES, AES, RSA. Using these algorithms we encrypt and decrypt the data and securely access the data.

Data Encryption Standard (DES) was symmetric-key algorithm for the encryption of data. DES is proposed by IBM in 1970. Using DES we encrypt the data but now days it's a insecure because of its small key size. DES uses a 56-bit key which can be broken using brute-force methods. Sometimes DES is use a 64-bit key, but 8 of the 64 bits are used only for parity checking, so the effective key size is 56 bits [A.A.Zaidan, Hamdan.O.Alanazi, B.B.Zaidan, Hamid A.Jalab, M.Shabbir and Y. Al-Nabhani, MARCH 2010].

In Two DES the key size is 112 bit, so any attacker can attack to generate all possible 2^{56} keys. So the extend 2DES in to Triple DES. Triple DES is block cipher, which applies the Data encryption Standard (DES) cipher algorithm three times data block. The combined key size is thus 168 bits (3 times 56), beyond the reach of brute-force techniques such as those used by the EFF DES Cracker [A.A.Zaidan, Hamdan.O.Alanazi, B.B.Zaidan, Hamid A.Jalab, M.Shabbir and Y. Al-Nabhani, MARCH 2010].

AES (Advanced Encryption Standard) was designed by NIST in 2001 [Anshu Parashar, Rachna Arora, Jul-Aug 2013]. The Advanced Encryption Standard (AES), also referenced as Rijndael. Its most widely used block cipher with three version (AES-128, AES-192, and AES-256) differ in key sizes 128, 192 and 256 and number of rounds 10, 12, 14 respectively.

RC4 is the most widely used stream cipher . These can be used for encryption by combining it with the plaintext using bitwise exclusive-or; decryption is performed the same way. Diffie–Hellman establishes a shared secret that can be used for secret communications while RSA is widely used Public-Key algorithm. RSA exchanging data over a public network. This authentication technique is used when data are exchange. In our proposed work, we are using RSA algorithm to encrypt the data to provide security so that only the concerned user can access it [Abhishek Sachdeva, Dr. Prerna Mahajan, [2013]

B. Through Authentication:

Various authentications techniques such as SHA, SHA512, Digital signature, are used to authenticate data. The Secure Hash Algorithm is a family of cryptographic hash functions published by the National Institute of Standards and Technology (NIST) as a U.S. Federal Information Processing Standard (FIPS). SHA-512 is a variant of SHA-256 which operates on eight 64-bit words. SHA 512 used to padding and breaking input data into 1024-bit blocks, and each block is processed with a loop which repeats 80 times a sequence of 4 *steps.*

The MD5 message-digest algorithm is a widely used cryptographic hash function producing a 128-bit (16-byte) hash value. MD5 has been utilized in a wide variety of cryptographic applications, and is also commonly used to verify data integrity. Digital signatures are asymmetric cryptography. It provides a layer of validation and security to messages sent through a non-secure channel.

Digital signature is a technique which is used to validate and authenticity and integrity of message. Digital signature is public key cryptography. Digital signature is used with any kind of data whether data is encrypted or not.

C. Combination of Confidentiality and Authentication:

Advanced Encryption Standard (AES) algorithm is used to encrypt and decrypt the data to provide security, but if we combine the AES with authentication algorithm is give a better result for secure data on cloud. Only use of encryption algorithm if anyone can use combination of AES and Digital Signature then Advance Encryption Standard provide confidentiality of stored data in cloud using encryption and decryption and digital signature provide authentication.

Advanced Encryption Standard (AES) algorithm is based on several substitutions, permutations and linear transformations. Each these operations executed on data blocks of 16 byte therefore AES is block cipher. At each time of each round, a unique round key is calculated out of the encryption key. Based on this block structure of AES, the change of a single bit either in the key, or in the plaintext block it generates a completely different cipher text block. The difference between AES-128, AES-192 and AES-256 is the length of the key: 128, 192 or 256 bit.

AES is more secure because cracking of 128 bit AES key which require longer time therefore no practicable attack against AES exists. So, AES is used for encryption standard for real world application such as governments, banks and high security systems around the world.

III. COMPARISON

Factor	AES	3DES	DES
Key length	128, 192 or 256 bits	(k1, k2 and k3) 168 bits (k1 and k2 same)112 bits	56 bits
Cipher Type	Symmetric block cipher	Symmetric block cipher	Symmetric block cipher
Block Size	128, 192 or 256 bits	64 bits	64 bits
Developed	2000	1978	1977
Cryptanalysis resistance	Strong against differential, truncated differential, linear, interpolation and square attacks	Vulnerable to differential, brute force attacker coude be analyze plain text using differential cryptanalysis.	Vulnerable to differential, and linear cryptanalysis, weak substitution tables
Security	Considered secure	One only weak which is exit in DES	Proven inadquate
Possible keys	2^{128} or 2^{192} or 2^{256}	2^{112} or 2^{168}	2^{56}
Possible ASCII printable character keys	95^{16}, 95^{24}, 95^{32}	95^{14} or 95^{21}	95^{7}

Table 1: Comparisons between AES, DES, Tripl DES

Factors	AE	DES	RSA
Key size	128, 192, 256 bits	56 bits	>1024 bits
Ciphering & deciphering key	Same	Same	Différent
Algorithm	Symmetric Algorithm	Symmetric Algorithm	Asymmetric Algorithm
Encryption and Decryption	Faster	Moderate	Slower
Power Consumption	Low	Low	High
Security	Secure for both provider and user	Not Secure	Secure for user only
Key Used	Same key used for Encrypt and Decrypt	Same key used for Encrypt and Decrypt	Different key used for Encrypt and Decrypt
Rounds	10/12/14	16	1
Execution time	Faster then other	Equals to AES	Requirs maximum time
Trojan Horse	Not proved	No	No
Ciphering & Deciphering Algorithm	Different	Different	Same
Inherent Vulnerabilities	Brute Forced Attack	Brute Forced, Linear and differential cryptanalysis attack	Brute Forced and Oracle attack

Table 2: Characteristics and Comparisons of Algorithms

Of the encryption-decryption techniques include private and public key encryption. In Table 1 a symmetric key encryption such as: DES, Triple DES use same key for encryption and decryption. From above comparisons we conclude that AES (Advanced Encryption Standard) is provide more Security compare to DES and Triple DES, because large Key size of AES. In DES 64 bit plain text given as a input and generate 64 bits of cipher text as a output. And in AES 128 bit, 192 bit and 256 bit keys are used for encryption and decryption. AES (Advanced Encryption Standard) algorithm used least time to execute and also provide more Security against various attacks.

Table 2 gives comparisons between AES, DES and RSA in which the AES and DES is used same key for encryption and decryption but AES use key form encrypt and decrypt the blocks and RSA used public key for encryption and private key for decryption. AES is better compare to DES and RSA because it requires less time to execute, provide more Security, use low memory and provide best authenticity. RSA is not best because it used for encryption of small amount of data more memory and maximum time is require executing.

IV. CONCLUSION

Security of data in cloud is one of the major issues in cloud computing environment. This paper reviewed the various existing security measures in cloud computing and compare their various security parameters. To provide better and powerful Security, combination of AES algorithm and authentication technique Digital Signature is used. These combinations provide more Security to secure data in Cloud. AES is more secure compare to other algorithm such as DES, RSA because Take least time to execute and its larger key size are difficult to creak. Combination of both Advanced Encryptions Standard (AES) and digital signature provide trusted computer environment to avoid data integrity in cloud and provide better Security.

REFERENCES

[1] Abomhara M., Khalifa Othman O., Zaidan A.A., Zaidan B.B., Zakaria Omar, , "Enhancing Selective Encryption For H.264/AVC Using Advance Encryption Standard ", International Journal of Computer and Electrical Engineering (IJCEE), ISSN: 1793-8198, Vol.2, NO.2, April 2010, Singapore.

[2] Dr. Mahajan Prerna & Sachdeva Abhishek "A Study of Encryption Algorithms AES, DES and RSA forSecurity", Global Journal of Computer Science and Technology Network, Web & Security Volume 13 Issue 15 Version 1.0 Year 2013, Online ISSN: 0975-4172 & Print ISSN: 0975-4350

[3] Alanazi Hamdan.O., Al-Nabhani Y., Jalab Hamid A., Shabbir M., Zaidan A.A. and Zaidan B.B., "New
Comparative Study between DES, 3DES and AESn Within Nine Factors", JOURNAL OF COMPUTING,
VOLUME 2, ISSUE 3, MARCH 2010, ISSN 2151-9617

[4] Arora Rachna and Parashar Anshu, "Secure User Data in Cloud Computing Using Encryption Algorithms", International Journal of Engineering Research And Applications (IJERA) ISSN: 2248-9622, www.ijera.com Vol. 3, Issue 4, Jul-Aug 2013, pp.1922-1926

[5] Chaudhari M.B. (HOD) and Patel Dhaval (ME scholar),"DATA SECURITY IN CLOUD COMPUTING USING DIGITAL SIGNATURE", International Journal For Technological Research In Engineering Volume 1, Issue 10

