A Survey on Data Security in Cloud Computing using Cryptography

M. Vedaraj
Assistant Professor
RMD Engineering College
Tamilnadu

M. Vigilson Prem, PhD
Professor
RMK College of Engineering and Technology
Tamilnadu

ABSTRACT
Cloud computing is the latest technology through which people can share resources, services and information among the people through use of internet. Since we share the data through the internet, security is considered as a major issue. In Cloud computing several security issues arises like confidentiality, integrity and authentication. Most of the time the data passed via internet might contain confidential or personal information which many people would want to be protected against attacks. Various data encryption algorithms has been developed to make sure that the data transmitted via internet is secure from any sort of hacking or attacks. Several cryptographic algorithms also have been developed for encryption and with each one having some advantages and disadvantages. This paper presents a detailed study of symmetric and asymmetric encryption/decryption algorithms and its advantages and disadvantages.

Keywords
Data security,Data cryptography, encrption, decrption and cloud.

1.INTRODUCTION
Cloud computing is the delivery of computing services over the Internet. Cloud services allow individuals and businesses to use software and hardware that are managed by third parties at remote locations. Examples of cloud services include online file storage, social networking sites, webmail, and online business applications. The cloud computing model allows access to information and computer resources from anywhere that a network connection is available. Cloud computing provides a shared pool of resources, including data storage space, networks, computer processing power, and specialized corporate and user applications. 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. Because of these benefits each and every organizations are moving their data to the cloud. So there is a need to protect that data against unauthorized access, modification or denial of services etc. To secure the Cloud means secure the treatments (calculations) and storage (databases hosted by the Cloud provider). Security goals of data include three points namely: Availability Confidentiality, and Integrity. Confidentiality of data in the cloud is accomplished by cryptography. Cryptography, in modern days is considered combination of three types of algorithms. They are

- Symmetric-key algorithms
- Asymmetric-key algorithms
- Hashing. Integrity of data is ensured by hashing algorithms.

Data cryptography mainly is the scrambling of the content of the data, such as text, image, audio, video and so forth to make the data unreadable, invisible or meaningless during transmission or storage is termed Encryption. The main aim of cryptography is to take care of data secure from invaders. The opposite process of getting back the original data from encrypted data is Decryption, which restores the original data. To encrypt data at cloud storage both symmetric-key and asymmetric-key algorithms can be used. Cloud storage contains a large set of databases and for such a large database asymmetric-key algorithm's performance is slower when compared to symmetric-key algorithms.

2.EXISTING ALGORITHMS FOR CLOUD SECURITY
There are a number of existing techniques used to implement security in cloud storage. Some of the existing encryption algorithms which were implemented in research work are as follows.

2.1 Symmetric (Secret) Key Cryptography
This cryptographic method uses of two different algorithms for encryption and decryption respectively, and a same key are used both the sender and the receiver. The sender uses this key and an encryption algorithm to encrypt data, the receiver uses the same key and the corresponding decryption algorithm to decrypt that data [19] [20].

The description of some widely used Symmetric key cryptographic algorithms is given below:

2.1.1 AES
AES (Advanced Encryption Standard) is a symmetric block encryption standard recommended by NIST (National Institute of Standards and Technology) [13] used for securing information. It uses the same key for both encryption and decryption. . It has variable key length of 128, 192, or 256 bits; default 256 [2][8]. It encrypts data blocks of 128 bits in 10, 12 and 14 round depending on the key size.

2.1.2 DES
DES (Data Encryption Standard) is a symmetric block encryption standard to be recommended by NIST [13]. The DES algorithm is the most broadly used encryption algorithm in the world. The same algorithm and key are used for encryption and decryption, with minor differences. DES accepts an input of 64-bit long plaintext and 56-bitkey (8 bits of parity) and produce output of 64 bit block .

2.1.3 3DES
Triple Data Encryption Algorithm (TDEA or Triple DEA) is a symmetric-key block cipher standard which is similar to DES method but increase encryption level 3 times than DES. As a result this is slower than other block cipher methods. The block size of 3DES is 64 bit with 192 bits key size[2] [17].

2.1.4 BLOWFISH
Blowfish is a symmetric key cryptographic algorithm that encrypts 64 bit blocks with a variable length key of 128-448 bits. Blowfish is the better than other algorithms in throughput and power consumption [2].

2.1.5 RC4
The RC4 (Rivest Cipher 4) is an encryption algorithm that is a shared key stream cipher algorithm requiring a secure exchange of a shared key [2] [4]. The RC4 encryption algorithm is used by standards such as IEEE 802.11 within WEP (Wireless Encryption Protocol) using 40 and 128-bit keys. To generate the key stream, the cipher makes use of a secret internal state which consists of two parts [2][4]:

1. A permutation of all 256 possible bytes.
2. Two 8-bit index-pointers.

The permutation is initialized with a variable length key, typically between 40 and 256 bits, using the key-scheduling algorithm (KSA).

2.1.6 International Data Encryption Algorithm (IDEA)
International Data Encryption Algorithm (IDEA), originally called Improved Proposed Encryption Standard (IPES), is a symmetric-key block cipher designed by James Massey of ETH Zurich and Xuejia Lai and was first described in 1991. The algorithm was intended as a replacement for the Data Encryption Standard (DES). International Data Encryption Algorithm (IDEA) is a symmetric key encryption technique that uses same key for both encryption and decryption. This key is of length 128-bit which secures 64-bit data. Also, it runs eight and a half rounds for encrypting and decrypting the data[12].

2.1.7 SEED
A block cipher uses 128-bit blocks and 128-bit keys. It was developed by the Korea Information Security Agency (KISA) and adopted as a national standard encryption algorithm in South Korea[5].

2.1.8 ARIA
A 128-bit block cipher employs 128-, 192- and 256-bit keys. It was developed by large group of researchers from academic institutions, research institutes and federal agencies in South Korea in 2003 and subsequently named a national standard [5].

2.2 Asymmetric (public) Key Cryptography
This cryptographic method makes use of two different algorithms for encryption and decryption respectively, a public key for encryption and a private key for decryption. The public key of the sender is used to encrypt the message by the sender. The receiver decrypts the cipher text with the help of a private key. The description of some widely used Asymmetric key cryptographic algorithms is given below [2].

2.2.1 RSA
RSA (Rivest-Shamir-Adleman) is broadly used an asymmetric encryption /decryption algorithm which involves a public key and a private key. The public key can be informed to everyone and is used for encrypting messages. Messages encrypted with the public key can only be decrypted using the private key. It secured user data assimilate encryption before to storage, user authentication procedures prior to storage or retrieval, and making secure channels for data transmission [2] [8] [4]. 4096 bit key size is used for execution of RSA algorithm. RSA algorithm involves these steps:

1. Key Generation
2. Encryption
3. Decryption

2.2.2 DIFFIE-HELLMAN
The scheme was first revealed by Whitfield Diffie and Martin Hellman in 1976. Diffie–Hellman key exchange is a specific method of exchanging cryptographic keys [2] [18]. It permits two parties that have no prior knowledge of each other to jointly make a shared secret key over an insecure communications channel. This key can then be used to encrypt posterior communications using a symmetric key cipher.

2.2.3 PAILLIER
The Paillier cryptosystem is an asymmetric algorithm. It has homomorphic property permits this scheme to do normal addition operations on several encrypted values and achieving the encrypted sum, the encrypted sum can be decrypted later without even knowing the values ever that made up the sum[2][5].

2.2.4 ELGAMAL
El-Gamal is the asymmetric key cryptography. It is a public key cryptography which is based on Diffie Hellman key exchange. It was introduced by Taher El-Gamal in 1985. It is consist of signature, encryption algorithms as well as discrete logarithm problems [2][5]. ElGamal encryption consists of three components: the key generator, the encryption algorithm, and the decryption algorithm.

2.2.5 Elliptic Curve Cryptography (ECC)
PKC algorithm is based upon elliptic curves. ECC can offer levels of security with small keys comparable to RSA and other PKC methods. It was designed for devices with limited computing power and/or memory, such as smart cards and PDAs[2][4][5].

2.3 Hashing Cryptography
Hash functions are a fundamental elementary in the field of cryptography, used widely in a broad spectrum of important applications involving: message integrity and authentication [2] [18], digital signatures, secure time stamping, and countless others. Hash functions, also called message digests and one-way encryption, are algorithms that use no key. Instead, a fixed-length hash value is computed based upon the plaintext that makes it impossible for either the contents or length of the plaintext to be recovered. Hash algorithms are typically used to provide a digital fingerprint of a file's contents, often used to ensure that the file has not been altered by an intruder or virus. Hash functions are also commonly employed by many operating systems to encrypt passwords. Hash functions, then, provide a measure of the integrity of a file. A hash function H is an efficiently-computable algorithm that takes as input an arbitrary-length message M and potentially a fixed-length key K (considering a keyed hash function), and makes a fixed-length output D called the message digest. H (K, M) = D. The description of some widely used Hashing cryptography algorithms are given below:

2.3.1 MD5

MD5 (Message Digest5) is a broadly used cryptographic hash function with a 128-bit hash value. It processes a variable-size message into a fixed-length output of 128 bits[2] [13]. The input message is divided into chunks of 512-bit blocks; then the message is padded for making its length divisible by 512[8]. In this sender use the public key of the receiver to encrypt the message and receiver use its private key to decrypt the message.

2.3.2 MD6

The MD6 Message-Digest Algorithm is a cryptographic hash function. MD6 makes use of a substantially different tree-based mode of operation that allows for greater parallelism [18]. MD6 may be viewed as a tree-like construction, with a 4-to-1 compression function reducing the overall length of the message at each level [19].

2.3.3 SHA

SHA (Secure Hashing Algorithm) is a hashing algorithm. SHA-1 is most extensively used SHA hash function, but very quickly it is going to be replaced by the newer and stronger SHA-2 hash function. It is currently used in a wide variety of applications, including TLS, SSL, SSH and PGP.SHA1 outputs a 160-bit digest of any sized file or input. SHA-256 algorithm produces an almost-unique, fixed size 256-bit (32-byte) hash [18]. This creates it suitable for password validation, challenge hash authentication, anti-tamper, digital signatures. SHA-256 is one of the successor hash functions to SHA-1, and is one of the strongest hash functions available. SHA-256 hash functions computed with 32-bit words.

2.3.4 Whirlpool

This algorithm was designed by V. Rijmen (co-inventor of Rijndael) and P.S.L.M. Barreto. Whirlpool is one of two hash functions endorsed by the New European Schemes for Signatures, Integrity and Encryption (NESSIE) competition (the other being SHA). Whirlpool operates on messages less than 2256 bits in length and produces a message digest of 512 bits. The design of this hash function is very different than that of MD5 and SHA-1, making it immune to the same attacks as on other hashes [5].

2.3.5 Tiger

It was designed by Ross Anderson and Eli Biham. Tiger is designed to be secure, run efficiently on 64-bit processors and easily replace MD4, MD5, SHA and SHA-1 in other applications. Tiger/192 produces a 192-bit output and is compatible with 64-bit architectures, whereas Tiger/128 and Tiger/160 produce a hash of length 128 and 160 bits, respectively, to provide compatibility with the other hash functions [5].

2.3.6. eD2k

It was named for the EDonkey2000 Network (eD2K). The eD2k hash is a root hash of an MD4 hash list of a given file. A root hash is used on peer-to-peer file transfer networks, where a file is broken into chunks. Each chunk has its own MD4 hash associated with it and the server maintains a file that contains the hash list of all of the chunks. The root hash is the hash of the hash list file[5].

Table-1: Characteristics of Cryptography Algorithms

Scheme	Algorithm	Designers	Block size	Key sizes	Rounds
AES	Symmetric	Rijindael	128 bits	128,192,256 bits	10 or 12 or 14
DES	Symmetric	IBM 75	64 bits	64 bits	16
3DES	Symmetric	IBM 78	64 bits	112 bits or 168 bits	48
BLOW FISH	Symmetric	Bruce Schneier 93	64 bits	32-448 bits	16
IDEA	Symmetric	James Massey	64 bits	128 bits	8
RC4	Symmetric	Ronald Rivest 87	40-2048	variable	256
RSA	Asymmetric	Rivest, Shamir, Adleman 77	1024	Minimum 512 bits.	1
DSA	Asymmetric	NIST 91	-	-	-
Diffie-Hellman	Asymmetric	Diffie, Hellman 76	-	-	-
EL-GAMAL	Asymmetric	Elgamal 84	-	-	-
Elliptic-Curve Cryptography (ECC)	Asymmetric	Neal Koblitz and Victor S.Miller	Stream size is variable	Smaller but effective key	1
MD5	Hashing	Rivest 91	512 bits	128 bits	-
MD6	Hashing	Prof. Rivest 08	-	-	-
SHA	Hashing	NIST 95	-	160 bits	-
Whirlpool	Hashing	V.Rijmen and P.S.L.M. Barreto	512 bits	.	10
Tiger	Hashing	Ross Anderson and Eli Biham	-	-	24

3. CONCLUSION AND FUTURE WORKS

Cloud computing is changing the way IT departments buy IT. Businesses have a range of paths to the cloud, including infrastructure, platforms and applications that are available from cloud providers as online services. Many people may be confused by the range of offerings and the terminology used to describe them and will be unsure of the risk and benefits. Security is a major requirement in cloud computing while we talk about data storage. There are number of existing techniques used to implement security in cloud. In this paper, we discussed number of symmetric and asymmetric algorithms. Our future will be considering some problems related to existing security algorithms and implement a better version of DES, 3DES, AES, RSA, IDES, Blowfish.

REFERENCES

[1] William Stallings, "Cryptography And network Security: Principles and Practice second edition", ISBN 0-13869017-0, 1995 by Prentice- Hall, Inc. Simon & Schuster / A Viacom Company Upper Saddle River, New Jersey 07458.

[2] Md. Alam Hossain, Md. Biddut Hossain, Md. Shafin Uddin, Shariar Md. Imtiaz, "Performance Analysis of Different Cryptography Algorithms", International Journal of Advanced Research in Computer Science and Software Engineering Volume 6, Issue 3, March 2016.

[3] Swati Kashyap, Er.Neeraj Madan "A Review on: Network Security and Cryptographic Algorithm" International Journal of Advanced Research in Computer Science and Software Engineering Volume 5, Issue 4, April 2015.

[4] B.Nithya, Dr.P.Sripriya, "A Review of Cryptographic Algorithms in Network Security" International Journal of Engineering and Technology (IJET) Vol 8 No 1 Feb-Mar 2016.

[5] Saurabh Sindhu, Divya Sindhu, "Cryptographic Algorithms: Applications in Network Security", International Journal of New Innovations in Engineering and Technology Volume 7 Issue 1– February 2017.

[6] Prerna Mahajan & Abhishek Sachdeva,"A study of Encryption Algorithms AES, DES and RSA for Security", Global journal of Computer Science and Technology, Vol.8,No.15, (2013) pp.15-22.

[7] Jitendra Singh Laser, Viny Jain, "A Comparative Survey of various Cryptographic Techniques" International Research Journal of Engineering and Technology (IRJET), Volume: 03 Issue: 03 | Mar-2016.

[8] Priyanka Arora, Arun Singh, Himanshu Tyagi " Evaluation and Comparison of Security Issues on Cloud Computing Environment" in World of Computer Science and Information Technology Journal (WCSIT) ISSN: 2221-0741 Vol. 2, No. 5, 179-183, 2012.

[9] E. Thambiraja, G. Ramesh and Dr. R. Umarani, "A Survey on Various Most Common Encryption Techniques", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 7, pp. 226-233, July 2012.

[10] Pushpendra Verma, Dr. Jayant Shekhar, Preety,Amit Asthana, "A Survey for Performance Analysis Various Cryptography Techniques Digital Contents", International Journal of Computer Science and Mobile Computing, Vol.4 Issue.1, January- 2015, pg. 522-531

[11] Sweta K.Parnar,Prof. K.C.Dave,"A review on various most common symmetric encryption algorithm",International journal for scientific research and development ,volume 1,issue 4,2013

[12]S.Artheeswari,Dr.RM.Chandrasekaran,"INTERNATIONAL DATA ENCRYPTION ALGORITHM (IDEA) FOR DATA SECURITY IN CLOUD", International Journal of Technology and Engineering System (IJTES)

[13] Vineet Kumar Singh, Dr. Maitreyee Dutta "ANALYZING CRYPTOGRAPHIC ALGORITHMS FOR SECURE CLOUD NETWORK" International Journal of advanced studies in Computer Science and Engineering IJASCSE Volume 3, Issue 6, 2014.

[14] S C Rachana, Dr. H S Guruprasad, "Emerging Security Issues and Challenges in Cloud Computing", International Journal of Engineering Science and Innovative Technology (IJESIT), Volume 3, Issue 2, March 2014, and ISSN: 2319-5967.

[15] Rajdeep Bhanot and Rahul Hans," A Review and Comparative Analysis of Various Encryption Algorithms", International Journal of Security and Its Applications Vol. 9, No. 4 (2015), pp. 289-306

[16] M. Kumar and E. G. Dharma, "A comparative analysis of symmetric key encryption algorithm", IJARCET, vol. 3, no. 2, (2014).

[17] 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, ISSN 2319 – 4847.

[18] Christopher Yale Crutchfield "Security Proofs for the MD6Hash Function Mode of Operation", Massachusetts Institute of Technology2008.