International Journal of Future Generation Communication and Networking
Vol. 13, No. 2s, (2020), pp. 1267–1274

A Survey Paper on "Data Storage & Security in Cloud Computing"

Shradha Parmeshwar Awatari
Dr. Sachin Chaudhari
Prof. Monali Gulhane

Department of Computer Science & Engineering
M. Tech Jhulelal Institute of Technology, Nagpur, Maharashtra, India

Abstract *:*
Cloud computing is group of services for example software system storage, network and hardware these type of services are provided to user. Cloud storage is easily access anywhere anytime of the data because cloud is work in remote location. It uses the storage service provided by the cloud provider. Data is not secure in the cloud because the unauthorized user can try to use of the private data. So providing the data security it uses the different encryption method to protect the data. So that in the proposed study it use the multilevel encryption algorithm. In the multilevel encryption it combines two different algorithms for providing the better security..

Keywords*: Data storage & cloud Computing, Cloud Computing, Cloud Storage,Cloud Environment, Cloud Security*

INTRODUCTION

The definition of cloud given by National Institute of standard and Technology (NIST) says that:"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 application and services)that can be rapidly provisioned and released with minimum management effort or service provider interaction [1]. In the cloud computing there is no need to store data in the desktop or fixed location computer. You can store the data in a server and you can access the data in any remote location using of the internet topology. Cloud computing provides a large amount of data can be easily stored in the cloud. The advantages of using cloud computing are: i) reduce hardware and maintenance cost ii) accessibility around the globe iii) flexibility and highly automated process. Characteristics of Cloud Computing.

1. Ultra large-scale: In the cloud computing there are many companies uses cloud server. Google has owned more than one million servers. Even in Amazon, IBM, Microsoft, Yahoo, they have more than hundreds of thousands servers. So that the scale of cloud is large
2. Virtualization: Cloud computing provides user to get service anywhere, through any kind of terminal. Users can attain or share it safely through an easy way, anytime, anywhere.
3. High reliability: Cloud uses data multitranscript fault tolerant, the computation node isomorphism exchangeable and so on to ensure the high reliability of the service. Using cloud computing is more reliable than local computer.
4. Versatility: Cloud computing can produce various applications supported by cloud, and one cloud
5. High extendibility: The scale of cloud can extend dynamically to meet the increasingly requirement.
6. On demand service: Cloud is a large resource pool that you can buy according to your need; cloud is just like running water, electric, and gas that can be charged by the amount that you used [2].

ISSN: 2233-7857 IJFGCN

Cloud computing provides the different services these services put into the three models: Software as service (Saas), Platform as service (Paas), and Infrastructure as service (Iaas).

Software as a Service (SaaS): In SaaS model, it performs application software. User can access databases and application software's on demand or need of users.

Platform as a Service (PaaS): In PaaS models, computing platform such as web server, operating system, database and the background for programming language execution is provided by the service providers.

Infrastructure as a Service (IaaS): According to IETF (Internet Engineering Task Force), computers or virtual machines, computing power and other physical resources like storage space are provided on demand by the IaaS providers [3].

Cryptography is technique applied for encryption and decryption. Encryption means the plain text is converted into the cipher text or some coded form using of the different encryption algorithm. For the purpose of data security and decryption is opposite of encryption. In the decryption the cipher text is converted into the plain text r original text using the decryption algorithm. Conventional cryptography is also referred as symmetric encryption or single key encryption. Same key is used for encryption and decryption. Public key.

cryptography is referred as asymmetric encryption or public key encryption. Separate keys are used for encryption and decryption. The encryption process consists of an algorithm and a key. The key is a value independent on the specific of the plain text. The algorithm will produce a different output depending on the specific key being used at that time. Changing the key changes the output of the algorithm. Once the cipher text is produced, it may be transmitted to cloud storage. Upon reception, the cipher text can be transformed back to the original plaintext by using a decryption algorithm with the same key that was used in encryption [4].

Although cloud computing service providers describe the security and reliability of their services, but actual there are a number of security issue are created in cloud computing services. The service is not as safe and reliable as they claim. In 2009, the major cloud computing vendors successively appeared several accidents. Amazon's Simple Storage Service was interrupted twice in February and July 2009. This accident resulted in some network sites relying on a single type of storage service were forced to a standstill. In March 2009, security vulnerabilities in Google Docs even led to serious leakage of user private information. Google Gmail also appeared a global failure up to 4 hours. It was exposed that there was serious security vulnerability in VMware virtualization software for Mac version in May 2009. People with ulterior motives can take advantage of the vulnerability in the Windows virtual machine on the host Mac to execute malicious code. Microsoft's Azure cloud computing platform also took place a serious outage accident for about 22 hours. Serious security incidents even lead to collapse of cloud computing vendors. As administrators' misuse leading to loss of 45% user data.

Now a day's data in the cloud is not safe and secure because some external entities are continuously visited to the cloud for hacking the data. To provide a security on a particular data we use encryption/cryptography method. There are different algorithm already exits but in this paper one more concept two different algorithm that are combine or joining each other for providing the better security. When only one algorithm is used for providing data security it gives less security. But more than one algorithm that are concatenating with each other then it work very efficient manner and also provide the better security as compare to the single algorithm. In this paper it uses to different algorithm than are joining to each other one is symmetric block cipher and another is asymmetric block cipher. Symmetric block cipher is uses only one key for encryption and asymmetric block cipher uses the private key as well

ISSN: 2233-7857 IJFGCN

as public key for encryption and decryption. Two algorithms that are combining each other are called as Hybrid encryption.

II. LITERATURE SURVEY

To secure the cloud security goals of the data include three points namely. Confidentiality, Integrity and availability (CIA).Encryption is used two types of algorithm symmetric and asymmetric algorithm. In the symmetric algorithm it uses private key for encryption and the same key is used for decryption. And asymmetric it uses the public key for encryption and private key is distributed to all using of the private key decrypt the data [6].

Data Encryption standard: DES is a block-cipher. It uses the 56 bit key and 64 bit blocks DES has a complex set of rules and data. It has fast hardware implementations and slow software implementations.DES takes 64 bit plain text and creates 64 bit cipher text at decryption side. It uses two permutation initial permutation and final permutation and 16 Feistel rounds. Each round uses different 48 bit round key [4].

Advanced Encryption Standard: Advanced Encryption Standard (AES) is symmetric key block cipher.AES is non Feistel cipher.AES encrypting data with block size 128 bit. It uses 10, 12, or 14 rounds. The key size may be used in the AES 128,192 or 256 bits. AES operates 4*4 columns matrix is called as state.

Triple-DES (3DES): It uses three 56-bit keys and performs three encryption/decryption passes over the block.

DESX: In DESX it combining 64 additional key bits to the plaintext prior to encryption, effectively increases the key length to 120 bits.

Rivets Ciphers: Named for Ron Rivets, it uses the different algorithms.

RC2: A 64-bit block cipher using variable-sized keys designed to replace DES. The key size was limited to 40 bits.

RC4: A stream cipher using variable-sized keys

RC5: A block-cipher supporting a variety of block sizes (32, 64, or 128 bits), key sizes, and number of encryption passes over the data.

Blowfish: A symmetric 64-bit block cipher invented by Bruce Schneider; optimized for 32-bit processors with large data caches, it is significantly faster than DES on a Pentium/PowerPC-class machine. Key lengths can vary from 32 to 448 bits in length. Blowfish, available freely and intended as a substitute for DES or IDEA, is in use in a large number of product.

RSA: RSA is Asymmetric encryption algorithm it means that public key is distributed to all for encryption and private key is used to decryption .The key size is 1024 bits. In the RSA modular exponential is used for encryption and decryption. It uses two exponents a and b where a is public key and b is private key.

Elliptic curve cryptography: The ECC is the public key cryptography it is based on algebraic structure over finite fields. Key length of the ECC is 135 bit and block size is variants not fixed size of block is used. The main advantage of ECC is smaller key size reducing storage and transmission

ISSN: 2233-7857 IJFGCN

requirements [5].

III. PROPOSED STUDY

In cloud computing data security is most important factor to protect the data from some external entities is the challenging task due to this task. It uses the different encryption algorithm there is symmetric and asymmetric method is used for encrypt and decrypt data. In symmetric private key is used for encryption and same key is used for decryption but main problem is maintaining the key is difficult task brute force attack can be occur.

In asymmetric encryption it uses two different key public key and private key. using of the private key it encrypt the data and public key is distributed to all the receiver then the using of the public key it decrypt the data. In this mechanism may also brute force attack or the problem of maintaining the key. For both algorithm when it uses single for the encryption it not provide the better security but when two algorithm are combining to each other then combining algorithm provide better security comparing to single algorithm.

In proposed study the two different algorithms that are uses DES and RSA. The DES is a symmetric encryption algorithm that uses only one key for both and RSA is a asymmetric encryption it uses two different key such as private key and public key using of private key it encrypt the data and public key it decrypt the data. But when only one DES algorithm is used for data encryption it provide less security or it also RSA is used it provide less security. But when we use both algorithms that are combine or join each other then it provide a better security. We use a multilevel encryption in the multilevel encryption the first time the plain text is encrypted using the DES algorithm then the DES generate the output as a first level encryption. After the first level encryption it again applies the RSA encryption to the first level encryption. After applying the RSA then it produce the output as a second level. These cipher text is stored in data base.

TABLE I. Comparison among different algorithms

	AES	**RSA**	**BLOWFISH**	**DES**	**ECC**
Key size	128,192,256 bits	1024 Bits	32-448 bits	56 bits	135 bits
Block size	128 bits	Variants	64 bit	64 bit	Variants
Introducer	Rijman Joan	Rivest Shamir	Bruce Schneier	IBM 75	Neal Koblitz, Vector Smiller
Data ency capaci	Encrypt large amount of data	Encrypt Small amount	Encrypt avg amount of data	Encryp tavg amount	-

ty		of data		of data	
Memory–usage	Low ram needed	Highest memory Usage	Execute in less than 5kb	High RAM needed	-
Execut ion Time	Faster	Require maximum time	Less timer e to execute	Faster	Fastest

There are a number of existing techniques used to implement security in cloud storage. Some of the existing encryption algorithms which were implemented as follows;

A. Data Encryption Standard (DES) Algorithm:

The Data Encryption Standard (DES) [6] is a symmetric- key block cipher published as FIPS-46 in the Federal Register in January 1977 by the National Institute of Standards and Technology (NIST). At the encryption site, DES takes a 64-bit plaintext and creates a 64-bit cipher text, at the decryption site, it takes a 64-bit cipher text and creates a 64-bit plaintext, and same 56 bit cipher key is used for both encryption and decryption. The encryption process is made of two permutations (P-boxes), which we call initial and final permutation and sixteen Feistel rounds [7]. Each round uses a different 48-bit round key generated from the cipher key. DES performs an initial permutation on the entire 64 bit block of data. It is then split into two, 32 bit sub-blocks, L0 and R0 which are then passed into what is known as Feistel rounds

.Each of the rounds are identical and the effects of increasing their number is twofold - the algorithms security is increased and its temporal efficiency decreased. At the end of the 16th round, the 32 bit L15 and R15 output quantities are swapped to create what is known as the pre-output. This [R15, L15] concatenation is permuted using a function which is the exact inverse of the initial permutation. The output of this final permutation is the 64 bit cipher text.

The function f is made up of four sections:

- Expansion P-box
- A whitener (that adds key)
- A group of S-boxes
- A straight P-box.

B. RSA Algorithm:

The RSA algorithm named after Ron Rivest, Adi Shamir, and Leonard Adelman. It is based on a property of positive integers. RSA uses modular exponential for encryption and decryption. RSA is an algorithm for public-key cryptography, involves a public key and a private key. The public key can be known to everyone and is used for encrypting messages. Messages encrypted with the public key can only be decrypted using the private key.

ISSN: 2233-7857 IJFGCN

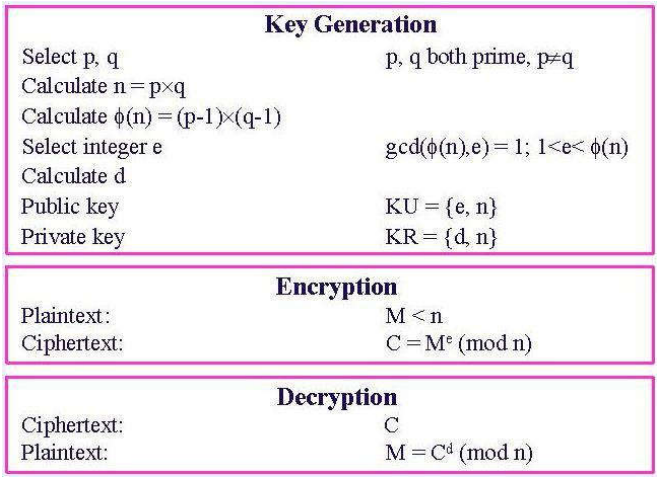

Figure 1. RSA Algorithm

RSA uses two exponents, e and d, where e is public and d is private. Let the plaintext is M and C is cipher text, then at Encryption
$C = M^e \bmod n$
And at decryption side

$M = C^d \bmod n$.

Where n is a very large number, created during key generation process.

DES algorithm and RSA algorithm provides security in cloud storage. In existing systems only single level encryption and decryption is applied to Cloud data storage. Cyber criminals can easily cracked single level encryption. Nowadays Cyber Criminals can easily access data storage. In Personal Cloud Storage important data, files and records are entrusted to a third party, which enables Data Security to become the main security issue in Cloud Computing. In Cloud Storage any organization's or individual's data is stored in and accessible from multiple distributed and connected resources that comprise a cloud. To provide secure communication over distributed and connected resources authentication of stored data becomes a mandatory task. We have proposed a combination of two different security algorithms to eliminate the security challenges of Personal Cloud Storage. We have taken a combination of algorithms like: DES and RSA. DES (Data Encryption Standard) is a symmetric key algorithm, in which a single key is used for both encryption/decryption of data. Whereas RSA is an asymmetric key algorithm, the algorithm that uses different keys for encryption and decryption purposes. A user can upload data in Personal Cloud Storage. Uploading file DES and RSA Encoding schemes are used to encrypt data.

The steps of Multi-level encryption will be as follows:

- Upload data.
- Now implementation of DES Algorithm takes place. The Data Encryption Standard (DES) is a block□cipher. It encrypts data in blocks of size 64 bits each. That is 64 bits of plain text goes as input to DES, which produces 64 bits of cipher text. The actual key used by DES algorithm for encryption is 56 bits in length. The encryption process is made of two permutations (P-boxes), which we call initial and final permutation, and sixteen Feistel rounds
- DES has 16 rounds, means the main algorithm is repeated 16 times to produce cipher text. As number of rounds increases, the security of system increases exponentially.
- The first level encryption is generated using DES algorithm
- Now apply RSA algorithm on encrypted output of DES algorithm to generate second level encryption.

ISSN: 2233-7857 IJFGCN

- In RSA algorithm public key is used for encryption.
- Once the data is encrypted using RSA algorithm, it will be stored in Database of Cloud Storage.

The steps of Multi-level decryption will be as follows:

- DES and RSA algorithms are used to decrypt data.
- First apply the RSA algorithm (decryption scheme) using private key. This algorithm will generate first level decrypt data.
- Now apply the DES decryption algorithm on first level decrypt data.
- DES decryption algorithm uses the same 56 bit length key for decryption.
- DES algorithm of decryption will generate Plain text.

In Our proposed algorithm, implementation of the DES algorithm takes place to generate first level encryption. And then we apply the RSA algorithm on the encrypted output of DES algorithm to generate second level encryption. And same Process takes place for decryption using DES and RSA algorithms. Means we applied multilevel Encryption and Decryption to provide security for cloud storage data.

IV. CONCLUSION

Cloud Computing can become more secure using cryptographic algorithms. Cryptography is the technique for data secure by converting the data into coded or non readable forms. But the existing cryptographic Algorithms are single level encryption algorithms. Unauthorized person can easily cracked single level encryption. Hence system which uses multilevel encryption and decryption it provides more security for Cloud Storage.

As our proposed algorithm is a Multilevel Encryption and Decryption algorithm. Thus, in our proposed work, only the authorized user can access the data. Even if some intruder (unauthorized user) gets the data accidentally or intentionally, he must have to decrypt the data at each level which is a very difficult task without a valid key. It is expected that using multilevel encryption will provide more security for Cloud Storage than using single level encryption.

REFERENCES

[1] P. Mell and T. Grance, The NIST Definition of Cloud Computing, version 15, October 7, 2009, National Institute of Standards and Technology (NIST), Information Technology Laboratory (www.csrc.nist.gov).
[2] Parneet Kaur and Sachin Majithia, "Various Aspects for Data Migration in Cloud Computing and Related Reviews", International Journal of Computer Sciences and Engineering, Volume-02, Issue-07, Page No (83-85), Jul -2014, E-ISSN: 2347-2693
[3] Sandha, M.Ganaga Durga," Study on Data Security Mechanism in Cloud Computing",IEEE conference no-33344.
[4] William Stallings, Cryptography and Network Security: Principles and Practices, Fifth edition, Prentice Hall, ISBN-13: 978- 0136097044, 2010.
[5] Balachandra Reddy Kandukuri, Rama Krishna Paturi and Dr. AtanuRakshit, "C loud security issues" In Services Computing, 2009. IEEE International Conference on, page 517520, 2009.
[6] Neha Jain and Gurpreet Kaur 'Implementing DES Algorithm in Cloud for Data Security" VSRD International Journal of CS & IT Vol. 2 Issue 4, pp. 316-321, 2012
[7] Amazon Web Services: Overview of Security Processes, may 2011.
[8] L. M. Kaufman, "Data security in the world of cloud computing,"IEEE Security & Privacy Magazine, vol. 7, pp. 61-64, July2009.
[9] P.Shanthi Bala," Intensification of Educational Cloud Computing and Crisis of Data Security in Public Clouds",IJCSE Vol. 02, No. 03, 2010, 741-745

ISSN: 2233-7857 IJFGCN

[10]K Hashizume et al., An analysis of security issues for cloud computing, Journal of Internet Services and Applications, a Springer open journal, pp 1-13, 2013.
[11]R. Chow, P. Golle, M. Jakobsson, E. Shi, J. Staddon, R. Masuoka,and J. Molina. Controlling data in the cloud: Outsourcing computation without outsourcing control. pages 85–90, 2009
[12]Wang, J.K.; Xinpei Jia, Data Security and Authentication in hybrid cloud computing model, Global High Tech Congress on Electronics (GHTCE), 2012 IEEE, On page(s): 117-120.
[13]Shivlal Mewada, Umesh Kumar Singh and Pradeep Sharma, "Security Enhancement in Cloud Computing (CC)", ISROSET-International Journal of Scientific Research in Computer Science and Engineering, Vol.-01, Issue-01, pp (31-37), Jan -Feb 2013.
[14]K. Dubey, M. Namdev, S. Shrivastava, "Cloud-User Security Based on RSA and MD5 Algorithm for Resource Attestation and Sharing in Java Environment", IEEE sixth international conference, 2012.
[15]Prakash G. L , Dr. Manish Prateek, Dr Inder Singh, ,"Efficient Data Security Method to Control Data in Cloud Storage System using Cryptographic Techniques ",IEEE International Conference on Recent Advances and Innovations in Engineering (ICRAIE-2014), May 09-11, 2014, Jaipur, India

ISSN: 2233-7857 IJFGCN