Survey on Encryption Algorithms to Overcome Security Issues in Cloud Computing

Amandeep Kaur Gill[#1], Charanjit Singh[*2]

[#] *M.Tech, Research Scholar,*
Department of Computer Science and Engineering,
RIMT-IET, Mandi Gobindgarh, Fatehgarh Sahib, Punjab, India
[1]er.amandeep_gill@yahoo.com

[*]*Assistant Professor,*
Department of Computer Science and Engineering,
RIMT-IET, Mandi Gobindgarh, Fatehgarh Sahib, Punjab, India
[2]2sehgal_cs@yahoo.com

***Abstract*— Cloud Computing is an emerging paradigm in which users can store data online on cloud storage and access anytime, anywhere according to their requirements. There are number of issues related to the cloud computing like Security, Access Control, Authentication, Auditing issues etc. but one of the most important issue is the DATA SECURITY as there is no particular area for the data storage of cloud users. In order to provide the security to the cloud network and data, different encryption methods are used. This paper focuses on the different encryption/decryption algorithms namely RSA, AES, DES and NTRU but concludes that NTRU is the fast encryption algorithm, which is a public-key method, in which two keys are used. One is private key and other is public key. Public Key is used to encrypt the data/plaintext or to verify the digital signature whereas Private Key is used to decrypt the cipher text into plaintext or to create the digital signature.**

***Keywords*— Cloud Computing, Data Security, Encryption, Decryption, RSA, NTRU, DES, AES.**

I. INTRODUCTION

A **cloud** is a large pool of easily accessible virtualised resources, such as hardware, software, development platforms and/or services like Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). So, the users don't need to store their data at their end as all the data is stored on remote server [5]. **Cloud Computing** refers to a network of computers sharing the resources given by the Cloud Service Provider catering to its user's need connected through internet. It means that Cloud Service Provider provide the IT services to the Cloud users with the help of internet. These services can be scaled up and down based on user needs. Users are billed for the services according to how much they have actually used the resources or services. Cloud Computing is also a model for enabling on-demand network access to a shared pool of configurable computing resources like networks, services, applications, storage and servers, that can be provisioned and released very fast with minimal service provider interaction or management effort [3].

II. CLOUD SERVICE AND DEPLOYMENT MODELS

A. Cloud Service Models

Cloud computing service providers offer their services according to several fundamental models: Infrastructure as a service (IaaS), Platform as a service (PaaS), and Software as a service (SaaS) where IaaS is the most basic and each higher model abstracts from the details of the lower models as shown in Fig. 1:

1) Infrastructure as a Service (IaaS): It refers to allow the users 'to access the servers' computational and storage infrastructure in a centralised service. In this, user can develop and deploy the random software either it is application software or operating system. Users have control over operating system and application which is deployed, storage and limited control on network components like firewall etc [3] [10]. *Example:* Amazon Web Services which allows remote access to the Amazon.com's computing services.

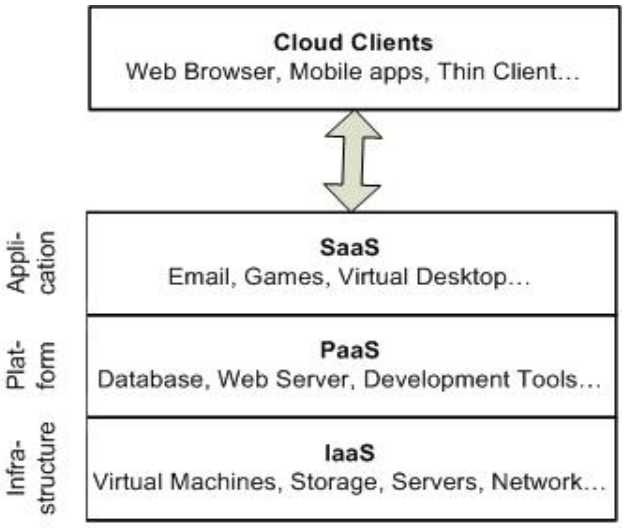

Fig. 1 Cloud Service Models

2) Platform as a Service (PaaS): It refers to allow the users to develop new applications by using any programming language or by any tool supported by the user and deployed them. In this, users have no right of management or control the base of infrastructure but have control over the deployed application [3][10]. *Example:* Google App Engine allows the users to create customized applications.

3) Software as a Service (SaaS): It is also known as Application Service Provider or ASP model, refers to service that gives the user an opportunity to access the cloud services by running simple software like Web Browser. In this, users have no right of management or controlling the base infrastructure like network, operating system, server, storage. But users have some limited user specific configuration setting with respect to application [3] [10]. *Example:* Gmail, Google Groups etc.

B. Cloud Deployment Models

Cloud Services can be deployed in different ways depending on organisation structure and the provisioning location. Four deployment models are widely distinguished namely: Private, Public, Community and Hybrid cloud service usage as shown in Fig. 2:

1) Private Cloud: In this, Cloud Service Provider provides the cloud infrastructure to be operated solely by the single organisation [3]. This infrastructure is managed by the organisation itself or by the third party. In this, Cloud users are considered as trusted users by the organisation, in which they are either employees or have contractual agreement with the organisation.

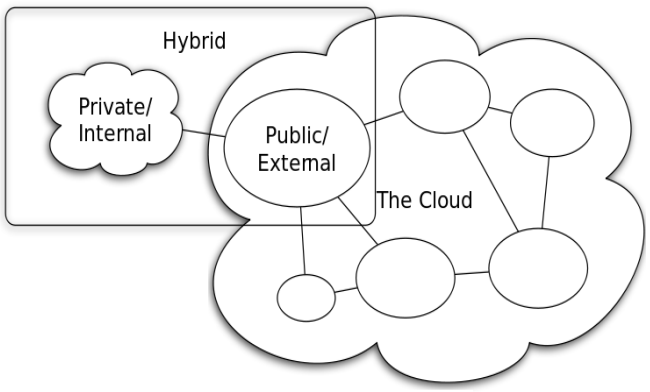

Fig. 2 Cloud Deployment Models

2) Community Cloud: In this, Cloud Service Provider provides the cloud infrastructure to be operated by the number of organisations [3]. This infrastructure is also managed by the organisation itself or by the third party. In this, Cloud users are considered as trusted users by the organisation that is the part of the community.

3) Public Cloud: In this, Cloud Service Provider provides the cloud infrastructure that is open for a large industry group or general public [3]. This is owned by the organisation by acquiring cloud services. In this, Cloud users are considered as untrusted users, means they have neither contractual agreement with the provider nor tied to the organisation as their employees.

4) Hybrid Cloud: In this, Cloud infrastructure is a combination of private, public and community clouds. Each part of the community is connected to the other with the help of gateway that controls the data and application flow from one part to another. Its users are considered as trusted as well as untrusted users. Untrusted users are prevented to access the resources of the private and community parts of the hybrid clouds [9].

III. BENEFITS OF CLOUD COMPUTING

1) *On-Demand Self-Service:* Cloud computing providers provide the resources on demand which means when the cloud user wants their resources. This is made possible by Self-Service and automation. Self-Service means that the user performs all the operations needed to acquire the service herself/himself instead of going through an IT department. The user request is then automatically processed by the cloud infrastructure without human intervention on provider's side [11].

2) *Reduce Cost:* It reduces the cost of hardware at the user end as user has no need to store the data at his/her end because data is already at remote server at some other location. So, instead of buying the hardware and software required to run the processes and to save the data, users are just renting the assets according to their requirements [11].

3) *Measured Service:* Cloud Computing's 'pay-per-use' model makes the cloud attractive solution to enterprises because cloud users are billed for the services according to how much they have actually used during billing period [11].

4) Broad Network Access: Broad network access refers to resources hosted in private cloud network that are available for access from a wide range of devices such as tablets, PCs and smartphones. These resources are also accessible from a wide range of locations that offer online access [11].

5) Resource pooling: The providers computing resources are pooled using a multi-tenant model to serve multiple users. According to user demand different physical and virtual resources are dynamically assigned and reassigned. Examples of resources include storage, memory, processing and network bandwidth [11].

IV. Encryption Algorithms in Cloud Computing

A. RSA

RSA stands for Ron Rivest, Adi Shamir and Leonard Adleman. It is a public key Cryptosystem used for secure data transmission. In this, two different keys are used. One is public key used for encryption and other is private key used for decryption. In [1], their work mainly focused on the data security issues in the cloud like:

1) Privacy and Confidentiality which means that once the user hosted the data in the cloud, there should be some guarantee that access to that hosted data will only be limited to the authorized access. It is ensured by the authentication services, security protocols and data encryption services.

2) Data Integrity which means data sent is same as the message received i.e. it is not altered in between. It is ensured by the firewalls and intrusion detection system (IDS).

3) Data Availability which means data should be available to users when they needed.

4) Data Location and Relocation which means data can be moved from one location to another because cloud providers have contracts with each other, so that they can use each other's resources.

In cloud computing environment, plain text is converted into cipher text by the cloud service provider and get back to the original data by the cloud user. Only the authorised user can access the data. If any unauthorised person gets the data intentionally or by mistake then he cannot get the original data [1].

In [2], their research addressed the secure hybrid framework to ensure the data security in cloud computing, which comprises public key algorithm RSA, private key algorithm AES and SHA algorithm which is used to convert arbitrary sized message into hash code with the help of hash function. They have integrated digital fingerprint mechanism to enhance the authentication process using RSA. They have achieved enhanced security framework with minimal cost and effort in. They concluded that their strategy is efficient, cost-effective and scalable for data access applications.

In [3], they have proposed security framework for clouds. In this RSA and TORDES were used for centralized database security in cloud. TORDES is symmetric key algorithm which is used for two factor authentication process. In two factor authentication, one way is to use authentication technique and other way is to use authentication format which means cloud user can access data and application related to his or her job.

1) Advantages: RSA's major advantage is that it uses public key encryption. So, RSA can be used for signing a message. It means that the receiver can verify that it was sent by the sender he or she assume to be.

2) Disadvantages: In cloud computing environment, its encryption and decryption time is high. Throughput is low and power is consumption is high. Key Generation process is also very slow [4].

B. DES

DES stands for Data Encryption Standard. It is a symmetric key algorithm which takes block size of 64 bits. Key size is also 64 bits but DES uses only 56 bits because 8 bits are used for checking parity bit. One bit in each 8- bit byte of the key is used for error detection in key generation, key distribution and key storage. Bits 8, 16, 24…..64 are used for ensuring that each byte is of odd parity.

In [8], their research proposed architecture for security of cloud storage using DES cipher block chaining, which eliminates the fraud who want to steal the sensitive data. DES is a symmetric key algorithm which has 16-round cipher. In Cipher Block Chaining (CBC) mode of operation of DES algorithm, each block of ECB (Electronic Code Book) encrypted cipher text is XORed with the next plain text block to be encrypted, so that all the blocks must be dependent on all the previous blocks as shown in Fig. 3. The first block to be encrypted has no previous cipher text, so, that plaintext block is XORed with the initialization vector, which is a 64-bit number. So, if the data is transmitted over phone line or network and there is a transmission error, then the error will be carried forward to all the subsequent blocks because each block is dependent upon all the previous blocks. So, this mode of operation is more secure than ECB (electronic code book) because of the extra XOR step that adds one more layer to the encryption process. They proposed that the security of cloud data must be considered to analyse the cloud data security risk, the cloud data security requirements, deployment of cloud security functions and the cloud data security process through encryption. In order to find out the plaintext of a particular block, One have to know the key, the Cipher text and the Cipher text of the previous block as shown in Fig. 4.

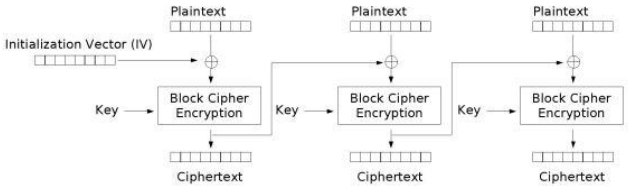

Fig. 3 Cipher Block Chaining (CBC) mode encryption

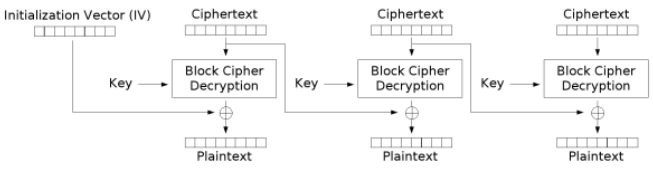

Fig. 4 Cipher Block Chaining (CBC) mode decryption

In [12], the paper work shows the comparison between the two algorithms namely RSA public key based algorithm, DES secret key algorithm. The comparison is done on the basis of two factors: ability to provide the security to data against attacks and encryption/decryption speed. According to data loads, the performance of two algorithms is different. It has been observed that DES has better performance than RSA because DES is more scalable due to varying the block and key size; power consumption is low so its throughput and confidentiality is very high.

1) Advantages: In cloud computing environment, its encryption and decryption time is less, throughput is high than RSA [4]. It is a scalable algorithm due to its varying block and key size. It provides security at both cloud service provider and client side [5].

2) Disadvantages: It is considered as insecure because brute force attack is possible. Hardware implementation of DES is very fast but DES is not designed for software and hence runs slowly. In this single key is used to encrypt and decrypt the data, so, if we lost the key then we can't decrypt the data at receiver end. As the technology is improving day by day, so, there is possibility of breaking the encrypted code. In DES, Large block size needed to hide frequency information.

C. AES

AES stands for Advanced Encryption Standard. It is a private key algorithm in which both sender and receiver use the same key for the encryption and decryption. It is a block cipher with a block length of 128 bits. It allows the three different key lengths 128 bits, 192 bits and 256 bits. AES works at multiple network layers simultaneously. For 128-bit keys, encryption process consists of 10 rounds, for 192-bit keys, 12 rounds are there and for 256-bit keys, 14 rounds are there. In each case, all the rounds are identical, except for the last round.

In [2], their research used hybrid framework which incorporates asymmetric key algorithm RSA and symmetric algorithm AES. They used RSA to provide better security in cloud by providing digital fingerprint feature. But asymmetric algorithm takes more computational time for key generation, so symmetric key algorithm AES is used to encrypt the actual message. AES provides better computational speed for cloud environment.

1) Advantages: It provides high efficiency for the security of data. It is very fast because symmetric key algorithms are fast than the asymmetric key algorithm. In this, different secret key is used for communication with every different party but if a key is compromised then only messages between a pair of sender and receiver are affected which means communication with others is still secure.

2) Disadvantages: It needs more processing as it requires - rounds of communication. It needs a secure channel for the key exchange. Since both sender and receiver use the same key, message cannot be verified to have come from a particular user.

D. SHA

SHA stands for Secure Hash Algorithm. It converts an arbitrary sized message to fixed size message digest or hash code by processing a message in blocks with the help of compression functions either custom or block cipher based mode. Hash function produces fixed length output for any sized message, so it is easy for computation.

In [2] fast enhanced authentication, the message digest is generated using secure hash algorithm which is combined with digital signature to form a concatenated string. This concatenated string is then encrypted with the help of public key of receiver and sent to the cloud user who requested data. Then deciphered message is converted into the message digest by SHA for data integrity verification and RSA is used to validate digital fingerprint.

1) Advantages: It produces a fixed length output by applying a hash function on the actual data. So, it's easy to compute fixed length output. It is a collision resistant algorithm and provides a one way hash. Its attack protection is also stronger than the other algorithms.

2) Disadvantages: It is a slower computational algorithm than MD5 algorithm. It has known security vulnerabilities. Choosing an effective hash function for a specific application is a difficult task.

E. NTRU

NTRU is a public key algorithm in which two keys are used: public key and private key. Public key is used for the encryption or to verify the digital signature but private key is used for decryption or to create digital signature. Its main characteristics are low memory and computational requirements as providing a high level security. It is based on polynomial arithmetic [6].

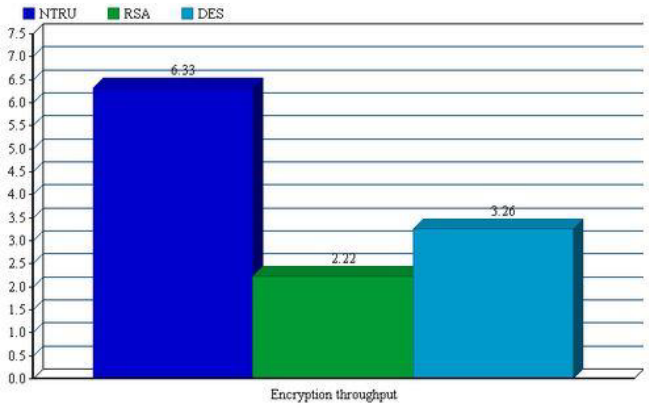

Fig. 5 Encryption speed of NTRU, DES, RSA

It involves three steps: Key generation, encryption and decryption, throughput. Throughput of the encryption/decryption algorithm is calculated by dividing total plaintext encrypted (in megabytes) to the total encryption time (in seconds). If the throughput value is increased then power consumption is decreased. So, encryption speed of the NTRU algorithm is more than the other encryption algorithms namely DES, RSA as shown in Fig. 5 and Fig. 6 [4].They have implemented NTRU algorithm on Cloud network with an Android platform.

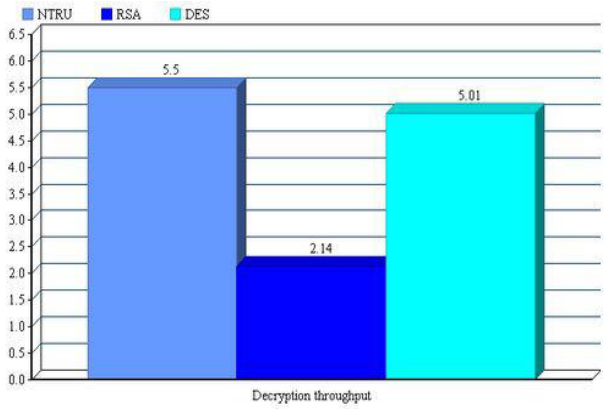

Fig. 6 Decryption speed of NTRU, DES, RSA

In [4], their work showed the comparison between NTRU public key algorithm, RSA public key algorithm and DES secret key algorithm based on three parameters: encryption time, decryption time and throughput, as shown in TABLE I. They concluded that NTRU algorithm is more secure and faster than other algorithms. It improved the security level, speed and provided reliable message with respect to key generation, encryption and decryption at the receiver end.

TABLE I

COMPARISON BETWEEN NTRU, DES, RSA ALGORITHMS

Features	NTRU	DES	RSA
Approach	Asymmetric	Symmetric	Asymmetric
Encryption Time	Low	Moderate	High
Decryption Time	Low	Moderate	High
Throughput	High	Moderate	Low
Power Consumption	Low	Moderate	High
Confidential	High	Moderate	Low

In [7], they have addressed about the Authentication, Confidentiality and Integrity in SMS (Short Message Services). The transfer of the SMS over the network is insecure, so, it is important to secure the SMS with the help of encryption algorithm. They have used the two parameters: its ability to secure the protected data against attacks by hackers and its speed and efficiency, to show the comparison between encryption algorithms like AES, DES, Triple DES, NTRU and Blowfish on different sizes of data blocks to evaluate the algorithm's speed, as shown in TABLE II. They have conducted the simulation in JAVA J2ME platform and on android operating system. Simulation program accepts three inputs: Cipher mode, data block size and algorithm. Their result showed the superiority of the NTRU algorithm in terms of the processing time over the other algorithms.

TABLE II

COMPARISON BETWEEN AES, DES, 3DES, NTRU, BLOWFISH ALGORITHMS

Input Size in (KB)	AES	3DES	DES	Blow Fish	NTRU
49	56	54	29	36	14
59	38	48	33	36	14
100	90	81	49	37	16
247	112	111	47	45	18
321	164	167	82	45	18
694	210	226	144	46	24
899	258	299	240	64	27
963	208	283	250	66	50
5345	228	1237	1466	122	94
7310	336	1366	1786	107	83
Average Time	374	452	389	60.3	35.8
Throughput (MB/Sec.)	4.174	3.45	4.01	25.892	29.3

1) Advantages: Its encryption and decryption is more efficient in both hardware and software implementations. Its key generation process is much faster than other algorithms as it allows the use of 'disposable keys' because in NTRU, keys are computationally cheap to create. Its throughput is very high because of very low power consumption. It also improves the security level and speed in cloud environment because it provides the reliable message at the receiver end with respect to encryption, decryption and key generation [4].

V. CONCLUSION

In this paper security in cloud computing is discussed. There are number of encryption/decryption methods such as RSA, DES, AES, and NTRU etc. for providing security. Some algorithms use public key encryption methods (RSA, NTRU) and other use private key encryption method (AES, DES). But NTRU is the fast encryption algorithm, which is a public-key method. NTRU algorithm is faster in encryption and decryption time which doesn't generates overhead on server and it provides better throughput than other.

ACKNOWLEDGEMENT

The authors wish to thank the reviewers and editors for their suggestions and constructive comments that help in bringing out the useful information and improve the content of paper.

REFERENCES

[1] Parsi Kalpana and Sudha Singaraju, *"Data Security in Cloud Computing using RSA Algorithm",* International Journal of Research in Computer and Communication technology, IJRCCT, ISSN 2278-5841, Vol 1, Issue 4, September 2012, pp-143-146.

[2] M.Sudha and M.Monica, "*Enhanced Security Framework to Ensure Data Security in Cloud Computing Using Cryptography*", Advances in Computer Science and its Applications ,Vol. 1, No. 1, March 2012, pp-32-37.

[3] Leena and Miss A.Kakoli rao, "*Centralized Database Security in Cloud*", International Journal of Advanced Research in Computer and Communication Engineering, Vol. 1, Issue 8, October 2012, pp-544-549.

[4] Sukhjinder Singh and Mr.Sachin Majithia, "*Implementation of NTRU on Cloud Network in an Android Platform and Comparison with DES and RSA* ", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 11, November 2013, pp-100-104.

[5] Dr.A.Padmapriya and P.Subhasri, "*Cloud Computing: Security Challenges & Encryption Practices*", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 3, March 2013, pp-255-259.

[6] Ranjeet Ranjan, Dr. A. S. Baghel and Sushil Kumar, "*Improvement of NTRU Cryptosystem*" International Journal of Advanced Research in Computer Science and Software Engineering , Volume 2, Issue 9, September 2012, pp-79-84.

[7] Yashpal Mote, Paritosh Nehete and Shekhar Gaikwad, "*Superior Security Data Encryption Algorithm(NTRU)*" An International Journal of Engineering Sciences ISSN: 2229-6913 Issue July 2012, Vol. 6, pp-171-181.

[8] *Neha Jain and Gurpreet Kaur* "*Implementing DES Algorithm in Cloud for Data Security*" VSRD-International Journal of Computer Science and Information Technology, Vol. 2 (4), 2012, pp- 316-321.

[9] Subedari Mithila and P. Pradeep Kumar, "*Data Security through Confidentiality in CloudComputing Environment*" (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 2 (5) , 2011, pp- 1836-1840.

[10] http://en.m.wikipedia.org/wiki/Cloud-computing.

[11] Sherif El-etriby and Eman M. Mohamed, "*Modern Encryption Techniques for Cloud Computing*" published in ©ICCIT 2012, pp-800-805.

[12] Aman Kumar, Dr. Sudesh Jakhar and Mr. Sunil Makkar, "*Comparative Analysis between DES and RSA Algorithm's*" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 7, July 2012, pp- 386-391.

