"SURVEY OF CRYPTOGRAPHIC TECHNIQUES TO CERTIFY SHARING OF INFORMATION IN CLOUD COMPUTING"

Nishigandha Sakharkar[1]

[1] *Assistant Professor, CMR Institute of Technology, Hyderabad, India*

Abstract - Now the world becomes the world of data where the large amount of data is shared over the Internet. Cloud storage is availing this data sharing, still there is lot of issues to get resolved to maintain the ACID properties of data. The uniform solution to this is the use of efficient encryption techniques which will provide cryptographic approach. This paper presents a view of security folds and analyses the feasibility of the application of encryption techniques to make data secure and private over the cloud. We also discussed about cloud security threats, workings and challenges that cloud service provider faces in cloud environment and presenting the study of efficient encryption techniques enhancing security of data. This paper will provide a broad view over these techniques.

Key Words: Cloud Computing, ACID, AES, Blowfish, DES, RSA, IDEA.

1. INTRODUCTION

Cloud computing is a computing standard, where lot of devices are connected privately or publicly in grid, to provide dynamic and extensible framework for applications, storage, minimizing the cost of computation, application development, data storage and speedy operations. Public, private and hybrid cloud are the classifications of cloud. Public clouds are managed as the whole responsibility of the cloud service provider. The same frameworks for composition, surveillance, and possible variances are shared between all the customers. Private clouds are exclusively limited to a single organization. Data surveillance and solitude are not the concerns of public cloud as it is opened to all the customers. Hybrid Clouds is merging of both public and private cloud models.

Cloud Providers provides three types of services.

1.1 Software as a Service (SaaS): This will provide a readymade solution for the end users where they can directly access the services. Multiple end users are serviced by this single set of services over cloud.

1.2 Platform as a Service (Paas): This is a layered architecture where the computing resources are together proposed as a service, upon which other upper layers of services can be erected. The user is free to create his own practices, according to the provider's prototype.

3. Infrastructure as a Service (Iaas): Over the network IaaS provides basic storing and processing capabilities as functional services. All computing resources are virtualized and proposed for processing. The end user can develop his own work practices on the framework.

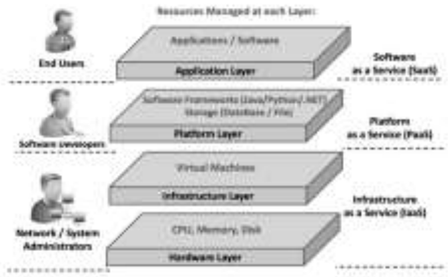

Resources Managed at each Layer:
End Users
Applications / Software
Application Layer
Software as a Service (SaaS)
Software Developers
Software Frameworks (Java/Python/.NET)
Storage (Database / File)
Platform Layer
Platform as a Service (PaaS)
Virtual Machines
Infrastructure Layer
Infrastructure as a Service (IaaS)
Network / System Administrators
CPU, Memory, Disk
Hardware Layer

Fig-1: Cloud Computing Architecture

2. CRITICAL THREATS TO CLOUD SECURITY

Cloud security is still a big challenge for application developers; as individuals wants to store and access their data more securely. With so many recent threats and technological attacks, maintaining security has become all the more important. The following threats may break the security of cloud:

a) An unauthorized user can access data which leads to data loss which can disturb businesses and consumers in a variety of ways.

b) Absence of extensible integrity approach, on-going computerized rotation of cryptographic keys, strong passwords and certificates.

c) Spectre and Meltdown one most disturbing cloud safety related issues, an erroneous set of design features in most modern devices has the capacity to allow content to be read from memory through the use of malignant JavaScript code.
d) Cloud customers also facing the problem of data loss and understanding the solutions and which body is responsible for data loss and under what circumstances is difficult.

e) High chances of DoS attacks which leads to shut down a system or network, making it idle to its intended user, this is accomplished by flooding the target with traffic, or sending it information that triggers a crash.

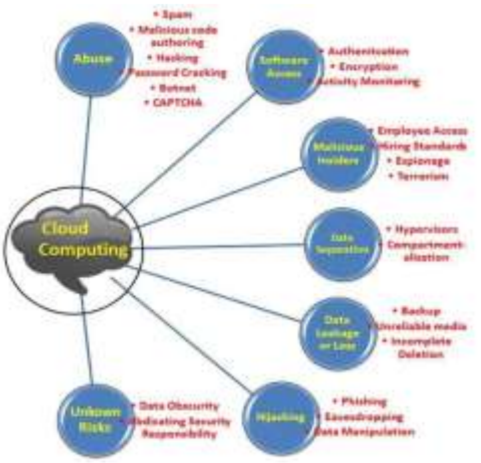


Fig-2: Threats to cloud security

3. RELATED WORK

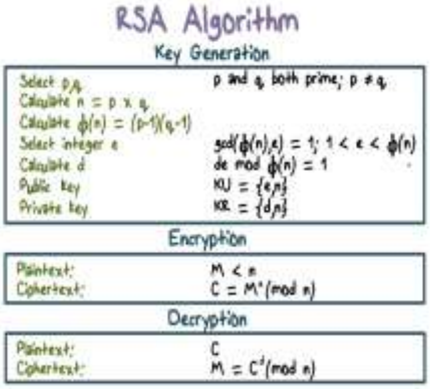
Lot of research work has been presented recently on procedures for data security and privacy in cloud computing. Many research works has been proposed on security and privacy of data by authors, still the security of data is a big concern as network capacity is increasing and needs to transfer from traditional way to cloud computing techniques.

Securing cloud does not include the security of whole system which is considered as another issue. Although so many models are proposed that ensures security of data exchanged between users and servers, but they do not provide encryption on the data exchanged. For making it tightly secure all the information needs to be coded so that any unauthorized user is not able to grab the information and its location. Some other secured models for cloud computing environment are also being proposed. But, these models also fail to solve some cloud computing security issues.

4 SECURITY TECHNIQUES IN CLOUD COMPUTING

4.1 RSA ALGORITHM

RSA is most commonly used and best encryption/decryption algorithm which is categorized in Public Key Algorithm, evolved by scientists Rivest, Shamir, and Adelman (RSA). RSA is an asymmetric encryption/decryption algorithm. It is asymmetric in a sense that it uses two separate keys for coding and decoding respectively. One key is known as public key used to perform an coding and it is known publically and second key known as private key used for decoding which is secretly used and not shared with anyone. RSA algorithm is widely used for secure data communication in cloud computing. It consists of plain text and cipher text in the form of integers between 0 to n-1.This algorithm makes the use of block cipher and each block has a value which is less than n in binary format. This algorithm is performed in three steps: Key generation, Encryption, Decryption



RSA Algorithm

Key Generation

Select p,q	p and q both prime; $p \neq q$
Calculate $n = p \times q$	
Calculate $\phi(n) = (p-1)(q-1)$	
Select integer e	$gcd(\phi(n),e) = 1; 1 < e < \phi(n)$
Calculate d	$de \bmod \phi(n) = 1$
Public key	$KU = \{e,n\}$
Private key	$KR = \{d,n\}$

Encryption

Plaintext:	$M < n$
Ciphertext:	$C = M^e (\bmod n)$

Decryption

Plaintext:	C
Ciphertext:	$M = C^d (\bmod n)$

Fig-3: RSA Encryption and Decryption

4.2 AES ALGORITHM

Advanced Encryption Standard (AES), is extensively used algorithm to encrypt and secure the data transmission. AES is a symmetric and block cipher method with 128 bits block size. Three distinct key lengths can be used in AES: 128, 192, or 256 bits. Mostly AES with 128 bit key length is popular. Execution of AES on cloud states that, first user will demand cloud services and the user data will be loaded on cloud. The User also submits his requirements to Cloud Service Provider (CSP) and chooses set of services that satisfy their needs. In future whenever any request is received to store information on cloud, this information will first encrypted using AES algorithm and then delivered to CSP. After the data is given to CSP if any application wants to access that data will first decrypt it into its original form and made available to the user.

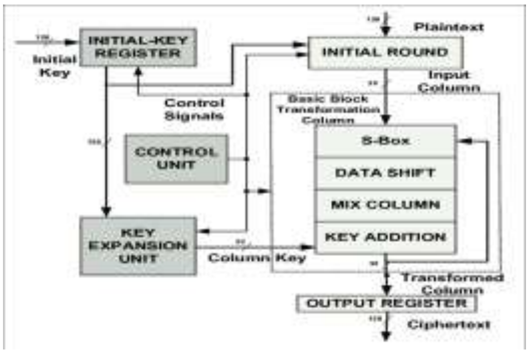


Fig-4: AES Encryption

4.3 DES ALGORITHM

Data Encryption Standard is first encryption standard. It uses block ciphers and each block of DES is of size 64 bits. It is a symmetric key encryption procedure that uses a secret key for encryption and decryption and also produces cipher text of 64 bits. The length of key which is supplied as input to the algorithm is of 56 bits. Thus there are 2^{56} keys are possible making the attacks impractical. DES is popular for satisfying the two properties of block cipher that is avalanche effect and completeness making it efficient.

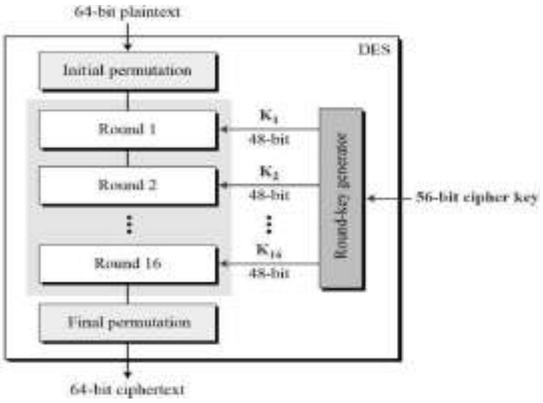


Fig-5: AES Encryption

4.4 BLOWFISH ALGORITHM

Blowfish is designed by Bruce Schneider which is much faster than DES and IDEA and can be used as an option to DES AND IDEA. It is block cipher procedure that can be effectively used for secure data transmission and uses a secret key for encryption and decryption. It uses a 64-bit size block and a variable-length key, from 32 bits to 448bits, making it tight to secure data. Blowfish Algorithm is a Feistel structure, which iterates a simple encryption function for 16 times.

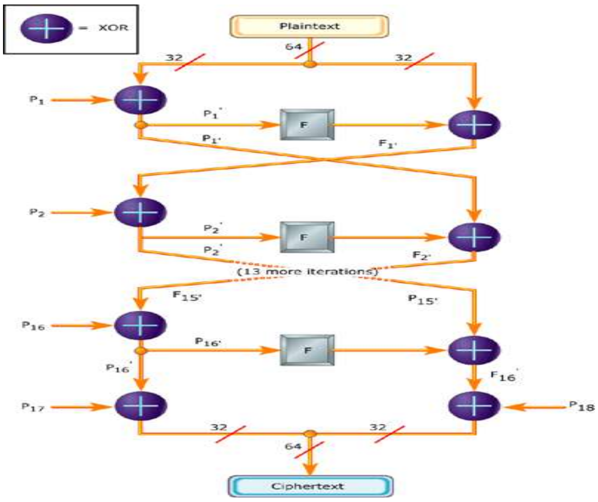


Fig-6: Blowfish Encryption

4.5 IDEA

In 1991 James Massey and XuejiaLai developed an International Data Encryption Algorithm which is a popular symmetric key algorithm. A 64 bits input data and key of length of 128 bits is used in IDEA. The 64 bits of actual data input is prorated into 4 blocks each of length 16 bits. Then exercises like sum, multiplication, modular division and bitwise exclusive OR (XOR) are tested on each block of 16 bits. Totally 52 number of keys are used to perform each individual rounds. For the first round six sub keys are generated termed as k1 to k6, sub key k1 has the first 16 bits of the actual key and k2 has the next 16 bits similarly for k3, k4, k5 and k6. Thus (16*6=96) 96 bits of actual key is used for the first round. This process is repeated for each round to make the cipher text strong and to make data more impossible to decode.

5. COMPARATIVE STUDIES OF ALGORITHMS

Characteristics	RSA	AES	DES	Blowfish	IDEA
Encryption Type	Asymmetric	Symmetric	Symmetric	Symmetric	Symmetric
Cipher Type	Neither block nor stream	Block cipher	Block cipher	Block cipher	Block cipher
Block size	Minimum 512 bits	128,192 or 256 bits	64 bits	64 bits	64 bits
Data Encryption Capacity	Used for encryption of huge amount of data	Used for encryption of less	Less than AES	Less than AES	encryption of small data
Key Size	>1024 bits	128,192 or 256 bits	56bits	32 to 448 bits	128 bits.
Memory Usage	Low RAM needed	Highest memory usage algorithm	Can execute in less than 5 kb	More than AES	Highest memory usage algorithm
Execution Time	Faster than others	Requires maximum time	Lesser time to execute	Equals to AES	Requires maximum time

Table-1: Comparative Study of Algorithms

6. CONCLUSION

This paper offers the study of all efficient algorithms that can be applied to cloud computing in order to do secure data transmission by defeating the challenges that may arise during data migration over the cloud. This paper also offers the comparative study of various encryption algorithms so that we can find the best choice of security algorithm. Each algorithm is equally efficient in different situations, still by applying single algorithm to secure data we can't trust on single level of security. So for making cloud based applications more secure we need to apply multilevel security architecture at each level of application.

REFERENCES

[1] T. A. Mohanaprakash, A. Irudayapaulraj Vinod: A STUDY OF SECURING CLOUD DATA USING ENCRYPTION ALGORITHMS, 2018 IJSRCSEIT | Volume 3 | Issue 1 | ISSN: 2456-3307

[2] Harjot Kaur& Prof. Dinesh Kumar: DATA MIGRATION FROM PRIVATE CLOUD TO PUBLIC CLOUD USING ENCRYPTION AND STEGANOGRAPHY TECHNIQUE, International journal of engineering sciences & research technology, February 2018

[3] B. Deepthi: CLOUD DATA STORAGE FOR SECURITY BY USING ATTRIBUTE-BASED ENCRYPTION", IJCESR, VOLUME-5, ISSUE-1, 2018

[4] Acqueela G Palathingal, Anmy George, Blessy Ann Thomas, Ann Rija Paul: ENHANCED CLOUD DATA SECURITY USING COMBINED ENCRYPTION AND STEGANOGRAPHY, International Research Journal of Engineering and Technology (IRJET) 2395-0056 Volume: 05 Issue: 03 | Mar-2018

[5] Omar G. Abood, Shawkat K. Guirguis,: A SURVEY ON CRYPTOGRAPHY ALGORITHMS, International Journal of Scientific and Research Publications, Volume 8, Issue 7, July 2018 ISSN 2250-3153

[6] Dr. V. Nandakumar: APPLICATION OF CO-OPERATIVE ENCRYPTION TO CLOUDS FOR DATA SECURITY, International Journal of Emerging Trends & Technology in Computer Science (IJETTCS) Volume 7, Issue 1, January - February 2018

[7] Prerna and Parul Agrawal: CRYPTOGRAPHY BASED SECURITY FOR CLOUD COMPUTING SYSTEM", Volume 8, No. 5, May-June 2017, International Journal of Advanced Research in Computer Science.

[8] Eng. Hashem H. Ramadan, Moussa Adamou Djamilou,: USING CRYPTOGRAPHY ALGORITHMS TO SECURE CLOUD COMPUTING DATA AND SERVICES", American Journal of Engineering Research (AJER) e-ISSN: 2320-0847 p-ISSN : 2320-0936 Volume-6, Issue-10, pp-334-337

[9] NishaYadav and Dr. Amit Sharma,: IMPLEMENTATION OF DATA SECURITY IN CLOUD COMPUTING", International journal of advanced technology in engineering and science, vol. no. 4, issue no.4, April2016

[10] Ankit Dhamija: A NOVEL CRYPTOGRAPHIC AND STEGNOGRAPHIC APPROACH FOR SECURE CLOUD DATA MIGRATION,2015 International Conference on Green Computing and Internet of Things (ICGCIoT).

[11] Akansha Deshmukh, Harneet KaurJanda, Sayalee Bhusari, :SECURITY ON CLOUD USING CRYPTOGRAPHY, Volume 5, Issue 3, March 2015,ISSN: 2277 128X, International Journal of Advanced Research in Computer Science and Software Engineering.

[12] V.Masthanamma, G.LakshmiPreya,: AN EFFICIENT DATA SECURITY IN CLOUD COMPUTING USING THE RSA ENCRYPTION PROCESS ALGORITHM, International Journal of Innovative Research in Science, Engineering and Technology (An ISO 3297: 2007 Certified Organization) Vol. 4, Issue 3, March 2015

[13] Abha Sachdev, Mohit Bhansali,: ENHANCING CLOUD COMPUTING SECURITY USING AES ALGORITHM, International Journal of Computer Applications (0975 – 8887) Volume 67– No.9, April 2013.

[14] Regil V Raju, M.Vasanth, Udaykumar P,: DATA INTEGRITY USING ENCRYPTION IN CLOUD COMPUTING, Volume 4, No. 5, May 2013 Journal of Global Research in Computer Science.