Cryptography in Cloud Computing: A Approach to Ensure Security in Cloud

Abstract— Cloud computing is the on-demand opportunity of computer system resources, mostly data storage and computing power, without direct active management by the user. The term is mainly used to describe data centres available to many users over the internet. Big clouds, main today, repeatedly have functions allocate over multiple locations from central's servers. If the connection to the user is relatively close, it may be desig- nated an edge servers. Cloud computing is an Internet-based computing model which give some resources through Cloud Service Provider(CSP)to cloud users(CU)on demand basis without buy the underlying infra- structure and follows pay-per-use basis.

Keywords - Cloud Computing, Cryptography, Security Issues Privacy, Security Algorithms, Encryption, Decryption.

INTRODUCTION

Cloud computing is one of the popular topics of the present world. Internet has started operate all these new technologies. Internet was designed firstly to be powerful, but not completely safe. Distributed appli- cations like these are much prone to attacks. Cloud Computing has all the feebleness associated with these internet usage and the extra threats arise from the combined, Virtualized and redistributed resources. There are multiple data privacy concerns in cloud computing. Wrong revelation of a data used in busi- nesses in cloud to third parties is one of the major is- sues that have been found. Encryption should be perfectly used and the crypto algorithms involve AES, RSA, DES and 3 DES. In this paper, we report about using crypto algorithms so as to expand security concern. Cloud Security can be make sure by data integrity, Secured data transfer and by Cryptography. The two variety of algorithms are Symmetric and Asymmetric encryption key algorithms. Symmetric accommodate algorithms like DES, AES, 3 DES and Blowfish algorithm. Asymmetric contains algorithms like RSA, Daffier - Hellman Key Exchange. A symmetric key and asymmetric key algorithm is used to encrypt and decrypt the data in cloud.

- *Akshay Tarade is currently pursuing masters degree program in Information Technology in Mumbai University, India, PH-9987506606.. E-mail: akshay- tarade4254@gmail.com*
- *Ashwini khillari is currently a head of depatment in PHCASC, Rasayan, India, PH-9860809283. E-mail: kashwini@mes.ac.in*

Methods*:*

a. In the paper[1] the authors deal with the problem of safety of data through data transmission. The main thing to fear about this paper is the encryption of data so that private and privateness can be easily achieved. The algorithm utilized here is Rijndael Encryption Al- gorithm along with EAP-CHAP.

A.Symmetric key algorithms:

Symmetric utilises single key, which works for both encryption and decryption. The symmetric systems provide a two channel system to their users. It secures authentication and authorization. Symmetric-key algo- rithms are those algorithms which utilises only 1 and only key for both. The secret's kept as secret. Symmet- ric algorithms have the advantage of not taking in an excessive amount of of calculation power and it works with high speed in encryption. Some

famous Symmetric-key algorithms employed in cloud computing incorporate: encoding Standard (DES), Triple- DES, and Advanced Encryption Standard (AES).

a)Advanced Encryption Standard (AES):
In cryptography, the Advanced Encryption Standard is[3] sort of symmetric-key encryption algorithm. Each of the ciphers has a 128-bit block size and hav- ing key sizes of 128, 192 and 256 bits, one by one. AES algorithm reassures that the hash code is encrypted in a secure way. AES has a block size of 128 bits. Its algorithm is : Key Expansion, Initial Round - Round Keys are added.

b) Data Encryption Standard (DES) :
The Data Encryption Standard (DES) is a block cipher and is under a symmetric key cryptography. start in January 1977 by the National Institute of Standards and Technology, named as NIST. At the encryption site, DES clearly takes a 64-bit plaintext and creates a 64-bit cipher text ,at the decryption operation, it takes a 64-bit cipher text and make a 64-bit plaintext, and same 56 bit cipher key is used for both encryption and decryption. The encryption process is made using two permutations (P-boxes), which we call early and final arrangement, and sixteen Fiestel rounds. Each round uses a different type of 48-bit round key which is developed from the cipher key according to a pre-set algorithm.

B.Asymmetric Key Algorithms :
It is comparatively a new concept unlike symmetric cryptosystem. Different keys are used for encryption and decryption. This is a possessions which set this scheme different than symmetric encryption scheme. Each receiver have a decryption key of its own, nor- mally mention to as his personal key. Receiver require to generate an encryption key, referred to as his public key. In General, this type of cryptosystem involves trusted third party which officially declares that a specific public key belongs to a specific person or entity only.

a)RSA Cryptosystem:
This cryptosystem is one the start systems and oldest of asymmetric cryptosystem. It remains employed and used cryptosystem even now. The system was gener- ate by three scholars named Ron Rivest, Adi Shamir, and Len Adleman and hence, it's call as RSA cryp- to system. This algorithm is employed for public-key cryptography and not personal key crptofra. it's the primary and still most regularly used asymmetric algorithm. It require two keys namely a public key and a personal key. the general public secret's used for encrypting messages and is understood to every one. Messages encrypted with the employment of public key will be decrypted only by using the private key. during this verification procedure, the server implements public key authentication by signing a particular message with its private key, which is named as digital signature. The signature is then returned to the client. Then it confirm using the server's known public key.

b) Diffie-Hellman Key Exchange:
Whitfield Diffie and Martin Hellman introduced a key exchange protocol with the help of the separate logarithm problem in 1976. In this key exchange protocol operator and receiver will manage to set up a secret key to their symmetric key system, using an insecure channel. To set up a key Alice
select a random integer aE[1; n] calculate ga, similarly Bob computes gb for random bE[1; n] and sends it to Alice. The secret key is gab, which Alice calculate by computing (gb)a and Bob by computing (ga)b. The main concepts on which the security of the Diffie-Hellman Protocols defend upon DDH, DHP, DLP like etc.

C.Hashing Algorithms:

MD5- (Message-Digest algorithm 5):

A universally used hash function algorithm in cryp- tography with a 128-bit hash value and possesses a

variable length message into a fixed-length output of 128 bits. First the input message is 2 part up into lump of 512- bit blocks then the message is extra service so its total length is divisible by 512. The sender of the information uses the general public key to encrypt the message and also the receiver uses its private key to decrypt the message.

Results:

The concerns regarding security problems in cloud computing has often kept organizations distant from uploading data in a secure manner, thus the introduction of encryption of data before being uploaded to the cloud the data is much more secure and private, being less prone to external intrusions or hacking. The data passes through the gateway in a safer way. Implemen- tation of AES encryption further enhances the security of data because of its advantages over other encryption algorithms such as DES or RSA.

Factors	DES	3DES	AES
Key Length	Key length is56 bits	Length is168 bits (k1, k2 and k3) Length is 112 bits (k1 and k2)	Length is 128, 192, 256 bits. It varies w.r.t rounds
Round(s)	It has 16 rounds	It has 48 rounds	For 10 rounds - 128bit Key For 12 rounds - 192 bit key For 14 rounds - 256 bit key
Block Size	64 bits	64 bits	128 bits
Speed	The speed is Slow	The speed is Very Slow	The speed is Fast
Security	Not Secure Enough	Sufficient Security	Relatively better Security practically

Conclusion :

Cloud computing is growing as a replacement thing and it's the new trend indeed and lots of of the organizations and massive companies are moving toward the cloud but lagging behind due to some security problems. Cloud security is an ultimate concept which is able to crush the drawbacks the acceptance of the cloud by the massive MNCs, companies and organizations. There are lots of security algorithms which can be implemented to the cloud. DES, Triple-DES, AES, and Blowfish etc are some symmetric algorithms. DES and AES are mostly used symmetric algorithms as they're relatively safer. DES is sort of simple to implement than AES. RSA and Diffie-Hellman Key Exchange is that the asymmetric algorithm. RSA and Diffie-Hellman Key Exchange is employed to come up with encryption keys for symmetric algorithms in cloud. But the protection algorithms which permit linear searching on decrypted data are required for cloud computing, which is able to make sure about the protection of the information. There is an oversized scope of improvement during this field of research. we are able to use cryptography in numerous places so as security in cloud. for instance, Cryptography may be used for maintaining cloud data access control, cloud data trust management, verifiable computing, cloud data authorization and authentication and secure data storage. except of these, Lattice based Cryptography and ID based Cryptography are the 2 important sectors which is ensuring cloud data security in present world. Still there's lots of research to be wiped out this field.

References :

1. Sanjoli Singla , Jasmeet Singh ,"Cloud computing security using encryption technique", IJARCET, vol.2, ISSUE 7.
2. R. Bala Chandar, M. S. Kavitha , K. Seenivasan," A proficient model for high end security in cloud compu- ting", International Journal of Emerging Research in Management &Technology, Vol.5, Issue 10.

3. Bokefode Jayant.D, Ubale Swapnaja A, Pingale Subhash V., Karane Kailash J. , Apate Sulabha S.
,"Developing Secure Cloud Storage System by Apply- ing AES and RSA Cryptography Algorithms with Role bases Access Control Model", International Journal of Computer Applications, Volume 118-No.12, May2015