DATA SECURITY ALGORITHMS IN CLOUD COMPUTING: A REVIEW

Charanjeet Kaur[1], Er. Gurjit Singh Bhathal[2]
[2]Asst. Prof., Department of Computer Engineering
Punjabi University Patiala

Abstract: Cloud computing term that is used to explain variety of computing concepts that involves large number of computer linked through a real time a communication network as the internet .it allow users to store up large amount of data on cloud and use that data as per requirement anyplace of the world. with increase of large amount of data and user on the cloud ,so security turns to be main point and apt technology for the decade it offer dynamic allocation, However many malicious action in cloud have coexist with the growth of cloud users. Main security challenge is data storage security on cloud. It should make possible for users to store their large amount of data on cloud and no worry about its integrity. Thus, there should be some mechanism that enables users to store their data on cloud without worry.

Keywords: Cloud, security, RSA, AES

I. INTRODUCTION

Cloud computing are these days attractive technology for the company and organization that own large data centers to rent their resources. Cloud computing is a kind of computing which provide the facility to use these resources offered on cloud system, in other words we can say that it is a paradigm where resources are retrieve through network, it also allows users to use this technology enabled services through the internet. Cloud computing is an internet based service where the user can easily use storage services on cloud without knowing how it is actually working .so the main point is about security . There are two types of security concerns from the service provider's point of view and cloud client's point of view" For example 23% of cloud service provider (CSP) says in a survey that developing and maintaining data security in cloud is one of the challenges that become obstruction for cloud acceptance and Another survey by Fujitsu [shows that cloud clients are worried about the accessibility of their data store on cloud. The security loop hole in public or private clouds are actually caused by the infrastructure of cloud computing because it depends on the substantial virtualization. The cloud service provider is reliable to ensure the security of cloud computing resources and client's data and applications by provide security tools. So data on the cloud centers must be safe and sound.

II. CLOUD COMPUTING

Cloud computing is an allegory for the internet. It is the allocation of computer or IT framework through the Internet. That is the amenities of shared resources, software, and services over the internet to meet the adaptable demand of the customer with minimum effort or interaction with the cloud service provider.

III. CLOUD COMPUTING SECURITY ISSUES

A. Identification & authentication

Cloud processing, dependent upon the sort of cloud and additionally the transmission model, specified clients should firstly be secured and accompanying access necessities and consents may be conceded in like manner. This methodology is focus at checking and appreciative singular cloud clients by utilize usernames and passwords assurances' to their cloud profiles Authorization is a vital information security requirement in Cloud computing to ensure referential integrity is maintain. It follows on in exerting control and civil liberties over process flows within Cloud computing. Authorization is maintained by cloud service provider.

B. Confidentiality

In Cloud processing, privacy has real influence particularly in administering of cloud service provider control over associations' information arranged across over different appropriated databases. It enable requirement when utilizing in Public because of directness nature. Declaring privacy of clients' outline and securing their information that is for purpose got to takes into account data security conventions to be authorized at different distinctive layers of cloud requisition.

C. Integrity

The honesty requirement lies in applying the due attentiveness inside the cloud area, fundamentally when getting to Information. Thusly atomicity, consistency, confinement are the properties of the cloud's information should indeed be powerfully forced over all Cloud registering convey models

D. Non-repudiation

Non-repudiation in Cloud registering might be acquired by applying the conventional e-trade security conventions and token facilities to information transmission inside cloud provisions, for example, advanced marks, timestamps and assertion receipts administrations.

.To overcomes these security issues in cloud computing many security encryption and decryption algorithms are proposed.

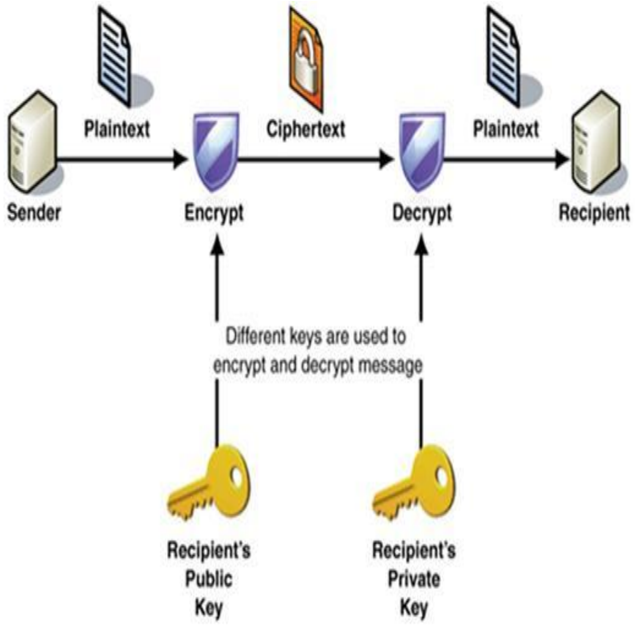

Fig 1.Process of cryptography.

IV. VARIOUS SECURITY ALGORITHMS

To enhance data security in cloud computing there are many existing algorithms .which are using of different encryption and decryption techniques to secure clients data on cloud. And user can store their data at cloud without any tension and can access their Data as per use. There are many security algorithms that provide security to users s' data on cloud and secure their data from malicious action. Different types of algorithms are proposed for security concern in cloud computing in which large amount of user data store at cloud and theses algorithms are provides specific mechanism CSP to secure users s'data on cloud.

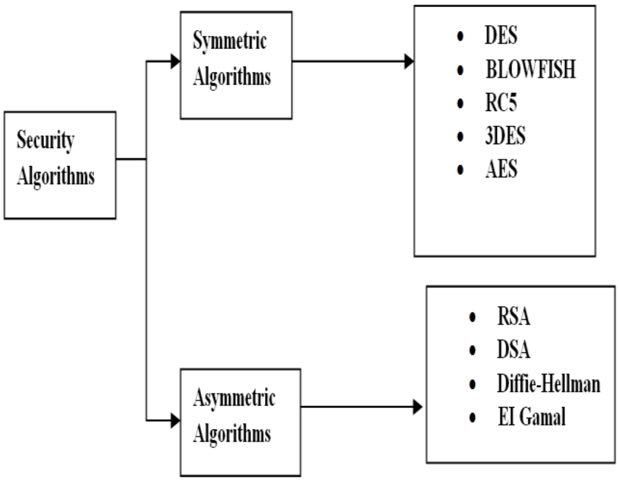

Fig 2.existing algorithms

V. SYMMETRIC KEY ALGORITHMS

1. Data Encryption Standard (DES): DES has a complex set of rules and transformations that were intended specifically to yield fast hardware implementations and slow software implementations. DES is a block-cipher employing a 56-bit key that applying on 64-bit blocks. Although this latter point is becoming less important today since the speed of computer processors is several orders of magnitude faster today than twenty years ago.

Two important variant that strengthen DES are:
Triple-DES (3DES): A variant of DES that employs up to three 56-bit keys and makes three encryption/decryption passes over the block.

DESX: A variant devised by Ron Rivets. By combining 64 additional key bits to the plaintext prior to encryption, effectively increases the key length to 120 bits

AES: Advanced Encryption Standard (AES): AES uses a symmetric key cryptography scheme called Rijndael, a block cipher designed by Belgian cryptographers Joan Daemen and Vincent Rijmen. The algorithm can use a variable block length and key length. The latest specification allowed any combination of keys lengths of 128, 192, or 256 bits and blocks of length 128, 192, or 256 bits

Rivets Ciphers (aka Ron's Code): Named for Ron Rivets, a series of SKC algorithms.

RC2: A 64-bit block cipher using variable-sized keys designed to replace DES. It's code has not been made public although many companies have licensed RC2 for use in their products because the key size was limited to 40 bits.

RC4: A stream cipher using variable-sized keys; it is widely used in commercial cryptography products.

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.

RC6: A 128-bit block cipher based upon, and an improvement over, RC5

Blowfish: A symmetric 64-bit block cipher invented by Bruce Schneier; 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

VI. SYMMETRIC KEY ALGORITHMS

Diffie-Hellman: D-H is used for secret-key key exchange only, and not for authentication or digital signatures.
Digital Signature Algorithm (DSA): The algorithm provides digital signature capability for the authentication of messages.

ElGamal: Designed by Taher Elgamal, a PKC system similar to Diffie-Hellman and used for key exchange.
Hash Functions
Hash functions, which are also called message digests and

single way encryption, are algorithms which do not use any key. They compute a fixed length hash value based upon the plain text. It becomes impossible to recover the contents or the length of plaintext. A digital fingerprint of the file's contents is provided by the hash algorithms, which makes it ensured that the file has not been altered by an intruder or virus. Hash functions are also employed commonly by many operating systems to encrypt passwords. In simple terms, the integrity of file is measured by hash functions.

Hash algorithms that are in common use today include:
1. Message Digest (MD) algorithms: A series of byte-oriented algorithms that produce a 128-bit hash value from an arbitrary-length message.
MD2: Designed for systems with limited memory, such as smart cards
MD4: Developed by Rivest, similar to MD2 but designed specifically for fast processing in software.
MD5: Also developed by Rivest after potential weaknesses were reported in MD4; this scheme is similar to MD4 but is slower because more manipulation is made to the original data.

2. Secure Hash Algorithm (SHA): Algorithm for NIST's Secure Hash Standard (SHS).
SHA-1 produces a 160-bit hash value
SHA-2, comprises five algorithms in the SHS: SHA-1 plus, SHA-224, SHA-256, SHA-384, and SHA-512 which can produce hash values that are 224, 256, 384, or 512 bits in length, respectively.
SHA-3 is a proposed new SHS algorithm. Although there have not been any successful attacks on SHA-2, NIST decided that having an alternative to SHA-2
ability to select multiple entities, improving the system's usability.

RSA Algorithm:
1.RSA: Very common and the first, PKC implementation, which is named for the three MIT mathematicians Ronald Rivest, Adi Shamir, and Leonard Adleman who developed it. RSA today is used in several software products and it can be used for digital signatures, key exchange, or encryption of small blocks of data. RSA uses a variable size key and a variable size encryption block. The key-pair is derived from a very large number, n, that is the product of two prime numbers chosen according to special rules; these primes may be 100 or more digits in length each, yielding an n with roughly twice as many digits as the prime factors. The public key information includes n and a derivative of one of the factors of n; an attacker cannot determine the prime factors of n (and, therefore, the private key) from this information alone and that is what makes the RSA algorithm so secure

Algorithm
Key Generation: KeyGen (p, q)
Input: Two large primes – p, q
Compute $n = p . q$
$\varphi (n) = (p - 1)(q - 1)$
Choose e such that $\gcd(e, \varphi (n)) = 1$
Determine d such that $e . d \equiv 1 \mod \varphi (n)$
Key:
public key = (e, n) and secret key= (d, n)
Encryption: c = me mod n where c is the cipher text and m is the plain text.

RSA has a multiplicative homomorphic property i.e., it is possible to find the product of the plain text by multiplying the cipher texts. The result of the operation will be the cipher text of the product.
Given ci = E(mi) = mi
e mod n, then
(c1 . c2) mod n = (m1 . m2)e mod n

VII. PROBLEM FORMULATION

In Cloud computing technology there are a set of important issues, which include issues of privacy, security, anonymity, telecommunications capacity, government surveillance, reliability, and liability, among others. But the most important between them is security and how cloud provider assures it. Generally, Cloud computing has several customers such as ordinary users, academia, and enterprises who have different motivation to move to cloud. If cloud clients are academia, security effect is on performance of computing and for them cloud provides a way to combine security and performance. For enterprises the most important problem is also security but with different vision. For them high performance may be not as critical as academia. So, as per the perspective of different users, the security point of view is different .security algorithms are used to enhance data security in cloud compuring.

VIII. CONCLUSION

This paper presented an independent study of security algorithms in cloud computing. Which provides the specific method to secure data on cloud computing. But there are many security problems. The researchers are try to mitigate these issues by building efficient algorithms.

REFERENCES

[1] B. Claybrook, "Moving to a private cloud: Technology choices and implementation issues," Retrieved on 5/4/2013, 2010. [Online]. Available
[2] Gartner, "What you need to know about cloud computing security andcompliance"(HeiserJ),[online]2009,https://www.gartner.com/doc/1071415/need-knowcloud-computing- Security (Accessed 23 December 2013).
[3] Cong Wang, Qian Wang, KuiRen and Wenjing Lou, "Ensuring Data Storage Security in Cloud Computing", In Quality of Service, 2009. 17th International Workshop on, page 19, 2009
[4] Balachandra Reddy Kandukuri, Rama Krishna Paturi and Dr. AtanuRakshit, "C loud security issues" In ServicesComputing, 2009. IEEE International Conference on, page 517520, 2009.[6] Kashish Goyal, Supriya Kinger" Modified Caesar Cipher for Better Security

[5] Amazon Web Services: Overview of Security Processes, may 2011.[6] 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

[6] P. Samarati and S. D. C. di Vimercati, ―Data protection in outsourcing scenarios: Issues and directions‖, in Proc. ASIACCS, Apr. 2010, pp. 1–14

[7] Gurpreet Singh, Supriya Kinger" Integrating AES, DES, and 3-DES Encryption Algorithms for Enhanced Data Security "International Journal of Scientific & Engineering Research, Volume 4, Issue 7, July-2013.

[8] Md Asif Mushtaque, H, Dhiman, S. Hussain and S. Maheshwari, "Evaluation of DES, TDES, AES, Blowfish and Two fish Encryption Algorithm: Based on Space Complexity", International Journal of Engineering Research & Technology (IJERT), Vol. 3 Issue 4, April – 2014.