International Journal of Interdisciplinary Innovative Research &Development(IJIIRD)

ISSN: 2456-236X

Vol. 04 Issue 02 | 2020

SECURING CLOUD DATA USING CRYPTOGRAPHIC ALGORITHMS

Sanjay R[1]

[1]MCA (Master of Computer application), Department of Computer Application, Jain Deemed-to-be University, Bangalore, Karnataka, India

ABSTRACT

Cloud computing model will allow the users to access a large amount of data from the cloud without having the hardware devices and software devices [1]. The cloud providers will try to provide high-security authenticity and integrity [2]. Therefore, when utilizing cloud infrastructure, we have certain benefits, such as cost-effective, modular and versatile structures, when delivering network access to the vast amount of customers at a time, for person and company uses, internally. [3]. Cloud computing will provide a centralized virtual environment such that we can access the data from the cloud without having a physical infrastructure [5]. Since the cloud is a collection of server and the user's data will be stored in these machines so it may get some security issues like confidentiality, integrity and availability (CIA). To overcome these security issues we have some security mechanisms like symmetric and asymmetric cryptography algorithms such as a DES,AES, RSA, RC6and BRA. But these algorithms have a chance of breaking by the hackers so we came to some other algorithm like Blowfish. Where Blowfish symmetric algorithm deals with the data confidentiality and where RSA will ensure the authentication and also we have secure hash algorithm-256 for data integrity [6]. If we see we have some algorithms like key oriented and keyless algorithm which is used in cloud computing.

Keyword:-Cloud computing, DES, AES, RSA, Blowfish, Secure hash-256

1. INTRODUCTION

Cloud computing may be a well and essential platform for electronic communication [5]. It offers a pay-as-you-go model it implies that for what we have a tendency to use we wish to procure that resources. Cloud computing is consistent and reliable because the organization no ought to build their own infrastructure by this the upkeep value is going to be reduced. Cloud computing has some benefits yet as disadvantages. it's some security problems like knowledge access management, identity management and risk communications encrypted by translating end-user knowledge to be transmitted in a very coded, undecipherable kind and by encrypting the decipherable format by taking the knowledge the info |the information} from the user and changing it into ciphertext and decrypting to the initial plain text with this capability approach cryptography provides the protection like data integrity, Authentication, Non-Repudiation, Confidentialitymanagement etc [6].So we have a tendency to came for to cloud cryptography wherever cryptography may be a technique wherever we will convert original knowledge into an undecipherable format.

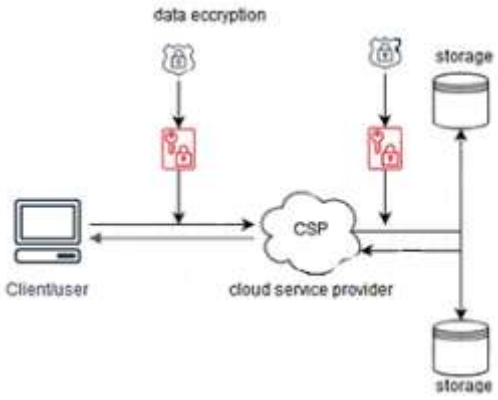

Fig -1: Introduction to cryptography

2. LITERATURE REVIEW ON CRYPTOGRAPHY ALGORITHMS:

When we sort sensitive data in the public cloud problems may arise when customers completely will be leaving in that environment because we can't tell whether the data exist in the cloud. So we have a necessity to use cryptography where we can convert the text into an unreadable format, cryptography has three algorithms namely key oriented, keyless, and hashing. By using the hash function the fixed-length signature will be created [4]. Where key algorithms are the symmetric and asymmetric algorithm. In symmetric key we use only one secret key for encryption and decryption whereas in asymmetric we use public key is used for encryption and a private key is used for decryption.

3. PROPOSED SYSTEM

This paper suggests totally different coding models and their application was contrasted in terms of the dynamics of time and space. Most of the models adopt a similar flow wherever the information is encrypted victimisation the coding algorithms, then the encrypted information is kept on the cloud service provider's servers.The different strategies of encrypting the information with different algorithms like DES(Data coding Standard),AES(Advanced coding Standard),RSA (Rivest,Shamir,Adleman), etc,.These square measure a number of the encryptions,techniques

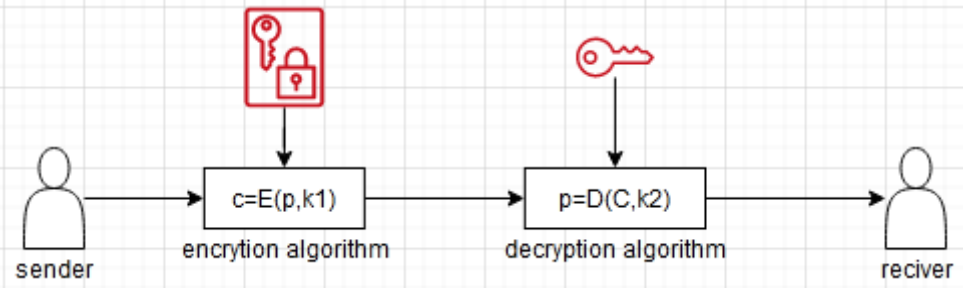

Fig-2: Encryption Algorithm

Cryptography uses mathematics to transform plain text content (P) into an unreadable ciphertext (C) format called encryption and turn the ciphertext back into a plain text called decryption using the Cryptographic Algorithms (E) constructed using encryption keys (k1 and k2) and the decryption algorithm (D) that reverses and generates the original plain text back from the Cryptographic Algorithms (E). This paper Explain the different mechanism of encryption techniques.

Cryptographic Algorithms are broadly classified as:

- **Symmetric Algorithms:** Symmetric Algorithm's shares one secret key to encrypt data and execute with higher speed. The shared key is recognized by the sender and the receiver. Example RC6,3DES,Blowfish[10].
- **Asymmetric Algorithms:** Asymmetric Encryption shares a pair of keys for encryption operations,keys are shared as a public key for encryption and private key for decryption. Compared with single-key symmetric algorithms, such algorithms have a large computing expense and thus slower speed.Example:RSA Diffie Hellman.
- **Hash Algorithms:**Compress the signing data to a set standard format. Example MD5, SHA
- **Signature Algorithms:**Used for signing and authenticating user data are focused on a single key. Example RSA, DH.

4.SYMMETRIC ALGORITHM

4.1 DES(Data Encryption Standard):

DES is the oldest symmetric-key block cypher introduced in the year 1977 by the NIST. As it uses block cypher it will be in the form of the block instead of having in the bits. It will work by using only one key for encrypting and for decrypting. The implementation of DES is done by using the Feistel cypher this will use round Feistel structure and it uses 64-bit as a block size. By using the 64-bit block size we can have the key-length of 56 bits. We can divide this DES has like three modules such as Expansion p-box, A straight p-box, A group of s-boxes. Because of key length, they introduced triple DES where it consists of 3*56=168 bits. By using triple we can encrypt-decrypt-encrypt process we can use triple DES for implementation of single DES by setting of k1,k2 and k3 can do the with the same value.

ISSN: 2456-236X

Vol. 04 Issue 02 | 2020

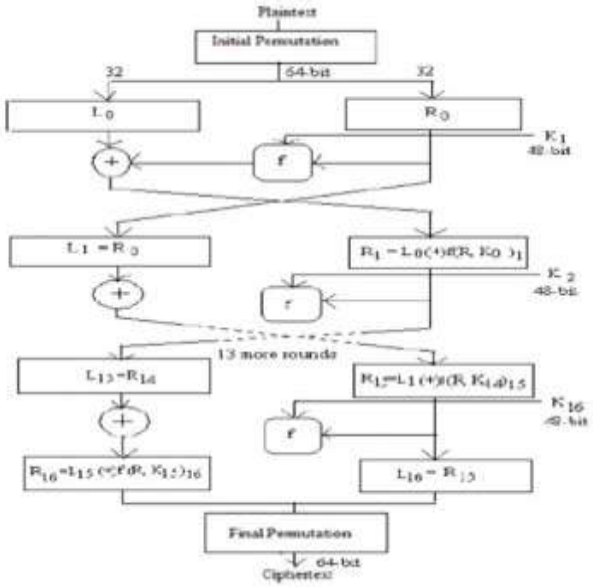

Fig-3:Symmetric Algorithm Mechanism

4.2 AES(Advanced Encryption Standard)

AES is a cruciform formula, that remains normally used every day and is sixfold faster than the DES formula, and it's substituted by AES. They went to the triple-DES however they found it's slow. it's 128-bit knowledge and it has 128/192/256-bit keys. we will additionally implement the package like java and C language. it'll use substitution permutation rather than Feistel cypher. It performs computation on bytes before DES was exploitation the bits by this issue we will tell that 128-bit block as sixteen bytes. In AES sixteen bytes are split into four equal rows and columns sort of a matrix-like Add spherical key: The sixteen bytes of the network are presently thought-about as 128 bits and XORed to the 128 bits of the spherical key.

- **Mix columns**: each column of the four bytes is currently modified employing a special mathematical calculation the output changes the complete column.
- **Shift rows:** In shift rows, the primary row can't be rapt and therefore the second row is rapt to 1 computer memory unit to left and therefore the thirdrow is rapt to the second row and at last, we wish to shift the fourth row and by doing this we'll get a new matrix with constant sixteen bytes.
- **Byte Substitution**: The rows and columns substitutes supported the mounted table (s-box)

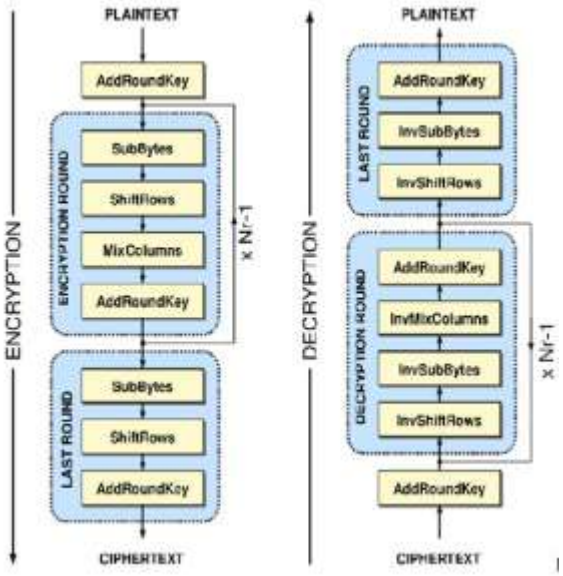

Fig-4:AES Encryption Mechanism

4.3 BlowFish Algorithm

Blowfish could be a regular cryptanalytic algorithmic program that is designed within the year 1993.BlowFish could be a general-purpose algorithmic program that is substituted rather than DEs algorithmic program. This algorithmic program uses a 1 key/single key for coding and coding. This algorithmic program contains an advanced scheduled key and contains a 64-bit block size with a keylength of 32-488 bit.BlowFish could be a sixteen round cypher and it implements an oversized key-dependent,s-boxes and stuck s-boxes. the first methodology in blowfish is to initialise the values victimization the p-array and s-boxes and it's extracted by victimization Pi's positional representation system digits and doesn't embody patterns. Blowfish algorithmic program has 2 elements a key-expansion half and additionally a data-encryption half wherever as key growth half can convert the variable length-key of at the most 448 bits into several subkeys arrays that the wholly it has 4168 bytes.

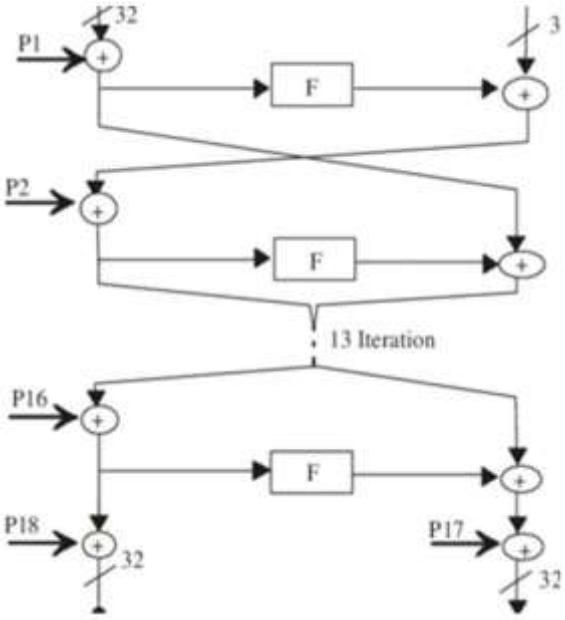

Fig-5:BlowFish encryption mechanism

5.ASYMMETRIC ALGORITHMS

5.1 RSA(Rivest, Shamir, Adleman):

This cryptosystem is one among the underpinnings. Even these days it still maintains the foremost used cryptosystem. 3 researchers Ron Rivest, Adi Shamir, and Len Adleman created the framework and afterwards, it's known as the RSA cryptosystem. we are able to see 2 elements of the RSA cryptosystem, at first the age of key pairs and additionally to measurements for secret writing coding.

RSA Key Pair Generation:
Any person or cluster concerned in communications mistreatment secret writing must build a number of keys to be distinctive public and a personal key.
RSA algorithmic program
• Generate two large prime numbers, p and q.
• Calculate their product, n = p x q.
• Compute φ(n) = (p -1) x (q-1).
• Choose a large integer, e, such that e is relatively prime to φ(n). [gcd(e, φ(n)) = 1].
• Select a value, d, such as e x d ≡ 1 mod φ(n). [i.e.,(e x d) – 1 is divisible by φ(n). Also, e and d are multiplied inverse of each other under φ(n) and gcd(d, φ(n)) = 1]. • Public key consists of the pair (e,n).
• The private key consists of the pair (d,n).
• A plaintext, P is encrypted to ciphertext, C as follows:

$$C = Pe \bmod n$$

The plaintext is recovered from the ciphertext as follows:

$$P = Cd \bmod n$$

5.2 Homomorphism Encryption:

Cloud vendee encodes its information before conveyance to the Cloud provider, at an equivalent time, likewise, he needs to figure thereupon information and wishes to decode the knowledge. The shoppers can propose the giving of a personal key to the server for the coding of the knowledge before to perform the calculations propose that has principally relied upon confidentiality of knowledge that is kept within the cloud. the most aim of the homomorphic coding is to perform the encrypted info while not coding of {the information|the knowledge|the information} it implements a mathematical operation to perform on the encrypted information while not compromising the coding it shows the transformation from one data set whereas having parts between the relationships of parts that square measure within each set.

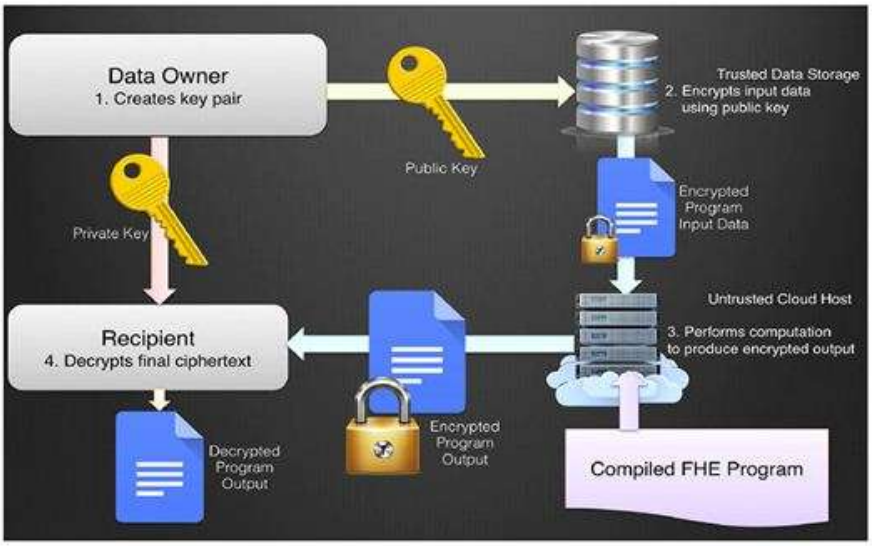

Fig-6:Homomorphism Encryption

6. HASHING ALGORITHM

6.1 SSH-256

It means a secure hash algorithm which is a cryptographic hash function with the length of 256 bits. It is a keyless hash function which is an MDC(manipulation detection code). The algorithm is a mathematical operation which runs on the digital data the text will be processed in the form of blocks of 512=16*32 bits for every block we need to processed 64 rounds we have to perform some basic operations are Boolean operations AND, XOR, and also OR and also integer addition module. It is implemented in the Digital signature, Generating numbers randomly, Key updates and derivations, one-way functions, User authentication, Malware deduction. Block size indicates the 64 bytes and Max allowed message length is 33 bytes.

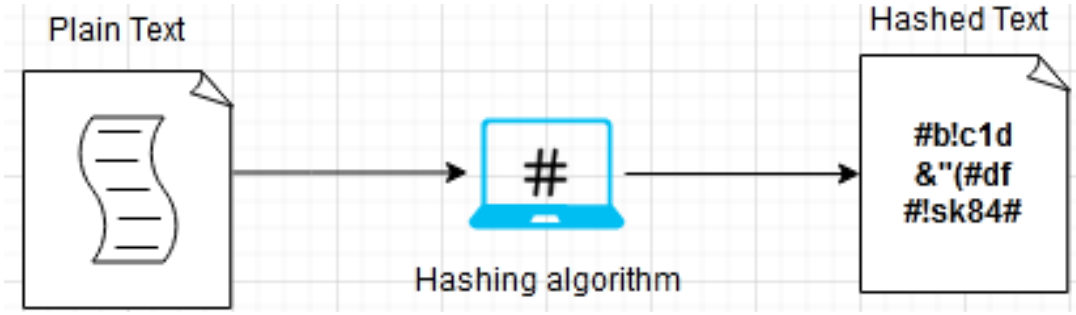

Fig-7: Hashing algorithm

7.COMPARISION:

Table-1:Comparing Encryption Algorithms

Algorithms	DES (Data Encryption Standard)	AES (Advanced Encryption Standard)	RSA(Rivest,Shamir,Adleman)
Encryption type and Key length	Symmetric - 56 bits	Symmetric - 128,192, 256	Asymmetric – 256
Implementation	Banking Industries	Web app login Financial transactions	Digital signature
Advantages	Faster execution	More robust	Eliminating the distribution of key
Level of security	Less secured	High-level security	High-level security
|Limitations	IT Can be broken by using brute force attack	Simple algebraic structure	Slower compare to other algorithms

8. CONCLUSIONS

Cloud computing is one of the well-known and essential platform for data communication. In order to maintain secured data communication, some efficient encryption and decryption algorithms should be considered. There are so many risks and challenges in key managements, as these keys are vulnerable to security threats. This paper mainly concentrates on some algorithms which can overcome key management issues. In this work, the comparison of Key and keyless algorithms are done and eases the process of algorithm selection to provide better security for data communication.

9. ACKNOWLEDGEMENT

I am sincerely thankful to Jain University for providing me with the opportunity to write a research paper on the topic "**Securing Cloud Data Using Cryptographic Algorithm**".I am also thankful to **Professor.Subarna Panda** for guiding me in every single stage of this research paper.Without his support, it would have been very difficult for me to prepare the paper so meaningful and interesting.I am also thankful to **Dr M N.Nachappa** (Head Of The Department) of Jain University who have helped me during the course of this research paper in different ways. Through this paper, I have learnt how the data is secure in the cloud platform.It has helped me analyze how the information can be secured and its advantages and disadvantages.

10. REFERENCES

[1] Nathan James "The Federal Prison Population Build up: Overview, Policy Changes, Issues, and Options" Congressional Research Service. 7-5700 www.crs.gov R42937.
[2] Dallin H. Oaks; Studying the Exclusionary Rule in Search and Seizure, THE UNIVERSITY OF CHICAGO LAW REVIEW Vol. 37, No.4, Summer 1970.
[3] Badri Nath, Franklin Reynolds, Roy Want, "RFID Technology and Applications," IEEE CS and IEEE ComSoc, Vol. 5, No. 1, 2006, pp. 22-24.
[4] Lei Zhang and Zhi Wang, "Integration of RFID into Wireless Sensor Networks: Architectures, Opportunities and Challenging Problems," Proceedings of the Fifth International Conference on Grid and Cooperative Computing Workshops, Hunan, 2006, pp.463-469.
[5] Ron Weinstein, "RFID: A Technical Overview and Its Application to the Enterprise," IT Professional, Vol. 7, No. 3, June 2005, pp. 27-33
[6] Elit Wireless Solutions (2007) GM862-GPS Hardware user guide. 1vv0300728 Rev. 8 - 20/09/07 World Academy of Science Engineering and Technology