Study & Comparative Analysis of Different Algorithms Used in Data Security in Cloud Environment

Janardan Pawar
Vice - Principal, Indira College of Commerce & Science, Pune
contactvijayak@iccs.ac.in, contactvijayak@yahoo.co.in

Vijaya Kumbhar
Asst.Professor, Indira College of Commerce & Science, Pune

Smrithi R. Bhat
Student (MCA-II) ,Indira College of Commerce & Science, Pune.
bhatSmrithi@iccs.ac.in

Abstract - Cloud Computing is an emerging technology in today's business era. It allows convenient on demand access to resources that involve large number of computers connected through Internet. Public clouds vendors offer many resources (application, storage, hardware, software's etc. The security issues present in public cloud is more challenging. As everything is accessed publically; many users have the threat to store and retrieve it publically.

As many organizations are moving data to the cloud there is a need to protect data against unauthorized access. Hence it is necessary to study the security issues in public cloud to secure data. The purpose of this paper is to provide an overview of pubic cloud computing and the security issues involved .This paper deals with the different algorithms or method used for securing data in public cloud.

Keywords - public cloud, cryptography.

I. *INTRODUCTION*

Public clouds are the latest evolution of computing, offering tremendous value to businesses in terms of better economics, agility, rapid elasticity, etc. The public cloud infrastructure is operated by a cloud service provider and the services are offered over the internet. As many organizations are moving their data on the cloud there is a need to protect the data against unauthorized users, denial of access, modifications etc. Data protection is achieved by implementing cryptographic algorithms. The use of public clouds requires trust of businesses on cloud service providers.

II. *SECURITY ISSUES IN PUBLIC CLOUD*

Even though the public cloud offers tremendous benefits, businesses cannot embrace public cloud services without taking some security considerations into account. In this section, we will highlight some of the security concerns in public cloud.

III. *MULTI-TENANCY AND PRIVACY ISSUES*

A Public cloud is offered at an affordable price because resources are shared between multiple tenants. Using the scalability feature, Public cloud providers offer the same infrastructure to multiple clients and scale up resources on a real-time basis. When you share CPU, memory and datacenter resources with multiple users, there is a risk of unauthorized access of your business networks. If there is any flaw in the cloud network, it allows other users to access your data or even read your network information. In addition, the Public Cloud allows people using the same hardware to hack your IP and MAC numbers and gain access to your business networks.

IV. *LIMITED CONTROL ON RUNNING TECHNOLOGIES*

Another important area of concern is that Public Cloud users do not have any control on the business processes managing the cloud. This lack of transparency about the technology used in the Public Cloud leaves you with limited control on your networks. For instance, you are not sure of which virtualization product is offering the virtualization feature, and the version of the software used. While choosing a Public Cloud, it is recommended to inquire about virtualization technologies used and features offered.

V. *DATA ENCRYPTION ISSUES*

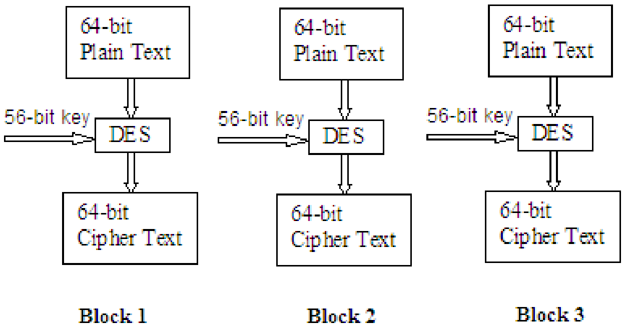
Data integrity and security is an important aspect for every business. With the increased scrutiny of data management techniques of companies by the government authorities, managing your data using proper storage methods has become even more important. In a Public cloud, data needs to be encrypted using highly secure methods. Unencrypted data can be vulnerable to hacking attacks. While choosing a Public Cloud, you need to check if private keys are shared with other users and how your data is processed.

In addition, data retention techniques need to be checked. Business data that is deleted or moved needs to be completely erased from the datacenter. However, you do not have the complete control on the datacenter infrastructure to use proper data sanitization techniques. If data is not properly erased, it can be accessed by other users and used in a harmful manner.

Cryptography - Symmetric Key Algorithms

Data Encryption Standard (DES)-

DES is a block cipher. It encrypts data in blocks of size of 64 bits each. The same algorithm is used for encryption and decryption. The key length is 56 bits. The basic idea is shown in the figure below



The conceptual working of DES

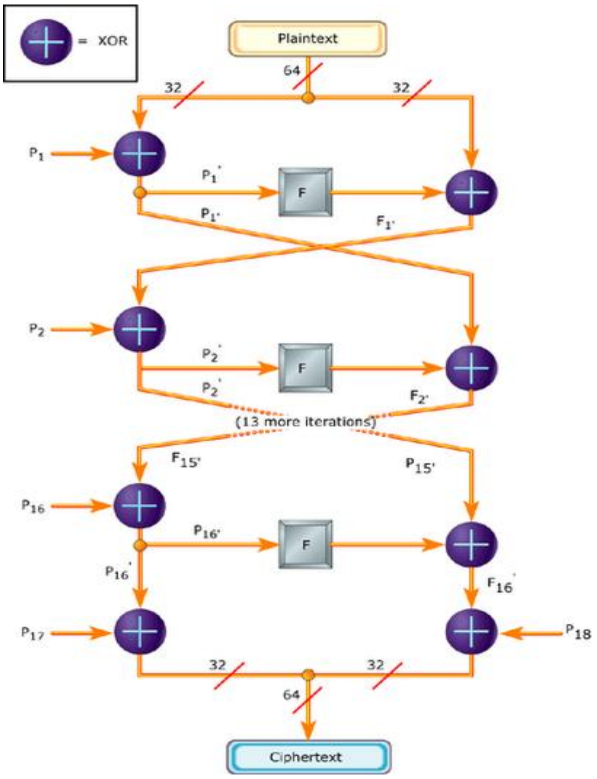
Blowfish

Blowfish was developed by Bruce Schneier and has the reputation of being a very strong symmetric key cryptographic algorithm .According to Schneier; Blowfish was designed with the following objectives in mind.

Fast-Blowfish encryption rate on 32 bit microprocessors is 26 clock cycles per byte

Compact-Blowfish can execute in less than 5kb memory. Data encryption happens with 16 round Feistel network as shown in the figure

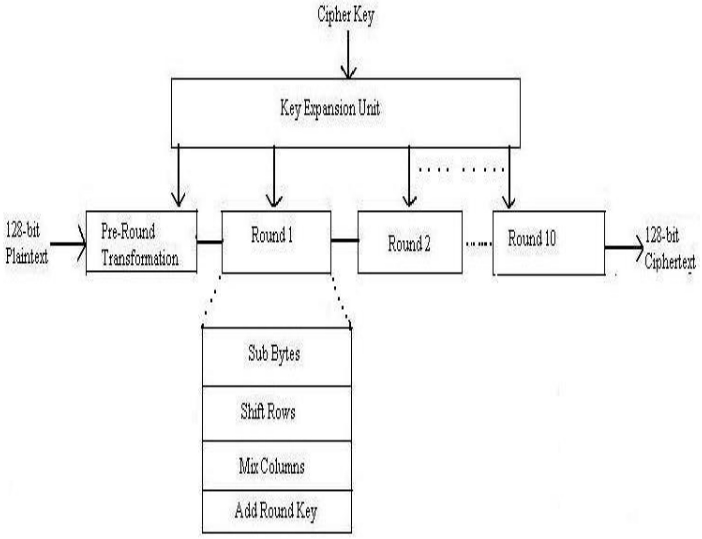
fig : Encryption with Blowfish



Asymmetric key Algorithms

Advanced Encryption Standard (AES)-

Advanced Encryption Standard is a symmetric- key block cipher published as FIPS-197 in the Federal Register in December 2001 by the National Institute of Standards and Technology (NIST). AES is a non-Feistel cipher. AES encrypts data with block size of 128-bits. It uses 10, 12, or fourteen rounds. Depending on the number of rounds, the key size may be 128, 192, or 256 bits as shown in figure. AES operates on a 4×4 column-major order matrix of bytes, known as the state.



RSA-Ronald Rivest, Adi Shamir and Leonard Adleman have invented the RSA algorithm and named it after the inventors.The RSA algoritm is based on mathematical fact that it is easy to find and multiply large prime numbers together but it is extremely difficult to factor their product. The private and public keys in RSA are based on very large (made up of 100 or more digits) prime numbers.

Diffie-Hellman Key Exchange-

WhiteField Diffie and Martin Hellman devised an amazing solution to the problem of key agreement or key exchange in 1976.The beauty of the scheme is that the two parties who want to communicate securely can agree on a symmetric key using this technique.

1. Firstly tow parties agree on two large prime numbers n and g. These two integers need not be kept secret. Both the parties can use an insecure channel to agree on them.

2. First party chooses another number x and calculates A such that :

$$A = g^x \bmod n$$

3. First part sends the number A to second party.

4. Second Party independently chooses another large random integer y and calculates B such that:

$$B= g^y \bmod n$$

5.Second Party sends the number B to first party

6. A now computes the secret key K1 as follows:

$$K2= B^X \bmod n$$

7. B now computes the secret key K2 as follows:

$$K2= A^y \bmod n$$

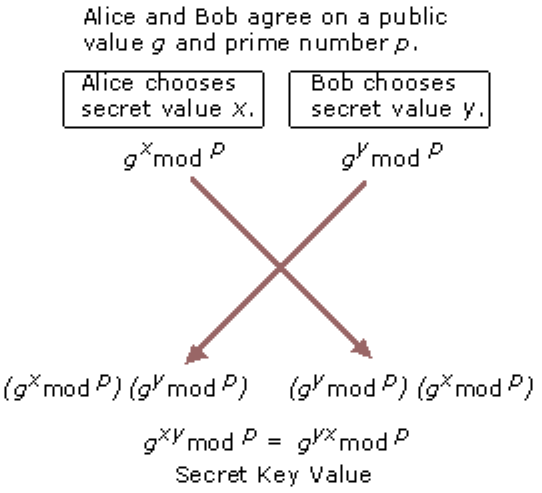

Alice and Bob agree on a public value g and prime number p.
Alice chooses secret value x.
Bob chooses secret value y.
g^xmod p
g^ymod p
$(g^x$mod $p)$ $(g^y$mod $p)$
$(g^y$mod $p)$ $(g^x$mod $p)$
g^{xy}mod p = g^{yx}mod p
Secret Key Value

Fig: Diffie-Hellman key exchange algorithm

Homomorphic Encryption -

Cloud consumer encrypts its data before sending to the Cloud provider, but each time he has to work on that will have to decrypt that data. The consumer will require giving the private key to the server to decrypt the data before to perform the calculations required, which might influence the confidentiality of data stored in the Cloud. Homomorphic Encryption systems are needed to perform operations on encrypted data without decryption (without knowing the private key); only the consumer will have the secret key. When we decrypt the result of any operation, it is the same as if we had performed the calculation on the plaintext (or original data). The Homomorphic encryption is distinguishing, according to the operations that are performed on raw data.

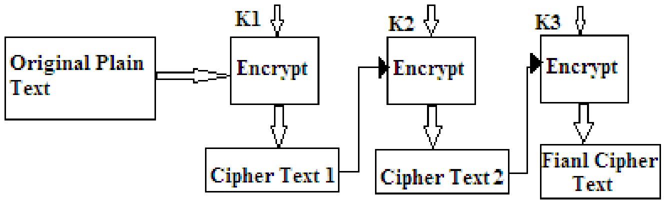
- Additive Homomorphic encryption: additions of the raw data.
- Multiplicative Homomorphic encryption: products for raw data.

Triple DES-

Although the meet-in-the-middle attack on Double DES is not quite practical yet, in cryptography, it is always better to take the minimum possible chances. Therefore Triple DES was invented. There are two forms of triple DES

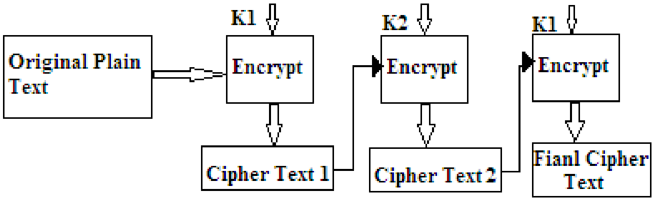
- Triple DES with three keys-The plain text is first encrypted with key K1 then with key K2 and finally with key K3 where all the three keys are different from each other.

fig:Triple DES with three keys



- Triple DES with two keys-Triple DE with three keys is highly secure but it requires 56x3 = 168 bits for the key, which can be slightly difficult in practical situations. Here only two keys are used K1 and K2.The plain text is encrypted using K1 and then with key K2 and finally again with key K1.

fig:Triple DES with two keys



Comparative Analysis of cryptographic algorithms:

Characteristic	Symmetric key cryptography	Asymmetric key cryptography
Key used for encryption/decryption	Same key is used	Different keys are used
Speed for encryption/decryption	Very fast	Slower
Size of resulting encrypted text	Usually same or less than the original clear text size	More than the original clear text size
Number of keys required as compared to the number of the participants in the message exchange	Equals the square of the number of the participants	Same as the number of participants
Usage	Mainly for encryption and decryption	For encryption and decryption as well as for digital signatures

Comparison of various algorithms used in cloud environment:

Algorithm name	Key size (bits)	Areas of Application	Advantages	Problems faced
DES	56-64	Electronic data	Fast	Brute Force attack Runs relatively slow
Blowfish	32-448	Bulk Encryption Packet encryption Hashing Random bit generation	Is used when key is not frequently changed. Fastest when executed in 32bit microprocessors. Flexible and secure	Not suitable in packet switching
AES	128,192 or 256	Used in smart cards	Easily adaptable in modern processsors.	Brute force attack Side channel attacks
RSA	80			Timing attacks Cipher text attacks Side channel attacks
Triple DES with three keys	168	Electronic data	Secure	Quite slow
Triple DES with two keys	112	Electronic data	Less secure than Triple DES eith three keys	Faster than Triple DES with three keys

VI. *CONCLUSION:*

In this paper, a comparative study of cryptography algorithms is done. It is clear from the study that none of the algorithm is excellent and none of this is weak. Cloud Security is the most wide research area as cloud users are increasing day by day. Though the algorithms are best, the data is inside cloud is stored at unknown location, managed by third party. Hence there is a need for the enhanced algorithm in data security so that cloud user should ensure about the data stored in cloud is safe to store and access.

VII. *REFERENCES:*

1. *Hongwei Li, Yuanshun Dai , Bo Yang, "Identity-Based Cryptography for Cloud Security"*
2. *Amar Gondaliya, "Security in Cloud Computing", Technical Paper Contest 2011, Hasmukh Goswami College of Engineering, Gujarat Technological University, Ahmedabad*
3. *Sherif El-etriby, Eman M. Mohamed, Hatem S. Abdul-kader, "Modern Encryption Techniques for Cloud Computing" ,ICCIT, 2012*
4. *S.Ezhil Arasu, B.Gowri, S.Ananthi,"Privacy-Preserving Public Auditing In Cloud Using HMAC Algorithm", International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-2, Issue-1, March 2013.*
5. *F. A. Alvi, B.S Choudary ,N. Jaferry , E.Pathan, "A review on cloud computing security issues & challenges" .*
6. *Huijun Xiong, Xinwen Zhang, Danfeng Yao, Xiaoxin Wu, Yonggang Wen," Towards End-to-End Secure Content Storage and Delivery with Public Cloud", CODASPY'12, February 7–9, 2012, San Antonio, Texas, USA.*
7. *Kuyoro S. O., Ibikunle F. & Awodele O."Cloud Computing Security Issues and Challenges", International Journal of Computer Networks (IJCN), Volume (3) : Issue (5) : 2011 247*
8. *Anthony Bisong1 and Syed (Shawon) M. Rahman, "An Overview Of The Security Concerns In Enterprise Cloud Computing", International Journal of Network Security &*

Its Applications (IJNSA), Vol.3, No.1, January 2011, DOI : 10.5121/ijnsa.2011.3103

9. *Rashmi Nigoti1, Manoj Jhuria2 Dr.Shailendra Singh,'' A Survey of Cryptographic Algorithms for Cloud Computing'', IJETCAS 13-123*
10. *Pankaj Arora, Rubal Chaudhry, Wadhawan Er. Satinder Pal Ahuja, " Cloud Computing Security Issues in Infrastructure as a Service", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 1, January 2012 ISSN: 2277 128X*