International Journal of Emerging Research in Management &Technology
ISSN: 2278-9359 (Volume-3, Issue-1)

Research Article | **January 2014**

Analysis of Encryption Algorithms in Cloud Computing

Pawan Kumar*
PhD Scholar, PTU, Kapurthala, Punjab, India

Dr. Sawtantar Singh
Professor CSE, BMSCE, Mukatsar, India

Dr. Surender Kumar
Associate Prof.CSE Deptt. HCTM India

Abstract-

Cloud computing grows very fast. Number of users stores their data on Cloud. Data storage security refers to the security of data on the storage media. So, Security is an important factor in cloud computing for ensuring clients data is placed on the secure mode in the cloud. Data must not be stolen by the third party so authentication of client becomes a mandatory task. In this paper, we discuss a number of existing techniques used to provide security in the field of cloud computing on the basis of different parameters. In Cloud computing technology there are a set of important policy 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 on performance of computing and for them cloud providers have to find 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. The Cipher Cloud is a framework that lets users keep their data confidentially on public cloud frameworks. To achieve this, the Cipher Cloud uses a two-step encryption process, in by which all the data sent from a client to a cloud server or vice versa is kept totally encrypted and confidential. The most thorough security controls needed to protect the most sensitive data may not be guaranteed in public cloud computing architectures, while they can be realized in private cloud computing architectures. As the most promising cloud computing approach, this paper suggests selective encryption techniques, which almost gives the data confidentiality just like private cloud models.

Keywords—Cloud Computing, Data Storage, Security

I. INTRODUCTION

In computer networking, cloud computing is a word which is describe different computing concepts which contains huge number of computers attached through a real-time communication like internet. Cloud computing is also called distributed computing over the network i.e. the ability to execute an application or a program on many computers at the same time. Cloud services provides software and hardware which from a remote locations which are managed by third party to the individual or businesses. The term "The cloud" is a phrase for internet. We are not bothering with what ain cloud is or what the process in it we are concerned with the safe sending and receiving of data. In this system there is a great amount of workload shift [1]. Local computers don't have to do the heavy lifting anymore when it comes to running application now a days it is handled by the cloud instead. On the users side the demand of the software and hardware have been decrease. The only think the user's system should have the basic configuration to run the cloud computing system software which is same as web servers. The networking of software and hardware are still there now there are higher level service capabilities which are used to builds the applications. There are data and computer resources behind the servers.

Cloud computing is growing fast with time. Cloud computing illustrate Information Technology as fundamentally diverse operating model that takes advantage of the maturity of web applications and networks and the rising Interoperability of computing systems to provide IT services. Data security is becoming a fundamental obstruction in cloud computing. There are some kind of solution that are providing some security with model, some technology.

Cloud computing refers to the delivery of computing resources over the Internet. Instead of keeping data on your own hard drive or updating applications for your needs, you use a service over the Internet, at another location, to store your information or use its applications. Doing so may give rise to certain privacy implications. Cloud computing is the delivery of computing services over the Internet. Cloud services allow individuals and businesses to use software and hardware that are managed by third parties at remote locations. Examples of cloud services include online file storage, social networking sites, webmail, and online business applications. The cloud computing model allows access to information and computer resources from anywhere that a network connection is available. Cloud computing provides a shared pool of resources, including data storage space, networks, computer processing power, and specialized corporate and user applications.

Cloud computing combines the data-sharing model and service statistical model. From a technical point of view, cloud computing has the following three basic characteristics [2]

- Hardware infrastructure architecture is based on the clusters, which is large-scale and low-cost. The infrastructure of cloud computing is composed of a large number of low-cost servers, and even the X86 server

architecture. Through the strong performance, the traditional mainframe's prices are also very expensive.

- Collaborative development of the underlying services and the applications is to achieve maximum resource utilization. By this way, application's construction is improved. But for traditional computing model, applications to be complete dependent on the underlying service.
- The redundant problem among multiple low-cost servers is solved by the software method. Because of using a large number of low-cost servers, Failure between nodes cannot be ignored, so the issue of fault tolerance among nodes should be taken into account, when designing software [2].

A. Benefits

The following are some of the possible benefits for those who offer cloud computing-based services and applications:

1) *Cost Savings* — Companies can reduce their capital expenditures and use operational expenditures for increasing their computing capabilities. This is a lower barrier to entry and also requires fewer in-house IT resources to provide system support.
2) *Scalability/Flexibility* — Companies can start with a small deployment and grow to a large deployment fairly rapidly, and then scale back if necessary. Also, the flexibility of cloud computing allows companies to use extra resources at peak times, enabling them to satisfy consumer demands.
3) *Reliability* — Services using multiple redundant sites can support business continuity and disaster recovery.
4) *Maintenance* — Cloud service providers do the system maintenance, and access is through APIs that do not require application installations onto PCs, thus further reducing maintenance requirements.
5) *Mobile Accessible* — Mobile workers have increased productivity due to systems accessible in an infrastructure available from anywhere.

B. Challenges

The following are some of the notable challenges associated with cloud computing, and although some of these may cause a slowdown when delivering more services in the cloud, most also can provide opportunities, if resolved with due care and attention in the planning stages.

1) *Security and Privacy* — Perhaps two of the more "hot button" issues surrounding cloud computing relate to storing and securing data, and monitoring the use of the cloud by the service providers. These issues are generally attributed to slowing the deployment of cloud services. These challenges can be addressed, for example, by storing the information internal to the organization, but allowing it to be used in the cloud. For this to occur, though, the security mechanisms between organization and the cloud need to be robust and a Hybrid cloud could support such a deployment.
2) *Lack of Standards* — Clouds have documented interfaces; however, no standards are associated with these, and thus it is unlikely that most clouds will be interoperable. The Open Grid Forum is developing an Open Cloud Computing Interface to resolve this issue and the Open Cloud Consortium is working on cloud computing standards and practices. The findings of these groups will need to mature, but it is not known whether they will address the needs of the people deploying the services and the specific interfaces these services need. However, keeping up to date on the latest standards as they evolve will allow them to be leveraged, if applicable.
3) *Continuously Evolving* — User requirements are continuously evolving, as are the requirements for interfaces, networking, and storage. This means that a "cloud," especially a public one, does not remain static and is also continuously evolving.

II. DATA STORAGE & SECURITY IN CLOUD COMPUTING

Cloud storage is a model of networked enterprise storage where data is stored not only in the user's computer, but in virtualized pools of storage which are generally hosted by third parties, too. Hosting companies operate large data centers, and people who require their data to be hosted buy or lease storage capacity from them. The data center operators, in the background, virtualized the resources according to the requirements of the customer and expose them as storage pools, which the customers can themselves use to store files or data objects. Physically, the resource may span across multiple servers. The safety of the files depends upon the hosting websites [3].

Cloud storage services may be accessed through a web service application programming interface (API), a cloud storage gateway or through a Web-based user interface.

Cloud storage is:

- made up of many distributed resources, but still acts as one
- highly fault tolerant through redundancy and distribution of data
- highly durable through the creation of versioned copies
- Typically eventually consistent with regard to data replicas.

Data storage security refers to the security of data on the storage media, which means non-volatile or fast recovery after loss. This security should be taken into account by software engineers in design stage of cloud storage services. It includes not only data redundancy and dynamic, but also isolation. Redundancy is the most basic measures to protect

data storage security, and dynamic means user data may often change, so effective measures are needed to ensure data consistency. Isolation is that since different user's data is stored in the same platform, to guarantee the independence between the data, which means user can only access their own data, and data changes of other users will not affect the current user [4].

A. Data Security Issues in Cloud Computing

With the gradual promotion of the application, any private information in the facilities of the cloud computing may be found on any equipment. In order to protect the user's information from reveal, Siani Pearson[5] put forward design principles in design process of cloud computing services to ensure that user's message and business information would not leaked out. It includes: Transmit and store user's information as little as possible. After systemic analysis, the cloud computing applications will collect and store the most necessary information only.

- Security measures will be adopted to prevent unauthorized access, copying, using or modifying personal information.
- Achieve user's control to the greatest degree. Firstly, it is necessary to allow the user to control the most critical and important personal information. Secondly, it is available to manage personal information by a trusted third party.
- Allow users to make choice. Users have the right to select the use of personal information. Besides, they can join or leave freely.
- Make clear and limit the purpose of use of data. Personal information must be used and handled by the person with specific identification for specific purpose and owner of information should be notified before using.
- Establish feedback mechanism to ensure that safety tips and detailed measures of the service will be provided to the user timely.
- It can maximize the security of user's data after introducing principles above [5].

III. EXISTING ALGORITHS FOR SECURITY

To provide secure communication over the network, encryption algorithm plays a vital role. It is the fundamental tool for protecting the data. Encryption algorithm converts the data into scrambled form by using "the key" and only user have the key to decrypt the data. In Symmetric key encryption, only one key is used to encrypt and decrypt the data. Another technique is using asymmetric key encryption; two keys- private and public keys are used. Public key is used for encryption and private key is used for decryption. Fig 1 shows some of the symmetric & asymmetric algorithms [6].

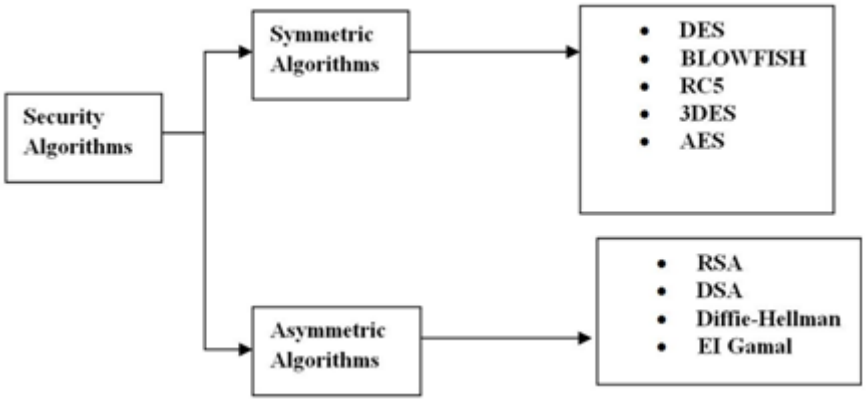

Figure 1: Security Algorithms

A. Symmetric Algorithms:

DES: This stands for Data Encryption Standard and it was developed in 1977. It was the first encryption standard to be recommended by NIST (National Institute of Standards and Technology). DES is 64 bits key size with 64 bits block size. Since that time, many attacks and methods have witnessed weaknesses of DES, which made it an insecure block cipher.[7]

Algorithm:

function DES_Encrypt (M, K) where M = (L, R) M
 IP(M)

For round 1 to 16 do
 K_i SK (K, round)
 L L xor F(R, K_i)
 swap(L, R)

end swap(L, R)

M □ IP^1(M)
return M
End

BLOWFISH: This was developed in 1993. It is one of the most common public algorithms provided by Bruce Schneier. Blowfish is a variable length key, 64-bit block cipher. No attack is known to be successful against this. Various experiments and research analysis proved the superiority of Blowfish algorithm over other algorithms in terms of the processing time. Blowfish is the better than other algorithms in throughput and power consumption [8]. **Algorithm**

Divide x into two 32-bit halves: x_L, x_R
For i = 1to 16:
$X_L = X_L$ XOR P_i
$x_R = F(X_L)$ XOR x_R
Swap X_L and x_R
Next i
Swap X_L and x_R (Undo the last swap.)
$x_R = x_R$ XOR P_{17}
$x_L = x_L$ XOR P_{18}
Recombine x_L and x_R

RC5: It was developed in 1994. The key length if RC5 is MAX2040 bit with a block size of 32, 64 or 128. The use of this algorithm shows that it is Secure. The speed of this algorithm is slow. [9]

Algorithm

A = A + S[0];
B = B + S[1]; for i
= 1 to r do
A = ((A Xor B) <<< B) + S[2 * i]
B = ((B Xor A) <<< A) + S[2 * i + 1]
Next

DES: This was developed in 1998 as an enhancement of DES. In this standard the encryption method is similar to the one in original DES but applied 3 times to increase the encryption level. But it is a known fact that 3DES is slower than other block cipher methods. This is an enhancement of DES and it is 64 bit block size with 192 bits key size. 3DES has low performance in terms of power consumption and throughput when compared with DES. It requires always more time than DES because of its triple phase encryption characteristics.[8][10].

Algorithm

For j = 1 to 3
{
$C_{j,0} = IV_j$
For i = 1 to n_j
{
$C_{j,i} = E_{KEY3}(D_{KEY2}(E_{KEY1}(P_{j,i} C_{j,i-1})))$
Output $C_{j,i}$
}}

AES: (Advanced Encryption Standard), is the new encryption standard recommended by NIST to replace DES. Brute force attack is the only effective attack known against it, in which the attacker tries to test all the characters combinations to unlock the encryption. Both AES and DES are block ciphers. It has variable key length of 128, 192, or 256 bits; default 256. It encrypts data blocks of 128 bits in 10, 12 and 14 round depending on the key size. AES encryption is fast and flexible; it can be implemented on various platforms especially in small devices. Also, AES has been carefully tested for many security applications.[9][10].

Algorithm

Cipher(byte[] input, byte[] output)
{
byte[4,4] State;
copy input[] into State[] AddRoundKey
for (round = 1; round < Nr-1; ++round)
{
SubBytes ShiftRows MixColumns AddRoundKey
}
SubBytes ShiftRows AddRoundKey
copy State[] to output[]
}

B. Asymmetric Algorithms:

RSA: This is an Internet encryption and authentication system that uses an algorithm developed in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman. The RSA algorithm is the most commonly used encryption. Till now it is the only algorithm used for private and public key generation and encryption. It is a fast encryption [11].

Algorithm

Key Generation: KeyGen(p, q)
Input: Two large primes – p, q
Compute n = p . q
φ (n) = (p - 1)(q - 1)
Choose e such that gcd(e, φ (n)) = 1
Determine d such that e . d ≡ 1 mod φ (n)

Key:
public key = (e, n)
secret key= (d, n)

Encryption: c = m^e 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 $c_i = E(m_i) = m_i^e$ mod n, then

$(c1 . c2) \bmod n = (m1 . m_2)^e \bmod n$

DSA: The Digital Signature Algorithm (DSA) is a Federal Information Processing Standard for digital signatures. It was proposed by the National Institute of Standards and Technology (NIST) in August 1991 for use in their Digital Signature Standard (DSS) and adopted as FIPS 186 in 1993. Four revisions to the initial specification have been released: FIPS 186-1 in 1996, FIPS 186-2 in 2000, FIPS 186-3 in 2009, and FIPS 186-4 in 2013. With DSA, the entropy, secrecy, and uniqueness of the random signature value *k* is critical [10]. It is so critical that violating any one of those three requirements can reveal the entire private key to an attacker. Using the same value twice (even while keeping *k* secret), using a predictable value, or leaking even a few bits of *k* in each of several signatures, is enough to break DSA. [11]

Diffie-Hellman Key Exchange (D-H): Diffie–Hellman key exchange is a specific method of exchanging cryptographic keys. It is one of the earliest practical examples of key exchange implemented within the field of cryptography. The Diffie–Hellman key exchange method allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure communications channel. This key can then be used to encrypt subsequent communications using a symmetric key cipher.

IV. COMPARISON OF EXISTING ALGORITHMS

In this section,we compare the existing symmetric algorithms on the basis of different parameters as shown in table 1,which includes Block Size, Key Length, Security, and Speed.

Table 1: Comparison of Existing Algorithms on the basis of different parameters

Characteristics	DES	Blowfish	RC5	3-DES	AES
Developed	1977	1993	1994	1998	2000
Block Size	64	64	32,64 or 128	64	128, 192 or 256
Key Length	56	32-448	MAX2040	112, 168	128, 192 or 256
Security	Proven Inadequate	Considered Secure	Considered Secure	Considered Secure	Considered Secure
Speed	Very slow	Fast	Slow	Slow	Very fast

V. CONCLUSION AND FUTURE WORK

Cloud computing is changing the way IT departments buy IT. Businesses have a range of paths to the cloud, including infrastructure, platforms and applications that are available from cloud providers as online services. Many people may be confused by the range of offerings and the terminology used to describe them and will be unsure of the risk and benefits. Security is a major requirement in cloud computing while we talk about data storage. There are number of existing techniques used to implement security in cloud. In this paper, we discussed number of symmetric and asymmetric algorithms. Our future will be considering some problems related to existing security algorithms and implement a better version of DES, 3DES, AES, RSA, IDES, Blowfish.

REFERENCES

[1] RuWei Huang, Si Yu, Wei Zhuang and XiaoLin Gui, "Design of Privacy-Preserving Cloud Storage Framework" 2010 Ninth International Conference on Grid and Cloud Computing.

[2] Dr. Chander Kant and Yogesh Sharma, "Enhanced Security Architecture for Cloud Data Security" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 5, May 2013, pp. 571-575.

[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] Cong Wang, Qian Wang, Kui Ren and Wenjing Lou "Ensuring Data Storage Security in Cloud Computing." IEEE 2009.

[5] Balachandra Reddy Kandukuri, Rama Krishna Paturi and Dr. AtanuRakshit, "Cloud security issues" In Services Computing, 2009. IEEE International Conference on, page 517520, 2009.

[6] Kashish Goyal, Supriya Kinger" Modified Caesar Cipher for Better Security Enhancement" International Journal of Computer Applications (0975 – 8887) Volume 73– No.3, July 2013.

[7] Yogesh Kumar, Rajiv Munjal and Harsh Sharma,"Comparison of Symmetric and Asymmetric Cryptography with Existing Vulnerabilities and Countermeasures" IJCSMS International Journal of Computer Science and Management Studies, Vol. 11, Issue 03, Oct 2011.

[8] Mr. Gurjeevan Singh, , Mr. Ashwani Singla and Mr. K S Sandha " Cryptography Algorithm Compaison For Security Enhancement In Wireless Intrusion Detection System" International Journal of Multidisciplinary Research Vol.1 Issue 4, August 2011.

[9] D. S. Abdul. Elminaam, H. M. Abdul Kader and M. M. Hadhoud ," Performance Evaluation of Symmetric Encryption Algorithms", Communications of the IBIMA Volume 8, 2009.

[10] 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.

[11] Uma Somani, "Implementing Digital Signature with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing," 2010 1st International Conference on Parallel, Distributed and Grid Computing (PDGC - 2010).