



COMPARATIVE STUDY OVER SECURITY ISSUES OF CLOUD COMPUTING

Jyoti Bhang¹, Priya Ambulkar², Vasudeo Bathe³, Rahul Rathi⁴

¹Computer Science & Engg, STC, Khamgaon

²Computer Science & Engg, STC, Khamgaon

³Computer Science & Engg, STC, Khamgaon

⁴Computer Science & Engg, STC, Khamgaon

Abstract –As more important informant information on cloud, it is necessary to maintain its security more than before. The ability of system to handle the growing amount of work on cloud is done very fast and can be accessed anywhere the user wants. The increased numbers of users on cloud is unfortunately accompanied compared with the growth in malicious activity on cloud. As the more increment in attacks and flaw are discovered it is necessary to increase and develop newer securities in cloud computing. The concept of data storage security refers to providing a security for user's data on the storage of cloud. That's, the security issue is most important aspect to maintain the trust of users on cloud and provide total security for users data on cloud. As the issues like stolen of data or coping of users data will not be happen however. So in this paper, we are going to look more closely and going to study the important theories of security comparatively.

Keywords- AES, DES, Blowfish, Cluster, Encryption.

I. INTRODUCTION

Cloud computing provides many opportunities for enterprises by offering arrange of computing services. In today's competitive environment, the service dynamism, elasticity, and choices offered by this highly scalable technology are too attractive for enterprises to ignore. 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 an in cloud is or what the process in it we are concerned with the safe sending and receiving of data. Cloud computing is growing fast with time. Cloud computing illustrate Information Technology as a 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 kinds 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.

1.1 Security Issues

As the new generation of today's era like it is mandatory for users or companies to work with cloud because they got many best recourses available on cloud which is mainly useful for digital marketing field. The benefit of using cloud for resources the operational cost of recourses get reduces. As everyone uses the cloud the data moved on cloud is in high rate because of which the security concerns get started or developed.

The biggest security issue on cloud is Data breaching means in a confirmed incident in which sensitive, confidential or otherwise protected data has been accessed or dislocated in an unauthorized fashion. A professional hacker can easily hacks and access the important data. The less valid and less effective API's can easily become targeted. The IT companies which provides cloud services to other companies and users can allow to 3rd party company to modify it and also allows introducing their functionality by which the 3rd party company can understand the inner functionality or working of cloud. [4]

II. ARCHITECTURE

It is a provider host their resources on the internet on virtual computers and makes them available to more than one client. Cloud computing architecture refers the component and subcomponent such as front end and back end. Multiple virtual computers can run on one physical computer sharing the resources such as storage, memory, the CPU and interfaces giving the feeling to the client that each client has his own dedicated hardware to work on. Virtualization provides ability to fulfil all hardware resources needs among multiple clients. Increasing the profits of providers by sharing resources by multiple clients helps and reducing the cost of hardware. Accessing or selling hardware in the form of virtual computers is known as Infrastructure as Service (IaaS) in the cloud computing terminology [6]. Once a client has got infrastructure from a service provider, it is free to install and run any Operating System platform. Any types of services that are made available via the cloud computing model are Platform as a Service (PaaS) and Software as a Service (SaaS). Figure, shows the architecture of a typical cloud computing system. hardware

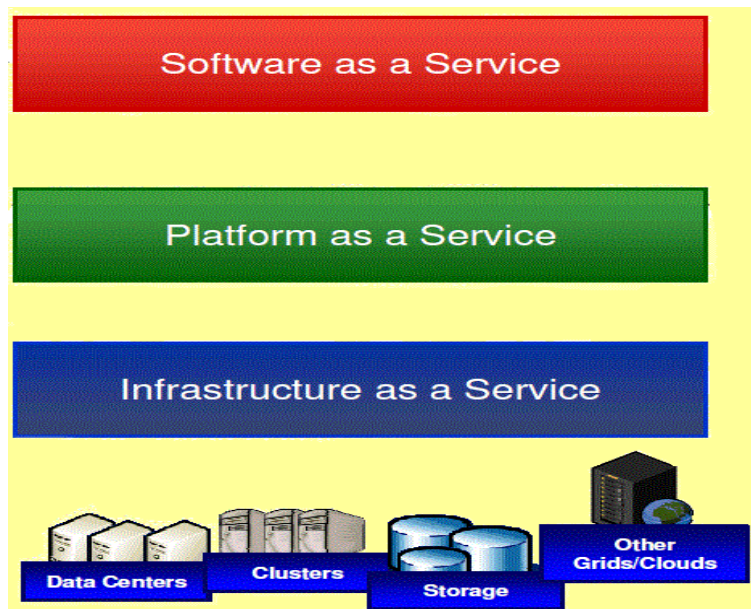


Fig 1: Architecture of cloud Computing

2.1 Comparative study on Encryption algorithm:

For providing a secure communication over the network, encryption algorithm plays a vital/important role. This is a the fundamental/basic 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 shows some of the symmetric & asymmetric algorithms [11].

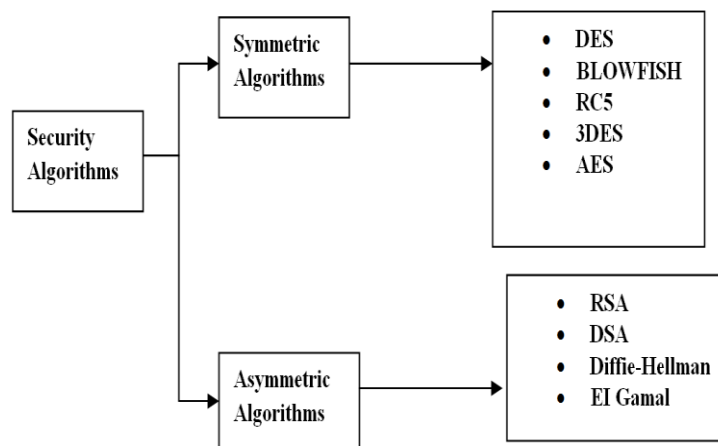


Fig 2:Security Algorithm

2.1.1 AES (Advanced Encryption Standard):

The basic steps in algorithm [8] are stated as:

Key Expansion - round keys are derived from the cipher key using Rijndael's key schedule

Initial Round AddRoundKey - each byte of the state is combined with the round key using bitwise xor

Rounds-

SubBytes - Every byte is replaced with another byte according to a looks towards table by the non-linear substitution steps.

ShiftRows - The transposition step where each row of the state is shifted cyclically a certain number of steps.

MixColumns - A mixing of columns operation which operates on the columns of the state, combining the four bytes in each column is called as mixcolumns.

AddRoundKey

d) Final Round (no MixColumns)- 1. SubBytes 2. ShiftRows 3. AddRoundKey

e) Key generation- This module handles key generation by the cryptographic module at client side. The server generates unique keys for users once they authenticate themselves with the server. The key is generated using instances of AES key generator class. This key is then transferred to the cloud client via the mail-server through a mail which receives and stores a copy for it for decrypting purpose.

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[]
}
```

2.1.2 DES:

The DES stands for Data Encryption Standard algorithm, 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.[9]

Algorithm:

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

M $\leftarrow$ IP(M)

For round $\square$ 1 to 16 do

Ki $\square$ SK (K, round)

L $\square$ L xor F(R, Ki)

swap(L, R)

end

swap(L, R)

M $\square$ IP-1(M)

return M

End

2.1.3 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 [10].

Algorithm

Divide x into two 32-bit halves: xL, xR

For i = 1 to 16:

XL = XL XOR Pi

xR = F(XL) XOR xR

Swap **xL** and **xR**
 Next **i**
 Swap **xL** and **xR** (Undo the last swap.)
 $xR = xR \text{ XOR } P17$
 $xL = xL \text{ XOR } P18$
 Recombine **xL** and **xR**

Parameter	DES	Blowfish	AES
Stands For	Data Encryptions Standard	Blowfish Encryptions Standard	Advanced Encryptions Standard
Developed	1977	1993	2000
Block Size	64	64	128, 192 or 256
Key Length	56	32-448	128, 192 or 256
Security	Proven Inadequate	Considered Secure	Considered Secure
Speed	Very slow	Fast	Very Fast
Cypher type	Symmetric block cipher	Symmetric block cipher block	Symmetric cipher block
Number of round	16	16	10
No. of boxes	8	4	1
structure	Feistel Network	Feistel Network	Substitution-permutation network

Table 1:Comparisons between algorithms

III. CONCLUSION

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.

IV. REFERENCES

- [1] Mr. Prasad I. Bhosle "Trust in Cloud Computing" International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 2, Issue 4, April 2013
- [2] 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.
- [3] Badger, L., Grance, T., Patt-Corner, R., & Voas, J. (2011). Draft Cloud Computing Synopsis and Recommendations. National Institute of Standards and Technology (NIST) Special Publication 800-146. US Department of Commerce. May 2011. Available online at: <http://csrc.nist.gov/publications/drafts/800-146/Draft-NIST-SP800-146.pdf> (Accessed on: November 20, 2012).
- [4] No author stated, The Notorious Nine, Cloud Security Alliance, February 2013 [Online] Available: <http://www.cloudsecurityalliance.org/topthreats>
- [5] Ted Samson, Nine Top Threats to Cloud Computing Security, Info World, February 25, 2013 [Online] Available: <http://www.infoworld.com>
- [6] RaduProdan and Simon Ostermann, "A Survey and Taxonomy of Infrastructure as a Service and Web Hosting Cloud Providers," in *10th IEEE/ACM International Conference on Grid Computing*, Banff, AB, Canada, 2009, pp. 17-25.
- [7] Michael Boniface et al., "Platform-as-a-Service Architecture for Real-Time Quality of Service Management in Clouds," in *Fifth International Conference on Internet and Web Applications and Services (ICIW)*, Barcelona, Spain, 2010, pp. 155-160.

- [8] M.Sudha, M.Monica, “Enhanced Security Framework to Ensure Data Security in Cloud Computing Using Cryptography”, *Advances in Computer Science and its Applications* 32 Vol. 1, No. 1, March 2012, P. 32-37.
- [9] 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
- [10] Mr. Gurjeevan Singh, , Mr. Ashwani Singla and Mr. K S Sandha “ Cryptography Algorithm Comparison For Security Enhancement In Wireless Intrusion Detection System” *International Journal of Multidisciplinary Research* Vol.1 Issue 4, August 2011
- [11] Kashish Goyal, Supriya Kinger” Modified Caesar Cipher for Better Security Enhancement” *International Journal of Computer Applications* (0975 – 8887) Volume 73– No.3, July 2013.