International Journal of Research In Science & Engineering e-ISSN: 2394-8299
Volume: 3 Issue: 2 March-April 2017 p-ISSN: 2394-8280

SECURITY IN DATA STORAGE ON CLOUD ENVIRONMENT USING BLOWFISH AND DIGITAL SIGNATURE

[1]Akash Mishara,[2]Nitin Rathod
[1]Research Scholar, Indore Institute of Science and Technology, Indore, M.P, India
[2]Assistant Professor, Indore Institute of Science and Technology, Indore, M.P, India
Department of Computer Science & Engineering.
[1]pusp1991@gmail.com

ABSTRACT:
In the cloud environment, resources are shared among all of the servers, users and individuals. So it is difficult for the cloud provider to ensure file security. As a result it is very easy for an intruder to access, misuse and destroy the original form of data. Security is one of the major issues which reduce the growth of cloud computing So Cloud computing entails encyclopedic security solutions .This thesis presented secure file exchanging on Cloud using Blowfish and Hash algorithms which is capable of solving data security, authentication, and integrity problems of files on the cloud. Data security is improved by cryptography algorithms. In our enhanced system we integrate symmetric, asymmetric and Hash algorithms which provide better results for performance parameters.
Keywords:- Hybrid Cryptosystem, Blowfish, File Splitting, Cloud Security

1. INTRODUCTION:

In the statements made by National Institute of Science and Technology (NIST), it is clearly stated that "Cloud computing is a model which enables on-demand network and shared pool of configurable computing resources (i.e. servers, storages, applications etc.) that can be rapidly provisioned and released with minimal management efforts or service provider's interaction" [2].

The resources about which NIST had been talking can be seen in an infrastructure footprint that is needed for outsourcing of Infrastructure as a Service (IaaS) is extremely important for any organization. This is the reason why the use of cloud computing has increased in many organizations rapidly. Cloud computing services provide quick access to applications, and reduction in infrastructure costs.

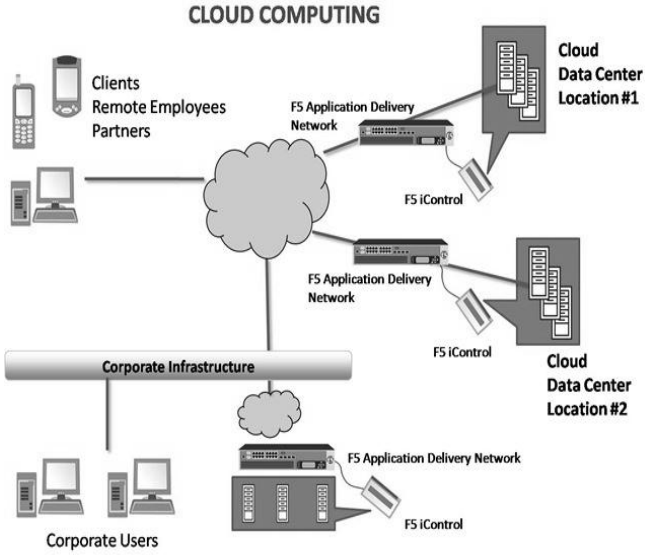

Figure 1. Cloud Computing

This provision of fast and minimum management efforts can help to provide scalable IT resources as a service with the use of Internet technology. Thus it can be said that cloud computing is a mean to add up capacity or capability in an infrastructure without putting money in building new infrastructure, training new people, or purchasing/licensing new software. It extends IT's capability by providing subscription based or pay per use services [3].

The rapid growth of computer resources has improved the performance of computers and decreased their cost. This low cost along with the facility of internet and high speed network would lead the computing environment to be mapped from multi cloud environments. In fact, researchers are working on this field to develop new architectures, which will be intended to share and coordinate resources and geographically distributed owners, who share the same goal of solving large-scale applications [4].

2. LITERATURE REVIEW:

Nesrine Kaaniche et al[2] has proposed ID based cryptography in which the data is firstly encrypted and stored on the public cloud server. This concept also offers access control so that only authorized users can use the data. With the help of this approach-unauthorized user even not get the data without client permission.

Neha Tirthani et al[3]explain about cloud security issues and then proposed a security model for cloud in which Diffie Hellman Key Exchange and Elliptical Curve Cryptography algorithms are used. The whole model is described in four steps in which first step establish connection, the second is account creation, third is authentication and last step contain data exchange.

Farzad Sabahi[4] describe about the scope of migrating to the cloud. The author also explains how the migration to the cloud will benefit to organizations.

Deyan Chen et al.[5] explain some serious security issues with cloud computing and then provide details of current security solution for data security and privacy protection in the cloud.

3. PROBLEM FORMULATION:

Due to multi-tenant characteristics of the cloud, the conventional security apparatus are no longer suitable for applications and data in cloud. Some of the matter are as following:

- All types of application and stuff of the cloud platform have no stable infrastructure and security boundaries only because of dynamic scalability, service and location transparency features of cloud computing model,. In the event of security violation, it is difficult to separate a fixed resource that has a threat or has been compromised.
- Resources and cloud services may be hold by multiple providers according to service serves models of Cloud computing. As there is a disputes of interest, it is difficult to post a unified security measure.
- Because of the openness of cloud and sharing virtualized resources by multitenant, user data may be enter by other unlegal users.

To resolve these security matter many cryptography algorithms are there. Cryptography[5] can serve services, such as:integrity checking—encourage the recipient of a message that the message has not been remodel since it was generated by a legal source and legal user .Protect the cloud means protect the storage database arrange by the cloud provider. Security goals reached by encryption /decryption process [10] Encryption/Decryption process are combin with three types of algorithms:

4. EXISTING SYSTEM:

4.1 Blowfish Algorithm:

Blowfish encryption algorithm is symmetric algorithm with following parameters

- Basic: It uses addition, XOR, lookup table with 32-bit operands.
- Compact: it run in very less memory compare to other
- Rapid: It encrypts data on large 32-bit microprocessors at a rate of 26 clock/byte.
- Secure: More secure due its key length from 32 to 448 bits. Default key length 128 bits

Pseudo code of blowfish describe below.

Step1: start the item size.

Step 2: 16 rounds are there in blowfish.

Step 3: x be the input of 64 bit data element.

Step 4: x will be divided into two halves x1 and x2.

Step 5: then, fori = 1 to 16:

$$X1 = x1 \text{ XOR } Pi \; x2 = F(x1) \text{ XOR } x2$$

Step 6: Swap x2and x2

Step 7: After the sixteenth round, swap x1 and x2 again to undo the last swap. Then, x2= x2 XOR P17 and x1 = x1 XOR P18.

Step 8: Recombine x1 and x2 to the cipher text

Step 9:Decryption in reverse order except p1,p2,.....p18.

Step 10:stop

5. PROPOSED WORK:

Our security analysis focuses on the model which defined as below. This evaluates the efficiency of our scheme via implementation of both file distribution operation and verification Process with valid credentials. In this proposed scheme, servers are required to operate on specified rows with correctness, verification for the calculation of requested token. This shows that "sampling" strategy on selected rows instead of all can greatly reduce the computational overhead on the server, while maintaining the detection of the data corruption with high probability. This method helpful for the client user because it speeds up the process of verification and validate the data.

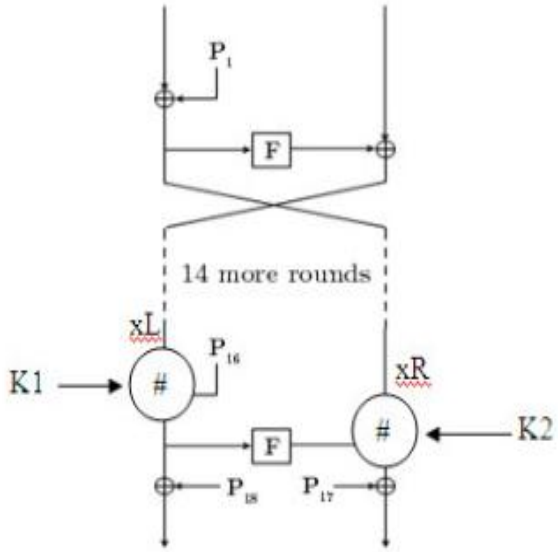

Figure2:

Step1: start the item size.

Step 2: 16 rounds are there in blowfish.

Step 3: x be the input of 64 bit data element.

Step 4: x will be divided into two halves x1 and x2.

X1=Convert_to_digit(x1) and x2=Convert_to_digit(x2)

Step 5: then, fori = 1 to 16:

X1 = x1 XOR PiXOR K1 x2 = F(x1) XOR x2XOR K2

Step 6: Swap x2and x2

Step 7: After the sixteenth round, swap x1 and x2 again to undo the last swap. Then, x2= x2 XOR P17 and x1 = x1 XOR P18.

Step 8: Recombine x1 and x2 to the cipher text

Step 9:Decryption in reverse order except p1,p2,p18.

Step 10:stop

Modified Blowfish Feistel Network

Therefore, two keys will double in each round from the original Blowfish, the first key K1will double with the xL and Pi to generate the next left component. The second key K2 will likely be used with F (xL) and xR to generate the right part. These three inputs on the '#' operation should become firstly converted from 32 bits to some 16 digits each could possibly be one of four expresses (0, 1, 2, 3), when i. e., each two bits converted to its equivalent decimal numbers. Pseudo code of modify blowfish describe below

6. CONCLUSION:

Data and privacy security are the main problems that need to be solved according to service delivery models and deployment models of cloud, Data Security and privacy matter exist in all levels in SPI service delivery models. The over mentioned model is fruitful in data as a service, which can be expand in other service models of cloud. Also it is examine in cloud environment like Open Shift, in future this can be post in other cloud terrtiory and the best among of all can be chosen.

REFERENCES

[1]Peter Mell and Tim Grance, "The NIST Definition of Cloud Computing", NIST, 2010.

[2]Akhil Behl, "Emerging Security Challenges in Cloud Computing**",** in Proc. of World Congress on Information and communication Technologies ,pp. 217-222, Dec. 2011.

[3]Srinivasarao D et al., "Analyzing the Superlative symmetric Cryptosystem Encryption Algorithm", Journal of Global Research in Computer Science, vol. 7, Jul. 2011

[4] Tingyuan Nie and Teng Zhang "A study of DES and Blowfish encryption algorithm", in Proc. IEEE Region 10 Conference, pp. 1-4 ,Jan. 2009.

[5] Jitendra Singh Yadav et al.," Modified RSA Public Key Cryptosystem Using Short Range Natural Number Algorithm" , International Journal of Advanced Research in Computer Science and Software Engineering ,vol. 2,Aug. 2012.

[6] Manikandan.G et al., "A modified cryptographic scheme enhancing data", Journal of Theoretical and Applied Information Technology**,** vol. 35, no.2, Jan. 2012.

[7] Nilesh Mangtani and Sukhada Bhingarkar, " The appraisal and Judgment of Nimbus, OpenNebula and Eucalyptus", International Journal of Computational Biology , vol. 3, issue 1, pp 44-47, 2012.

[8] A. Juels and B. S. Kaliski, Jr., (2007) ―*Pors: proofs of retrievability for large files,"* in CCS '07: Proceedings of the 14th ACM conference on Computer and Communications security. New York, NY, USA: ACM, 584–597.

[9] Cody, Brian; Madigan, Justin; MacDonald, Spencer; Hsu, Kenneth W.;, "*High speed SOC design for blowfish cryptographic algorithm,*" Very Large Scale Integration, 2007. VLSI SoC 2007. IFIP International Conference on , vol., no., pp.284-287, 15-17 Oct. 2007.

[10] Govinda.K1 Mythili and Geetha Priya(2014),‖ *Data Security in Cloud using Blowfish Algorithm*‖, International Journal for Scientific Research & Development| Vol. 2, Issue 09.

[11] J. Guo, S. Ling, C. Rechberger, and H. Wang, *Advanced Meetin-the-Middle Preimage Attacks: First Results on Full Tiger, and Improved Results on MD4 and SHA-2*,‖ pp. 1–20.

[12] Gurpreet Kaur and Manish Mahajan (2013), *Analyzing Data Security for Cloud Computing Using Cryptography Algorithms*‖, International Journal Of Engineering Research and Application, Vol.-3,782-786.