Implementing Clouds Data Security by Encryption Using Blowfish Algorithm

F. Sammy
Assistant Professor, Ambo University, Ethiopia
fvr.sammy@gmail.com

Abstract— Cloud Computing provides us a means by which we can access the applications as utilities, over the internet. It allows us to create, configure, and customize the business applications online. The concept of cloud computing grows very rapidly in recent years. Nowadays many users store their data on Cloud. Data storage security refers to the security of data on the storage media. So, Security is an major concern 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. Data in cloud should be stored in encrypted form. This paper deals with the methods of providing security by data encryption using Blowfish Algorithm and to ensure that unauthorized intruder can't access your file or data in cloud.

Keywords— Authentication, cloud computing, MFA, encryption, blowfish algorithm

I. INTRODUCTION

Cloud computing is defined as the set of resources or services offered through the internet to the users on their demand by cloud providers. It bears everything as a service over the internet based on user demand, for instance operating system, network hardware, storage, resources, and software. As each and every organization is moving its data to the cloud, means it uses the storage service provided by the cloud provider [1], [2], and [3].

The main attributes of cloud computing are illustrated as follows [4]:

1. Shared resources (Multi-tenancy): Cloud computing is based on a business model in which resources are shared (i.e., multiple users use the same resource) at the network level, host level, and application level.
2. Scalability: Cloud computing provides the ability to scale to tens of thousands of systems, as well as the ability to massively scale bandwidth and storage space.
3. Elasticity: Users can rapidly increase and decrease their computing resources as needed.
4. Utility Style Costing: Users to pay for only the resources they actually use and for only the time they require them.
5. Self-provisioning of resources: Users self-provision resources, such as additional systems (processing capability, software, storage) and network resources. [5]

A. Security in Cloud Computing

In today's era, cloud computing is the most interesting and enticing technology which is offering the services to its users on demand over the internet. Since Cloud Computing stores the data in the open environment, security has become the main obstacle which is hampering the deployment of Cloud

environments. [6] In the light of all the advantages of migrating to the cloud, one of the primary disadvantages of the cloud platform is the security aspect. The security concerns fall into two main categories

1. Cloud provider concerns
2. Client based concerns

The cloud provider should ensure that the architecture and the infrastructure are secure and that the data and applications of the client are not compromised. On the other hand, the client should make sure that the provider has taken all measures to secure their data in the cloud. One of the methods to resolve these issues is the encryption of data. Encryption can be done in three ways:-

(a) Server-side Encryption

With this option all data is encrypted in storage by the cloud platform itself. Server-side encryption really only protects against a single threat: lost media. It is more a compliance tool than an actual security tool because the cloud administrators have the keys anyway. Server-side encryption offers no protection against cloud administrators.

(b) Client/Agent Encryption

If you don't trust the storage environment your best option is to encrypt the data before sending it up. In it we turn a shared public resource into a private one by encrypting it while retaining the keys.

(c) Proxy Encryption

One of the best options for business-scale use of object storage, especially public object storage, is an inline or cloud hosted proxy. There are two main topologies:

• The proxy resides on your network, and all data access runs through it for encryption and decryption.

• The proxy runs as a virtual appliance in either a public or private cloud. [7]

II. PROBLEM DEFINITION

While cloud computing greatly facilitating users with storage resources, the greatest challenge or the existing problem comes from the security. The security challenges if not well resolved may impede the fast growth of cloud computing. Previously security is provided to data at rest i.e. encryption is done by the cloud service provider at the cloud side. But it leaves the data insecure while user outsources it to the cloud as the data travel in the original form. So we need method that provides security to both data at rest and data while moving. Also some mechanism is required to ensure that the cloud must give access of data only to the authorized user.

III. METHODOLOGY

Security of data and trust problem has always been a primary and challenging issue in cloud computing. This section describes a methodology to ensure security in cloud computing. The two different approaches used are as follows:

A. Multifactor authentication (MFA)

Multifactor authentication (MFA) is a security system that requires more than one method of authentication from independent categories of credentials to verify the user's identity for a login or other transaction. Multifactor authentication combines two or more independent credentials: what the user knows (password), what the user has (security token) and what the user is (biometric verification). The goal of MFA is to create a layered defense and make it more difficult for an unauthorized person to access a target such as a physical location, computing device, network or database. If one factor is compromised or broken, the attacker still has at least one more barrier to breach before successfully breaking into the target. [8]

B. Blowfish Algorithm

This was developed in 1993. It is one of the most common public algorithms provided by Bruce Schneider. B low fish 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 [9].

Algorithm:

Divide x into two 32-bit halves: X_L, X_R

For i = 1 to 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

IV. IMPLEMENTATION DETAILS

Using Java Net Beans IDE 7.2 and XAMPP 1.7.0, we have implemented methodology which provides better security as secret key is only known to the user and authenticity of user is ensured by Cloud.

We have created two pages: Client Page and Cloud Server Page shown in Figure 1, 2.

Fig 1: Client Side

Fig 2: Server Side

The steps of the implementation are given below:-

1. User sends the authentication request to the Cloud Service Provider (CSP).
2. CSP checks the authorization using Multifactor authentication and sends the acknowledgement back to the user.
3. User first encrypts his data and then outsources it to the server.
4. When the user downloads his data from CSP, it is received in the encrypted form.
5. To use the data user can decrypt it using same key used for encryption.

V. RESULTS

The results of the above mentioned system are shown in Table 1 and Figure 3.

	File Size(in Bytes			
	51	577	776	975
Encryption Time (ms)	15	33	47	51
Decryption Time (ms)	15	21	25	31
Delay Time (ms)	46	66	72	78

Table1: Result Analysis

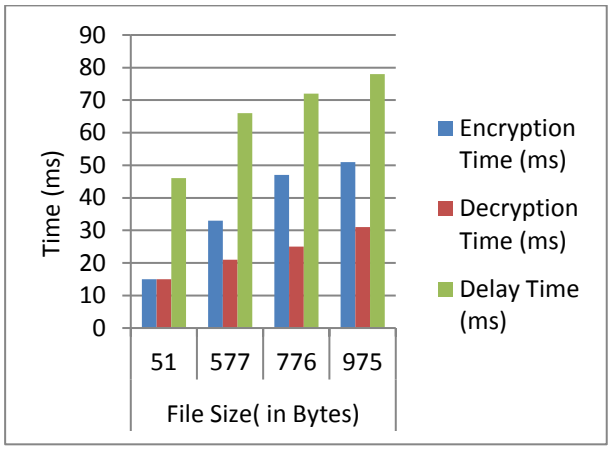

Fig: 3 Graph showing results of encryption and decryption

VI. CONCLUSION

Although cloud computing has many advantages, there are still many actual problems that need to be solved. The main problem is to maintain the privacy and the confidentiality of the data. Data confidentiality can be achieved by encrypted outsourced content before outsourcing to cloud servers and for privacy it is required that only the authorized user can access the data. Even if some intruder (Unauthorized user) gets access of the data accidentally or intentionally, he will not be able to decrypt it. In my work, I have used Blowfish Encryption algorithm to provide security to the data and Multifactor authentication for authentication purpose. In future the above approach can be enhanced further by including an integrity check mechanism.

REFERENCES

[1] Mohammad, John, Ingo," An Analysis of the Cloud Computing Security Problem", APSEC 2010 Proceeding – Cloud Workshop, Sydney, Australia, 30th NOV 2010.

[2] Mandeep, Manish, "Implementing Various Encryption Algorithms to Enhance the Data Security of Cloud in Cloud Computing", International Journal of Computer Science and Information Technology, Vol.2 No.10 October 2012.

[3] A. Padmapriya, P. Subhasri, "Cloud Computing: Security Challenges and Encryption Practices ", International Journal of Advanced Research in Computer Science and Software Engineering, vol. 3, issue 3 March 2013.

[4] Saurabh Kumar, Jaideep Dhok, "Towards Analyzing Data Security Risks in Cloud Computing Environments" International Institute of Information Technology, Hyderabad.

[5] Emam M.Mohamed, Sherif El-Etriby, "Data Security Model for Cloud Computing", The Twelfth International Conference on Networks (ICN), 2013.

[6] Parsi Kalpana, Sudha Singaraju," Data Security in Cloud Computing using RSA Algorithm",International Journal of Research in Computer and Communication technology, IJRCCT, ISSN 2278-5841, Vol 1, Issue 4, September 2012.

[7] Defending Cloud Data with Infrastructure Encryption, Version 1.0, July 12, 2013.

[8] WebSite:http://searchsecurity.techtarget.com/definition/multifactor-authentication MFA

[9] 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.

BIOGRAPHY

The author F. SAMMY working as an Assistant Professor in Information Technology Department from Ambo University Ethiopia, Her area of interest is networking, network security and data mining. She has published around more than four papers in refereed journals and conference proceedings in these areas.