Global Journal of Computer Science and Technology
Cloud and Distributed
Volume 13 Issue 4 Version 1.0 Year 2013
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Implementing Cloud Data Security by Encryption using Rijndael Algorithm

By Sanjoli Singla & Jasmeet Singh
Lovely Professional University, India

Abstract - Cloud computing emerges as a new computing paradigm which aims to provide reliable, customized and QoS guaranteed dynamic computing environments for endusers. However, adopting a cloud computing paradigm may have positive as well as negative effects on the data security of service consumers. In a cloud computing environment, data and the application is controlled by the service provider. This leads to a natural concern about data safety and also its protection from internal as well as external threats. The major issues in cloud computing is the security of data being stored on the provider's cloud and privacy while the data is being transmitted. This paper deals with the methods of providing security by data encryption and to ensure that unauthorized intruder can't access your file or data in cloud.

Keywords : *authentication, cloud, eap-chap, encryption, rijndael algorithm.*

GJCST-B Classification : *C.1.4*

Strictly as per the compliance and regulations of:

Implementing Cloud Data Security by Encryption using Rijndael Algorithm

Sanjoli Singla [α] & Jasmeet Singh [σ]

Abstract - Cloud computing emerges as a new computing paradigm which aims to provide reliable, customized and QoS guaranteed dynamic computing environments for endusers. However, adopting a cloud computing paradigm may have positive as well as negative effects on the data security of service consumers. In a cloud computing environment, data and the application is controlled by the service provider. This leads to a natural concern about data safety and also its protection from internal as well as external threats. The major issues in cloud computing is the security of data being stored on the provider's cloud and privacy while the data is being transmitted. This paper deals with the methods of providing security by data encryption and to ensure that unauthorized intruder can't access your file or data in cloud.

Keywords : authentication, cloud, eap-chap, encryption, rijndael algorithm.

I. Introduction

Cloud computing is the next stage in the Internet's evolution, providing the means through which everything — from computing power to computing infrastructure, applications, business processes to personal collaboration — can be delivered to you as a service wherever and whenever you need. The "cloud" in cloud computing can be defined as the set of hardware, networks, storage, services, and interfaces that combine to deliver aspects of computing as a service as shown in figure 1.[3] It is extremely useful for small and medium enterprises to leverage the advantages provided by the cloud.

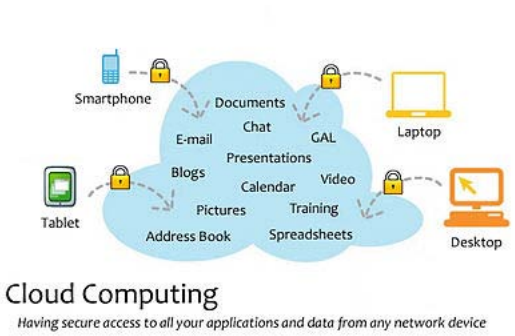

Figure 1 : Cloud Computing

Author α : M.TECH (Computer Science and Engineering), RIMT-IET, Mandi Gobindgarh, Punjab (India). E-mail : sanjoli_11@yahoo.co.in
Author σ : Asst. Professor(CSE Department), RIMT-IET, Mandi Gobindgarh, Punjab (India). E-mail : jasmeetgurm@gmail.com

The main attributes of cloud computing are illustrated as follows [1]:

1. *Multi-tenancy (shared resources):* 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. *Massive 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. *Pay as you used:* 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 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.[7]

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:-

1. *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.

2. *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.

3. *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.[8]

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 as shown in figure 2 to ensure security in cloud computing. The two different approaches used are as follows:-

a) Extensible Authentication Protocol-CHAP

EAP stands for Extensible Authentication Protocol. It offers a basic framework for authentication. Many different authentication protocols can be used over it. New authentication protocols can be easily added. EAP works over a secure line. A client may not support all authentication methods so EAP must support authentication method negotiation. It also allows for mutual authentication by running the protocol in both directions. In our purposed model we use Challenge-Handshake Authentication Protocol (CHAP) for authentication.[10]

b) Rijndael encryption Algorithm

The Rijndael is a symmetric block cipher algorithm with key sizes ranging from 128, 192, and 256. A symmetric algorithm is one in which the cryptographic keys for encrypting plain text and decrypting cipher text are the same. There are two types of symmetric encryption algorithms: stream ciphers and block ciphers. Stream ciphers encrypt data each digits separately and individually whereas block cipher algorithms encrypt text in blocks an pad original plain text so that the size it matches the block size. It uses the encryption of 128 bit blocks. Rijndael is an iterated block cipher, the encryption or decryption of a block of data is accomplished by the iteration (a round) of a specific transformation (a round function). [2,6]

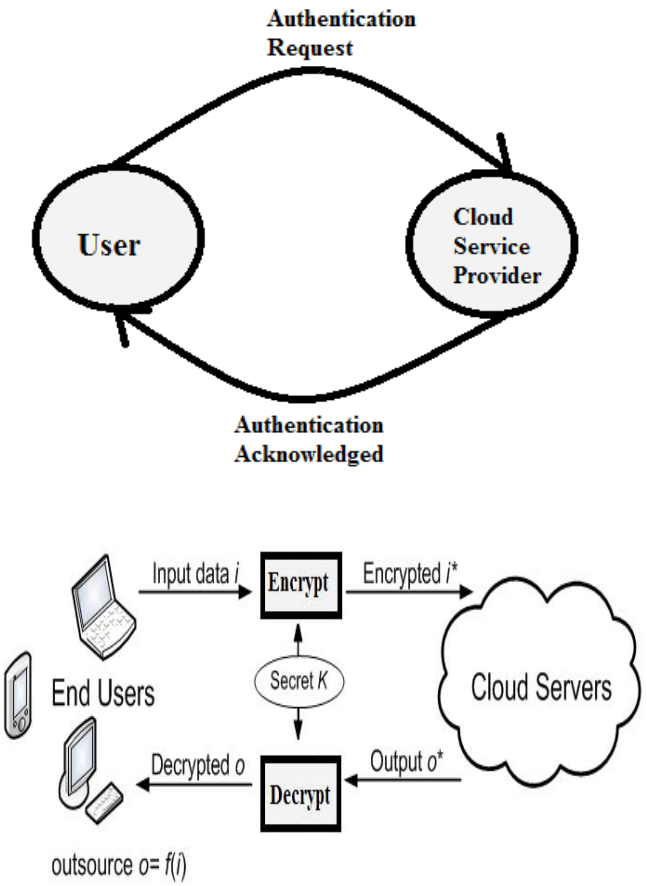

Figure 2 : Methodology

IV. Implementation Details

Using Java NetBeans 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 3,4.

1. Client Side

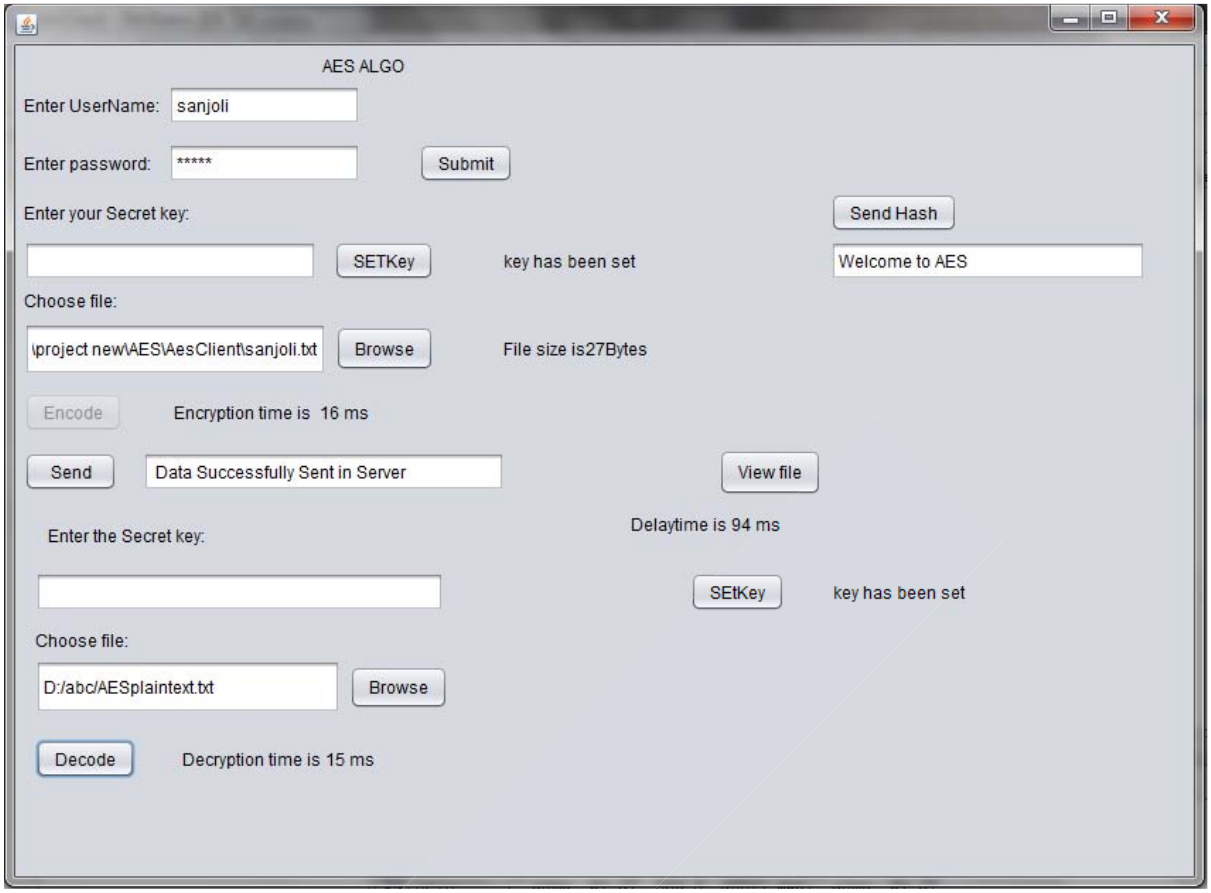

Figure 3 : Client Page

2. Cloud Server Side

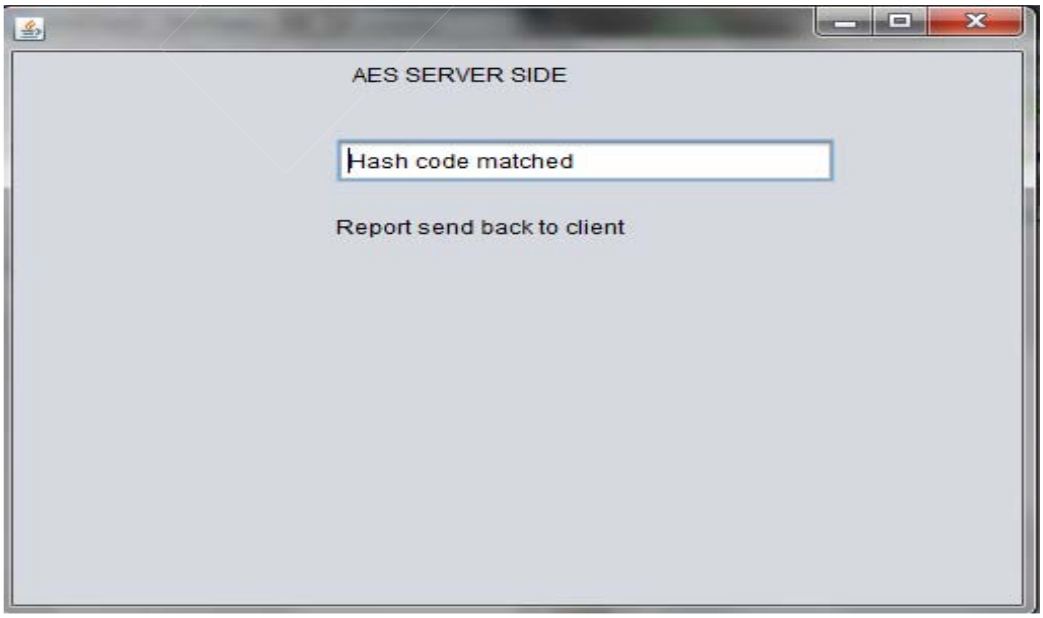

Figure 4 : Cloud Server Page

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 EAP-CHAP 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 5.

Table 1 : Result Analysis

	File Size(in Bytes)			
	51	577	776	975
Encryption Time(ms)	16	32	47	51
Decryption Time(ms)	16	20	25	32
Delay Time(ms)	47	65	72	79

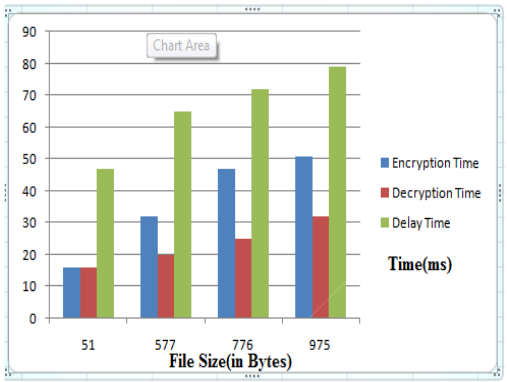

Figure 5 : Graph showing results of encryption and decryption

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 Rijndael Encryption algorithm to provide security to the data and EAP-CHAP for authentication purpose.

In future the above approach can be enhanced further by including an integrity check mechanism.

References Références Referencias

1. Saurabh Kumar, Jaideep Dhok, "Towards Analyzing Data Security Risks in Cloud Computing Environments" International Institute of Information Technology, Hyderabad.
2. Sonali Madireddi, "Implementing Cloud Security by Encryption using Block Cipher Algorithms", International Journal of Applied Information Systems (IJAIS), Vol. 4-No. 11, December 2012.
3. Tejas P. Bhatt, Ashish Maheta, "Security in Cloud Computing using File Encryption", International Journal of Engineering Research and Technology(IJERT), Vol. 1 Issue 9, November 2012.
4. Deyan Chen, Hong Zhao, "Data Security and Privacy Protection Issues in Cloud Computing", International Conference on Computer Science and Electronics Engineering, 2012.
5. Emam M.Mohamed, Sherif El-Etriby, "Data Security Model for Cloud Computing", The Twelfth International Conference on Networks (ICN), 2013.
6. Prashant Rewagad, Yogita Pawar, "Use of Digital Signature and Rijndael encryption Algorithm to Enhanced Security of data in Cloud computing Services", Proceeding published in International Journal of Computer Applications (IJCA), 2012.
7. 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.
8. Defending Cloud Data with Infrastructure Encryption, Version 1.0, July 12, 2013.
9. Pratiyush Guleria, Vikas Sharma,"Development and Usage of Software as a Service for a Cloud and Non-Cloud based Enviroment-An Empirical Study", International Journal of Cloud Computing and Services Sciences(IJ-CLOSER), Vol. 2, No. 1, February 2013.
10. G.Jai Arul Jose, C.Sajeev, "Implementation of Data Security in Cloud Computing", International Journals of P2P Network Trends and Technology, Vol. 1, Issue 1, 2011.
11. http://thegadgetsquare.com/1552/what-is-cloud-computing/
12. http://en.wikipedia.org/wiki/Cloud_computing
13. http://en.wikipedia.org/wiki/Advanced_Encryption_Standard.
14. https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol