Global Journals LaTeX JournalKaleidoscope™

Artificial Intelligence formulated this projection for compatibility purposes from the original article published at Global Journals. However, this technology is currently in beta. *Therefore, kindly ignore odd layouts, missed formulae, text, tables, or figures.*

# Cloud Data Security using Authentication and Encryption Technique

Sanjoli Singla[1] and Jasmeet Singh[2]

[1] RIMT-IET, Mandi Gobindgarh/ Punjab Techincal University

*Received: 11 April 2013 Accepted: 4 May 2013 Published: 15 May 2013*

## Abstract

Cloud Computing has been envisioned as the next generation architecture of IT Enterprise.In cloud computing application software and databases are moving to the centralized large data centers. This mechanism brings about many new challenges, which have not been well understood. Security and privacy concerns, however, are among the top concerns standing in the way of wider adoption of cloud. In cloud computing the main concern is to provide the security to end user to protect files or data from unauthorized user. Security is the main intention of any technology through which unauthorized intruder can't access your file or data in cloud. We have designed one proposed design and architecture that can help to encrypt and decrypt the file at the user side that provide security to data at rest as well as while moving. In this research paper, we have used the Rijndael Encryption Algorithm along with EAP-CHAP.

***Index terms***— authentication, cloud, EAP-CHAP, encryption, rijndael algorithm.

## 1 Introduction

loud 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 [1].

## 2 a) Cloud Computing Deployment Models

The various cloud deployment models are shown in figure 1 given below: i. Public Clouds In public cloud vendors dynamically allocate resources on a per-user basis through web applications. For example: Drop Box, SkyDrive and Google drive. Securing data is always of vital importance as shown in figure 3 and because of the critical nature of cloud computing and large amounts of complex data it carries, the need is even important. Therefore, data privacy and security are issues that need to be resolved as they are acting as a major obstacle in the adoption of cloud computing services. The major security issues with cloud are:

## 3 Privacy and Confidentiality

Once the clients outsource data to the cloud there must be some assurance that data is accessible to only authorized users. The cloud user should be assured that data stored on the cloud will be confidential.

## 4 Security and Data Integrity

Data security can be provided using various encryption and decryption techniques. With providing the security of the data, cloud service provider should also implement mechanism to monitor integrity of the data at the cloud. [3] II.

# 5 Problem Formulation

Users who put their large data files in the cloud storage servers can relieve the burden of storage and computation. At the same time, it is critically important for users to ensure that their data are being stored correctly and safely. So, users should be equipped with their data is safe. The major concern is the security of data at rest and while moving. So to handle this problem it is required that data at both user and server end must be in encrypted form.

# 6 III.

# 7 Proposed Work Plan

The two different approaches used for ensuring security in cloud are as follows: Implementation of EAP-CHAP in Cloud Computing will solve the authentication and authorization problems. [5] Table **??**

# 8 : Rijndael Encryption Code

The User data is encrypted by using Rijndeal Encryption. Symmetric key is used for encryption. The Rijndeal can be implemented easily and it is one of the most secure algorithms in the world. Rijndeal implementation has 128,192or 256 bit key lengths. Size of data blocks to be encrypted with Rijndeal is always 128 bits. Initial round of Rijndeal is AddRoundKey, this is followed by four iterative round including subBytes, shiftRows, mixColumns and add round key. Rijndeal with 128 bit key length has 10 rounds,192-bit has 12 rounds and 256 bit has 14 rounds. Each round consists of the following steps. 1. Initial AddRoundKey 2. SubBytes () Transformation 3. Substitutional Box Created For Subbytes 4. MixColumns () Transformation

# 9 AddRoundKey () transformation

The inverse process of encryption gives decryption text. [4] Rijndael Algorithm : Encryption/Decryption Process for Rijndael Algorithm is shown in Figure **??**. The code for encryption process is given in table **??**.

# 10 a. The SubBytes Step

The SubByte step is a non-linear byte substitution that operates on each of the 'state' bytes independently, where a state is an intermediate cipher result. Here each byte in the state matrix is replaced with a SubByte using an 8-bit substitution box, the Rijndael S-box.

# 11 b.

The ShiftRows step operates on the rows of the state; it cyclically shifts the bytes in each row by a certain offset. For AES, the first row is left unchanged. Each byte of the second row is shifted one to the left. Similarly, the third and fourth rows are shifted by offsets of two and three respectively. For blocks of sizes 128 bits and 192 bits, the shifting pattern is the same. Row n is shifted left circular by n-1 bytes.

# 12 c. The MixColumns step

During this operation, each column is multiplied by the known matrix that for the 128-bit key is:

The multiplication operation is defined as: multiplication by 1 means no change, multiplication by 2 means shifting to the left, and multiplication by 3 means shifting to the left and then performing xor with the initial unshifted value. After shifting, a conditional xor with 0x11B should be performed if the shifted value is larger than 0xFF. In more general sense, each column is treated as a polynomial over GF (2 8 ) and is then multiplied modulo x 4 +1 with a fixed polynomial c(x) = 0x03 ? x 3 + x 2 + x + 0x02. state with the corresponding byte of the subkey using bitwise XOR. [3] IV.

# 13 Conclusion

Data security has become the vital issue of cloud computing security. From the consumers' perspective, cloud computing security concerns, especially data security and privacy protection issues, remain the primary inhibitor for adoption of cloud computing services. So in this we focused on client side security In our proposed system, 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. Also it is proposed that encryption must be done by the user to provide better security. Henceforth, security is provided using Rijndael Algorithm.

# 14 Global Journal of Computer Science and Technology

[1]

[1]

1

OPEN ASSOCIATION OF RESEARCH SOCIETY, USA
RESEARCH | DIVERSITY | ETHICS

Figure 1: Figure 1 :

2

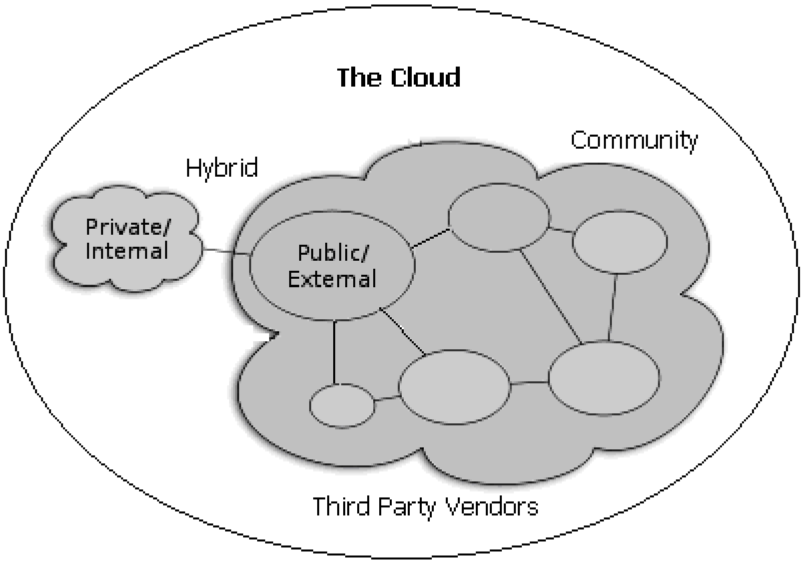


Figure 2: Figure 2 :

3

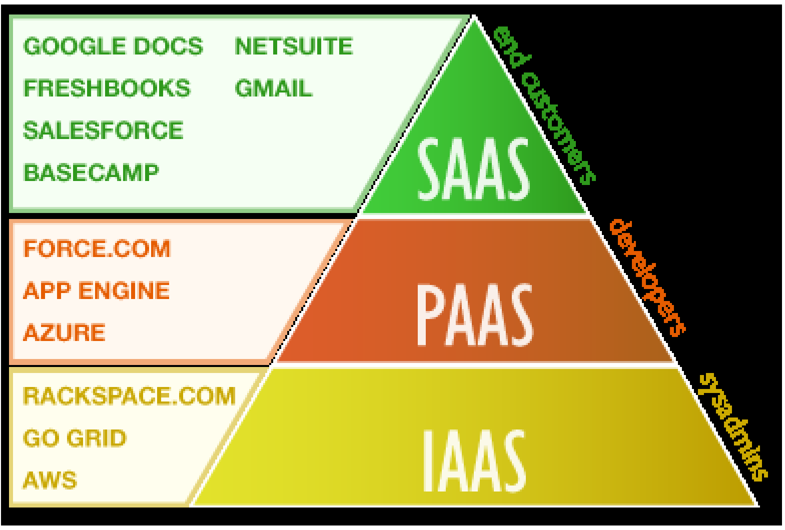


Figure 3: Figure 3 :

14

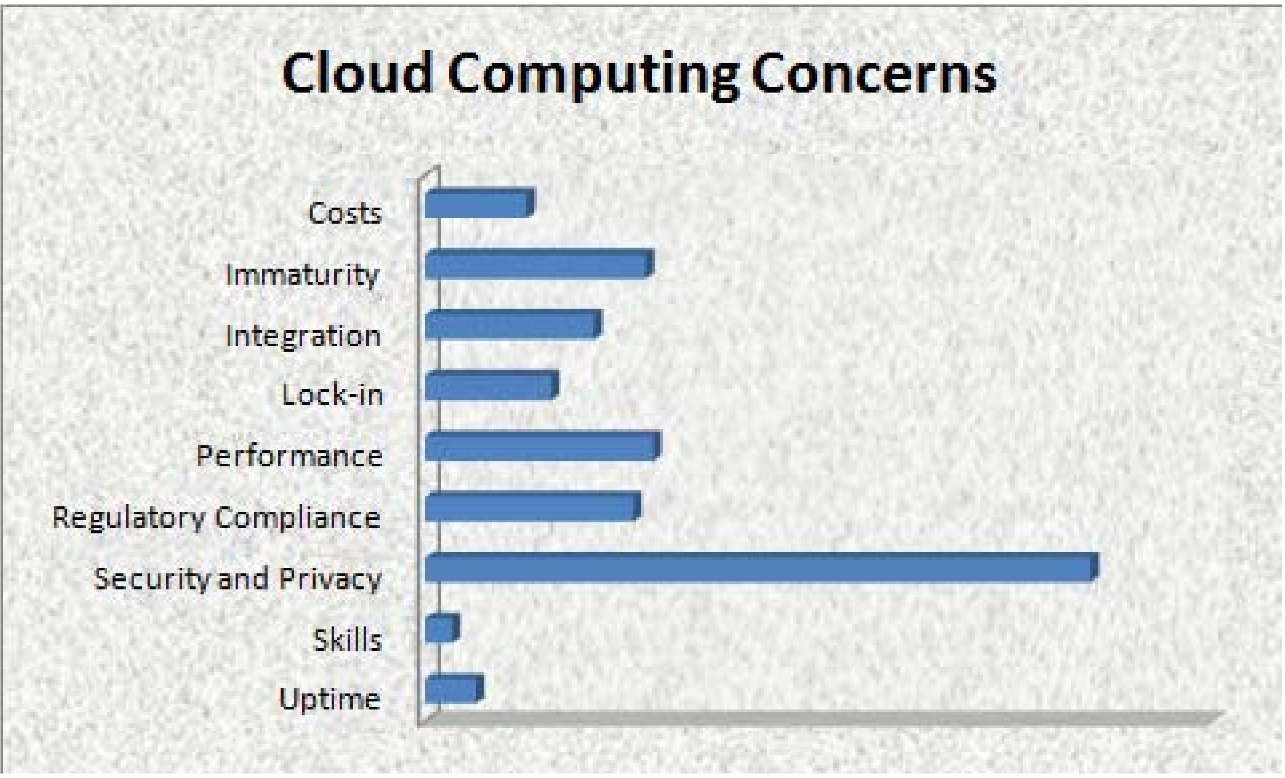
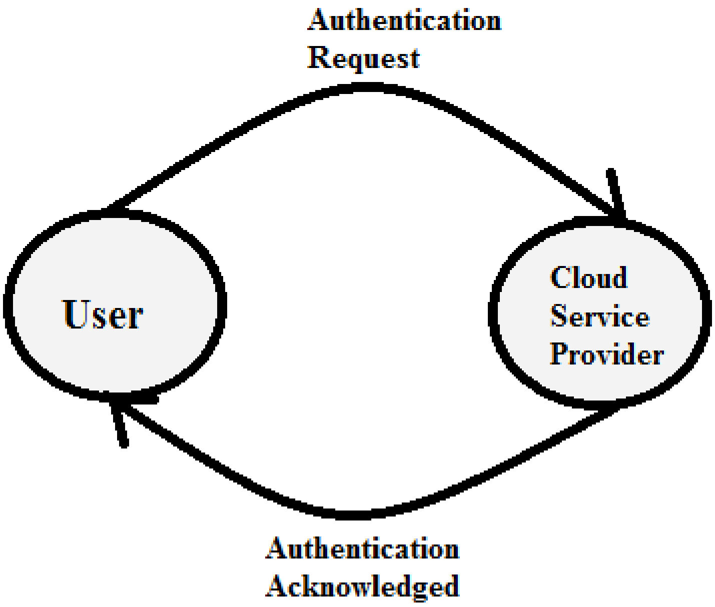


Figure 4: 1 .Figure 4 :B



**5**

Figure 5: Figure 5 :

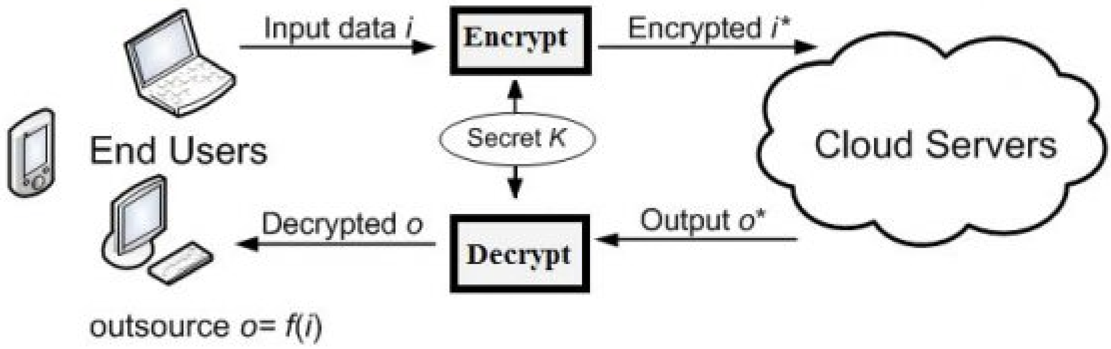


Figure 6:

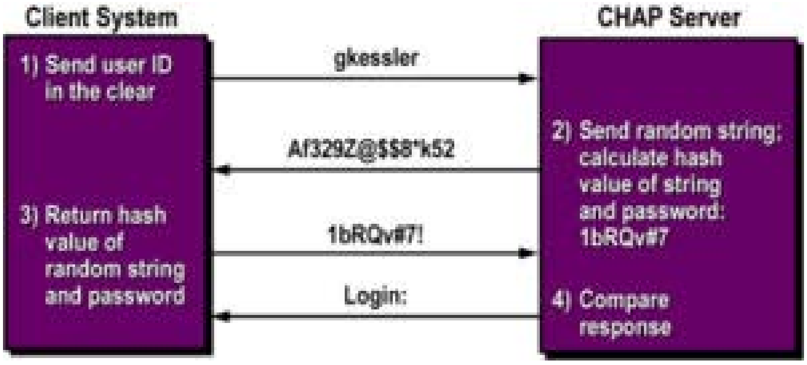

Client System
CHAP Server
1) Send user ID in the clear
gkessler
2) Send random string; calculate hash value of string and password: 1bRQv#7
Af329Z@$$8*k52
3) Return hash value of random string and password
1bRQv#7!
Login:
4) Compare response

Figure 7: VolumeB

[Guleria and Sharma (2013)] 'Development and Usage of Software as a Service for a Cloud and Non-Cloud based Enviroment-An Empirical Study'. Pratiyush Guleria , Vikas Sharma . *International Journal of Cloud Computing and Services Sciences(IJ-CLOSER)* February 2013. 2 (1) .

[Jose and Sajeev ()] 'Implementation of Data Security in Cloud Computing'. G.Jai Arul Jose , C Sajeev . *International Journals of P2P Network Trends and Technology*, 2011. 1.

[Marium et al. ()] 'Implementation of EAP with RSA for enhancing the security of cloud computing'. Sadia Marium , Qamar Nazir , Aftab Ahmed , Saira Ahthasham , Aamir Mirza , Mehmood . *International Journal of Basics and Applied Sciences* 2012. 1 (3) p. .

[Tejas et al. (2012)] 'Security in Cloud Computing using File Encryption'. . P Tejas , Ashish Bhatt , Maheta . *International Journal of Engineering Research and Technology (IJERT)* November 2012. 1 (9) .

[Singla and Singh ()] 'Survey on Enhancing Cloud Data Security using EAP with Rijndael Encryption Algorithm'. Sanjoli Singla , Jasmeet Singh . *Global Journal of Computer Science and Technology (GJCST)* 2013. 13 (5) .

[Rewagad and Pawar ()] 'Use of Digital Signature and Rijndael encryption Algorithm to Enhanced Security of data in Cloud computing Services'. Prashant Rewagad , Yogita Pawar . *Proceeding published in International Journal of Computer Applications (IJCA)*, (eeding published in International Journal of Computer Applications (IJCA)) 2012.