Global Journal of Computer Science and Technology
Software & Data Engineering
Volume 13 Issue 5 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

Survey on Enhancing Cloud Data Security using EAP with Rijndael Encryption Algorithm

By Sanjoli Singla & Jasmeet Singh
RIMT-IET, Mandi Gobindgarh, India

Abstract - Cloud computing is an amazing technology where users can remotely store their data into the cloud to enjoy high quality application and services. Cloud being the most vulnerable next generation architecture consist of two major design elements i.e. the Cloud Service Provider(CSP) and the Client. Even though the cloud computing is promising and efficient, there are many challenges for data privacy and security. This paper explores the security of data at rest as well as security of data while moving.

Keywords : *authentication, cloud, encryption, rijndael algorithm.*

GJCST-C Classification *: H.2.7*

Strictly as per the compliance and regulations of:

Survey on Enhancing Cloud Data Security using EAP with Rijndael Encryption Algorithm

Sanjoli Singla [α] & Jasmeet Singh [σ]

Abstract - **Cloud computing is an amazing technology where users can remotely store their data into the cloud to enjoy high quality application and services. Cloud being the most vulnerable next generation architecture consist of two major design elements i.e. the Cloud Service Provider(CSP) and the Client. Even though the cloud computing is promising and efficient, there are many challenges for data privacy and security. This paper explores the security of data at rest as well as security of data while moving.**

Keywords : authentication, cloud, encryption, rijndael algorithm.

I. Introduction

The cloud computing is a model for enabling convenient, on demand network access to a shared pool of configurable resources such as networks, servers, files storage, applications and services. The cloud computing field is growing day by day with a increasing number of businesses and government establishments going for cloud computing based services.[1]The cloud computing incorporates combination of:-

1. IaaS (Infrastructure as a Service)
2. PaaS (Platform as a Service)
3. SaaS (Software as a Service)

These are collectively called as *aaS (Everything as a Service) which means a service-oriented architecture. The first benefit of the cloud computing is that it reduces the cost of hardware used at user end. As the data is stored at the cloud, so instead of buying the whole infrastructure required to run the processes user just rent the assets according to his requirement. The similar idea is behind all cloud networks as shown in figure 1. [2]

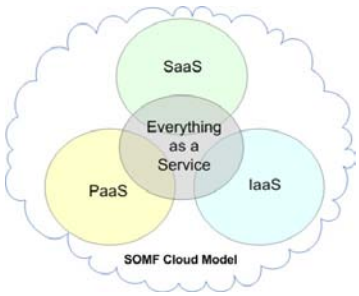

Figure 1 : Cloud Service Models

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

Cloud Computing deployment models are:-

Private Cloud

Enterprise owner or leased.

Community Cloud

Cloud infrastructure that supports a specific community with shared concerns.

Public Cloud

Available to the public and owned by an organization selling cloud services.

Hybrid Cloud

Composition of two or more clouds(Private, Community, Public). [4]

a) Data security issues in the cloud

Securing data is always of vital importance 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:-

i. *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.

ii. *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. Related Work

In [3] paper author's main concern with reference to the security of the data is how to ensure security of data at rest. In it RSA (Ron Rivest, Adi Shamir and Len Adleman) algorithm is used which consist of public key and private key. Encryption is done by Cloud Service Provider using public key and decryption is done by cloud using corresponding private key.

In [8] paper author main focus is on service provider side security. To ensure security (Privacy & Confidentiality) he proposes EAP with Challenge Handshaking Protocol for the authorization of the user and RSA for encryption at server side.

In [1] paper author proposes the combination of Rijndael with Digital Signature for enhancement of security. CSP first converts the data into hash and then encrypt it using digital signature and finally encrypt using Rijndael algorithm with user's public key. On the other side user can decrypt data with its private key and uses CSP's public key for verification of signature.

In all the approaches mentioned above we analyze that security is only provided to data at rest i.e. encryption is done at the cloud side. So when the user outsources the data to the cloud, data can be attacked while on the way. To resolve this issue encryption must be done at the user side. So that data can travel in encrypted form only. For this strong encryption algorithm i.e. Rijndael Encryption Algorithm can be used. Also to prevent user's data from unauthorized access EAP-CHAP can be used.

III. Techniques

a) Authentication Protocol

EAP will implement on Cloud environment for authentication purpose. However different categories EAP are classified by authentication method. In our purposed model we use Challenge-Handshake Authentication Protocol (CHAP) for authentication. When client demands data or any service of cloud computing. Service Provider Authenticator (SPA) first requests for client identity. The whole process between client and Cloud provide explain in a figure 2 given below.

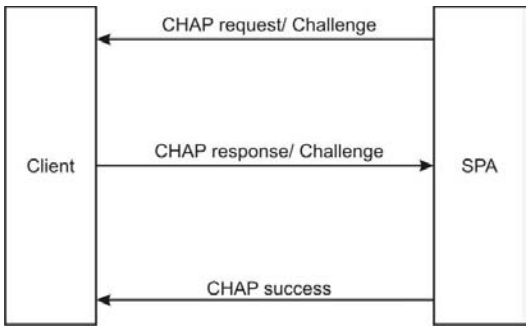

Figure 2 : Implementation of CHAP in cloud computing

Authentication of CHAP performs in three steps

1. When client demands a service, Service Provider Authentication sends a "challenge" message to client.
2. Client responds with a value that is calculated by using one way hash function on the challenge.
3. Authenticator verifies the response value against its own calculated hash value. If the values match, the Cloud provider will give service, otherwise it should terminate the connection.

Implementation of EAP-CHAP in Cloud Computing will solve the authentication and authorization problems. [8]

b) Rijndael Encryption Algorithm

Rijndael is the block cipher algorithm recently chosen by the National Institute of Science and Technology (NIST) as the Advanced Encryption Standard (AES). It supersedes the Data Encryption Standard (DES). Rijndael is a standard symmetric key encryption algorithm used to encrypt sensitive information. The choice was based on a careful and comprehensive analysis of the security and efficiency characteristics of Rijndael's algorithm.

Rijndael is an iterated block cipher. Therefore, the encryption or decryption of a block of data is accomplished by the iteration (a round) of a specific transformation (a round function). Rijndael also defines a method to generate a series of sub keys from the original key. The generated sub keys are used as input with the round function. Rijndael was designed based on the following three criteria:

1. Resistance against all known attacks;
2. Speed and code compactness on a wide range of platforms;
3. Design simplicity

Rijndael is the best combination of security, performance, efficiency, ease of implementation and flexibility. The Rijndael algorithm supports key sizes of 128, 192 and 256 bits, with data handled in 128-bit blocks. Rijndael uses a variable number of rounds, depending on key/block sizes, as follows: 9 rounds if the key/block size is 128 bits, 11 rounds if the key/block size is 192 bits, and 13 rounds if the key/block size is 256 bits.

Rijndael is a substitution linear transformation cipher. It uses triple discreet invertible uniform transformations (layers). Specifically, these are: Linear Mix Transform; Non-linear Transform and Key Addition Transform. Even before the first round, a simple key addition layer is performed, which adds to security. Thereafter, there are Nr-1 rounds and then the final round. The transformations form a State when started but before completion of the entire process. [1]

i. *High-level description of the algorithm*

a. *Key Expansion*

Round keys are derived from the cipher key using Rijndael's Key schedule.

b. *Initial Round*

Add Round Key each byte of the state is combined with the round key using bitwise xor.

c. *Rounds*

- SubBytes
- ShiftRows
- MixColumns
- AddRoundKey

d. *Final Round (no MixColumns)*

- SubBytes
- ShiftRows

- Add Round Key

e. *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. The S-box used is derived from the multiplicative inverse over GF(2^8) and then an affine transformation is applied.

f. *The ShiftRows Step*

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. In this way, each column of the output state of the ShiftRows step is composed of bytes from each column of the input state. Rijndael variants with a larger block size have slightly different offsets. For a 256-bit block, the first row is unchanged and the shifting for the second, third and fourth row is 1 byte, 3 bytes and 4 bytes respectively—this change only applies for the Rijndael cipher when used with a 256-bit block as AES does not use 256-bit blocks.

g. *The MixColumns Step*

In the MixColumns step, the four bytes of each column of the state are combined using an invertible linear tranformation. The MixColumns function takes four bytes as input and outputs four bytes, where each input byte affects all four output bytes. Together with ShiftRows, MixColumns provides diffusion in the cipher.

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

$$\begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix}.$$

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 $c(x) = 0x03 \cdot x^3 + x^2 + x + 0x02$. The coefficients are displayed in their hexadecimal equivalent of the binary representation of bit polynomials from GF(2)[x]. The MixColumns step can also be viewed as a multiplication by a particular MDS matrix in a finite field.

h. *The AddRoundKey step*

In the AddRoundKey step, the subkey is combined with the state. For each round, a subkey is derived from the main key using Rijndael's key schedule; each subkey is the same size as the state. The subkey is added by combining each byte of the state with the corresponding byte of the subkey using bitwise XOR. [11]

IV. Conclusion

Data security has become the vital issue of cloud computing security. It depends upon the way Cloud Service Provider (CSP) allows its client to get registered with his cloud network. In our survey we analyze how security is provided to the data at rest i.e. encryption is done by the cloud service provider. But we noticed that this is not sufficient as when the user outsources the data to the cloud data must also be secured on the way to the cloud. So it is preferred that encryption must be done by the user to provide better security.

References Références Referencias

1. 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.
2. Mandeep Kaur, Manish Mahajan, "Using encryption Algorithms to enhance the Data security in Cloud computing", International Journal of Communication and Computer Technologies (IJCCTS), Vol. 01, Issue: 03, January 2013.
3. Parsi Kalpana, Sudha Singaraju, "Data Security in Cloud Computing using RSA Algorithm", International Journal of Research in Computer and Communication Technology (IJRCCT) , Vol. 1, Issue 4, September 2012.
4. Eman M.Mohamed, Hatem S.Abdelkader,Sherif El-Etriby, "Data Security Model for Cloud Computing", The Twelfth International Conference on Networks: ICN 2013.
5. C. Bagyalakshmi, Dr. R. Manicka Chezian, "A Survey on Cloud Data Security using Encryption Technique", International Journal of Advanced Research in Computer Engineering and Technology, Vol. 1, Issue 5, July 2012.
6. Jiyi Wu, Qianli Shen, Tong Wang, Ji Zhu, Jianlin Zhang, "Recent Advances in Cloud Security" Journal of Computers, Vol. 6, No. 10, October 2011.

7. Muneshwara M.S, Arvind Tejas Chandral, "Monitoring the integrity of dynamic data stored in Cloud Computing", International Journal of Engineering Research & Technology (IJERT), Vol. 1, Issue 4, June 2012.
8. Sadia Marium, Qamar Nazir, Aftab Ahmed, Saira Ahthasham, Mirza Aamir Mehmood," Implementation of EAP with RSA for enhancing the security of cloud computing", International Journal of Basics and Applied Sciences, 1 (3) 2012 177-183.
9. http://www.efgh.com/software/rijndael.htm
10. http://en.wikipedia.org/wiki/Cloud_computing
11. http://en.wikipedia.org/wiki/Advanced_Encryption_Standard