Cloud Data Security using Authentication and Encryption Technique

Anuj Kumar, Ashutosh Sharma, Anil Kumar

***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 centres. 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**

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[1].

A. Cloud Computing Deployment Models

The various cloud deployment models are shown

1. 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.

2. Private Clouds:

Due to security and availability issues more and more companies are choosing Private Clouds. It provides more secure platform to the employees and customers of an organization. For example Banks, In banks all the employees and customers can access the bank data which is assigned to them particularly.

3. Hybrid Cloud:

Hybrid cloud is the combination of the of the Public cloud and private cloud. In this type of cloud services the internal resources, stays under the control of the customer, and external resources delivered by a cloud service provider.

4. Community Cloud:

The community cloud shares the infrastructure around several organizations which can be managed and hosted internally or by third party providers.[7]

B. Cloud Models or Layers

The various layers of cloud are shown

1) SAAS(Software as a service) – In this companies host applications in the cloud that many users access through internet connections. E.g. Gmail, facebook.

2) PAAS (Platform as a service) – Developers can design, build and test applications that run on the cloud provider's infrastructure. E.g. Google app Engine.[2]

3) IAAS (infrastructure as a service) – This part is basically belong to the admin part or we can say the service provider. In this part the service provider provides the user with the basic infrastructure. Like platform and the end applications which become the interface between users and
the cloud.[7]

C. Data security issues in the cloud

Securing data is always of vital importance as shown 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 problem it is required that data at both user and server end must be in encrypted form.

II. PROPOSED WORK PLAN

The two different approaches used for ensuring security in cloud are as follows:-

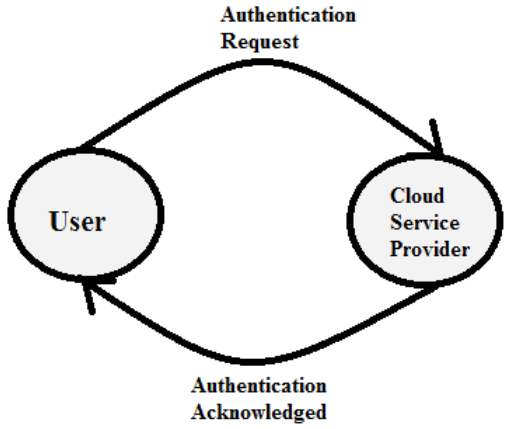
1. Extensible Authentication Protocol-CHAP:

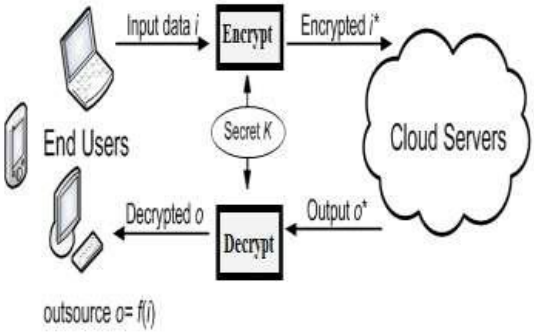
EAP(Extensible Authentication Protocol) will implement on Cloud environment for authentication purpose. It is used for the transport and usage of keying material and parameters generated by EAP methods. In our purposed model

we use Challenge Handshake Authentication Protocol (CHAP) for authentication. [10]

2. **Rijndael encryption Algorithm**-Rijndael as the standard symmetric key encryption algorithm to be used to encrypt sensitive information. 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). As input, Rijndael accepts one-dimensional 8-bit byte arrays that create data blocks.

The plaintext is input and then mapped onto state bytes. The cipher key is also a one-dimensional 8-bit byte array. With an iterated block cipher, the different transformations operate in sequence on intermediate cipher results (states). [6]





Methodology

The steps of the methodology shown in figure 4 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.

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. 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 theresponse 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.[5]

B. Rijndael Encryption Algorithm Implementation

Encryption:

The code for encryption process is given in table 1.

```
Rijndael(State, CipherKey)
{
KeyExpansion(CipherKey,ExpandedKey);
AddRoundKey(State,ExpandedKey);
For( i=1; iFinalRound(State,ExpandedKey +
Nb*Nr);
}
And the round function is defined as:
Round(State, RoundKey)
{ ByteSub(State);
ShiftRow(State);
MixColumn(State);
AddRoundKey(State,RoundKey);
}
```

Table 1. 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

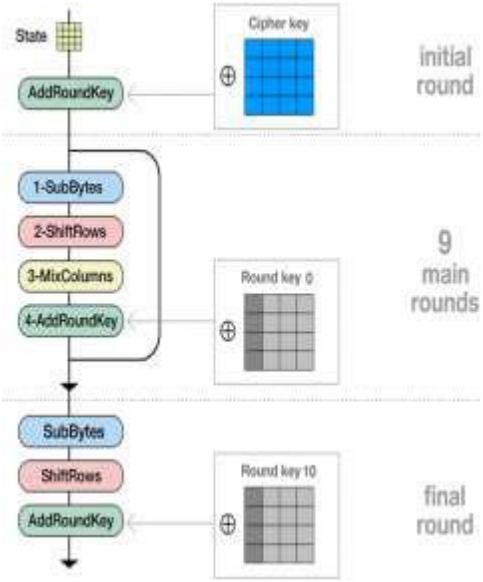
lengths. Size of data blocks to be encrypted with Rijndeal is always 128 bits. Initial round of Rijndeal is Add Round Key, this is followed by four iterative round including sub Bytes, shift Rows, mix Columns and add
round key. Rijndeal with 128 bit key length has 10 rounds,192-bit has 12 rounds and 256 bit has 14 rounds.

Each round consists of the following steps.

1. Initial Add Round Key
2. Sub Bytes () Transformation
3. Substitutional Box Created For Sub bytes
4. Mix Columns () Transformation
5. Add Round Key () transformation

The inverse process of encryption gives decryption text.[4]

A.Rijndael Algorithm: Encryption/Decryption Process for
Rijndael Algorithm is shown



Rijndael Algorithm

1) The Sub Bytes step

The Sub Byte 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 Sub Byte using an 8-bit substitution box, the Rijndael S-box.

2) The Shift Rows step

The Shift Rows 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

3) The MixColumns step

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**(*28*)
and is then multiplied modulo x4+1 with a fixed polynomial

$c(x) = 0x03 \cdot x3 + x2 + x + 0x02$

4) The Add Round Key step

In the Add Round Key step, the sub key is combined with the
state. For each round, a sub key is derived from the main key using Rijndael's key schedule; each sub key is the same size as the state. The sub key is added by combining each byte of the state with the corresponding byte of the sub key using bitwise XOR.[3]

III. 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

REFERENCES

[1] 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.

[2] 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.

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

[4] 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.

[5] 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.

[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]http://thegadgetsquare.com/1552/what-is-cloud-computing/

[8]http://en.wikipedia.org/wiki/Cloud_computing

[9]http://en.wikipedia.org/wiki/Advanced_Encryption_Standard.

[10]https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol