IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

CLOUD DATA SECURITY USING AUTHENTICATION AND ENCRYPTION TECHNIQUE

Amrutha A Nair, Geethu Wilson
MSc Scholar, Assistant Professor
Department of computer science
St. Joseph's College (Autonomous), Irinjalakuda, Thrissur, India

Abstract: Cloud computing emerges as a replacement computer paradigm that aims to supply a reliable, customized and dynamic computing environment for end-users. The major issue of cloud computing is that the security of knowledge is stored on the provider's cloud and privacy while the information is being transmitted. Any unauthorized persons can access our files or data in the cloud so that the security gradually losses, so we have designed architecture that can help to encrypt and decrypt the file on the user side. It provides security to data at any time. In this paper, we have used the Extensible Authentication Protocol CHAP and Rijndael Encryption Algorithm.

Index Terms : EAP-CHAP Encryption, Rijndael Algorithm, cloud.

I. INTRODUCTION

Cloud computing is the delivery of computing services such as servers, storage, databases, networking, software, analytics, intelligence, and moreover the cloud(internet). With an associate degree on-premises datacentre, we've to manage everything, like getting and putting in hardware, virtualization, putting in the package, and the other needed applications, fitting the network, configuring the firewall, and fitting storage for knowledge.

Example: Dropbox, Gmail, Facebook

a) Cloud Computing Deployment Models [1]

1. PUBLIC CLOUD

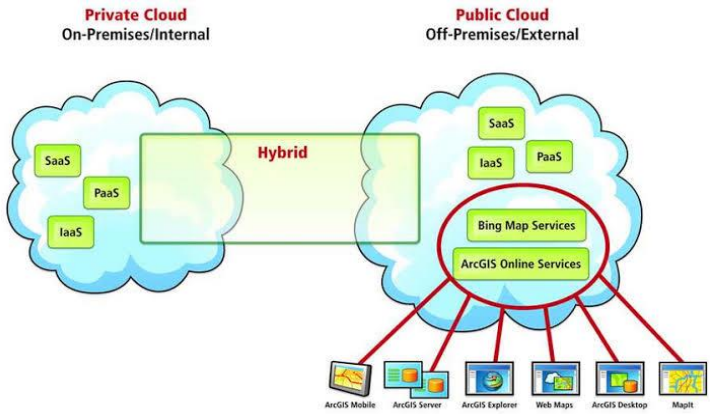
A public cloud is a type of computing in which a service provider makes resources available to the public via the internet. The resource varies the provider but may include storage capabilities, applications, or virtual machines.

2. PRIVATE CLOUD

The cloud computing resources that are exclusively used inside one business organization are termed personal cloud. A personal cloud may physically be located on the company's on-site data centre or hosted by a third-party service provider.

3. HYBRID CLOUD

It is the mix of public and personal clouds, which are finite along by the technology that enables knowledge applications shall be shared between them. The hybrid cloud provides flexibility and a lot of preparation choices for the business.



b) Cloud Model Layers [7]

1. INFRASTRUCTURE AS A SERVICE (IaaS)

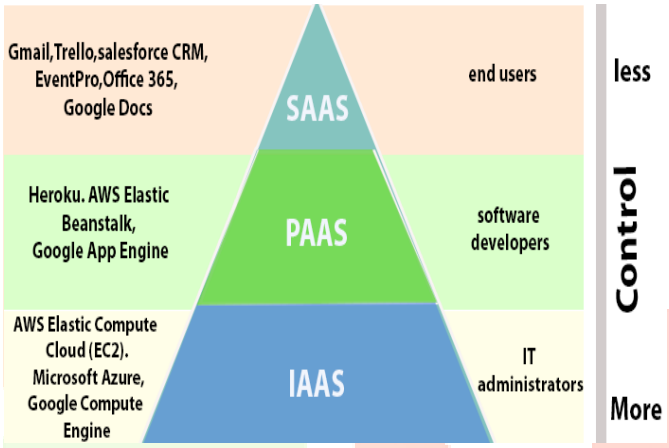
In IaaS, we will rent IT infrastructures like servers and virtual machines (VMs), storage, networks, operational systems from a cloud service merchandiser. We will produce VM running Windows or UNIX and install something we would like thereon. Using IaaS, we tend to don't have to be compelled to care concerning the hardware or everything else. Using IaaS, we tend to get the most flexibility, but still, we'd like to place additional effort into maintenance.

2. PLATFORM AS A SERVICE (PaaS)

The service provides an on- demand atmosphere for developing, testing, delivering, and managing software system applications. The developer is liable for the appliance, and also the PaaS merchant provides the power to deploy and run it. Using PaaS, the flexibleness gets the scale back, however, the management of the atmosphere is taken care of by the cloud.

3. SOFTWARE AS A SERVICE (SaaS)

It provides centrally hosted and managed code services to the end-users. It delivers a code over the internet, on-demand, and typically on a subscription basis. The SaaS is used to attenuate an operational value to the utmost extent.



II. PROPOSED WORK PLAN

Two different techniques are used,

1. EXTENSIABLE AUTHENTICATION PROTOCOL – CHAP

EAP will implement in a cloud environment. It is used for generating parameters and a mode of transport using the EAP method. In the proposed model, we used CHAP for authentication.

2. RIJNDAEL ENCRYPTION ALGORITHM

The algorithm has described by AES is a symmetric key algorithm meaning the same key used for both encrypting and decrypting the data. Rijndael is a family of ciphers with different key and block sizes. Each with block size of 128 bits, but three different key lengths: 128, 192, 256. The input is also plain text and mapped to byte state. The cipher key is one -dimensional 8-bit array.

a) AUTHENTICATION PROTOCOL

CHAP is primarily used for security purposes. It is the process of authenticating a user to a network entity which may be any server (web or ISP).

b) RIJNDAEL ENCRYPTION ALGORITHM IMPLEMENTATION

i) ENCRYPTION

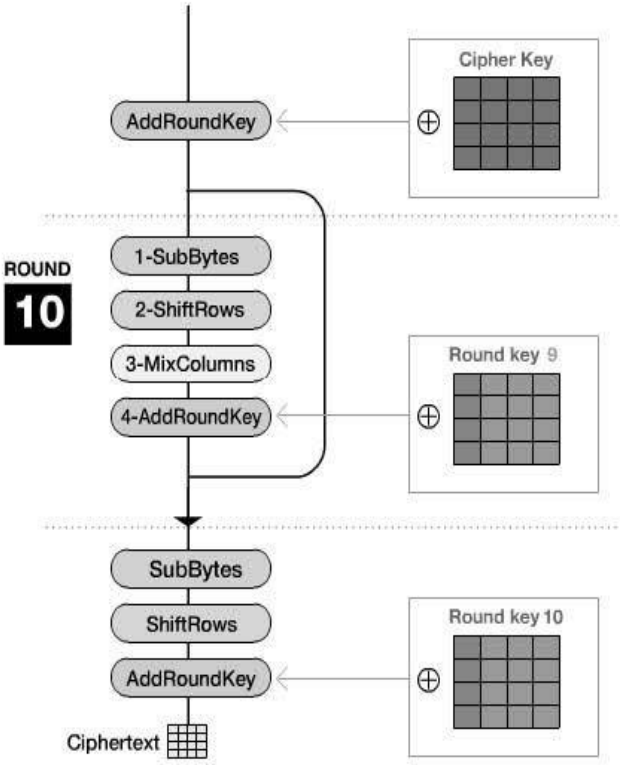
The code for encryption:

```
Rijndael (State,CipherKey)
 {
KeyExpansion(CipherKey,ExpandedKey);
AddRoundKey(State,ExpandedKey);
For( i=1 ; i
 FinalRound(State,ExpandedKey + Nb*Nr);
}

And the round function is defined as:

Round(State,RoundKey)
 {
ByteSub(State);
ShiftRow(State);
MixColumn(State);
AddRoundKey(State,RoundKey);
}
```

This encryption method encrypts the user's data. The symmetric key is used for encryption. The size of data blocks also 128 bits in Rijndael encryption. The first round of Rijndael is ADDROUNDKEY this is followed by other 4 iterative rounds that are SubByte , shiftRows, mixColumns, and addround key.



A. The subByte Step

In the SubBytes step, every computer memory unit a (i,j) within the state array is replaced with a SubByte S (i,j) a mistreatment associate degree 8-bit substitution box. This operation provides the non-linearity within the cipher. The S-box has used springs from the reciprocal over the GF (2^8), legendary to possess sensible non-linearity properties. To avoid attacks have supported by easy pure mathematics properties, the S-box is made by combining the mathematical function with an associate degree invertible.

B. The ShiftRow Step

Shift the left, every four rows of the matrix are shifted to the left. Any entries that 'fall off' square measure re-inserted on the proper facet of the row.

The shift is disbursed as follows –

- The first row isn't shifted.
- Shift second row, one position to the left.
- Shift third row, two positions to the left.
- Shift fourth row, three positions to the left.

C. The MixColumns Step

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

In this case multiplication by 1 indicates no change, the multiplication with 2 indicates a shift to left, and the multiplication with 3 means Shift has left and performed an XOR with an unshifted value. Each column has had treated as a polynomial over GF (2^8).

D. The AddRoundKey Step

For every spherical, a subkey springs from the most key victimization Rijndael's key schedule; every subkey is that the same size because of the state. The subkey is a value-added by combining every computer memory unit of the state with the corresponding computer memory unit of the subkey victimization bitwise XOR.

III. CONCLUSION

Data security has becoming a major issue of cloud computing security. In this case, we target on client side security in proposed system. Data can access only for authorized users, unauthorized users can't access the data. In this case we use the encryption method for good security. The security is provided by Rijndael Encryption Algorithm.

REFERENCES

[1] 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

[2] Akhil K.M , Praveen Kumar M , Pushpa B.R , "Enhanced Cloud Data Security using AES Algorithm" International Conference on Intelligent Computing and control(12C2), 2017

[3] Sanjoli Singla, Jasmeet Singh, " Implementing Cloud Data Security by Encryption using Rijndael Algorithm" Global Journal of computer science and technology(GJCST), Vol. 13, Issue 4, 2013

[4] D. Gayathri, Manjula . A , "Double Encryption Using Rijndael Algorithm for Data Security in Cloud Computing" International Journal of Emerging Technologies in Engineering Research (IJETER), Volume 5, Issue 2, 2017

[5] Prashant Rewagad, Yogita Pawer, "Use of Digital Signature and Rijndeal encryption algorithm to Enhanced Security of data in Cloud computing Services", proceeding published in international journal of Computer Applications (IJCA), 2012

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

[7] https://www.visma.com/blog/cloud-basics-the-layers/