International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 08 | Aug-2016 www.irjet.net p-ISSN: 2395-0072

An Advanced Architecture for Securing Data in Cloud

Naga Durga Saile.K[1], K.Navatha [2]

[1]Asst.Professor, Dept.of CSE , St.Martin's Engg.college ,Telangana, India.
[2]Asst.Professor, Dept.of CSE ,St.Martin's Engg.college ,Telangana, India

---

Abstract: *Technology enhancements with the increased connectivity and usage of large amounts of data resulted in cloud architecture .Cloud computing technology is where the users can use the services in the form of servers and enables the users that can use high end services of storing their data in cloud and access the data anywhere. Security to this data is a challenging issue. Using different encryption techniques security is provided but security is still a hindrance in this field. In this research paper we have proposed an architecture, for secure connection establishment as well as key generations and thus providing a better security mechanism to the data in cloud.*

Key Words: Cloud, Security issues, Architecture, Key Generations, Diffie Hellman Key Exchange, Two Fish algorithm, Base 64 Encoding.

1. INTRODUCTION

We live in the age of information and technology. As the world changes the technology also changing rapidly. With the advent of technology a lot of digital information is also exchanged over the network. The information with is confidential needs utmost security measures to be taken for exchange of data as well as storage of data .These days most of the data is stored in the cloud and this transformative paradigm that involves services over the internet is known as cloud computing. Cloud computing involves providing computing, networking and storage resources to the users. Cloud computing involves provides Broad network access, Resource pooling, Reduced cost, Improved performance, Measured services, outsourced management and on demand self-service.

The cloud had 4 different deployment models which include public cloud-available for public use or a large industry group, Private cloud-operated for exclusive use of a single organisation, Community cloud-available for shared use of several organisations belonging or supporting a specific community. Hybrid cloud-that combines multiple clouds(public and private)that remain unique but bound together to offer application and data portability.

Cloud Computing offers 3 service models.

1) Software as a service (SaaS): Applications management and user interfaces are provided over a network.

2) Platform as a service (PaaS):Application development frameworks, operating systems and deployment frame works.

3) Infrastructure as a service (IaaS): Virtual computing, storage and network resources that can be provisioned on demand.

Security is a major challenge in cloud computing. In

addition to the traditional threats the cloud application have additional vulnerabilities because of shared usage of resources and virtualised rescuers. The key security challenges include authentication, authorisation, security of data at rest, data in motion, data integrity and auditing.

In cloud computing authentication is provided by mechanism such as SSO (Single Sign On), Saml-token(Security assertion markup language),One time password ,Kerberos etc. and authorisation by the open standard OAuth. Securing data is critical in cloud computing. Mainly for the applications as the data flows from applications to storage and vice-versa. Data in cloud are prone to main in middle attacks, denial of service ,etc.

The security of data can be provided using symmetric and asymmetric encryption depending upon the data at rest ,motion or in use.

In this paper we propose a methodology for server connection establishment and authentication of the user and encryption while storing the data in the cloud.

2. CLOUD SECURITY ISSUES

Availability, Confidentiality and Integrity are the three main issues of cloud computing known as ACI traid.

Availability: It is the attestation that the data will be available to the user irrespective of the location

Confidentiality: Avoidance of unauthorised user exposure and access.

Integrity: Assurance that the data sent and received are same and no alteration is done.

3. PROBLEM STATEMENT

Since cloud computing deals with data storage on the web various issues like data leakage, data theft, unauthorised access etc. occurs. In order to avoid all these cryptographic techniques are used for data encryption and decryption and thus provided a secured data access to the user. There are different encryption algorithms used for the data protection ,but still we find adverse security effects on the network. The security of data over the net is a challenging issue. The complexity and the generation of keys for encryption plays a vital role and there is a need for a strong architecture for encryption process.

4. Proposed system

Here we aim to provide the security for the data in cloud by using encryption techniques ,encoding techniques and key exchange protocols, We used Diffie Hellman key exchange, Two fish encryption technique. And Base 64 encoding and proposed a new architecture for encrypting data in the cloud and thus provide better security and reliability and also providing data integrity.

The architecture involves the following steps:

1) Connection establishment

2) Account creation

3) Authentication

4) Data Exchange

1) Connection establishment

In order to use any cloud service the user first needs to establish a connection with the server. The establishment of connection with the server can be done with HTTPS and TSL/SSL Handshake process.

The following is the handshake process:

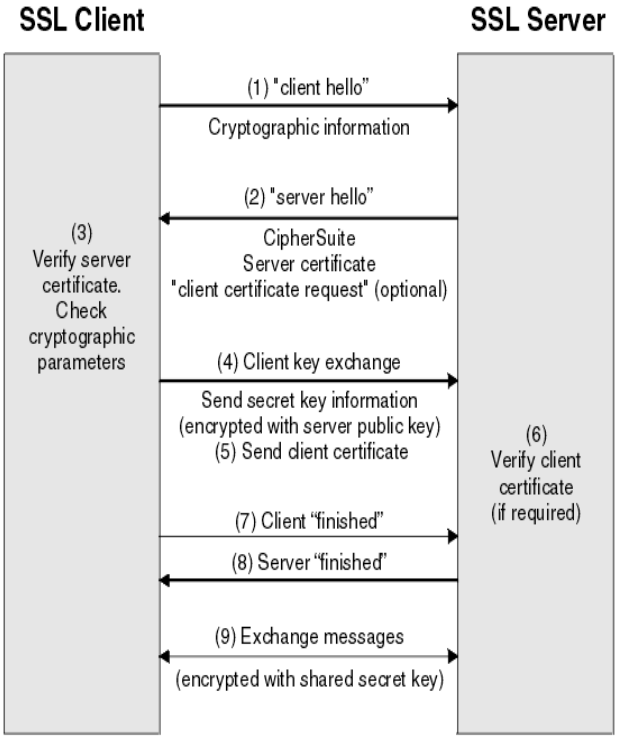


Fig: Client Server Hand Shake Process

2) Account Creation

Once the connection is established with the server the user is asked to fill in his credentials for creating an account on the cloud. The details are sent to the server. Now, using the Diffie hellman key exchange protocol, the server generates a key to the client which is his unique identifier number. Apart from the username created this is an additional security number where the user have to remember and kept secret for further authentication process.

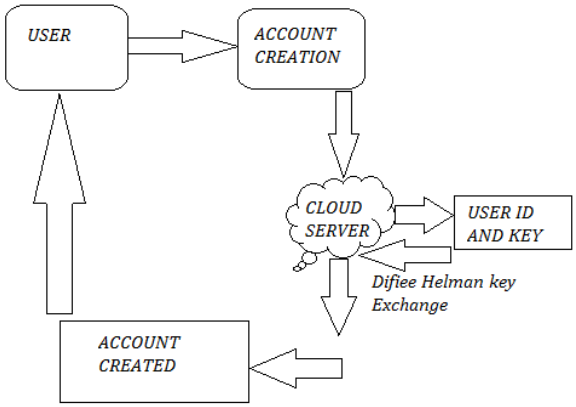


Fig: Account Creation using Diffie Hellman Key Exchange

3) Authentication

As the user opens the home page of the cloud service provider, SSL connection is established. As the account creation is also done ,the user is asked for his authentication by entering the valid credentials and the unique number that was generated during the authentication process.

The server authenticates the user by checking with the Diffie Hellman equivalent key and user id. If both match then the user is authenticated for further data exchange.

4) Data Exchange

In this step the user exchanges the data with

cloud server. As security is the major issue in cloud computing we use the base 64 encoding and Two Fish encryption technique, for the further encryption process.

4.1 Encryption Process

1) First the Diffie Hellman key that is generated during the connection establishment is identified.(DH)

2) Next ,a base 64 encoding(BE) is implemented on that key(DH)

3) This encoded value is used as a key for TWO Fish Encryption.

IMPLEMETATION

1) Let the **DH value =1012**

2) A Base 64 encoding is done on DH

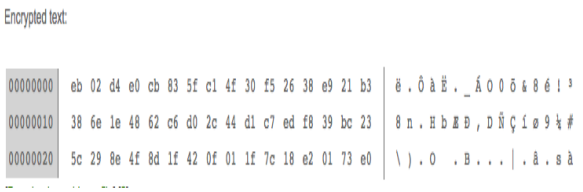
BE=MTAxMg==

3)This BE is used as a key for Two Fish Encryption

Plain text :This is and sample encryption model

Key:MTAxMg==

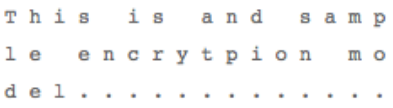
Encrypted Text as follows:



4.2 Decryption Process

1) Enter the encrypted data and the key

2) The resultant plain text is as follows:



Using the above methodology both encryption and decryption are done.

5.Encryption Techniques

The description of Diffie Hellman key Exchange, Base 64 Encoding, Two Fish Encryption are discussed below

5.1 Diffie Hellman Key Exchange.

The Diffie-Hellman protocol is a method for two computer users to generate a shared private key with which they can then exchange information across an insecure channel. Let the users be named Alice and Bob. First, they agree on two prime numbers g and p, where p is large (typically at least 512 bits) and g is a primitive root modulo p. (In practice, it is a good idea to choose p such that $(p-1)/2$ is also prime.) The bers g and p need not be kept secret from other users. Now Alice chooses a large random number a as her private key and Bob similarly chooses a large number b. Alice then computes $A = g^a \pmod p$, which she sends to Bob, and Bob computes $B = g^b \pmod p$, which he sends to Alice.

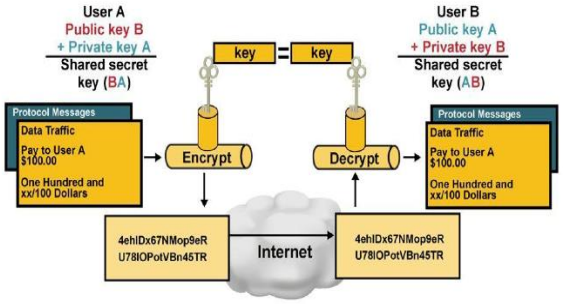
Now both Alice and Bob compute their shared key $K = g^{ab} \pmod p$, which Alice computes as

$$K = B^a \pmod p = \left(g^b\right)^a \pmod p$$

and Bob computes as

$K = A^b \pmod{p} = (g^a)^b \pmod{p}$.

Alice and Bob can now use their shared key K to exchange information without worrying about other users obtaining this information. In order for a potential eavesdropper (Eve) to do so, she would first need to obtain $K = g^{a\,b} \pmod{p}$ knowing only g, p, $A = g^a \pmod{p}$ and $B = g^b \pmod{p}$.



5.2 BASE64

Base64 is a group of similar binary-to-text encoding schemes that represent binary data in an ASCII string format by translating it into a radix-64 representation. The particular set of 64 characters chosen to represent the 64 place-values for the base varies between implementations. The general strategy is to choose 64 characters that are both members of a subset common to most encodings, and also printable. This combination leaves the data unlikely to be modified in transit through information systems, such as email, that were traditionally not 8-bit clean. For example, MIME's Base64 implementation uses A–Z, a–z, and 0–9 for the first 62 values. Other variations share this property but differ in the symbols chosen for the last two values.

5.3 Two Fish algorithm

In, Twofish is a symmetric cryptography with a block 128 buts and key sizes up to 256 bits. It was one of the five finalists of the Advanced encryption standards but it was not selected for standardization. Two fish is related to the earlier block cipher Blowfish.

S-Boxes

S-boxes An S-box is a table-driven non-linear substitution operation used in most block ciphers. S-boxes vary in both input size and output size, and can be created either randomly or algorithmically. S-boxes were first used in Lucifer, then DES, and afterwards in most encryption algorithms. Twofish uses four different, bijective, key-dependent, 8-by-8-bit S-boxes. These S-boxes are built using two fixed 8-by-8-bit permutations and key material.

MDS Matrices

MDS Matrices A maximum distance separable (MDS) code over a field is a linear mapping from a field elements to b field elements, producing a composite vector of a+b elements, with the property that the minimum number of non-zero elements in any non-zero vector is at least b + 1 [MS77]. Put another way, the “distance” (i.e., the number of elements that differ) between any two distinct vectors produced by the MDS mapping is at least b + 1. It can easily be shown that no mapping can have a larger minimum distance between two distinct vectors, hence the term maximum distance separable. MDS mappings can be represented by an MDS matrix consisting of a × b elements. Reed-

Solomon (RS) error-correcting codes are known to be MDS. A necessary and sufficient condition for an a × b matrix to be MDS is that all possible square submatrices, obtained by discarding rows or columns, are non-singular. Serge Vaudenay first proposed MDS matrices as a cipher design element [Vau95]. Shark [RDP+96] and Square [DKR97] use MDS matrices (see also [YMT97]), although we first saw the construction used in the unpublished cipher Manta3 [Fer96]. Twofish uses a single 4-by-4 MDS matrix over GF(28).

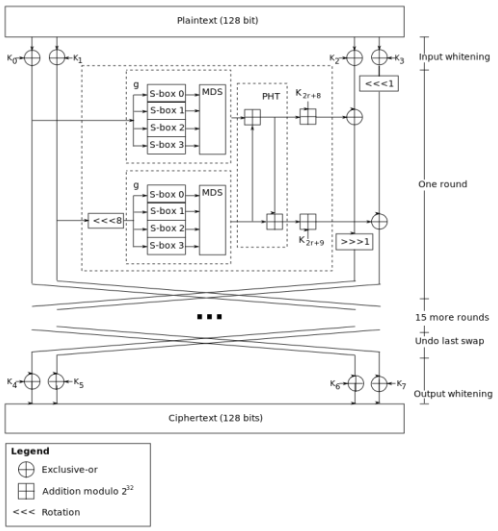


Fig :Two Fish Encryption algorithm structure

6. Conclusion and Future Work

In this paper ,we analysed the security challenges faced in cloud computing. Data security is provided by using different cryptographic techniques. Here, we proposed an architecture for secured connection establishment using Diffie Hellman key exchange and further encryption process using Base64 encoding and TwoFish encryption algorithm. TwoFish encryption provides a good security because the number of steps involved for encryption and the round functionality which is used helps to generate a good encryption and since Base64 is also used a combination of both these has less chance for eavesdropping since he is unaware of the key that will be used for the encryption. And also the keys that are generated using Two Fish are strong and has very less chance of breaking.

Hence this architecture and proposed methodology works effectively and provides much more security. In future the enhancement can be provided with image encryption.

REFERENCES

[1}https://www.schneier.com/academic/paperfiles/paper-twofish-paper.pdf.

[2] Farzad Sabahi. Cloud Computing Security Threats and Responses. Communication Software and Networks (ICCSN), 2011 IEEE 3rd International Conference.

[3] Ashish Agarwal, Aparna Agarwal. The Security Risks Associated with Cloud Computing. International Journal of Computer Applications in Engineering Sciences [VOL I, SPECIAL ISSUE ON CNS, JULY 2011] [ISSN: 2231-4946].

[4] Ashutosh Kumar Dubey, Animesh Kumar Dubey, Mayank Namdev, Shiv Shakti Shrivastava. Cloud-User Security Based on RSA and MD5 Algorithm for Resource Attestation and Sharing in Java Environment. Software Engineering (CONSEG), CSI

Sixth International Conference, Sept. 2012

[5] M.Venkatesh, M.R.Sumalatha, Mr.C.SelvaKumar. Improving Public Auditability, Data Possession in Data Storage Security for Cloud Computing. Recent Trends In Information Technology (ICRTIT), 2012 International Conference, April 2012.

[6] Prashant Rewagad, Yogita Pawar in. Use of Digital Signature with Diffie Hellman Key Exchange and AES Encryption Algorithm to Enhance Data Security in Cloud Computing. 2013 International Conference on Communication Systems and Network Technologies.

[7] Hai Yan, Zhijie Jerry Shi. Software Implementations of Elliptic Curve Cryptography. Information Technology: New Generations, Third International Conference, April 2006.

[8] W. Diffie and M.E. Hellman. New directions in cryptography. IEEE Transactions on Information Theory, 1976.

[9]. https://eprint.iacr.org/2014/049.pdf

[10]. https://en.wikipedia.org/wiki/Base64