TO INCREASE SECURITY IN CLOUD USING RELIABLE RE-ENCRYPTION

Hrushabh G. Saysardar
(9764086922, hrushusays@gmail.com)

Shubham M. Bobade
(8087755839, Shu.bobade@gmail.com)

Hemant P. Naranware
(9175461241, hemantnaranware@gmail.com)

Mohashil R. Upare
(9604657086, uparemoshil@gmail.com)

(I.T DEPARTMENT)

(K.D.K COLLEGE OF ENGINEERING)

Abstract*-- *In this paper, we proposed advanced encryption technique using web server or cloud. This scheme is best suited for efficient data retrieval from web server & cloud, which enables the cloud or web server to automatically re-encrypt the data. It prevent revoked users from decrypting the data by using their own keys.

Index Terms- Advanced encryption scheme, web server or cloud, proxy re-encryption.

1. INTRODUCTION

Cloud is distributed system where there are many cloud serves. In cloud servers owner's data is stored on multiple cloud servers. Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

Cloud computing refers to both the applications delivered as services over the Internet and the hardware and systems software in the datacenters that provide those services. Cloud computing enhances collaboration, agility, scale, availability and provides the potential for cost reduction through optimize and efficient computing.

To enhance the security of cloud computing and cloud resources through reliable security features of encryption. Our objective is to increase security of cloud computing through required security algorithms and through re-encryption schemas.

Lack of control is transparency in the cloud implementation – somewhat contrary to the original promise of cloud computing in which cloud implementation is to be relevant. Cloud computing is clearly one of the most enticing technology areas of the current times due, at least in part to its cost-efficiency and flexibility. However, despite the surge in activity and interest, there are significant, persistent concerns about cloud computing that are impeding the momentum and will eventually compromise the vision of cloud computing as a new IT procurement model. Transparency is needed for regulatory reasons and to ease concern over the potential for data breaches. In short, the potential of the cloud is not yet being realized.

2. TYPES OF CLOUD

There are basically four types of clouds, which are described below.

Public cloud: This is the one of the cloud in which cloud services are being available to users via a service provider over the Internet. It provides a control mechanism for them. The services may be free or offered on a pay-per usage model.

Private Cloud: This provides many of the benefits of public, but the main difference among two is that the data is managed properly within the organization only, without the limits of network bandwidth.

Community Cloud: This type of cloud is basically managed by group of originations that have a common objective to achieve. The members share access to the data in the cloud.

Hybrid Cloud: This is the combination of public as well as private cloud. It can also be defined as multiple cloud systems that are connected in a way that allows programs and data to be moved easily from one system to another.

3. CHARACTERISTICS OF CLOUD COMPUTING

There are several characteristics of cloud computing, which are described below-

Virtualization: Through Cloud computing, user is able to get service anywhere through any kind of terminal. User can attain or share it safely anytime.

High Reliability: Cloud uses data fault tolerant to ensure the high reliability of the service.

Versatility: Cloud computing can produce various applications supported by cloud, and one cloud can support different applications running it at the same time.

On Demand Service: Cloud is a large resource pool that a user can buy according to his/her need; cloud is just like running water, and gas that can be charged by the amount that user used.

Extremely Inexpensive: The centered management of cloud make the enterprise needn't undertake the management cost of data center that increase very fast. The versatility can increase the utilization rate of the available resources compared with traditional system, so users can fully take advantage of low cost.

Some advantages are listed below-

- Cloud computing do not need high quality equipment for user and it is easy to use.
- Cloud computing can realize data sharing between different systems.

- Cloud computing provides dependable and secure data storage center. You don't worry the problems such as data loss or virus.

4. DATA SECURITY ISSUES IN THE CLOUD

PRIVACY AND CONFIDENTIALITY –

Once the client host data to the cloud there should be some guarantee that access to that data will only be limited to the authorized access. Inappropriate access to customer sensitive data by cloud personnel is another risk that can pose potential threat to cloud data. Assurances should be provided to the clients and proper practices and privacy policies and procedures should be in place to assure the cloud users of the data safety.

The cloud seeker should be assured that data hosted on the cloud will be confidential.

DATA INTEGRITY-

With providing the security of data, cloud service providers should implement mechanisms to ensure data integrity and be able to tell what happened to a certain dataset and at what point.

For compliance purposes, it may be necessary to have exact records as to what data was placed in a public cloud, when it occurred, what virtual memories (VMs) and storage it resided on, and where it was processed.

DATA LOCATION AND RELOCATION-

Cloud Computing offers a high degree of data mobility. Consumers do not always know the location of their data. However, when an enterprise has some sensitive data that is kept on a storage device in the Cloud, they may want to know the location of it. Also, cloud providers should take responsibility to ensure the security of systems (including data) and provide robust authentication to safeguard customers' information.

Another issue is the movement of data from one location to another. Data is initially stored at an appropriate location decide by the Cloud provider. However, it is often moved from one place to another. Cloud providers have contracts with each other and they use each other's resources.

DATA AVAILABILITY-

Customer data is normally stored in chunk on different servers often residing in different locations or in different Clouds. In this case, data availability becomes a major legitimate issue as the availability of uninterruptible and seamless provision becomes relatively difficult.

STORAGE BACKUP AND RECOVERY-

When you decide to move your data to the cloud the cloud provider should ensure adequate data resilience storage systems. At a minimum they should be able to provide RAID (Redundant Array of Independent Disks) storage systems although most cloud providers will store the data in multiple copies across many independent servers.

In addition to that, most cloud providers should be able to provide options on backup services which are certainly important for those businesses that run cloud based applications so that in the event of a serious hardware failure they can roll back to an earlier state.

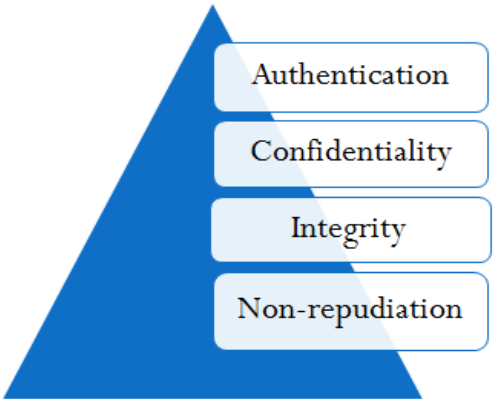

Fig 1. Goals of Security

5. PROPOSED WORK

To access a cloud based web application that will try to eliminate the concerns regarding data privacy, segregation.

AES is a block cipher with a block length of 128 bits. It allows three different key lengths: 128, 192, or 256 bits. We propose AES with 128 bit key length. The encryption process consists of 10 rounds of processing for 128-bit keys. Except for the last round in each case, all other rounds are identical. 16 byte encryption key, in the form of 4-byte words is expanded into a key schedule consisting of 44 4-byte words. The 4 x 4 matrix of bytes made from 128-bit input block is referred to as the state array. Before any round-based processing for encryption can begin, input state is XORed with the first four words of the schedule.

For encryption, each round consists of the following four steps:

SubBytes – a non-linear substitution step where each byte is replaced with another according to a lookup table (S-box).

ShiftRows – a transposition step where each row of the state is shifted cyclically a certain number of times.

MixColumns – a mixing operation which operates on the columns of the state, combining the four bytes in each column

AddRoundKey – each byte of the state is combined with the round key; each round key is derived from the cipher key using a key schedule.

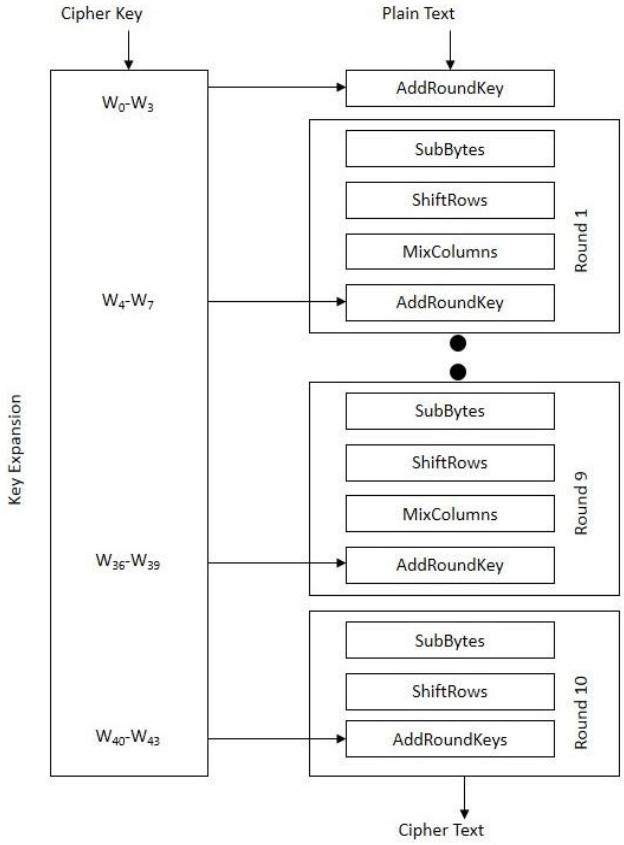

Fig 2. AES Encryption

a. SubBytes

The purpose of this step is to give ample resistance from differential and linear cryptanalysis attacks.

This is byte-by-byte substitution where each byte is substituted independently using Substitution table (S-box). Each input byte is divided into 24-bit patterns, representing an integer value between 0 and 15 which can then be interpreted as hexadecimal values. Left digit defines the row index and right digit defines the column index of S-box. At the intersection of row and column, value given is substituted. There are sixteen distinct byte-by-byte substitutions. S-box is constructed by a combination of GF (28) arithmetic and bit mangling.

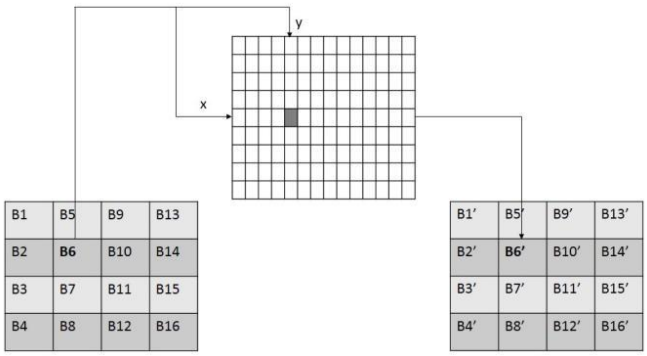

Fig 3. SubBytes

b. ShiftRows

The purpose of this step is to provide diffusion of the bits over multiple rounds. The row 0 in the matrix is not shifted, row 1 is circular left shifted by one byte, row 2 is circular left shifted by two bytes, and row 3 is circular left shifted by three bytes.

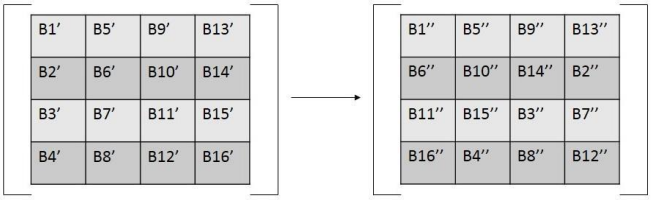

Fig 4. ShiftRows

c. Mixcolums

Like previous step, the purpose of this step is to provide diffusion of the bits over multiple rounds. This is achieved by performing multiplication one column at a time. Each value in the column is multiplied against every row value of a standard matrix. The results of these multiplication are XORed together. For e.g. value of first byte B1'' is multiplied with 02, 03, 01 and 01 and XORed to produce new B1''' of resulting matrix. The multiplication continues against one matrix row at a time against each value of a state column.

Fig 4. Mix column Transformation step

d. AddRoundKey

In this step, the matrix is XORed with the round key. The original key consists of 128 bits/16 bytes which are represented as a 4x4 matrix. This 4 words key where each word is of 4 bytes, is converted to a 43 words key. The first four words represent W[0], W[1], W[2], and W[3] The rest of expanded key i.e. W[4] to W[43] is generated as follows:-

```
        for (i=4; i<44; i++)
{
        T = W[i-1];
        if (i mod 4 = = 0)
                T = Substitute (Rotate (T))
        XOR RConstant [i/4];
        W[i] = W[i-4] XOR T;
}
```

Here

Rotate means - perform a one byte left circular rotation on the 4-byte word.

Substitute means - perform a byte substitution for each byte of the word, using S-box, also used in the SubBytes step.

RConstant means – Round Constant (size of 4 bytes) which is XORed with the bytes. The rightmost three bytes of the round constant are zero.

In this way, W [4]… W [43] of the key schedule are generated from the initial four words. Although, overall, the same steps are used in decryption, as in encryption, the order in which the steps are carried out is different.

6. CONCLUSION

Cloud Computing is still a new and evolving paradigm where computing is regarded as on-demand service. Once the organization takes the decision to move to the cloud, it loses control over the data. Thus, the amount of protection needed to secure data is directly proportional to the value of the data. Security of the Cloud relies on trusted computing and cryptography.

Thus, in our proposed work, only the authorized user can access the data. Even if some intruder (unauthorized user) gets the data accidentally or intentionally if he captures the data also, he can't decrypt it and get back the original data from it. Hence forth, data security is provided by implementing AES algorithm.

7. REFERENCES

[1] S. Kamara and K. Lauter, "Cryptographic cloud storage," *Financial Cryptography and Data Security*, 2010.

[2] M. Armbrust, A. Fox, R. Griffith, A. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, and I. Stoica, "A view of cloud computing," *Communications of the ACM*, 2010.

[3] A. Sahai and B. Waters, "Fuzzy identity-based encryption," *Advances inCryptology EUROCRYPT*, 2005.

[4] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in *Proc. Of ACM,2006.*