International Journal of Applied Information Systems (IJAIS) – ISSN : 2249-0868
Foundation of Computer Science FCS, New York, USA
Volume 4– No.11, December 2012 – www.ijais.org

Implementing Cloud Security by Encryption using Block Cipher Algorithms

Sonali Madireddi
San Jose State University
One Washington Square
San Jose, California

ABSTRACT
Revolutionizing Technology has drastically changed the direction of computing. Starting from the evolution of the Web in 1990's to the growth of the internet in 2000, cloud Technology has proven to be next technology milestone surpassed by the previous era of ingenuity. The Business's which were considered to be fixed on-premise infrastructure oriented services have converted to cloud shared business's where the Business's don't have to spend high capital resources for the infrastructure, since the hardware provided by the service provider is now shared by multiple organizations, thus reducing cost and improving usability and performance for both the cloud user and the provider. Cloud enables more time and resources to be spent on the idea construction and application development, rather than spending time on deciding the hardware and computer software stack needed for the application. This results in fast deployment and early feedback. One of the major issues in cloud computing is the security of data being stored on the provider's cloud and privacy while the data is being transmitted. This paper deals with the methods of providing security by data encryption. Various encryption methods of block cipher algorithms such as Rijndael, Blowfish and Triple DES are implemented for providing solutions to cloud security.

General Terms
Cloud Security, Encryption Algorithm for the Cloud

Keywords
Cloud Security, data encryption, Rijndael, Blowfish, Triple DES.

1. INTRODUCTION
Cloud computing provides the means of transferring services previously only available from an enterprise's hardware resources, into the cloud platform where these services are more easily accessible. It is extremely useful for small and medium enterprises to leverage the advantages provided by the cloud. Because of this technology, the smaller companies can utilize the same business intelligence capabilities of larger organizations. Furthermore, since the cloud gives the qualities of reuse and scalability, smaller companies with limited resources will not feel the pressure during peak periods and during periods of unexpected growth.

On the other hand, companies with ample infrastructure may still go through a bottleneck period when the hardware is not able to accommodate the pressures of higher unexpected loads.

In the light of all the advantages of migrating to the cloud, one of the primary disadvantages of the cloud platform is the security aspect. The security concerns fall into two main categories of cloud provider concerns and the client based concerns. The cloud provider should ensure that the architecture and the infrastructure are secure and that the data and applications of the client are not compromised. On the other hand, the client should make sure that the provider has taken all measures to secure their data in the cloud. [1]

This paper deals with the different data encryption algorithms that the provider can implement to ensure security for their clients data and applications. The encryption algorithms that this paper discusses are Rijndael, Blowfish and Triple DES. In the context of providing more secure channels to the client, this paper examines the encryption algorithms in detail.

2. CHARACTERISTICS OF CLOUD COMPUTING INFRASTRUCTURE
The important characteristics of the cloud environment are given as follows:

2.1 Elasticity:
Cloud architecture should be able to quickly increase or decrease the amount of computing resources that an application is provisioned. There should be an option of either, providing the maximum or the minimum number of virtual resources to the client. The actual number of resources utilized will depend upon the load of the application at any given time. One of the advantages of this feature is that as soon as a new virtual resource is needed, its allocation will take very minimal time and will in no way interrupt the client's operations.

2.2 On-Demand Self- Service

By having all infrastructure usage and access in the cloud, these services can be easily obtained by either self- or auto-provisioning. Obtaining new services is as simple as logging in with a customer account and requesting new resources.

2.3 Network Access
Cloud features should be able to be accessible from desktops, laptops, mobile phones and other wireless devices. In this

way, all heavy computational workloads of the application will be shifted to the cloud infrastructure and the client application will contain only the front–end interface with the user.

2.4 Resource Pooling

The cloud technology is multi-tenant, in that many clients can access the same infrastructure simultaneously without interference. Any and all infrastructure resources will be shared by multiple clients. The clients' data and application are stored in a separate address space where the data and instructions of one client do not get interchanged with another client.

2.5 "Pay as you go"

While using cloud resources, the client will only have to pay for the actual resources used by the application. In contrast, organizations which do not use cloud resources will need to estimate their application and business needs and purchase licenses and infrastructure in advance. This will likely result in both over-provisioning of resources during off-peak hours and possibly bottle neck the performance during peak hours.

3. DEPLOYMENT MODELS

3.1 Private Cloud

This consists of cloud infrastructure which is owned solely by the enterprise. Either the organization or a third party will run the private cloud, and it can be present on-site or present off-site.

3.2 Public Cloud

It consists of cloud infrastructure owned by the cloud provider and provides cloud services to the public for commercial services.

3.3 Community Cloud

It consists of cloud infrastructure that is owned by a community of multiple organizations that have a common purpose.

3.4 Hybrid Cloud

It consists of mixtures of different deployments, where there can be a combination of public and private.

4 SERVICES PROVIDED BY THE CLOUD

4.1 Infrastructure as a Service

This service provides to the user direct access to all software and hardware resources. Thus, the capacity to use the processing capabilities, compute, network, and storage systems of the infrastructure and run their respective operating systems and software on this virtual network. The user of this service uses the infrastructure allocated to him and connects to it by using remote login.This offers the cloud customer the most control over their application and environment.

4.2 Platform as a service

This service consists of a preconfigured operating system and other software libraries. The user will be able to deploy the applications on the platform of the provider. These applications will be produced using high-level programming languages and similar tools. The user will not be involved with the underlying infrastructure of the provider[2].

4.3 Software as a service

The use of this service is such that the user will be able to interact with the applications hosted by the provider on the cloud infrastructure. The user can neither change the underlying infrastructure nor applications offered by the provider except for some limited application configuration settings.[3]

5. DATA ENCRYPTION ALGORITHMS

5.1. Rijndael Encryption Algorithm

The Rijndael is a symmetric block cipher algorithm with key sizes ranging from 128, 192, and 256. A symmetric algorithm is one in which the cryptographic keys for encrypting plain text and decrypting cipher text are the same. There are two types of symmetric encryption algorithms: stream ciphers and block ciphers. Stream ciphers encrypt data each digits separately and individually whereas block cipher algorithms encrypt text in blocks an pad original plain text so that the size it matches the block size. It uses the encryption of 128 bit blocks. [4]

The working of the Rijndael Encryption Algorithm:

```
Step 1 :
Divide the plain text into blocks of 1
byte * 16 which will create a 4 cross
4 matrix which is known as the state
matrix.

State[Row,Column] =

byte[row+4,column

Step 2:
Rijndael_Algorithm(byte []
data,byte [] key)

end
add_key(state[],expanded_key[0]);

do(Nr-1)
    round(state,expanded_key[i]);
    last_round(state,expanded_key[Nr]);
    end

 Step 3:
 round(state,expa
 nded_key[i]) do

        Substi
        tute
        Bytes
```

```
        shift
        rows
        Mix Columns
        add_key(state[],exp
        anded_key[i]);

        end

last_round(state[],ex
panded_key[Nr]

        subst
        itute
        bytes
        shift
        rows
        add
        key(state[],expanded_key[i]);
        end

Step 4:
expand_key
procedure
        1.Expand the key from the cipher
        key
        2.Select a round key for each
        round

Step 5:
add_key
procedure
        1.Called at the beginning of the
        round
        2.Called Nr-1 times during the
        rounds
        3. Called during the last round
```

In the Rijndael Procedure, substitute bytes indicates that the algorithm should substitute the byte of the state[] with a byte from the S-box,which replaces each byte with the inverse transformation. The shift row procedure indicated that it does not change the value of the row elements but changes their order and does a circular left shift to the rows. Advantages of the Rijndael Algorithm are:

Security : Rijndael is one of the more secure algorithms. Due to the ease of access to various components of the code, the security breaches that may arise can be detected very easily and corrected efficiently

Memory: Rijndael does not require excessive memory to complete its functionality. The maximum bits used for encryption is 128 bits and this allows memory saving for both hardware and the software features.

Flexibility: Rijndael algorithm works for a combination of a large number of blocks and bits. This encryption algorithm is very versatile and customizable since it can be modified depending on the problem to which it is applied.[5]

5. DATA ENCRYPTION ALGORITHMS

5.1 Blowfish Encryption Algorithm

The blowfish encryption algorithm is a variable length block cipher algorithm. The key can extend between 32 bits to 448 bits, where the block size is 128 bits. Blowfish algorithm is one of the Feistel networks which transforms a function into a permutation and the this case it iterates through the function 16 times. The efficiency of this algorithm is very high since it works effectively on 32 bit microprocessors.

5.2 The working of the Blowfish algorithm:

```
Step 1:
Sub key computation. Each sub key is
represented as P1, P2,,,Pi

Step 2:
Divide the
input into
two 32-bit
halves, L &R

       Then for i=1 to 16
              L=L
              XOR Pi
              R=F(L)
              XOR R
              Swap L
              & R
       end
              swap L & R to undo last swap
              R=R XOR P17 and L=L
              XOR P18 combine both L
              & R to get cipher text
Step 3 :
Decrypti
on
Similar to encryption but the order of
sub keys(P1,P2...Pi) will be reversed to
(Pi....P2,P1)[6]
```

5.3 3DES Encryption Algorithm:

3DES is an extension of the DES algorithm. It consists of 64 bit keys, which can be extended up to 192 bit keys. 3DES is more secure than DES and it is 3 times slower than the regular DES. Because of the reliability and a longer key length, it eliminates the the shortcomings of DES.

```
Step 1 : The input is the plain text and
the key is broken down into 3 sub keys

Step 2: The data is encrypted with the
user input key, which is encrypted. This
becomes key 1.This procedure is
repeated 3 time, thus the name 3DES.

Step 3 : The data is decrypted with the
second key-dependent

Step 4 : The data is encrypted again with
the third key.[7]
```

6. CONCLUSION

Most organizations are transitioning to cloud platforms since it provides a comparative advantage in operational costs. The

requisite hardware is offered as virtual resources and allocated on-demand to cloud-powered businesses. These businesses deploy their data and services to the cloud platform, and are provisioned application resources depending on their needs. This ensures the optimum usage and efficiency of resources since many organizations use the same servers, network and computational processing. Security is a major concern for any business looking to take advantage of the benefits offered by cloud providers. Block cipher encryption algorithms such as Rijndael, Blowfish and Triple DES can provide these security features. This paper also discusses the characteristics of the cloud, the different deployment models and the service models on cloud platforms.

7. REFERENCES

[1] Pritesh Jain Dheeraj Rane Shyam Patidar,' *A Survey and Analysis of Cloud Model-Based Security for Computing'*, World Congress on Information and Communication Technologies, 2011

[2] Gurudatt Kulkarni & Jayant Gambhir Tejswini Patil Amruta Dongare,' *A Security Aspects in Cloud Computing',* Institute of Electrical and Electronic Engineers(IEEE),IEEE 3rd International Conference on software engineering and service science 2012

[3] Shubhashis Sengupta, Vikrant Kaulgud, Vibhu Saujanya Sharma , *Cloud Computing Security - Trends and Research Directions* ,IEEE computer Society, world Congress on services, 2011

[4] Jamil Tariq,'*The Rijndael Algorithm*',Potentials IEEE,Volume 23,Issue 2

[5] C. Sanchez-Avilaf & R. Sanchez-Reillot,'*The Rijndael Block Cipher (AES Proposal): A Comparison with DES* ', security conference, 35 th International Carnahan Conference, 2001

[6] Tingyuan Nie,Chuanwang Song, Xulong Zhi,*Performance Evaluation of DES and Blowfish Algorithms',* Biomedical Engineering & computer science, 2010 International Conference.