Implementation of Data Security in Cloud Computing

G. Jai Arul Jose[1], C. Sajeev[2], Dr. C. Suyambulingom[3]
[1,2] *Research Scholar, Sathyabama University, Chennai, INDIA*
[1]*aruljose@yahoo.com*
[2]*painkulamcsajeev@yahoo.co.in*
[3]*Professor (Rtd.), Tamil Nadu Agricultural University, Coimbatore, INDIA*

***Abstract* —** Cloud computing provides people the way to share distributed resources and services that belong to different organizations or sites. Since cloud computing share distributed resources via the network in the open environment, thus it makes security problems important for us to develop the cloud computing application. On one hand, an individual has full control on data and processes in his/her computer. On the other hand, we have the cloud computing wherein, the service and data maintenance is provided by some vendor which leaves the client/customer unaware of where the processes are running or where the data is stored. So the client has no control over it. The cloud computing uses the internet as the communication media. The vendor has to provide some assurance for security of data in the cloud computing. Organizations use cloud computing as a service infrastructure, critically like to examine the security and confidentiality issues for their business critical insensitive applications. Yet, guaranteeing the security of corporate data in the "cloud" is difficult, if not impossible, as they provide different services like Software as a service (SaaS), Platform as a service (PaaS), and Infrastructure as a service (IaaS). Each service has their own security issues. Data Protection Application Security Privacy is important security issues that have to be included in cloud computing. We propose a model system in which cloud computing system is combined with Cluster Load balancing, ssl over aes and secure session In this model, some important security services, including authentication, confidentiality and integrity, are provided in cloud computing system.

***Keywords*—** Cryptography, Cloud Computing, Public Key, AES

I. INTRODUCTION

In cloud computing the data and applications exist on a "cloud" of Web servers. When talking about a cloud computing system, it's helpful to divide it into two sections: the front end and the back end. The front end is the side the computer user, or client, sees. The back end of the system is the various computers, servers and data storage systems that create the "cloud" of computing services. They connect to each other through a network, usually the internet. All cloud computing systems don't have the same user interface. All servers are run with its own independent operating system. In theory; a cloud computing system could include practically any computer program, from data processing to E mail. Usually, each application will have its own server. A central server administers the system, monitoring traffic and client demands to ensure everything runs smoothly. It follows a set of rules called protocols and uses a special kind of software called middleware. Middleware allows networked computers to communicate with each other. With the right middleware, a cloud computing system could execute all the programs a normal computer could run. A cloud computing system must make a copy of all its clients' information and store it on other devices. These copies are enabling to the central server to access backup machines to retrieve data. The applications of cloud computing are practically limitless. Clients would be able to access their applications and data from anywhere at any time. The client access the cloud computing system using any computer linked to the Internet. Data wouldn't be confined to a hard drive on one user's computer or even a corporation's internal network. Cloud computing systems would reduce the need for advanced hardware on the client side. No need to buy the fastest computer with the most memory, because the cloud system would take care of those needs for you. There are a few standard hacker tricks that could cause cloud computing failure. One of those is called key logging. A key logging program records keystrokes. If a hacker manages successfully to load a key logging program on a victim's computer, he or she can study the keystrokes to discover user names and passwords. The biggest concerns about cloud computing are security and privacy. If a client can log in from any location to access data and applications, it's possible the client's privacy could be compromised. Cloud computing will need to find ways to protect client privacy. One way is to use authentication techniques such as user names and passwords. Another is to employ an authorization format -- each user can access only the data and applications relevant to his or her job. Cloud has centralized server administration system Centralized server administers the system, balances client supply, adjusts demands, monitors traffic Here, all the data are backed up at multiple locations. In cloud computing, it is very common to store data of multiple customers at one common location. Cloud

computing should have provide proper techniques for data security and confidentiality. Cloud computing is cost-effective. Here cost is greatly reduced, Maintenance cost is reduced. The data is secured through SSL; AES based Cryptography, Server clustering and Server Load balancing.

II. Problem Related to Attacks

A. Problem Related to passive Attacks

In passive attacks in cloud , the attacker only watches the transmission of cloud data's and does not try to modify data packets or don't do anything that user may realize that someone's watching him. Further it is divided into two types.

B. Release of Message Contents

In release of cloud message contents, the attacker only looks the messages and reads them in an unauthorized way.

C. Traffic Analysis

In traffic analysis, the attacker mask (does not change) the message in such a way that the authorized user either cannot access it or cannot understand the message properly.

D. Problem Related to Active Attacks

This attack involves reading of data messages along the messages and read them in an unauthorized way. In this case, sometimes, the attacker creates his new message and sends it to the destination instead of the original. In such an attack, the actual path of the data changes and the message is sent from user C while it appears to be coming from user A to user B. Sometimes unauthorized user may appear to be an authorized one to the other users as shown below:In such case, attacker manipulates everything according to his wish. In former case, the message is modified by the attacker. So such an active attack is called modification of messages. In the latter one the message appears to be coming from an authorized user while it is not so; this attacker is called Masquerade.

E. Problem Related to Session level DOS

When a client is successfully authenticated by a service and a secure session is established with the service, the service keeps track of the session until the client cancels it or the session expires. Every established session counts against the limit for the maximum number of active simultaneous sessions with a service. When this limit is reached, clients that attempt to create a new session with that service are rejected until one or more active sessions expire or are canceled by a client. A client can have multiple sessions with a service, and each one of those sessions' counts toward the limit.

F. Problem Related to Port level DOS

The sudden increase in traffic can cause the site to load very slowly for legitimate users. Sometimes the traffic is enough to shut the site down completely. We call this kind of an attack a Distributed Denial of Service (DDoS) attack. Here the hacking program blocks the port that the server sends message.

G. Problem Related to packet level DOS

A packet denial-of-service attack (DoS attack) or distributed denial-of-service attack (DDoS attack) is an attempt to make a computer resource unavailable to its intended users. Although the means to carry out, motives for, and targets of a DoS attack may vary, it generally consists of the concerted, malevolent efforts of a person or persons to prevent an Internet site or service from functioning efficiently or at all, temporarily or indefinitely. Perpetrators of DoS attacks typically target sites or services hosted on high-profile web servers such as banks, credit card payment gateways, and even root name servers. One common method of attack involves saturating the target (victim) machine with external communications requests, such that it cannot respond to legitimate traffic, or responds so slowly as to be rendered effectively unavailable. In general terms, DoS attacks are implemented by either forcing the targeted computer(s) to reset, or consuming its resources so that it can no longer provide its intended service or obstructing the communication media between the intended users and the victim so that they can no longer communicate adequately.

H. Problem Related to Dictionary Attacks

In cryptanalysis and computer security, a dictionary attack is a technique for defeating a cipher or authentication mechanism by trying to determine its decryption key or passphrase by searching likely possibilities' dictionary attack uses a brute-force technique of successively trying all the words in an exhaustive list called a dictionary (from a pre-arranged list of values). In contrast with a normal brute force attack, where a large proportion key space is searched systematically, a dictionary attack tries only those possibilities which are most likely to succeed, typically derived from a list of words for example a dictionary (hence the phase dictionary attack) or a bible etc. Generally, dictionary attacks succeed because many people have a tendency to choose passwords which are short (7 characters or fewer), single words found in dictionaries or simple, easily-predicted variations on words, such as appending a digit

I. Problem Related to "Man in the Middle Attack" and Eavesdropping

In the man-in-the-middle attack (often abbreviated MITM), or bucket-brigade attack, or sometimes Janus attack, is a form of active eavesdropping in which the attacker makes independent connections with the victims and relays messages between them, making them believe that they are talking directly to each other over a private connection, when in fact the entire conversation is controlled by the attacker.

The attacker must be able to intercept all messages going between the two victims and inject new ones, which is straightforward in many circumstances.

J. Problem related to Smurf Attack and Viruses

In this attack, the perpetrator sends an IP ping (or "echo my message back to me") request to a receiving site The ping packet specifies that it be broadcast to a number of hosts within the receiving site's local network. The packet also indicates that the request is from another site, the target site that is to receive the denial of service. (Sending a packet with someone else's return address in it is called spoofing the return address.) The result will be lots of ping replies flooding back to the innocent, spoofed host. If the flood is great enough, the spoofed host will no longer be able to receive or distinguish real traffic.

III. Architectural Design

Figure 1 Architectural Diagram

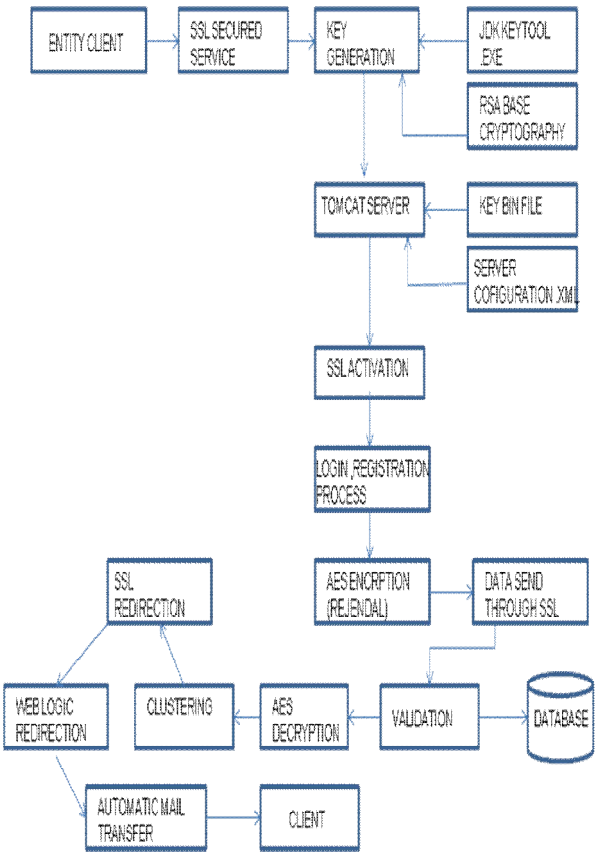


Figure 2 Context Level Diagram

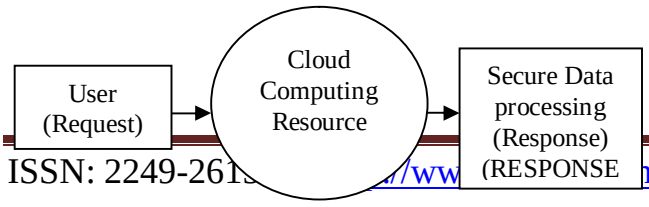


Figure 3 Key tool Generation

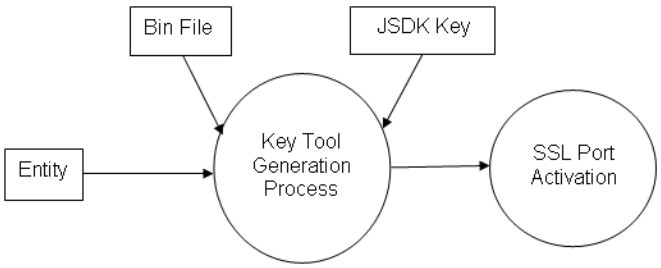


Figure 4 Data Security Process

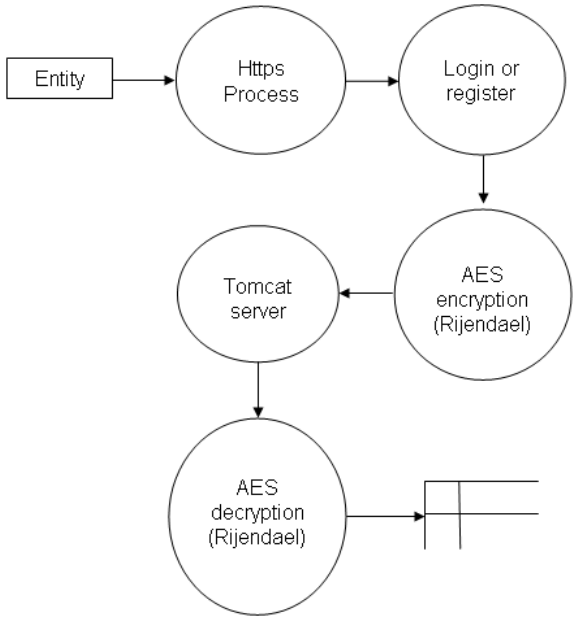
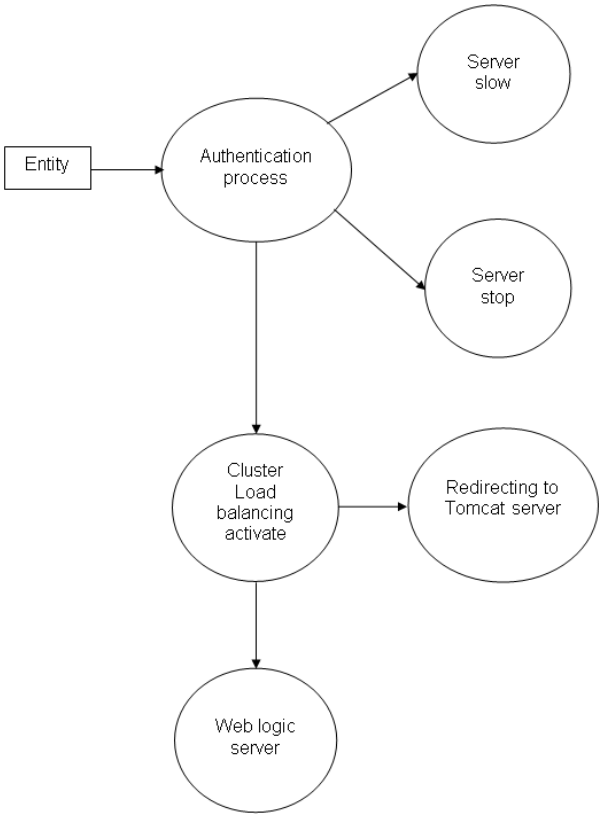


Figure 5 Authentication Process



IV. IMPLEMENTATION

A. Integration of cloud computing entities

a) Presentation Layer (ClientTier)
- Control Node (Tomcat server)

b) Business Layer (Middle Tier)
- Application Server (WebLogic Server)

c) EIS Layer (backend tier)
- Remote DataBase server (MYSQL Server)

In the presentation Layer the presentation layer components are integrated with other layers by changing control Server web.xml file .In the Web.Xml file the init parameter component has been changed according application server and remote database server locations. Secure grant permission has been given to database server for making SQL queries constraints.

B. Secure Socket Layer Implementation

Key Tool Generation Algorithm: The key store file is the one which would store the details of the certificates necessary to make the protocol secured. Certificates contain the information as to who is the source from which you are receiving the application data and to authenticate whether it is the intended party or not.

Start KeytoolGeneration
Run Keytool.exe
Set genKey parameter.
Set keypass
Set keystore
Call Enter
Do Create Certificate.bin
END DO
END

PKC base key certificate generation(RSA Algorithm): In RSA Public keys and Private Keys are generated for public and private access. Consider two large prime numbers for generating keys.Find multiplication of prime numbers that denotes n and find m that is multiplication of p-1 and q-1.Find co prime to m .Find d that denotes de%m=1.Here n and d denoting public key and private key. Then using encryption formula for finding encryption and using decryption for finding ciphertext.This encrypted and decrypted text is used for creating Certificate.

Implementation of certificate (BIN file): Implement Certificate Binary file inside control node configuration file and making cloud data flow secure. The control node sends data through SecureSocketLayer after certificate activation.

V. AES RIJENDAEL ALGORITHM IMPLEMENTATION FOR SECURED USER DATA

A. Encryption & Decryption

Encryption:

```
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);
}
```

The User Details are encrypted by using Rijendeal Encryption. Symmetric key is used for encryption. The Rijendeal can be implemented easily and it is one of the most secure algorithms in the world. Rijendeal implementation has 128,192or 256 bit key lengths. Size of data blocks to be encrypted with Rijendeal is always 128 bits. Initial round of Rijendeal is AddRoundKey, this is followed by four iterative round including subBytes, shiftRows, mixColumns and add round key. Rijendeal with 128 bit key length has 10 rounds,192-bit has 12 rounds and 256 bit has 14 rounds. The AES algorithm is a symmetric block cipher that can encrypt (encipher) and decrypt (decipher) information. Encryption converts data to an unintelligible form called cipher text; decrypting the cipher text converts the data back into its original form, called plain text. Each round consists of the following steps.

1. Initial AddRoundKey
2. SubBytes () Transformation
3. Substitutional Box Created For Subbytes
4. MixColumns () Transformation
5. AddRoundKey () transformation

The Inverse process of Encryption gives Decryption text.

VI. Clustering, Load balancing and Redirection for DOS and Dictionary attacks

If a user is attempt to login falsely for many times, our system automatically slowing the service and temporarily stop the account service for the particular user. Our program activates dictionary attack denial components for stopping. Suppose if number of session objects is created inside server regardless of user, dos components activated for secure dataflow.

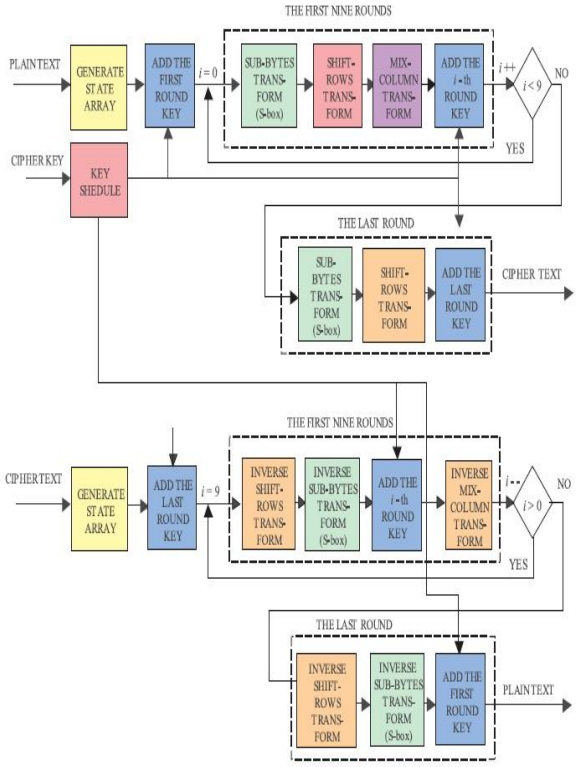
VII. Multi Tier Based Secure Application services implementation (Mail service) using EJB components

In Multitier Secure Application web components are created and deployed in web container and secure mail application are deployed inside ejb container.Session beans are created for calling business logic.Database records are accessed in secure manner by using session and entity beans.

VIII. Algorithm

A. Rijendeal Algorithm: Encryption/Decryption Process

Figure 6 Rijendeal Algorithm: Encryption/Decryption Process



IX. Conclusion

In this work Cloud Computing Resources are integrated in a flexible manner. Layers are separated according to Security Rules. Active Attacks obtained in cloud computing resources are deeply scrutinized. Dictionary attacks are effectively analyzed and denied by making Server Redirection using server's clustering load balancing technique. Denial of Service attacks are deeply analyzed in port, session and service levels by making either server service is temporarily stopped or making service slow.

References

[1] S. Singh, "Different Cloud Computing Standards a Huge Challenge", The Economic times, 4 June 2009.
[2] J. Urquhart, "The Biggest Cloud computing Issue of 2009is Trust", C-Net News, 7 Jan 2009.
[3] Wangetai, "Scientific Cloud Computing: Early Definition and Experience", Proc. 10th International Conference High-Performance Computing and Communications (HPCC 03)
[4] William Stallings, "Cryptography and Network Security Principles and Practices", Prentice Hall, New Delhi.
[5] National Institute of Standards and Technology. "Request for Candidate Algorithm Nominations for the Advanced Encryption Standard." Federal Register, September 12, 1997.
[6] Nechvatal, J., et al. Report on the Development of the Advanced Encryption Standard. National Institute of Standards and Technology. October 2, 2000.
[7] Needham, R., and Schroeder, M. "Using Encryption for Authentication in Large Networks of Computers." Communications of the ACM, December 1978.
[8] Daemen, J., and Rijmen, V. "Rijndael: The Advanced Encryption Standard." Dr. Dobb's Journal, March 2001.
[9] Daemen, J., and Rijmen, V. The Design of Rijndael: The Wide Trail Strategy Explained. New York, Springer-Verlag, 2002.