A Study of SAAS Model for Security System

Sabapathi.V[1] M. Muniyappan[2]
[1,2]Assistant Professor
[1,2]Vel Tech High Tech Dr.Rangarajan and Dr.Sakunthala Engineering College, Chennai

Abstract— A study of SAAS of cloud computing securing methodology against Poodle Attack" are taken for discussion. Cloud –It's a resource centric technology. So secure it's a main concern like POODLE (Padding Oracle on Downgraded Legacy Encryption) attack will affect SSL based connection system between client and server which is a serious cost. POODLE will disconnect the SSL connections. In Cloud it's a open connectivity, over the network we can access the resources for user requirement. Connection Setup, recently everywhere used SSL. So far, Strong Authentication in connection setup, Server side authentication should be in Cloud. For sever side Keystone which is in OPENSTACK, for sever side authentication. So in this paper for mainly for SAAS (Secure As A Service) model for Cloud Environment.

Key words: POODLE, SAAS Model, SSL

I. INTRODUCTION

Cloud it's a resource centric technology, so that we can access the resources over the internet.

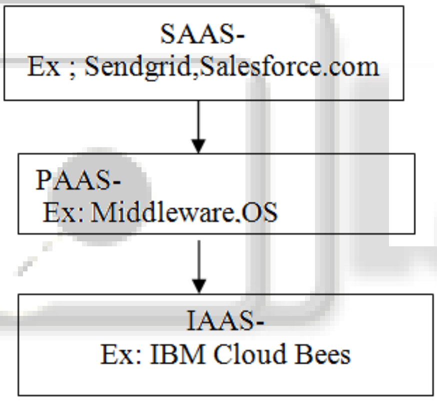

Fig. 1: Basic Cloud Services

If the resource that may be the application, software, storage as the services like PAAS(Platform As A Service) SAAS(Software As A Service),IAAS(Infrastructure As A Service) respective service.

SAAS-functional specific subscription based application on demand .Ex: Send grid, PAAS-Development Platforms. Ex: Middleware, OS.IAAS-using for compute, storage Ex: Amazon EC2, Racks Space. These are basic services from the cloud service provider.

In this paper POODLE (This vulnerability discovered by Google Team at September 2014) will crack secure connection setup[1] . So against POODLE VULNERABLE and keystone Authentication at server side and Elliptic Curve Cryptography for key generating, Diffie Hellman Key exchange protocol was used for Secure key exchange. But actually cloud computing is basic concept of separating everything.

Security it's the most important thing for Cloud development and using the cloud in real time and long-term usage. Once the technology wants to be developing that should be user friendly and confidential with more secure.

II. RELATED WORK

In 2010, Joshi et al. [3] provide an overview of different data security issues related to cloud computing. This piece of work focuses on ensuring security in cloud computing by providing secured trustworthy cloud environment. FarzadSabahi [4] explains about the scope of various enterprises migrating to cloud. The author explains how migration to cloud can benefit various enterprises. Cloud computing migration involves considering the gravity of issue of security. In 2011, Ashish Agarwal et al. [5] talk about security issues concerned with cloud computing. This paper has talked about some serious security threats that prevails this field. Ashutosh Kumar et al. [6] focused on providing a secure architectural framework for sharing and data gathering. This cynosure of this work is that the authors have made a permission hierarchy at different levels.

1) Compute (Nova)
2) Object Storage (Swift)
3) Block Storage (Cinder)
4) Networking (Neutron)
5) Identity Service (Keystone)
6) Image Service (Glance)
7) Orchestration (Heat)
8) Database (Trove)

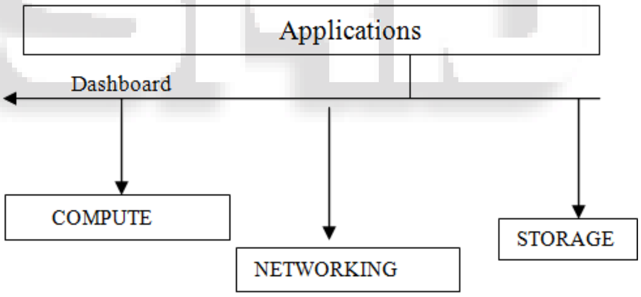

Fig. 2: Openstack –Cloud Management

The authors have focused on security but with view of use hierarchy. In 2012, M.Venkatesh el al [7]proposes RSASS system for data security. In this project we need to deploy the private cloud .So we decide Open stack for private cloud deployment. Because Open Stack it's a Cloud OS that can manage and control large pools of compute, storage and

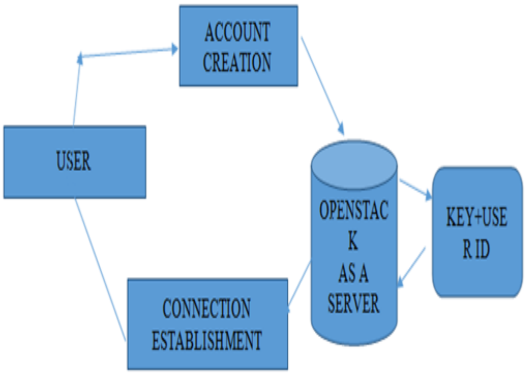

Fig. 3: Secure Service Model-Private Cloud

network resources throughout a datacenter, all managed by dashboard, it's a GUI[2],which is shown in Figure [2].

III. SYSTEM AND MODELS

Our system model involves cloud service provider which includes cloud system administrators, tenant administrators n (or operators) who manage the tenant virtual machines, and tenant users (or tenant's customers) who use the applications and services running in the tenant virtual machines. Cloud providers are entities such as Amazon EC2 and Microsoft Azure who have a vested interest in protecting their reputations. The cloud system administrators are individuals from these corporations entrusted with system tasks and maintaining cloud infrastructures, who will have access to privileged domains. We assume that as cloud providers have a vested interest in protecting their reputations and resources, the adversaries from

IV. METHODOLOGIES

In this paper mainly concentrate on multi security way over the network. So that

1) Connection setup using HTTPS/TLS against POODLE Vulnerability.
2) Account Creation form –Collecting Peculiar details from individual user for if he forgotten password or hacker try for hacking password so can make login details little bit tougher.
3) In server side authentication Keystone authentication tool.
4) Server backend Elliptic curve cryptography based key generation for speedy computation's) Diffie Hellman key exchange protocol for secure connection establishment to the user OPENSTACK Components were install for Cloud Platform.

Hence Keystone (Authentication) Service is used for authentication will help to more secure connectivity

V. MODULES

In this paper we define five modules, are following

A. Login Module

User wants to login he should be register with every detail, in that register form he should fill up his ID proof and he have to fill some of his USER'S PSYCHE IDENTITY personal interest and USER'S PHYSICAL IDENTITY identity of his appearance (Like MOLE on his body), they have enter. If some Id will loss hacker may try, but these may little bit stronger login we can make secure.

B. Connection Setup

HTTPS/SSLV3 for initially used in cloud setup for connection establishment.
Hence SSL 3.0 will disable by the POODLE Hacker,

C. HTTPS-TLS

Hence connection establish via HTTPS/TLS SETUP prevent from POODLE Attack So, this connection establishment become more important while using internet in the Cloud.

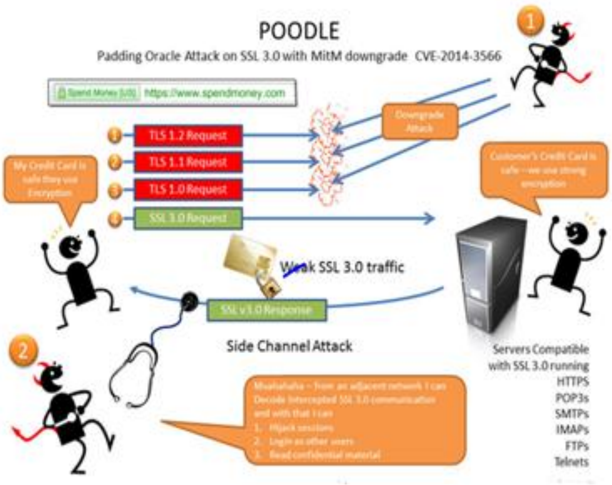
POODLE
Padding Oracle Attack on SSL 3.0 with MitM downgrade CVE-2014-3566
1
Spend Money [US] https://www.spendmoney.com
Downgrade Attack
1 TLS 1.2 Request
2 TLS 1.1 Request
3 TLS 1.0 Request
4 SSL 3.0 Request
My Credit Card is safe they use Encryption
Customer's Credit Card is safe – we use strong encryption
Weak SSL 3.0 traffic
SSL v3.0 Response
Side Channel Attack
2
Mwahahaha – from an adjacent network I can Decode Intercepted SSL 3.0 communication and with that I can
1. Hijack sessions
2. Login as other users
3. Read confidential material
Servers Compatible with SSL 3.0 running
HTTPS
POP3s
SMTPs
IMAPs
FTPs
Telnets

Fig. 4: Poodle Attacker

D. Server Authentication

In this project we deploy Open Stack act as local server .Open Stack is a collection of software that can manage the cloud environment [2].

E. Unique ID Generating

Using Elliptic Curve Cryptography, we can generate the around 160 bits providing same security level as 1024 bits. So that Computation speed is high. Less Memory, long term battery life. So ECC will generate key efficiently

F. Key Exchange

Diffie Hellman (DH) fey exchange algorithm were used for key exchange protocol. It's a Public key cryptography .It uses two keys, for sending message to server using with his private key and send with his public key. Receiver side using his private key for decrypt and response using his public key. DH for Handshaking, connection establishes supports.

VI. CONCLUSION

In this paper, we propose as SAAS (Secure as a Service) model using TLS 1.2 channel for connection establishment. Registration Login form ,we make as much as unique details from the user because if user forget the password or Loss his ID proof hacker may attack .In server side we provide keystone authentication technology and ECC algorithm for small and speedy unique ID and key is generating. DH for secure handshaking key transfer between user and server. The paper described the design of the security architecture and discussed how different types of attacks are counteracted by the proposed architecture.

REFERENCES

[1] http://en.wikipedia.org/wiki/POODLE
[2] https://www.openstack.org/software/
[3] Joshi, J.B.D., Gail-Joon Ahn. Security and Privacy Challenges in Cloud Computing Environments. IEEE Security Privacy Magazine, Vol 8, IEEE Computer Society, 2010, p.24-31.
[4] Farzad Sabahi. Cloud Computing Security Threats and Responses. Communication Software and Networks (ICCSN), 2011 IEEE 3rd International Conference.

[5] 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].

[6] 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

[7] 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.