Framework Design of Secure Cloud Transmission Protocol

Dinesha H A[1] Prof.V.K Agrawal[2]

[1] **Assistant Professor, Dept of ISE and CORI, PES Institute of Technology, 100 Feet Ring Road, Banashankari 3rd Stage, Bangalore-560085, India**

[2]**Professor ISE, Director CORI, PES Institute of Technology, 100 Feet Ring Road, Banashankari 3rd Stage, Bangalore-560085, India**

Abstract

Cloud computing technologies are in high demand because of several benefits. Many business organizations are looking into cloud computing services to reduce the cost and complexity of their business infrastructure and its preservation. However, there are certain security issues in cloud computing technologies. To overcome those security issues, we propose secure cloud transmission protocol design. This framework design details will help us in developing a secure protocol for the customers who are using cloud computing technologies over insecure internet. In this paper we discuss: i) Overview model of proposed secure cloud transmission system in internet ii) Security requirements iii) roles and responsibilities of secure transmission protocol in OSI and iv) Framework Design of secure cloud transmission.

Keywords**:** *Cloud Computing, Protocol, Security, Secure cloud transmission protocol.*

I. Introduction

SINCE entering into 21st century, there has been a rapid boom of computer network development, Information technology is now more and more blended into our daily life at the coming of electronic era. The concept of cloud computing was jointly proposed by Google and IBM in 2007 [1]. Today due to the advancement of technologies and high-speed internet facilities, it is possible to realize cloud computing. Many organizations around the world are providing cloud services. Cloud computing is an internet- based model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) [2]. In internet, cloud computing technology provides four major services such as: i) Software as a Service ii) Data Storage as a Service iii) Platform as a Service and iv) Infrastructure as a Service [3], as shown in Fig. 1. Cloud service activities are upgraded or improved by the cloud service provider based on the customer needs. Our objective is to ensure security while customers are using cloud service over insecure internet.

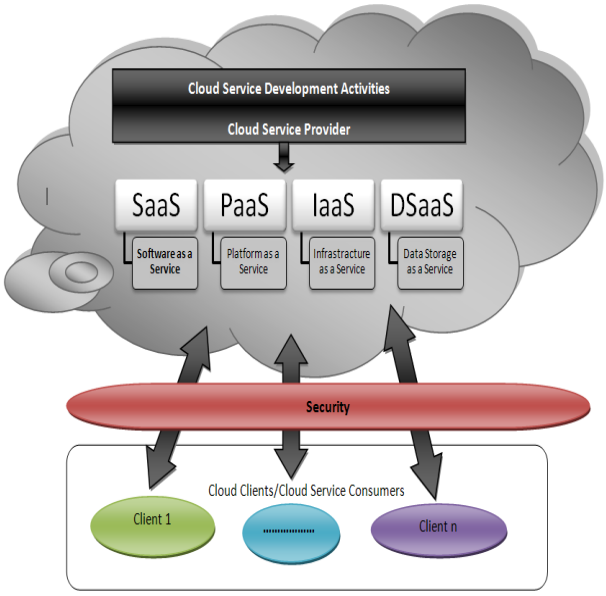

Fig. 1: Four major category services of cloud computing.

In internet services confidentiality, integrity and availability are the key challenges. The way to access any services over internet is through web browser. Web browsers typically use HTTP's protocols such as HTTP, HTTPS and S-HTTP. HTTP helps to communicate with web servers. In general, in HTTP, sending and receiving information between web server and web browser happens without encrypting messages [4]. However for sensitive transactions, such as Internet e-commerce or online access to financial accounts, the browser and server encrypt this information, referred as HTTPS [5]. HTTPS has been designed to withstand data hacking and provides data confidentiality [5]. HTTPS also facing some of the challenges such as : i) Complex encryption method[5] ii) Browser incompatibility in decrypting messages [5] iii) User needs to wait for long time to get session ends [5] iv) Man-in-the-middle attack [7] v) Eaves dropper attack [4]. Out of these drawbacks, only complex encryption has been addressed in Secured HTTP (SHTTP) [6]. Hence to overcome the rest of the security drawbacks and to establish secure channel, it is necessary to investigate a protocol which sits on top of HTTP and provide secured channel over an insecure

internet for cloud transmission, known as secure cloud transmission protocol.

The paper is organized in the following manner: In section II, we brief about the cloud computing background, cloud services and its deployment types. In section III, we present the identified security issues, both in http protocols and cloud computing services. It also presents the requirements, roles in OSI architecture and framework of secure transmission protocol. Section IV concludes this paper along with the future work.

2. Cloud Computing

Cloud computing provides computation, software, data access, and storage services that do not require end-user knowledge of the physical location and configuration of the system that delivers the services [4]. Cloud computing services benefits in i) Reducing hardware installation & maintenance cost ii) Reducing infrastructure maintenance cost iii) E-waste minimization iv) On demand, anywhere, from any device services v) Efficient usage of electrical power vi) Flexibility and highly automated v) Virtual Business setup vi) Easier to replace and upgrade vii) Easier Maintenance and Management. Cloud computing helps customers by having its own intelligent features like i) Portability ii) Encrypted data storage iii) Fault Tolerance & Disaster Recovery iv) Elasticity vi) High Availability vii) Intelligent Management viii) Performance ix) On demand self services x) Service measurement xi) Resource pooling. In the following discussion, we briefly describe various services offered by cloud computing and deployment types of cloud services.

Cloud computing Services:

Cloud computing providers deliver applications via the internet, which are accessed from web browsers, desktop and mobile apps, while the business software and data are stored on servers at a remote location. As shown in fig. 2 Cloud Computing Technologies are grouped into 4 sections, they are SaaS, DSaaS, IaaS and PaaS[8] [3].

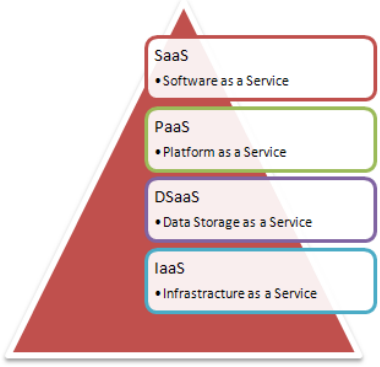

Fig. 2: cloud computing services

SaaS (Software as a Service) is on demand application service. It delivers software as a service over the Internet, eliminating the need to install and run the application on the customer's own computers [8] [3]. Fig. 3 shows that without installing, client can access the required application from cloud SaaS service provider over internet.

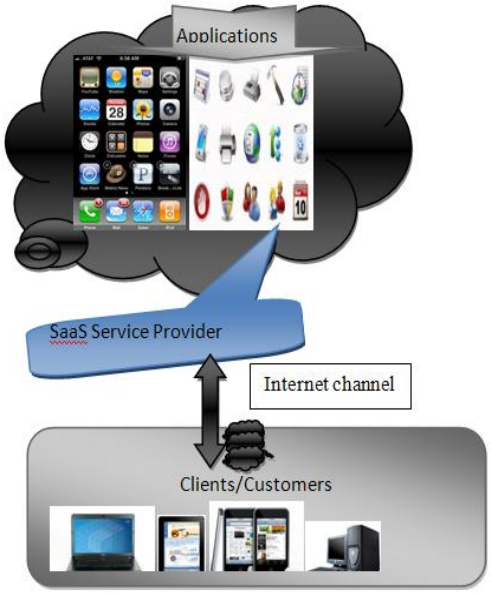

Fig. 3: Overview Model of Software as a Service

PaaS (Platform as a Service) is on demand platform service to host customer application. PaaS is delivery of computing platforms and/or solution stack as a service, often consuming cloud infrastructure and sustaining cloud applications. It facilitates deployment of applications without the cost and complexity of buying and managing the underlying hardware and software layers [8] [3]. Fig. 4 shows that the customer can access the required platforms remotely from PaaS service providers. It improves the flexibility in having multiple platforms in business environment.

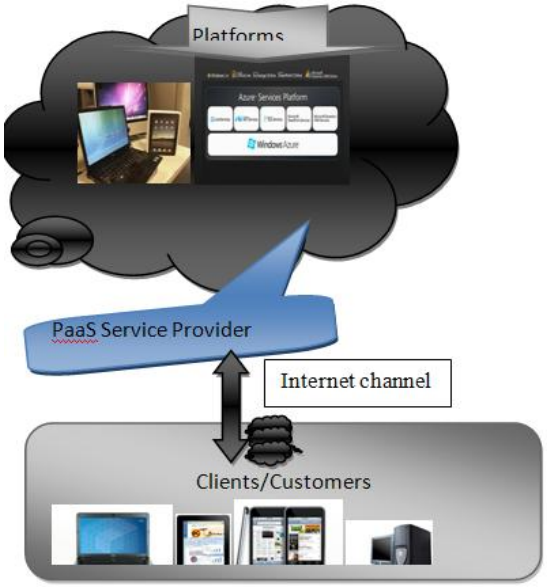

Fig. 4: Overview Model of Platform as a Service

DSaaS (Data Storage as Services) is on demand storage service. Cloud computing provides internet- based on demand back up storage services to customer [8] [3]. Fig. 5 shows the on demand accession of DsaaS services. In this service, customers can keep their data backup remotely over internet servers. These backup data maintenance is taken care by DsaaS service Provider. Cloud DsaaS service providers are responsible for customer data to keep confidentially. Here customers need not worry on setting up the large discs array to keep their huge amount of data.

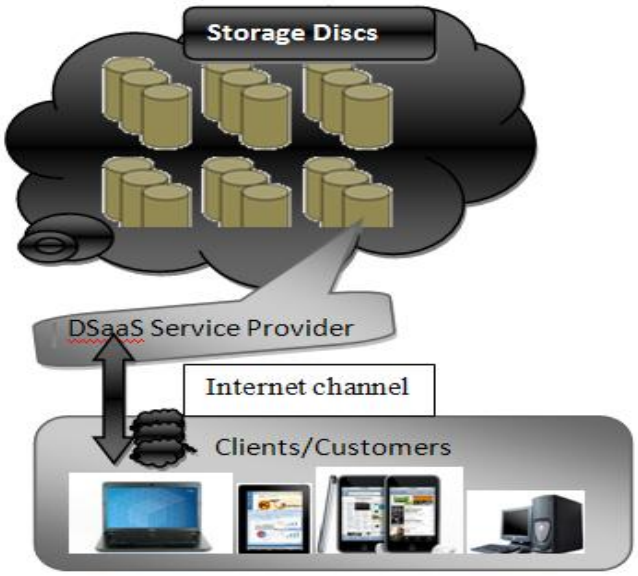

Fig. 5: Overview Model of Data Storage as a Service

IaaS (Infrastructure as a Service) is on demand infrastructure service. It delivers the computer infrastructure – typically a platform virtualization environment – as a service, along with raw (block) storage and networking. Rather than purchasing servers, software, data-center space or network equipment, clients can buy those resources as a fully outsourced service [8] [3]. Fig. 6 shows that customers can access infrastructure from IaaS service provider over internet.

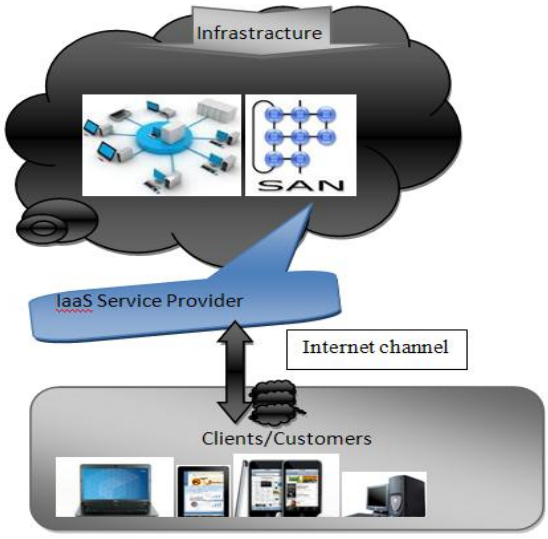

Fig. 6: Overview Model of Infrastructure as a Service

Deployment Types

Any organization can setup/use the cloud for its business maintenance purpose. There are four types of deployment that a customer can establish such as: Private, Public, Community and Hybrid [8].

Private cloud is a cloud service created with own/ rented resources. As shown in Fig. 7 the cloud infrastructure is owned or leased by a single organization and is operated solely for that organization

Fig. 7: private cloud

Community cloud: The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, and compliance considerations).Fig 8 shows the community cloud created with similar group of customers with same set of resource requirements.

Public cloud: The cloud infrastructure is owned by an organization selling cloud services to the general public or to a large industry group. Fig. 9 shows the cloud infrastructure created with standard specification to any organization.

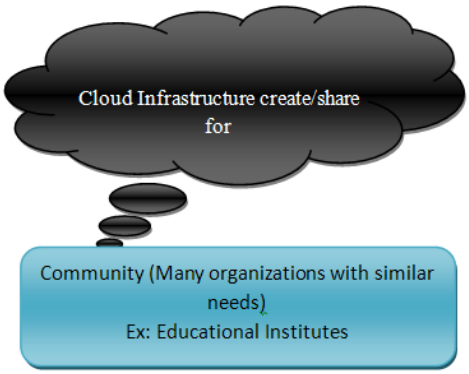

Fig. 8: Community cloud

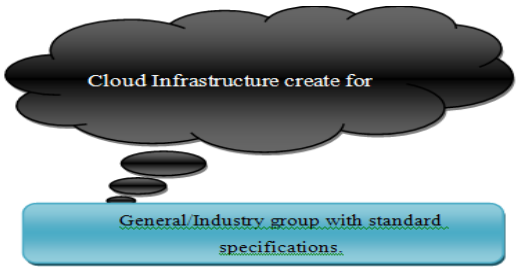

Fig. 9: Public cloud

Hybrid cloud: The cloud infrastructure is a composition of two or more clouds (internal, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability. Fig 10 shows the hybrid cloud infrastructure created with any combination of public, private and community.

Fig. 10: Hybrid cloud

3. Secure Cloud Transmission Protocol (SCTP) Design

In internet, services are accessed through web browser using http's protocols such as HTTP, HTTPS & S-HTTP. However these protocols have some security issues which are discussed in [4] [5] [6]. HTTP is an application layer protocol which helps in sending and receiving the information. HTTP is not suitable for sensitive information transaction because it is not a secure protocol [4]. HTTPS is another protocol designed to provide security. This protocol works in presentation layer in encrypting the sensitive transaction. HTTPS is not effective because, along with message body it also encrypts the message header [5]. S-HTTP is designed in such a way that it encrypts only a message body [6]. These protocols do not help the security challenges such as man- in- middle attack, data integrity, strict authentication and authorized techniques and intruder detection [4][5][6]. Tables 1 discuss the security issues of HTTPs protocols. Based on the information given in Table 1, we suggest the security requirements such as secure channel, strict authentication and efficient cryptographic techniques.

Protocol Name	Description	Security Issues
HTTP	Application layer Request-response protocol with no security.	Data confidentiality, Integrity, Man-in-the-middle, Eavesdropping attacks.
HTTPS	I t is a Combination of HTTP and SSL/TLS. Performs the encryption to entire messages at Presentation layer. Provides authenticated public key certificate for web server	Man-in-the-middle attack Breakable by brute force technique, hackers can attack with login data (brute force technique). The encryption which performs at presentation layer (not efficient) happens to entire message. Browser dependability while encrypting and session transmission, hence long wait time.
S-HTTP	It's a HTTPS with efficient encryption	Man- in- middle attack.

Table 1: Security issues in existing protocol [4] [5] [6].

Another issue which needs to be handled by secure cloud transmission protocol is about cloud service. In SaaS, it needs to ensure user authentication with correct privileges checking before using any application [8] [9] [10]. In PaaS, before providing platform to launch customer application, it needs to ensure bug, vulnerability of platforms, Multi-tenanted application isolation, authentication privileges to particular user. In DSaaS, before using storage service, it needs to ensure Data Protection, Integrity, vulnerability and security from intruder. In IaaS, before taking infrastructure, it needs to ensure Physical Security, Privileged access rights, control and monitoring infrastructure, maintaining infrastructure, communication channel security, intruder detection, privileges to access the infrastructure and auditing techniques. The above issues are summarized in Table2 [8] [9] [10].

Name	**On demand service for**	**Control**	**Ensure security challenge**
SaaS	Application	No control on OS, H/W, N/W infrastructure.	Privileged access Authenticated access User Types
PaaS	Platforms (Hosting	Can control hosting	Bug, vulnerability

	Environment)	environment not on OS, H/W, and N/W infrastructure.	of platforms. Multi-tenanted application isolation, authentication privileges to particular user
DSaaS	Storage Area	No Control	Data Protection, Integrity, vulnerability and security from intruder
IaaS	Infrastructure : Computing Resources, Storage, Network or middleware	Can control OS, Storage. Applications not on cloud infrastructure	Physical Security, Privileged access rights, control and monitoring infrastructure, maintaining infrastructure, communication channel security, intruder detection , privileges to access the infrastructure, auditing techniques

Table 2: Cloud services security issues [8] [9] [10]

Overview of proposed protocol

To address the some of the important security challenges which are discussed in Table1 and Table 2, we are proposing secure cloud transmission protocol (SCTP). Expected objective of secure cloud transmission protocol is to provide secure channel over insecure internet independent of its devices, browsers and physical locations. As shown in Fig. 11, SCTP one of the features is to work independent of physical location, computation devices and browser types.

SCTP requirements and roles

Expected objectives of SCTP are to provide secured internet channel with effective authentication techniques and efficient cryptographic algorithms. An effective authentication technique is needed for ensuring strict user authentication and authorization. By considering Table 1 and Table 2, security issues, identified and analyzed SCTP requirements are:

- Strict Authentication (It applies strict techniques : Multilevel, multifactor password generation)
- Efficient Cryptographic Approach (Encryption and Decryption)
- Secure Channel (Fully protected media)
- Intrusion detection (Finding out attackers)

Fig. 12 proposes the SCTP roles in OSI Layers. We expect SCTP to perform the strict authenticated privilege access at application layer and efficient encryption at presentation layer.

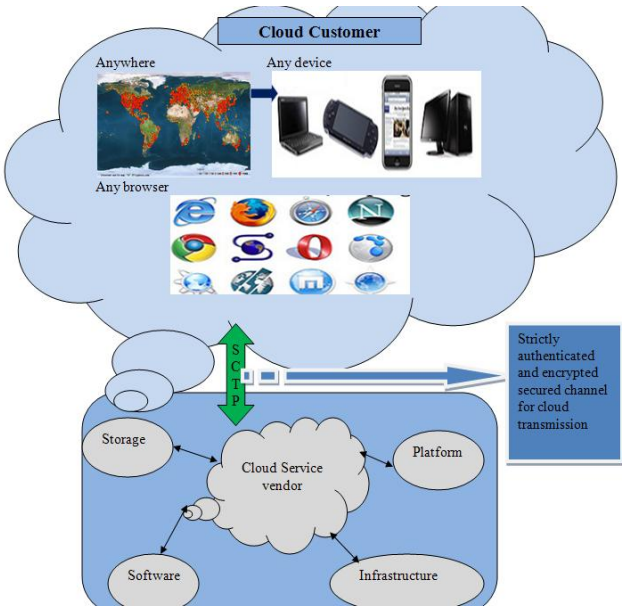

Fig. 11: Overview model of Secure Cloud Transmission Protocol (SCTP)

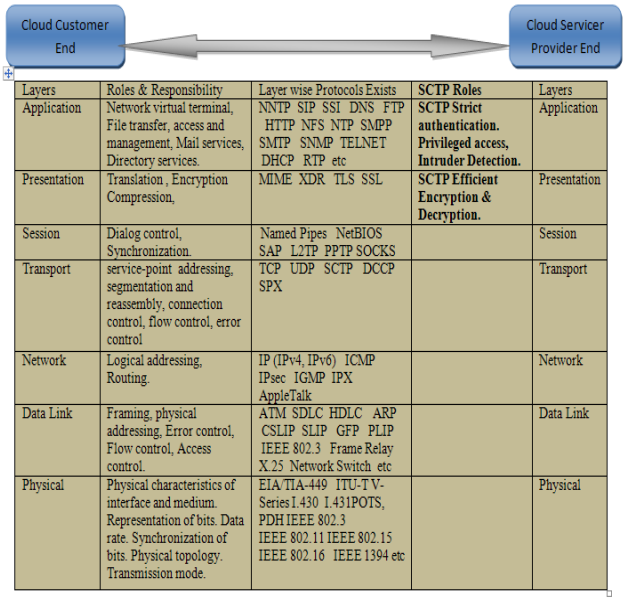

Fig. 12: SCTP roles & responsibilities with OSI layers roles.

SCTP Framework Design

After we analyzed the requirements of SCTP, In SCTP framework expected to involve: i) Strict Authentication

Techniques before using cloud services ii) efficient cryptographic approach to encrypt/decrypt the data over internet iii) ensuring the secure channel over insecure internet iv) intrusion detection. Fig. 13 is the functionalities framework diagram of SCTP which represents the identified functionalities of SCTP.

Actor documentation

Customer is an actor/setup who uses the cloud services for their business. **Cloud Service Provider** is the actor/setup who provides the cloud services over internet. **Intruder** can be person, tool and machine who do customized attacks against web applications, to identify and exploit all kinds of security vulnerabilities.

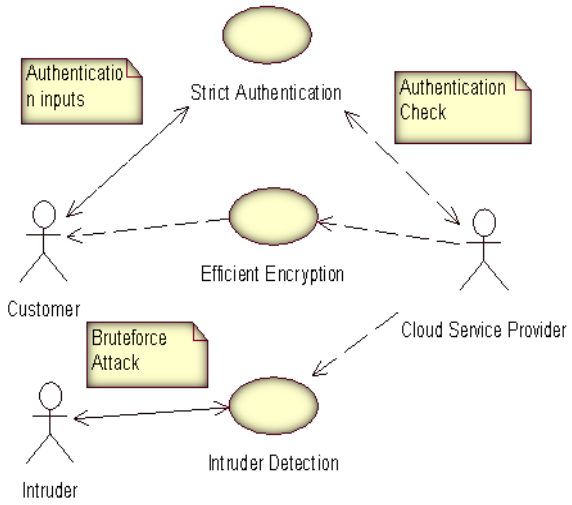

Fig. 13: SCTP framework for indentified functionalities

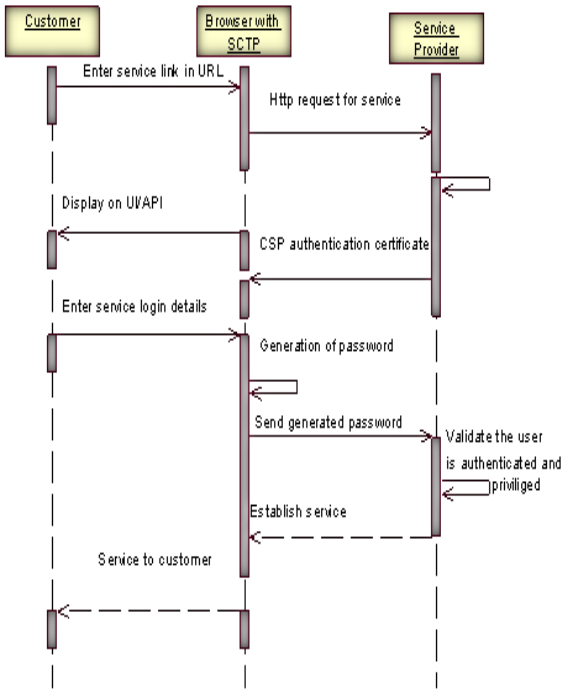

Fig. 14: SCTP Strict authentication

Functionalities:

Function: Strict Authentication
Description: This method is to ensure that the customer is authorized and authenticated before providing the service. This has multidimensional password generation, biometric and image- authorized techniques.
Flow of Events: (As Fig. 14 shown)
1. Send a service request
2. Enter login details
3. Generate password & authenticate the customer

Pre-Condition: Request for cloud service
Post-Condition: Find out whether authenticated customer or intruder
Function: Efficient Encryption
Description: This method is to ensure that the data transmission happens in encrypted form.
Flow of Events: (As Fig. 15 shown)
1. Enter encryption details
2. Generate key
3. Provide encrypted transmission

Pre-Condition: Should ask for data transmission
Post-Condition: Efficient encryption and data transferred over secure channel for authenticated customer
Function: Intruder detection
Description: This method is to find intruder.
Flow of Events: (As Fig. 16 shown)
1. Find if any unauthenticated customer is trying with brute force attack.
2. If intruder is suspected it then generate and report complaints to CSP.
3. Reject connection

Pre-Condition: Should be unauthenticated try
Post-Condition: Register complaints to CSP

Fig. 14, 15, 16 shows the sequence of operation in SCTP Strict authentication, efficient encryption/decryption and intruder detection respectively.

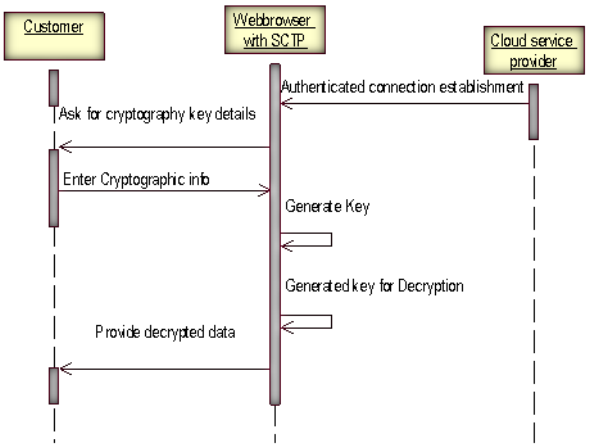

Fig. 15: SCTP encryption/decryption

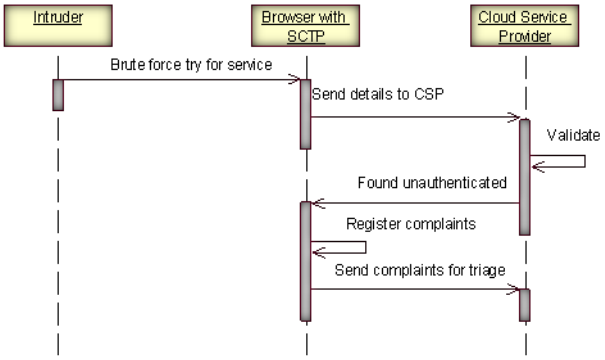

Fig. 16: Intruder detection system in SCTP

Secure cloud transmission protocol expected to works under many execution states such as connection establishment, authentication check, encryption/decryption, service use, measuring the service and connection end. Fig. 17 is a state chart diagram of SCTP which shows different states of SCTP during its execution.

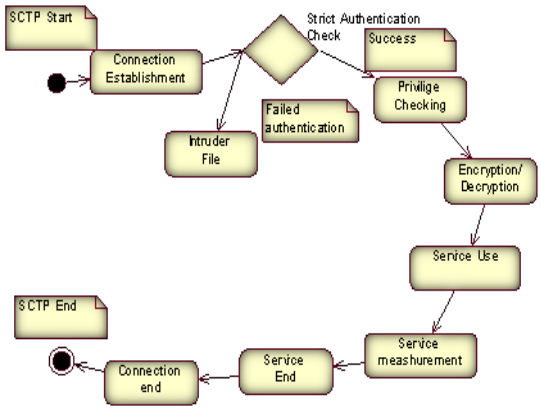

Fig. 17: SCTP State Chart Diagram

4. Conclusion and Future Enhancement

Cloud computing is a technology that uses the internet and central remote servers to maintain data, platforms, infrastructure and applications. Cloud computing allows consumers and businesses to use applications, platforms, infrastructure without installation and access their personal files at any computer with internet access. However there are internet security issues that need to be addressed. We propose a framework design of secure cloud transmission protocol (SCTP). SCTP is expected to create such secure channel over insecure internet. SCTP has proposed with strict authentication techniques and cryptographic approaches. SCTP design details which are presented in this paper may help us to fix the major security challenges which are identified in http protocols and cloud computing services. Our future plan is to carry out the SCTP detailed design along with its security proof.

Acknowledgment

Our sincere thanks to Prof. K N B Murthy, Principal and Prof. Shylaja S S, HOD, Department of Information Science and Engineering, PESIT, Bangalore, for their constant encouragement

References

[1]. Center Bo Wang, HongYu Xing "The Application of Cloud Computing in Education Informatization, Modern Educational Tech..." Computer Science and Service System (CSSS), 2011 International Conference on IEEE, 27-29 June 2011, 978-1-4244-9762-1, pp 2673 – 2676.

[2]. NIST Definition http://www.au.af.mil/au/awc/awcgate/nist/cloud-def-v15.doc

[3]. Cloud Computing services & comparisons http://www.thbs.com/pdfs/Comparison%20of%20Cloud%20computing%20services.pdf

[4]. Hyper Text Transmission Protocol: Communication Technology Proceedings-2003. ICCT 2003. International Conference on Study on conformance testing of hypertext transfer protocol by Xiaoli Yu; Jianping Wu; Xia Yin; Dept. of Comput. Sci., Tsinghua Univ., Beijing, China

[5]. hyper text transmission protocol with security: A Performance Analysis of Secure HTTP Protocol by Xubin He, Member, IEEE. http://en.wikipedia.org/wiki/HTTP_Secure. http://www.technolozy.net/difference-between-http-and-https-protocols.html.

[6]. S-HTTP: Secure Hypertext Transfer Protocol: http://www.javvin.com/protocolHTTPS.html. http://en.wikipedia.org/wiki/Secure_Hypertext_Transfer_Protocol

[7]. Man in the middle attack Moxie Marlinspike (2009). "HTTPS ... pwned !". http://blogs.orange-business.com/securite/2009/02/ssl-pwned.html. Retrieved 2011-06-20

[8]. A User Identity Management Protocol for Cloud Computing Paradigm Safiriyu Eludiora1, Olatunde Abiona2, Ayodeji Oluwatope1, Adeniran Oluwaranti1, Clement Onime3,Lawrence Kehinde apered in Int. J. Communications, Network and System Sciences, 2011, 4, 152-163

[9]. Cloud Computing Challenges and Related Security Issues: a survey project report on Cloud Computing Challenges and Related Security Issues by Traian Andrei and Prof. Raj Jain

[10]. Protocols for Secure Cloud Computing IBM Research – Zurich Christian Cachin April 2011

Author Biographies

First Author Dinesha H A was working with VMware pvt India ltd. Now he is with PES Institute of Technology, Assistant Professor in ISE & Research Scientist in CORI,100ft Ring Road, BSK III Stage, Bangalore -560085, Karnataka India (phone: +91-9945870006; FAX: 08026720886, email:sridini@gmail.com)

Second Author Dr V. K Agrawal was working in ISRO, now he is with the PES Institute of Technology, Professor in ISE & Director in CORI,100ft Ring Road, BSK III Stage, Bangalore -560085, Karnataka India (Ph: 080-26720783 FAX: 08026720886,email:vk.agrawal@pes.edu)