International Journal of Current Advanced Research
ISSN: O: 2319-6475, ISSN: P: 2319-6505, Impact Factor: SJIF: 5.995
Available Online at www.journalijcar.org
Volume 7; Issue 1(I); January 2018; Page No. 9333-9337
DOI: http://dx.doi.org/10.24327/ijcar.2018.9337.1539

Research Article

FRAMEWORK FOR SECURE CLOUD TRANSMISSION PROTOCOL IN WIRELESS SENSOR NETWORK

Hemalatha K.L*

Department of Information Science and Engineering, SKIT, Bangalore, India

A R T I C L E I N F O

Article History:

Received 10th October, 2017
Received in revised form 20th November, 2017
Accepted 6th December, 2017
Published online 28th January, 2018

Key words:

Cloud computing technologies, framework, OSI, SCTP.

A B S T R A C T

Cloud Computing technologies are becoming popular because of several benefits. Many enterprises are adopting cloud computing technologies to reduce the cost and complexity of business infrastructure and its maintenance. Recent developments in sensor networking emphasized the need for sensor networks with the cloud. This improves the power processing and battery life of the sensor nodes. Once the sensor data is routed to the cloud possible measures need to be adopted to secure the sensor data. However there are certain cloud sensor security issues with respect to these technologies. To overcome these issues we propose secure cloud transmission protocol framework. Thus framework will help us in developing a high security protocol for the customers who are using cloud computing technologies over insecure internet. In this paper we discuss i) overview model of secure cloud transmission in internet ii) sensor cloud security requirements iii) roles and responsibilities of STP in OSI iv) High level framework of secure cloud transmission.

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 in the upcoming electronic era. Recent advances in electronic and computer technologies have paved the way for the proliferation of wireless sensor network (WSN) [1].

WSNs are autonomous systems consisting of tiny sensors. These are associated with integrated sensing, limited battery lifetime, resource constraints, and limited range. The limited battery lifetime limitation can be overcome by integrating the WSNs and the cloud computing technology. The cloud technology is an internet-based model which enables convenient and on demand network access to a shared pool of configurable computing resources [2]. Various services such as a software, hardware, data storage and infrastructure are provided over internet. These are accessed from web browsers, desktop and mobile applications.

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 iv) infrastructure as a service [3] as shown in figure 1. Cloud service activities are upgraded or improved by the cloud service provider based on the customer needs.

Corresponding author:* **Hemalatha K.L
Department of Information Science and Engineering, SKIT, Bangalore, India

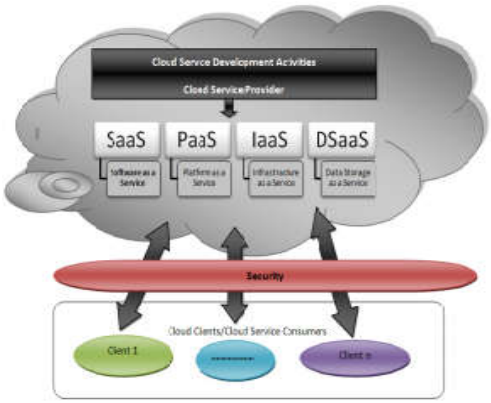

Figure 1 Major categories of cloud computing

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, HTTOS and S-HTTP. HTTP helps to communicate with web servers. Generally, 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 provision of data confidentiality [5]. HTTPS is 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 [6]. Hence to overcome the rest of the security drawbacks and to establish secure channel, it is necessary to investigate a protocol known as SCTP. This can be embedded HTTP to provide a secured channel over an insecure internet for cloud transmission.

This paper is organized in the following manner: In section 2, we present a brief description about the cloud computing background, and cloud services. In section 3, the detailed picture of the identified security issues, both in http protocols and wireless sensor cloud services. Along with this the requirements, roles in OSI architecture and framework of SCTP are also described. We finally conclude this paper along with the future work in section 4.

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]. On utilizing the services provided by the cloud one can be benefitted as follows: i) Reduce hardware installation & maintenance cost ii) reduce infrastructure maintenance cost iii) e-waste minimization iv) obtain on demand access, anywhere from an device services v) efficient usage of electrical power vi) flexibility and highly automated vii) virtual business setup viii) easier to replace and upgrade ix) easier maintenance and management. Cloud computing helps customers by having its own intelligent features like i) portability ii) encrypted data and storage iii) fault tolerance and 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 section, we briefly describe various services offered by cloud computing.

Cloud computing service 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 portrayed in figure 2 cloud computing technologies are grouped into 4 sections. They are SaaS, DsaaS, IaaS and PaaS [8] [3].

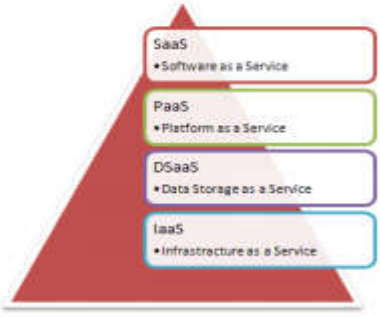

Figure 2 Cloud computing services

SaaS (Software as a Service)

It is an on demand application service. It delivers software as a service over the internet, eliminating the need to install and run the application on the customers own computers [8] [3]. Figure 3 shows that without installing, client can access the required application from cloud SaaS service provider over internet.

Figure 3 Model of SaaS

PaaS (Platform as a Service)

It is an on demand platform service to host computer application. PaaS provides the delivery of computing platform 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]. Figure 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.

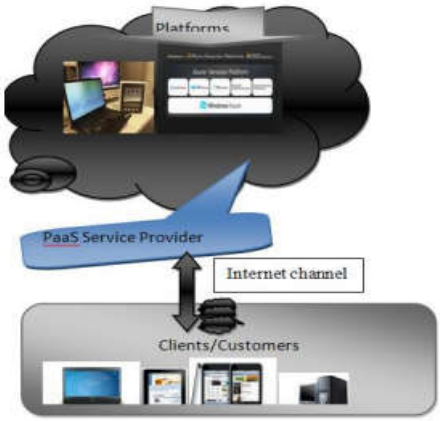

Figure 4 Model of PaaS

DsaaS (Data Storage as a Service)

It is on demand storage service. Cloud computing provides internet-based on demand back up storage services to customer [8] [3]. Figure 5 shows the on demand accession of DsaaS services. In this service, customers can keep their data backup remotely over internet servers. This backup data maintenance is taken care by DsaaS service provider. Cloud DsaaS service providers are responsible for the confidentiality of the customer data. Here customers need not worry on setting up the large discs array to keep their huge amount of data.

IaaS (Infrastructure as a Service)

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

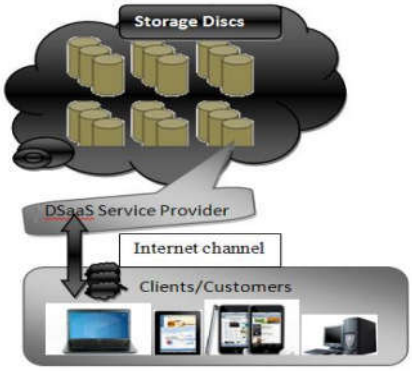

Figure 5 Model of DSaaS

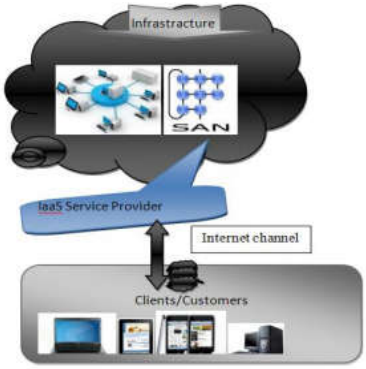

Figure 6 Model of IaaS

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. But it 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]. Table 1 discusses 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. Another issue which needs to be dealt by the secure cloud transmission protocol is about cloud service. In SaaS, it needs to ensure user authentication with correct privileges 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, maintaining infrastructure, communication channel security, intruder detection, privileges to access the infrastructure and auditing techniques. The above mentioned issues are summarized in Table2 [8] [9] [10]. Overview of proposed protocol to address some of the important security challenges which are discussed in Table 1 and Table 2, we are proposing secure cloud

Table 1 Wireless sensor cloud security issues in existing protocols

Protocol Name	Description	Security Issues
HTTP	Application layer Request-response protocol with no security	Data confidentiality, Integrity, Man-in-the-middle attack, eaves dropping attacks
HTTPS	It 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. The encryption which performs at presentation layer happens to entire message. Browser dependability while encrypting and session transmission, hence long wit time.
S-HTTPS	It's a HTTPS with efficient encryption	Man-in-the-middle attack

Table 2 Cloud services security issues

Name	On demand services	Control	Ensure sensor cloud security challenge
SaaS	Application	No control on OS, hardware, network infrastructure	Privileged access, Authenticated access, User Types
PaaS	Platforms hosting environment	Can control hosting environment not on OS, hardware, network infrastructure	Bug, vulnerability of platforms, multi-demand 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 sights, control and monitoring infrastructure, maintaining infrastructure, communication channel security, intruder detections, privileges to access the infrastructure, auditing techniques

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 the Fig. 7, one of the features of SCTP 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. 8 proposes the SCTP roles in OSI Layers. We expect SCTP to perform the strict authentication privilege access at application layer and efficient encryption at presentation layer.

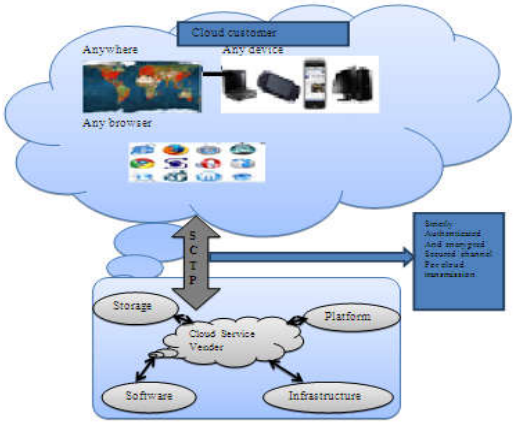

Figure 7 Model of SCTP

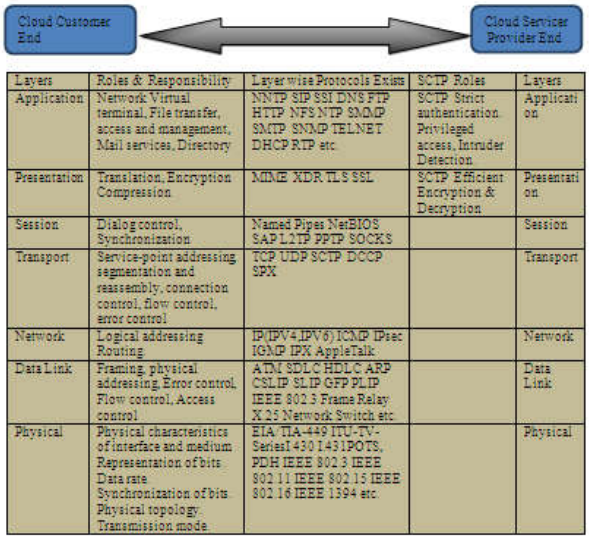

Figure 8 SCTP roles & responsibilities with OSI layer roles

SCTP High Level Design

Based on the analyzed requirements of SCTP the expected framework connotes : 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. 9 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 perform customized attacks against web applications, in order to identify and exploit all kinds of security vulnerabilities.

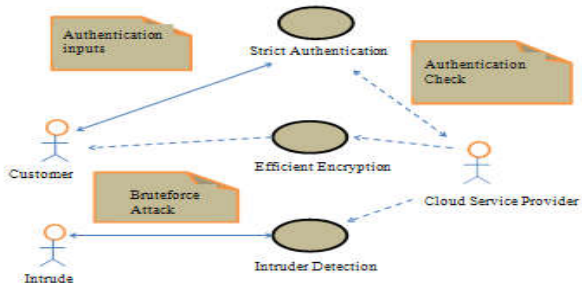

Figure 9 SCTP framework for identified function

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.10 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.11 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.12 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. 10, 11, 12 shows the sequence of operation in SCTP Strict authentication, efficient Encryption / decryption and intruder Detection respectively

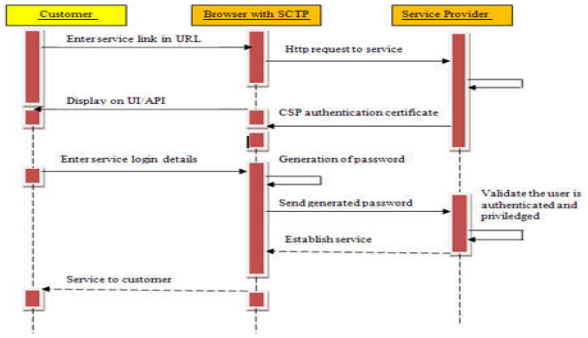

Figure 10 SCTP Strict authentications

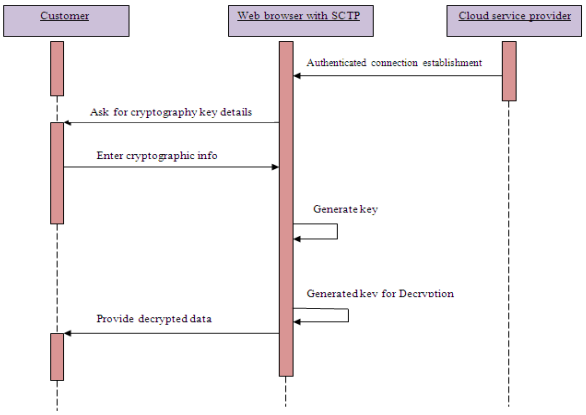

Figure 11 SCTP encryption/decryption

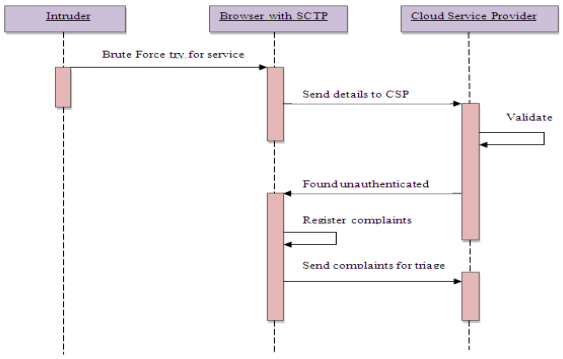

Figure 12 Intruder detection system in SCTP

Secure cloud transmission protocol expected to work under many execution states such as connection establishment, authentication check, encryption/decryption, service use, measuring the connection end. Fig. 13 portrays a state chart diagram of SCTP which shows different states of SCTP during its execution.

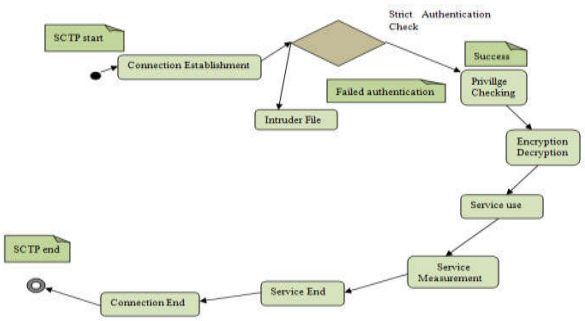

Figure 13 SCTP state chart diagram

CONCLUSION AND FUTURE ENHANCEMENT

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

References

1. IEEE – Center Bo Wang, Hong Yu Xing, Hong Yu Xing"The Application of Cloud Computing in Educational Informatization, Modern Educational Technology Tech", computer science and service system.
2. 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 of Study on Conformance testing of hypertext transfer protocol by Xiaoli Yu; Jianping Wu; Xia Yin; Dept. of Compute. Sci., Tsinghua Univ., Beijing, China.
5. Hypertext transmission protocol with security: A Performance Analysis of secure HTTP Protocol by XubinHe,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. A User Identity Management Protocol for Cloud Computing Paradigm Safiriyu Eludioral, Olatunde Abiona2, Ayodeji Oluwatope2, Adeniran Oluwaranti2, Clement Onime3, Lawrence Kehindeapered in Int. J. Communications, Network and System Sciences,pp-152-163,2011.
8. Cloud Computing Challenges and Related Security Issues: a survey project report on Computing Challenges and Related Security Issues by Traian Andrei and Prof. Raj Jain
9. Protocols for Secure Cloud Computing IBM Research–Zurich Christian Cachin April 2011