iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 7 **Issue:** II **Month of publication:** February

DOI: http://doi.org/10.22214/ijraset.2019.2158

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 7 Issue II, Feb 2019- Available at www.ijraset.com

Study on Various Approaches used by Security as a Service Model in Cloud Computing

Jeba Nadar[1], Shraddha Tiwari[2], Sehba Siddiqui[3]
[1, 2, 3]*Computer Science Department, Mumbai University*

Abstract: Cloud computing is the way of using remote servers placed on the Internet for storing, managing, and processing data, rather than using a local server or a personal computer. In cloud computing, security and privacy are the major issues. However, there are many challenges for securing the cloud from various attacks. The main responsibility of the Security as a Service model is to provide flexible security to its users to prevent these attacks. The approaches used by the Security as a Service model are SLA based approach via SPECS and Crypto Coprocessor approach for providing flexible security to its users. In this paper, we do a study on various approaches used by the Security as a Service model and to propose a system which provides maximum security to the cloud users.

Keywords: **Cloud computing; security; integrity; threats; attacks**

I. INTRODUCTION

A. Cloud Computing

Cloud computing is a model for convenient, ubiquitous and a way for using a shared pool of computing resources like networks, servers, services and applications. The architecture of the cloud computing is based upon some delivery models: Security as a Service (SaaS) which provides application level software service; Platform as a Service (PaaS) which provides software services, libraries and software platforms which supports the development of application level services; Infrastructure as a Service (IaaS) which allows the use of remote hardware resources in an elastic way. There are many deployment ways for implementing the cloud architecture [5].

The security issues faces by the cloud computing in today's life are: the duplication of Authentication and Identity Information by different Cloud Service Providers, lack of Privacy and Trust Management in cloud, lack of Auditing and Accountability [6].

B. Security-as-a -Service

Security as a Service (Secaas) is a cloud computing models which provides security services for the cloud based customers [7]. The main use of the Security as a Service model is to provide security to the providers and also to the tenants of the cloud. The Security as a Service gives additional security to the customers as per their requirements [1]. The SaaS model allows the user to define their own data security. After the advancement of technology too, the privacy and security of data are some major issues [8].

C. Security-as-a-Service Architecture

The basic security architecture of the Security as a Service model includes various elements like Tenant Virtual Machines (TVM), Host Based Security Tools (HBST), Tenant Specific Attack Detection (TSAD), and Service Provider attack Detection (SPAD), Node Controllers and then the physical devices [1].

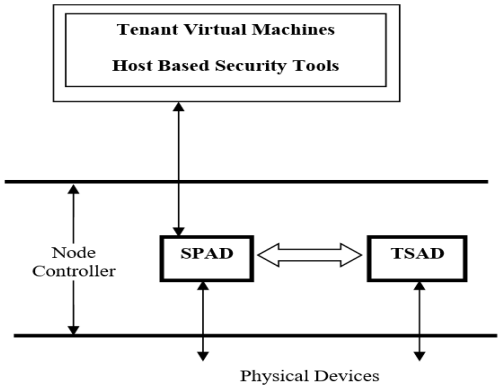


Fig. 1. Basic Security Architecture

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 7 Issue II, Feb 2019- Available at www.ijraset.com

II. RELATED WORK

Many researches have taken place in the design of a secure cryptographic co-processor and data security in the cloud environment. A complete outline on various researches and trends in cloud computing has been presented in [10].Multiple researches for provides data security is still going on [5]. A Service Level Agreement based approach is used for providing a strong security to the cloud users [5]. Also, in [8] the author designed coprocessor architecture for providing security to the user data.

In [1], security architecture is designed for providing security to the users. Here, the security is provided as a service to the cloud users. In this the users are provided with the security required by them during the Service Level Agreement (SLA) period. Joel-Ahmed M.Mondol, in his paper [11] explained about using Field Programmable Gate Arrays for Cloud security. As the cloud technology is growing vastly, the security concerns are also increasing. Henceforth, the cloud security became an important research field. The authors of [1] gave an outline about the confidentiality, integrity, and availability issues faced by the users of the cloud

III.THE SPECS APPROACH

The SPECS approach is created on the idea of security parameters included in cloud SLAs. The core notion in SPECS is the security management in Service Level Agreement. This will enable the negotiation, the continuous monitoring and the enforcement of security levels. An end user may negotiate his security features through the dedicated SPECS platform [2].

A typical SLA life cycle can be characterized by three main phases:

1) Negotiation Phase: the customer(s) and provider(s) conduct a negotiation process on requirements/services to find agreement on what the SLA should effectively offer.

2) Monitoring Phase: A signed SLA is checked for its actual degree of conformance or for penalties if in violation.

3) Enforcement Phase: The actions needed to respect the SLA (i.e., to keep a sustained QoSec) are effectively taken.

The SPECS targets to offer contrivances to specify cloud security requirements and to evaluate the security features offered by CSPs. SPECS aims to offer systematic methods to negotiate, to monitor and to enforce the security parameters specified in SLA. The SPECS approach purposes at resolving the delineated cloud security open issues, offering tools to manage the security demanded in SLAs as a foundation for enabling Secaas.

The SPECS has three potential usage scenarios to indicate different ways for using the platform and to run cloud applications and services:

a) Third Party Security Platform: The SPECS administrators run the Platform on resources attained from public/ private cloud and provide security services to cloud end Users.

b) Hosted Platform: SPECS runs on local resources and it offer s additional security services to sustain an agreed QoSec

c) User Software: Cloud end users that use SPECS on their local resources to install required security features.

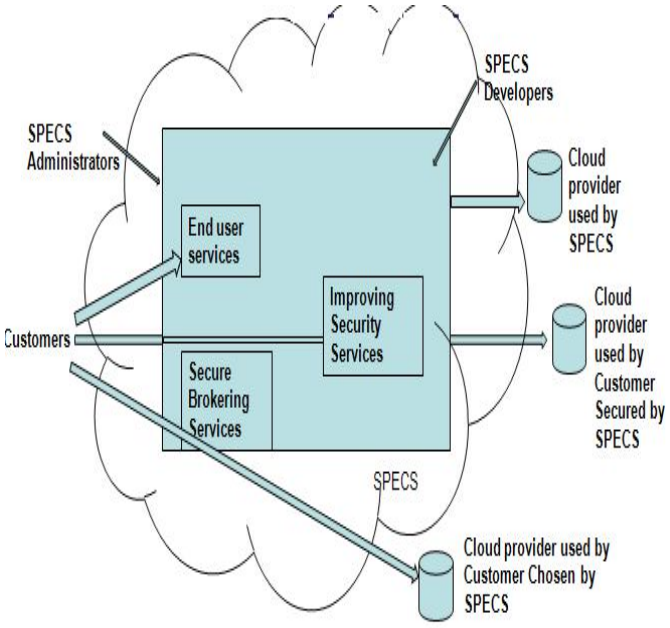


Fig.2. SPECS Third Party Security Interaction

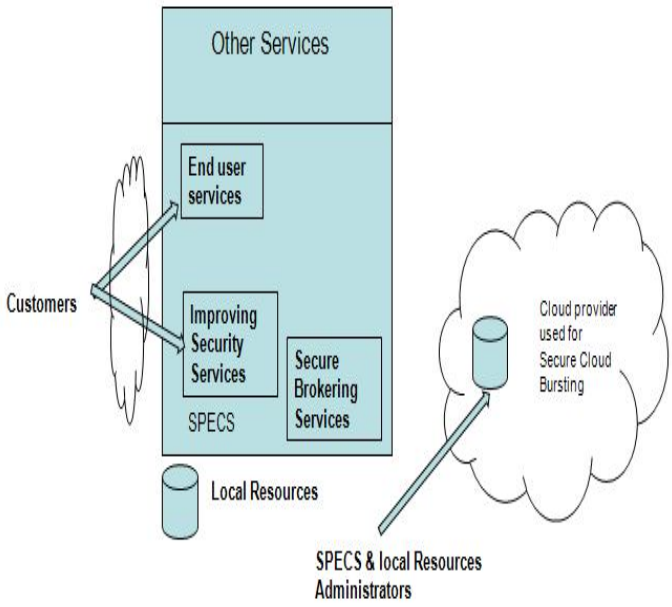


Fig.3. SPECS Hosted Platform Interaction Model

IV. THE CRYPTO CO-PROCESSOR APPROACH

A. An Overview of Crypto Coprocessor

Co-processors are a secondary processor which helps to increase system performance by controlling the processor intensive applications and tasks. Co-processors cannot fetch instructions from the Memory like the Processors. It implements the security protocols. Cryptographic co-processors focus only on encryption and decryption.

The Cryptographic co-processors permit key management by storing the keys securely. The secret key values are nested in the co-processor subsystem. The host systems are not able to find the secret key values. It permits the parallel processing.

B. Crypto Coprocessor Architecture

The Crypto coprocessor securely doing the encryption and decryption process. The security and privacy can be improved after giving the complete control to the consumer. The co-processor contains three main components [3].

1) *The Algorithm Core:* contains set of encryption and decryption standards. A random bit generator is placed for generating required keys.
2) *The Operation Controller:* operates the signal from the host. It works on the signal and passes to the algorithm core.
3) *Buffers:* There are two buffers: incoming and the outgoing. The buffers work as the temporary storage. The buffers get activated after getting instructions from the operational controller. Initially the user chooses the encryption algorithm from the algorithm core, and then the co-processor is instructed by the operational controller for downloading the algorithm from the core. At the end, the co-processor processes the data.

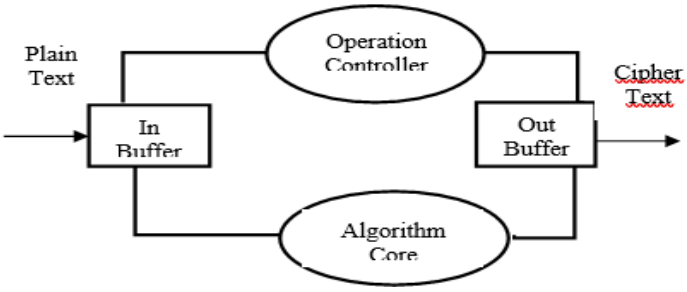


Fig.5. Cypto Co-processor Architecture

V. THE PROPOSED SYSTEM

In spite of the security provided by various CSP's, the cloud users are facing various security and privacy issues. The data is getting corrupted or stolen by other parties as they are working on a same cloud. So for achieving integrity of the data, we are proposing a Secaas architecture which includes the authentication and authorization modules [7].

Our proposed system contains data and privacy attributes security points, security protection and measures, and public safety services. In this paper, the authentication and authorization of the users is introduced. The proposed system in fig.6 is for the safety of the legitimate users by using the authentication and the authorization.

A. OpenSSL-Based Identity Authentication

For authentication, the OpenSSL-Based Identity Authentication is used.

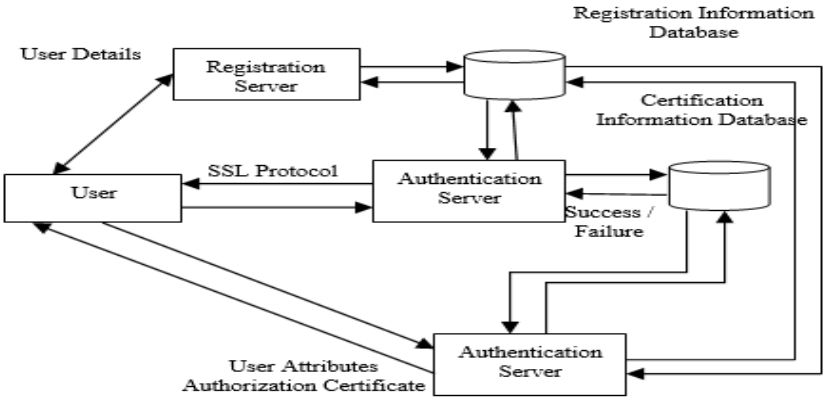


Fig.6.Authentication and Authorization module of Secaas

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 7 Issue II, Feb 2019- Available at www.ijraset.com

The Netscape Corporation designed the Secure Sockets Layer (SSL). The main aim of the SSL is to provide secure network Fig.6.Authentication and Authorization module of Secaas transmission, for thwarting communication content from being overheard. SSL provides integrity, confidentiality, and authentication of data. The SSL is placed between the application and transport layer of the network.

1) SSL protocol is divided into two layers.

a) SSL Record Protocol: This provides encryption support, compression, high-level protocol for data encryption and other basic functions. It is placed on top of the reliable transport protocol.

b) SSL Handshake protocol: It is placed on top of the SSL record protocol. It helps the data transmission before initializing the communication.

2) The characteristics of the SSL protocol are as follows.

a) The connection between the user and the server is secured by the SSL protocol. It uses the encryption algorithm for encrypting the data, thus providing the data integrity.

b) Implementation of the SSL protocol is easy. It is also built on most of the web browsers and servers. We can use the SSL protocol in the systems easily without any changes.

c) SSL protocol is easy to use, fast, and low cost.

Open SSL uses C language for the development, and supports most algorithm agreement. It provides variety of encryption algorithms, key exchange algorithms and digest algorithms, and general purpose cryptography library. The establishing of the SSL communication process is shown in the Fig. 7.

Initially the client sends the hello message to the server, then the server should respond with a hello message or else error will occur and the connection will fail. The hello message of the client and the server establishes the security enhancements between the client and the server. The key exchange includes four messages: the client certificate and the key exchange, the server key exchange and the certificate.

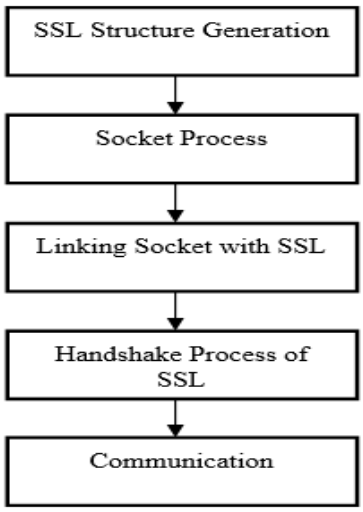


Fig.7. SSL communication process establishment

B. Attribute Based Access Control

Authorization is basically used for controlling users accessing to directories, servers, files and other network resources. It prevents access to the objects of the subjects for make sure for the data resources to use within certain range. Attribute-based authorization achieves large data authorization service, and develops the authorization.

Due to this users and data can be made fine-grained based on the attributes. Because of this system, the security issues can be solved.

VI. CONCLUSION

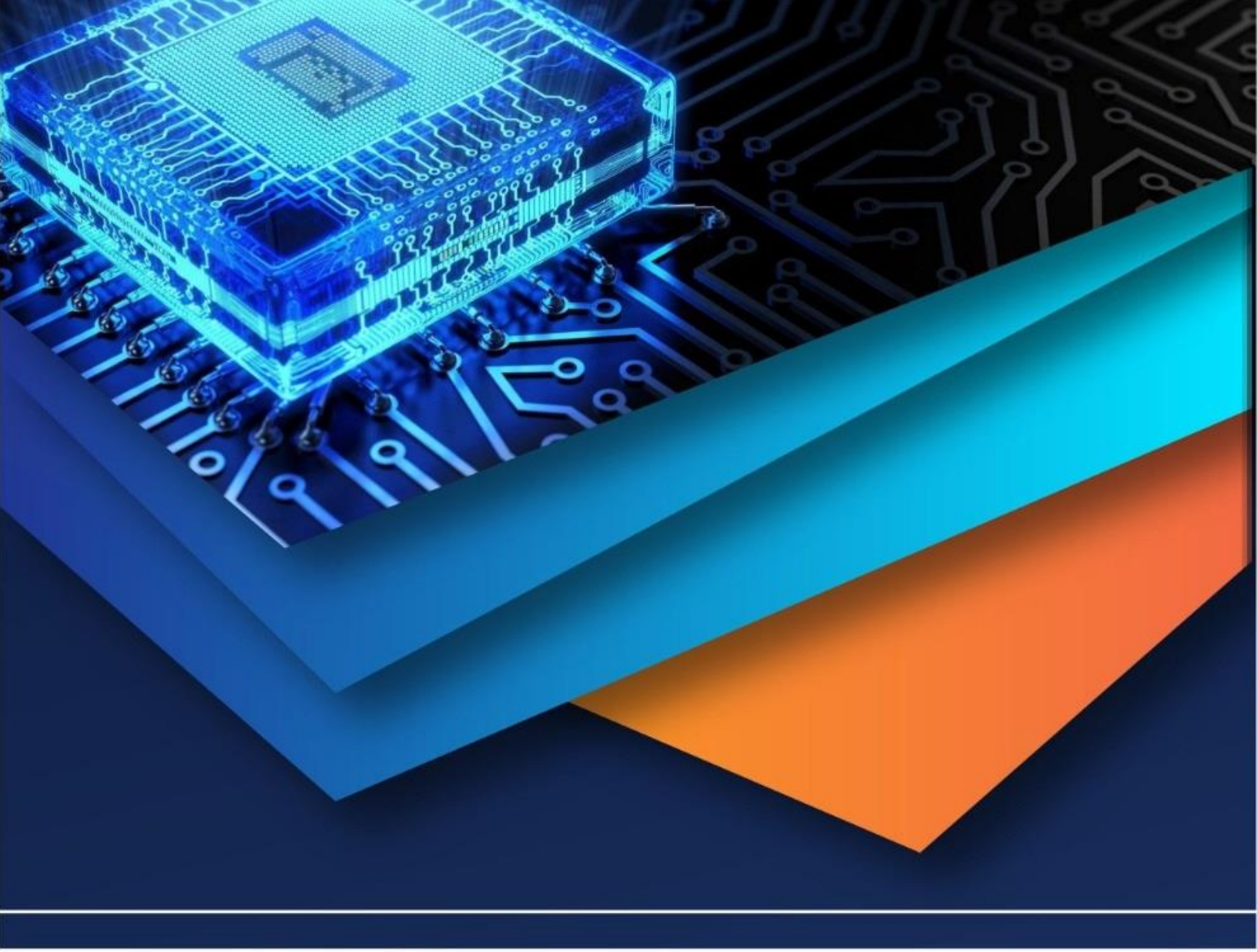
In this paper, we presented our authentication and authorization based SecaaS architecture. Our proposed system provides better security than the various approaches that we have explained earlier in this paper. The Secaas integrates the security services in a joint infrastructure.

VII. ACKNOWLEDGEMENT

I would like to thank the coauthors who have given me their insights and helped to write this survey paper, without whom this would have not been possible. Also, would like to thank the institute for support and motivation in this paper completion.

REFERENCES

[1] V. Varadharajan, and U. Tupakula, "Security as a Service Model for Cloud Environment", IEEE Trans. On Network And Service Management, vol. 11, no. 1, pp. 60-75, Mar 2014
[2] M. Rak, N. Suri, J. Luna, V. Casola and U. Villano, "Security as a Serrvice Using an SLA based Approach via SPECS", IEEE International Conference on Cloud Computing Technology and Science,2011.
[3] P. Ram , Sreenivaasan, "Security as a Service Securing user data by Coprocessor and Distributing the Data", IEEE, 2011
[4] S. Chaisiri , Ryan K.L.Ko and D. Niyato, "A Joint Optimization Approach to Security-as-a-Service Allocation and Cyber Insurance Management", IEEE Trustcom/BigDataSE/ISPA, 2015
[5] A. Furfaro, A. Garro, A. Tundis, "Towards Security as a Serrvice: on the modeling of Security Services for Cloud Computing" , IEEE, 2014.
[6] D. Krishnan, M. Chatterjee, "Cloud Security Management Suite – Security-as-a-Service", IEEE, 2012.
[7] Wu Zhijun, Wang Caiyun, "Security-as-a-Service in Big Data of Civil Aviation", IEEE, 2015
[8] Mladen A. Vouk, "Cloud Computing – Issues, Research and Implementations", Proc. of the ITI 2008 30th Int. Conf. on Information Technology Interfaces, June 23-26, 2008, Cavtat, Croatia.
[9] Joel-Ahmed M.Mondol, "Cloud Security So;utions using FPGA, IEEE, 2011
[10] M. Menzel, R. Warschofsky, I. Thomas, C. Willems, C. Meinel, "The Service Security Lab: A Model-Driven Platform to Compose and Explore Service Security in the Cloud", IEEE 6th World Congress on Services,2010



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY