International Journal of Basic and Applied Sciences, 1 (3) (2012) 177-183
©Science Publishing Corporation
www.sciencepubco.com/index.php/IJBAS

Implementation of Eap with RSA for Enhancing The Security of Cloud Computing

Sadia Marium, Qamar Nazir, Aftab Ahmed, Saira Ahthasham
Mirza Aamir Mehmood

Department of Computer Science, SZABIST, Islamabad
Email: sun_sad119@yahoo.com
Department of Computer Science, SZABIST, Islamabad
Email: qamar_nazir@hotmail.com
Department of Computer Science, BUTIEMS, Quetta
Email: aftab.ahmed@buitms.edu.pk
Islamabad College for Girls, Islamabad
Email: sairaimtiaz@gmail.com
Department of Computer Science, BUTIEMS, Quetta
Email: Mirza.aamir@buitms.edu.pk

Abstract

Cloud Computing is emerging approach because of high availability, efficient cost and performance. In Cloud Computing, services providers will provide the storage for data along with services. But due the lack of proper security policies, many business companies are reluctant to adopt the Cloud Computing technology. This paper has been written to highlight cloud security and privacy issues. Our research is mainly focus on service provider's side security. They must protect their client data by unauthorized access, modification or miss use, denial of services and repudiation. To ensure the security of client data in cloud, we purpose the implementation of Extensible Authentication Protocol through three way hand shake with RSA.

Keywords: *RSA, EAP, Cloud Computing, Authentication, Encryption.*

1 Introduction

Availability, scalability and cost effective, these three factors are involved in the discovery of new technology, abacus to tablet pcs and super computer to grid computing, all these happen due to these three factors.[1]
Cloud Computing is a general term that provides hosted services over internet. Broadly speaking, these services are divided into three categories: Infrastructure-

as-a-Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS). IaaS provides physical resources such as CPU, network and storage etc. PaaS provides a platform for execution of application. SaaS provides different type of application and web services to the end users.

Clouds can be deploy into: Public: available publically, Private: accessible only within a private network and Partner: cloud services offered by a provider to a limited number of parties. The types of Cloud computing can be classified according to deployment. This deployment can increase or decrease the major cloud computer problems, the security and privacy can be increase or decrease upon the choice of cloud. These classifications are also based on different parameters like, the customer requirement, location of cloud and by their architecture. The advantage of Cloud Computing is cost saving, because it gives a platform for the execution of different tasks on cloud rather than the execution of tasks on user Personal Computer or Server. [2]

However, prime disadvantage of Cloud Computing is security. Commonly, user data has been encrypted by using different encryption algorithms in order to protect data from intruders. This approach is also used in cloud computing environment. But when multiple services using at the same time to perform work involving linking of task between those services, the reliability may not be assured. More over Cloud platform is shared by several customers, if a malicious program affects the service, that is used by other customers effect the environment used by all.

[3] Integrity, availability and confidentially are common security risk for Cloud Computing. In Cloud, attacks can be of two types, Internal Attacks & External Attacks. Internal attacks are those, in which the insider wants to gain the normal access to the network and disturbs the network activities, either by learn password or authentication information or gain control of VMs. While in External Attacks, outsider aims to propagate fake routing information or disturb nodes from providing services. Internal intrusion is more hazardous than external.

Organization of this paper is as follows. Literature survey is discussed in Section II. Proposed model is discussed in Section III. Section IV and V give details of conclusion and direction of future work.

2 Literature Survey

Balakarishnan.S et al [4] introduce TPA (Third Party Auditor) between client and cloud service provider, which acts as external auditor to audit the user outsource data. This scheme provides secure and efficient dynamic operations (data update, delete and append) on data blocks stored in the cloud. But the method how to secure client's resources reside on cloud server is beyond the scope of this paper.

Joshi Ashay.M et al [5] argue that Asymmetric Cryptography Algorithms and Digital Signature techniques are reliable and efficient to provide more security user's data in Cloud Computing. The potentiality of their paper is that, they have seeded the idea of using two different keys algorithms. However, they are failed

to give the model or methodology that how and where these algorithms should be implemented.

Richard Chow et al [6] describe a framework for supporting authentication decision, which they call in their paper as Trust Cube. They give a high-level architecture of authentication flows. In that architecture they consider four participants: client devices, data aggregators, an authentication engine, and authentication consumers. Client device, data aggregators and authentication consumers must be authenticated themselves through authentication engine before exchange of data. The strength of this paper is that they give model of cloud authentication. However this article only focus on one threat (Authentication), facing Cloud Computing. Other threats in Cloud environment such as Repudiation, Denial of Services and Spoofing identity are probably ignored by authors.

Honywei Li et al [7] present a Hierarchical Architecture for Cloud Computing. Then they proposed Identity-Base Encryption and Identity-Based Signature for that Hierarchical Architecture. Finally, they give Authentication Protocol for Cloud Computing (APCC). In the end they conclude that APCC is more light weight and efficient as compared SSL Authentication Protocol, on base of performance analysis. The merits of their research works are they give Cloud Computing model along with Authentication Protocol for that model. Moreover, they give the simulation results to support their proposed APCC. The major drawback of this paper is that they have given least preference to security element in their protocol.

Dai Yuefa et al [8] analyze basic problem of Cloud Computing that is data security. They get data security requirement of Cloud Computing and give a mathematical model on the base of these requirements. Their data security model is a worth addition in world of Cloud Computing security. However, writers are not able to give a comprehensive solution for security of Cloud Computing.

Qiu-Xin.F et al [9] propose a multi-layer and multi-level secure architecture for Cloud Computing according to the characteristics of mobile user. And they propose the idea of SeaaS (Security as a Service). Plus point of this article is that the implementation of that architecture is flexible to different scale system to different requirements and can integrate different operating system and heterogeneous network. While researchers neither discuss the component of secure architecture in detail nor give the prototype system for verification of theory.

3 Proposed Model

We divide our proposed solution into two sections. In first section, we analyze a security problem for Cloud Computing data. In second section, we evaluate a solution for security and privacy of Cloud data on the base of these problems.

3.1 Section I

In this area, we learn the threat model of Cloud computing by identifying attackers, examining client assets and analyzing threats. Further we break part I into:

In this step we identify attackers in Cloud environment. There are two kinds of attackers, Inside attackers and outside attackers. Inside attackers can be one of the following:

- Malicious employees at client side: These attackers can learn password and other authentication information. They gain access to VM after getting this information.
- Malicious employees at Cloud provider side: These attackers can log into network communication.
- Cloud provider itself: if the Cloud provider is intruder, then he can read unencrypted, make copies of user data and monitor client communication.

In step II, we examine the client's assets. Broadly speaking client asset involves client data, which resides on Cloud servers. Client needs Confidentiality, Integrity & Availability (CIA) of his information. Now what does CIA mean in Cloud Computing?
Confidentiality means to prevent disclosure of Cloud client information to unauthorized person or system. Integrity means the client data store on Cloud cannot modify. Availably means Cloud infrastructure such as SaaS and PaaS must be available when it is needed by user.

In step III, we analyze the potential threats facing client data in Cloud computing environment. Then we present each threat in a table along with it level of risk in Cloud Computing scalable threats are:

- Spoofing Identity Theft: This refers to Man-in-Middle attack. Attackers may use IP spoofing, MAC spoofing or ARP spoofing to sniff the client data on Cloud network and to modify the packets.
- Data Tampering Threat: Data Tampering can be employed by intruders to surreptitiously change personal or business data of Cloud client.
- Repudiation Attack: In this attack unauthenticated person demands the services of Cloud.
- Information Disclosure on up/download Intra-Cloud: This issue allows remote attackers to disclose the sensitive information of Cloud client. Moreover, in some cases, Cloud provider sells the information of client or use itself.
- Denial of Services Attack: In DoS attack, attackers attempt to make Cloud resources unavailable to its intended users.

- Lock- in: Now it is difficult for a Cloud customer to migrate one provider to another. Currently, Cloud provider has a lack of security tools, procedures or standards that could guarantee data and service portability.

The following table shows the risk assessment of above threats and purposed mitigation techniques. In compiling estimated risk level, we surveyed existing work on cloud security risks and mitigation including Security Guidance for Critical Areas of Focus in Cloud Computing and Assessing the Security Risks of Cloud Computing.

Table 1: Potential threat with risk assessment

Threat Type	Risk Level	Mitigation technique
Spoofing Identity Theft	Medium	Authentication Don't save secrets
Data Tempering Threat	Medium	Authorization EAP
Repudiation Attack	High	EAP Timestamps
Information Disclosure Threat	High	Authorization Encryption
DoS Attack	High	Authentication Authorization
Lock- in	High	Authentication Encryption

3.2 Section II

Now Cloud Computing threat model helps in giving appropriate solution and security countermeasures. Table 1 depicts that using strong encryption and authentication protocols can prevent the discussed threats. We purpose Extensible Authentication Protocol (EAP) for Authentication and RSA for encryption of client data.

First, we discuss that how EAP will implement on Cloud environment for authentication purpose. However different categories EAP are classified by authentication method. For instant one category user name and password while other use X.509 certificate for authentication. In our purposed model we use Challenge-Handshake Authentication Protocol (CHAP) for authentication. When client demands data or any service of cloud computing. Service Provider Authenticator (SPA) first requests for client identity. The whole process between client and Cloud provide explain in a figure given below.

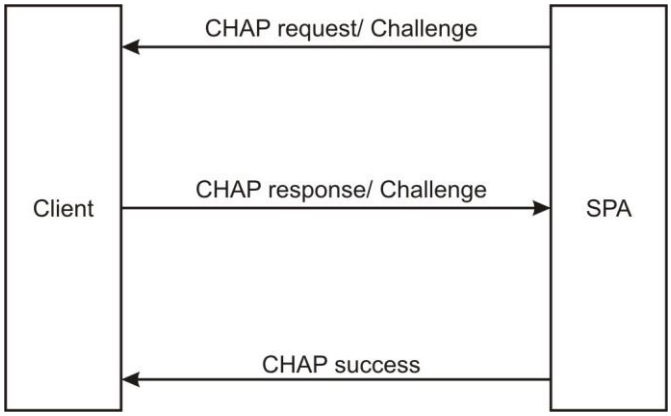


Fig 1: Implementation of CHAP in Cloud Computing.

Authentication of CHAP performs in three steps

- When client demands a service, Service Provider Authentication sends a "challenge" message to client.
- Client responds with a value calculated by using one way has function on the challenge.
- Authenticator checks the response value against its own calculated hash value. If values match, the Cloud provider will give service, otherwise it should terminate the connection.

Implementation of EAP-CHAP in Cloud Computing will solve the authentication and authorization problems. The impact of this: it subjugates Spoofing Identity Theft, Data tempering threat and DoS attack.

Second, we require strong encryption algorithm in Cloud environment. So that data transfer between client and Cloud provider and Client data reside on Cloud server, must be in encrypted form. In our research we support asymmetric key encryption (RSA) encryption algorithm for cryptography. In RSA, anyone can encrypt messages using the public key, but only the holder of the paired private key can decrypt. Security depends on the secrecy of that private key and two parts of the key pair are mathematically linked.

It is unlikely Cloud Computing can completely prevent unauthorized to transmission medium and on Cloud server. It is more practical way to protect information is to alter it so that only an authorized user can read it. Data Tempering & Information Disclosure are not new issues to computer era. So RSA encrypted communication should be held between Cloud provider and Cloud costumer. Furthermore, client data on Cloud data base must in the form cipher text by using same algorithm. Implementations of EAP with RSA in Cloud computing control the above discussed threats and provide better security.

4 Conclusion

Cloud computing is fast growing technology used by modern world but needs to be covered some open area which is affecting its robust features. In our survey we come to this point that users have very serious concerns about its open nature of privacy and security. As well as we analysis the cloud nature and list out some categories of threats that needs to be address. Security depends upon the way Cloud service provider allows its client to come and get registered with his cloud network. EAP-CHAP and RSA are best solution to provide to any type of Cloud customer. Moreover, they will use low as compared to previous one.

5 Future Works

The future work is to research every component of the secure architecture in detail, develop a prototype system and use simulation result for the verification of theory. Furthermore we will define a central/ combine law so that all stock holders implement their country law in it.

References

[1] Mayayuki Okuhara , Tetsuo Shiozaki , Takuya Suzuki. "Security Architectures for Cloud Computing", 2009.

[2] Dai Yuefa, Wu Bo, Gu Yaqiang, Zhang Quan, Tang Chaojing , Proceedings of the 2009 International Workshop on Information Security and Application (IWISA 2009) , ISBN 978-952-5726-06-0.

[3] http://www.guardian.co.uk/technology/blog/2010/sep/21/twitter-bug-malicious- exploit-

[4] Balakarishnan.S, Saranya.G, Shobana.S, Karthikeyan.S "Introducing Effective Third Party Auditing (TPA) for Data Storage Security in Cloud", IJCST Vol. 2, Iss ue 2, June 2011.

[5] Joshi Ashay.M et al, "Enhancing Security in Cloud Computing", ISSN 2224-5758 (Paper) ISSN 2224-896X (Online) Vol 1, No.1, 2011

[6] Richard Chow, Markus Jakobsson, Ryusuke Masuoka, Jesus Molina, Yuan Niu, Elaine Shi, Zhexuan Song. "Authentication in the Clouds: A Framework and its Application to Mobile Users", CCSW'10, October 8, 2010, Chicago, Illinois, USA.

[7] Honywei Li, Yuanshun Dai, Bo Yang. "Identity-Based Cryptography for Cloud Security".

[8] Dai Yuefa, Wu Bo, Gu Yaqiang, Zhang Quan, Tang Chaojing. "Data Security Model for Cloud Computing", ISBN 978-952-5726-06-0, Qingdao, China, November 21-22, 2009.

[9] Qiu Xiu-feng, Liu Jian-Wei, Zhao Peng-Chuan. "Secure Cloud Computing Architecture on Mobile Internet", IEEE 2011.