International Journal of Advanced Research Methodology in Engineering & Technology, ISSN 2456-6446
Volume 1, Issue 5, December 2017.

SRP Based Shared Resource Protecting in Cloud Environment

Mr. Dhinakaran. K
Department Of Computer Science and Engineering,
Rajalakshmi Institute Of Technology,Chennai,
maildhina.k@gmail.com

Ms. Harshatha.J
Department Of Computer Science and Engineering,
Rajalakshmi Institute Of Technology,Chennai,
harshatha.janarthanan@gmail.com

Ms. Kirtana.K.R
Department Of Computer Science and Engineering,
Rajalakshmi Institute Of Technology,Chennai
kirtanaravichandran@gmail.com

Ms. Harini.G
Department Of Computer Science and Engineering,
Rajalakshmi Institute Of Technology,Chennai
harinigopal96@gmail.com

***ABSTRACT*— The cloud computing is the predominant change happening in the domain of information technology. At present a major concern in cloud adoption is towards its security and privacy. In the advancement of cloud computing the application part of virtualization eventually increases, the scope of the security and privacy gradually expands. The users avail the cloud technology for two major factors that is Data privacy and security. Cloud security delivers all the services based on users need-firewalls, URL filters, sandboxes, SSL inspection, antivirus and the rest in a unified platform .It is a airtight security without the cost and complexity of appliances which closes the security gaps created by BYOD and mobility. Even though cloud computing provides security there are some backlogs.The lack of data redundancy and compliance standards risks the cloud security.This paper presents the security algorithm by using SRP protocol which is a strong authentication protocol(one time guess per connection attempt) that resist all wellknown active and passive attack over the network.**

Keywords: cloud computing ,cloud severs, SRP, security ,authentication, virtual machine

I. INTRODUCTION

The challenges in the cloud computing is majorly falls into three categorized as follows: Data Protection. User Authentication ,Disaster and Data Breach. Data Protection is The strategy used for Implementing the cloud computing is placing the critical data in the hands of third party for ensuring the data security both at rest as well as during the transmission. The data needs to be encrypted every time and the only way to ensure the encrypted data's confidentiality that resides on a storage server is for the client to manage and own the encryption keys. Second User Authentication is the data stored in the cloud are need to be accessed only by the authorized users. It is ensured by monitoring that who is accessing the companies data through the cloud and also ensures the integrity of user's authentication. The companies need to be capable of viewing the data access logs and audit trails to verify that only authorized users are accessing the data's stored in the cloud. These access logs and audit trails are need to be secured and maintained for the company needs.

Finally Disaster and Data Breach is the cloud is served as a single centralized repository for companies so, there is a risk of losing data due to natural disasters. The companies need to be aware of how their data are being secured and what measures has been taken by the service providers to ensure the integrity and availability of data's stored. When considering cloud computing providers, a company must address about the inaccessibility of data's due to data breaches or natural disasters occurred. Further, companies should have a contingency plan in the events if their cloud provider breaks or goes insolvent.

Cloud computing is basically web-based technology. It automatically upgrades at regular time periods and rolls to recent solutions so it will become an essential part to manage the data in business sectors.In recent years, nearly 85 percentage of the business sectors are using multi-cloud strategy. The cloud users mainly try to optimize the cost of the cloud and access their applications at an average of 1.8 public clouds and 2.3 private clouds. The workloads of the respondents are supervised to run 41 percent in in public cloud and 38 percent in private cloud in general cases but among the enterprises, the workloads are done 32 percent in public cloud and

43 percent in private cloud. Enterprise central IT has enhanced this year by selecting public clouds (65 percent), determining which apps move to cloud (63 percent), and choosing private clouds (63 percent).In contrast, respondents in enterprises are less likely to entrust central IT for selecting public clouds (41 percent), determining which apps move to cloud (45 percent), and choosing private clouds (38 percent). Enterprise central IT has enhanced this year by selecting public clouds (65 percent), determining which apps move to cloud (63 percent), and choosing private clouds (63 percent).In contrast, respondents in enterprises are less likely to entrust central IT for selecting public clouds (41 percent), determining which apps move to cloud (45 percent), and choosing private clouds (38 percent).

In this paper, we focus on the risks in the cloud and the solutions that address these risks. Our work is structured as follows: in the first and second sections, we will define cloud computing and its various models. In the third section, we related the services that inspired cloud computing, and in the forth section, we evocate the various advantages and disadvantages of this technology. Section five exposes some challenges facing the cloud and existing solutions. Finally, we conclude with a summary and a future proposal that will be our next work in this area.

II. BACKGROUND WORK:

In this proposed system, to provide a secured communication between the data owner and user a security algorithm with SRP protocol is used. Secure Remote Protocol(SRP) is a Password-authenticated Key agreement(PAKE), mainly designed to work around patents. This protocol is used for authentication purpose, when an authorized user wants to access the data a verification process has to be done by providing the password. SRP is used to keep the password secured from the attackers. The SRP protocol is highly secured, the eaves droppers or the man in the middle can't break the information to guess the password even by using the Active and Passive attack techniques. In SRP, only one password can be guessed per connection attempt. SRP has number of desirable properties, one among them is, even one or two cryptographic primitives are used for breaking the information it is still secured.

Cloud computing will continue to have a prolonged future due to the following capabilities:

Serverless Computing:Serverless computing gaining importance these years because the user need not have to use a large amount of machines and servers worthlessly on trivial machines. it will save cost of infrastructure and operation.Amazon , IBM, Microsoft use serverless computing technology.

Providers to Focus on Long-term Customer Success: The cloud owners challenges have been reduced so they provide a notable care to their customers to provide them an effortless product services and adoption in excess limits. they also provide combined services for easy working to produce maximum productivity. Security among the transactions in reliability and transperancy has been enhanced which improves the customers support.

Cloud Monitoring as a Service: The enterprises use cloud monitoring as a **service (CMaS)** feature to supervise their resource and infrastructure which leads to:

(1) End-to-end monitoring: monitoring the resources and infrastructure of the cloud continuously.

(2)providing optimal performance for the IT infrastructure

(3) Delivering the issues in the infrastructure is immediately identified by the cloud administrators and solutions are found.

The Multi-Vendor Approach: The enterprises have shifted to the multi-vendor approach because they can choose the best fit solutions among many cloud providers. as multi- vendor approach uses both public and private clouds, it is indispensible to follow a particular solution.

Securing and Auditing Services: when enterprises move the data between clouds it can be hacked so they try to safeguard their data from being hacked.according to the General Data Protection Regulation (GDPR), integrating and enhancing the data protection is very essential.the data governance policy is handed over during the auditing policy.

III. PROPOSED SYSTEM:

In the shared resource technology there is only one physical server and many virtual machines where all the data in the cloud are stored. A single

user can access all the information in the physical server. Due to this, a user can loot ,modify,delete other users data. Hence, there is no security for the stored data. The proposed system, tries to overcome the data insecurity using SRP protocol.

The architecture allows the user to login into the cloud using an authentication. Only the authorized users can be allowed to access the data stored in the cloud. If the authentication fails the user will be considered as an attacker. In the second stage the architecture uses a security protocol (SRP) for password security in which the user is allowed to guess the password for only one wrong attempt. Above the security protocol layer the virtual machine instances are placed. A set of virtual machines form the cloud network and the data stored in the physical server can be accessed across all the virtual machines. The user can create a virtual machine instance and access the virtual machine. The final stage in the architecture is the application. The instances are interfaced with the user applications.

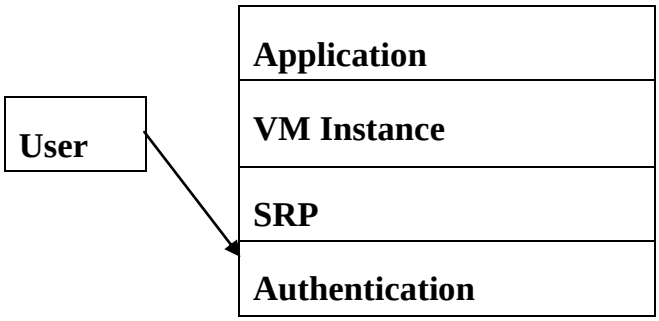

Fig: Architecture using SRP Protocol

SRP ALGORITHM:

The algorithm bellow describes the implementation of Secure Remote Password protocol (SRP). The algorithm describes a simple client-server(cloud) communication where the client needs to authenticate (user name + password) before entering into the the service. Once the authentication is complete the further communication is encrypted using the key 'k' which was calculated during the authentication process and the key 'k' unique for each and every connection.

STEPS:

1. Initially generates key k randomly using M,g parameters

   Where,

   M=large prime number, g=2

   K=hash(M,g)

2. In the client side before login generates a random secret ephemeral value 'a' and calculates a public ephemeral value 'A' using the value 'a'.

   A=(g^a) %M

After calculating the values the login request (username, A) will be sent to cloud server.

3. In the cloud sever side verifies the received request by retrieving salt 's' and verifier 'v' from database.
4. As same in the client side server side also generates a random secret ephemeral value'b' and by using the value 'b' public ephemeral value 'B' is calculated.

   B=[K*V+((g^b)%M)]%M

5. Then calculates scrambling parameter 'u', session key 'k' and stores [A,B,K,S] for later use.

   U=hash(A, B)

   S= [(A*((V^u]%M))^b]%M

   After the calculation login response (s,B) is sent to the client.

6. In client side after receiving the login response scrambling parameter 'u', private key 'X' and session key 'K' is calculated.

   U=hash (A, B)

   X=hash (S, password)

   S=[(B-K*(g^X%M))^(a+u*X)]%M

7. Now, the client sends the message M1 to the server to prove that it has correct key K.

M1= hash (A,B,K)

8. The server calculates the message M1 and then verifies it by equating the calculated message M1 and the received message M1 from the client.

   M1= hash (A,B,K)

   If received M1== calculated M1

   The client is authenticate

   If not

   The client is not authenticated.

9. The authenticated client only can do the further processes.

IV. IMPLEMENTATION:

The proposed work cloud security is achieved by first creating and configuring Amazon Web Service account. Then EC2 instance is launched for ubuntu 14.04. After the launch of ubuntu, SRP plugin is created which provides the user with only one wrong guess thus enhancing the security in the client side. In the server side, a new windows server 2008 instanced is launched and then the user applications.

V. CONCLUSION:

The usage of cloud computing is tremendously increasing due to its services in mobility and considered to have a prolonged future. In the proposed model, the shared resources between the cloud provider and the tenant are secured based on authentication checking using the SRP protocol. In future the data security can be enhanced in public and private cloud.

VI. REFERENCES:

(1) The Research of Data Security Mechanism Based on Cloud Computing by Changyou Guo and Xuefeng Zheng published on International Journal of Security and Its Applications Vol. 9, No. 3 (2015).

(2) Data Security and Privacy in Cloud Computing by YunchuanSun,1 JunshengZhang,2 YongpingXiong,3 andGuangyuZhu4 on International Journal of Distributed Sensor Networks Volume 2014.

(3) Cloud Computing And Security Issues In The Cloud by Monjur Ahmed and Mohammad Ashraf Hossain on International Journal of Network Security & Its Applications (IJNSA), Vol.6, No.1, January 2014.

(4) Security Issues with Possible Solutions in Cloud Computing-A Survey by Abhinay B.Angadi, Akshata B.Angadi and Karuna C.Gull on International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 2, Issue 2, February 2013.

(5) A Survey on Security Issues and the Existing Solutions in Cloud Computing by Y. Ghebghoub, S. Oukid, and O. Boussaid on International Journal of Computer and Electrical Engineering, Vol. 5, No. 6, December 2013.

(6) Cloud Computing: Security Issues and Research Challenges by Rabi Prasad Padhy , Manas Ranjan Patra and Suresh Chandra Satapathy on IRACST - International Journal of Computer Science and Information Technology & Security (IJCSITS) Vol. 1, No. 2, December 2011.