European Journal of Molecular & Clinical Medicine
ISSN 2515-8260 Volume 7, Issue 4, 2020

VM based Shared Resource Protecting in Cloud Environment

Subbiah Swaminathan[1], Gnanavel R [2], Duraimurugan N[3]

[1]*Professor, Department of Computer Science and Engineering, Saveetha school of Engineering,Saveetha Institute of Medical and Technical Sciences, Chennai, India.*

[2]*Assistant Professor, Department of Computer Science and Engineering, Rajalakshmi Institute of Technology, Chennai, India.*

[3]*Assistant Professor, Department of Computer Science and Engineering, Rajalakshmi Engineering College, Chennai, India.*

E-mail: subbussp2007@gmail.com

Abstract. Cloud computing is the prevalent change occurring in the area of data innovation. At present a significant concern in cloud appropriation is towards its security and protection. In the progression of distributed computing the application part of virtualization in the long run builds, the extent of the security and protection steadily extends. The clients profit from cloud innovation for two main considerations that are Data protection and security. Cloud security conveys all the administrations dependent on clients need-firewalls, URL channels, sandboxes, SSL assessment, antivirus and remaining in a unified platform. It is an airtight security without the expense and multifaceted nature of apparatuses which shuts the security holes made by BYOD and portability. Despite the fact that distributed computing gives security there are some backlogs. The cloud security is hazards due to absence of information excess and consistency. Here, it represents the calculation of security by utilizing SRP convention which is a solid confirmation protocol (one-time guess per association endeavour) that oppose all well-known dynamic and detached assault over the system.
Keywords: cloud, cloud severs, SRP, security, authentication, virtual machine

1. Introduction

The major challenges in the cloud computing is categorized into three. They are Data Protection, User Authentication, Disaster and Data Breach. Data Protection is the process for implementing the cloud computing. Here the data is handled to the third parity for providing the enhanced security when it is at rest as well as during transfer of data. The encryption of data must be done for every and only way to verify the confidentiality of encryption that belongs to the server storage to manage and own encryption keys. The next challenge is user authentication which allows only the authorized user to retrieve the data which is stored in cloud. It is ensured by monitoring that who is accessing the company's data and also make sure about the probity of user's authentication. Here the companies should keep track of their data in the cloud that only the authenticated users alone accessing it by verifying the access logs and audit trails which are maintained securely by companies for future requirements.

Another challenge is Disaster and Data Breach. If the company is provided with single centralized storage repository in cloud, then there occur any natural disasters there may be risk of losing of data. So, the companies should have conscious to store their data with high protectivity and they need to ensure how the providers are providing such security to the data. When considering cloud computing providers, a company must address about the inaccessibility of their data, expose of confidentiality of data and storage of data during natural disasters. Further, companies should have a plan what if these above-mentioned issues happen or during the cloud provider breakdown.

Cloud computing is delivery of hardware and software services over the internet. It gets updated regularly with latest technology, more flexible to work, reduces the cost rather than the managing and maintaining the IT systems. So, in business sectors cloud computing technology is used. In recent years, nearly 85 percentage of the business sectors are using multiple cloud computing technology. The users mainly try to reduce the cost of the cloud and use their applications at an average of 1.8 in public clouds and 2.3 in private clouds. The workloads of the respondents are supervised to run 41 percent and 38 percent in public cloud and private cloud respectively in general cases, but among the enterprises, the workloads are done 32 percent in public and 43 percent in private cloud. Further enterprise central IT has enhanced the percentage of use in cloud as 65 percent in public cloud and choosing the private cloud in 63 percent. In contrast, respondents in enterprises are less likely to entrust central IT for selecting public clouds for 41 percent, 45 percent of determining which apps move to cloud, and 38 percent in choosing private clouds.

In this paper, it examines the problem in cloud and the solution to sort out those issues. The work is explained as sections. In first two section, it describes about the cloud computing technologies and varies approaches that are used in this field to enhance their usage with high security of data in cloud. In the third section, it explains about the features that are involved in propounded systems. In forth section, the discussion is made on merits and demerits of cloud computing technology. Section five exposes some challenges facing in cloud, its existing solutions and implementation of the innovation. At last, it is concluded with future work that need to be done in this are for enhancing the technology.

2. Background work

The proposed system, a secured communication is provided 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 copyrights. This protocol is used for authentication purpose, when an user need to access the data, verification must be done on the user by providing the password. SRP is used to keep the password secured from the hackers. The SRP is the most secured medium where no one can break the security by guessing the password even though the active and passive techniques are used. In SRP that provide security that allows user to attempt the wrong password only once. 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.

The concept of cloud computing technology is said to be prolonged due to the following capabilities:

2.1. Serverless Computing

Serverless computing gaining importance these years because in cloud all the services are provide through internets. So, there is no need of large number of machines. it will save cost of infrastructure and operation. Amazon, IBM, Microsoft use serverless computing technology and also called as cloud service providers.

2.2. Providers to Focus on Long-term Customer Success

The cloud owners' challenges have been reduced. So, they focus on the customers' requirements and provide them the requiring product services. And it made more versatile for everyone. And to maximize the productivity they allocate combined services also. Security among the transactions in reliability and transparency has been enhanced which improves the customers support.

2.3. Cloud Monitoring as a Service

Many organizations use cloud monitoring as a **service (CMaS)** used to oversee 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) Any fault occurs in infrastructure or cloud, they are identifying instantly and rectified by the cloud admin.

2.4. The Multi-Vendor Approach

it uses both public and private clouds, so the enterprises have shifted to the multi-vendor approach. it is indispensable to follow a particular solution.

2.5. Securing and Auditing Services

The data is transferred between the clouds by the enterprises. During this transfer there is a possibility of hacking so they try to safeguard their data from being hacked. according to the General Data Protection Regulation (GDPR), integrating and enhancing the privacy of data is necessary.

3. Proposed system

In the shared resource technology, it has number of VMs with single physical server. Here, every data is stored in the cloud. In this, an individual user can access every information in the server. Because of this there is chance for loot, or theft of information, modifying, or misusing of data may happen. Thus, this leads to the insecurity of the data. To get a better of these issues the propounded system uses the SRP protocol.

The first layer in architecture of propounded system is authentication that allows only the authenticated user to login in cloud. So that, the accessibility of data in the cloud is provided only to the authorized user. If the verification of user is failed, then they are said as hackers. And the next layer is SRP layer which is a security protocol layer that provide security that allows user to attempt the wrong password only once. VM instance are placed over the security protocol layer. Here data of a VM can be accessed by all other VMs in the physical server in cloud network. The virtual machines are accessed only by their instances. All the above layer is application where the instance is interfaced with the user application.

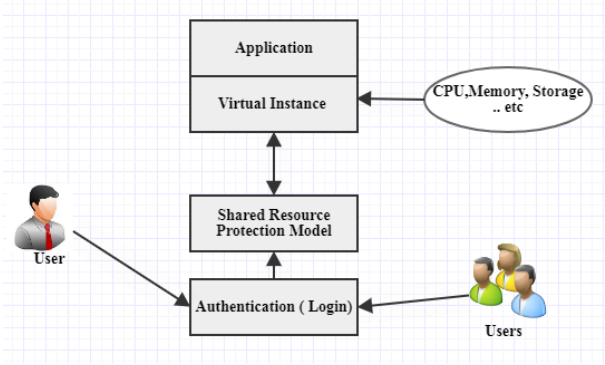

Fig: Architecture using SRP Protocol

4. SRP Algorithm

The algorithm bellow describes the implementation of Secure Remote Password protocol (SRP). The algorithm describes a simple client-server(cloud) communication where a small authentication process is carried out by entering username and password that allows access to the services.Upon authorization, the username and passwords are encrypted using key ‘k’ which is distinctive for each and every connection.

STEPS:

1) Initially generates key k randomly using M,g parameters
    a. Where,
    b. M=large prime number, g=2
    c. K=hash(M,g)

2) Before login by the customer, ephemeral value ‘a’ is generated from which the public ephemeral value ‘A’ is computed.
    a. A=(g^a) %M
    b. After calculating the values, the login request along with username and public ephemeral value as (username, A) send to the server of cloud.

3) Then the verification is done with the request from the customer side in the server side. By the verification, the value of ‘s’ and ‘v’ is obtained from the database. S denotes to salt and v denotes to verifier.

4) Similarly, secrete ephemeral value ‘b’ is created from which the public ephemeral value ‘B’ is calculated in customer side.
    a. B= [K*V + ((g ^ b) %M)] % M

5) After that, the parameters ‘u’, session key ‘k’ are calculated and stores the values A, B, K, S for future use.
    a. U= hash (A, B)
    b. S= [(A*([V ^ u] %M)) ^ b] % M
    c. Login response of s and B, (s, B) is sent after the computation.

6) After receiving login response, scrambling parameter ‘u’, private key ‘X’ and session key ‘K’ is calculated in customer side.
    a. U=hash (A, B)
    b. X=hash (S, password)
    c. S= [(B-K*(g ^ X%M)) ^ (a + u *X)] % M

7) Now, the message is sent from the client to the server in order to prove correct key K.
    a. M1= hash (A, B, K)

8) The message M1 is computed by server and then verifies it by equating the calculated M1 and the received M1 from the client.
    a. M1= hash (A,B,K)
    b. If received M1== calculated M1
        i. The client is authenticating
    c. If not
    d. The client is not authenticated.

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

5. Implementation

The proposed work cloud security is achieved by first creating and configuring Amazon Web Service account. For launching ubuntu 14.04, EC2 instance is initiated. At the next, SRP plugin is created. This plugin provides enhanced security for the customer by allowing user with single wrong guess. In the server side, a new windows server 2008 instanced is launched and then the user applications.

6. Conclusion

The usage of cloud computing is tremendously increasing due its versatile and prolonged services. In this propounded paper, SRP protocols is used for the authentication while resource sharing is done between the provider and customer requested for services in cloud. Additionally, the improvement in data security are done in both public and private cloud environment. In the future the same SRP protocol will be applied in the container services.

References

[1] Security as a Service Model for Cloud Environment by Vijay Varadharajan and UdayaTupakula published on IEEE Transaction on Network and Service Management, Vol. 11, No. 1, March 2014.

[2] Multilevel classification of security concerns in cloud computing by Syed Asad Hussain a, Mehwish Fatima, Atif Saeed, Imran Raza, Raja Khurram Shahzad on Applied Computing and Informatics Volume 13, Issue 1, January 2017.

[3] Cloud Hooks: Security and Privacy Issues in Cloud Computing by Wayne A. Jansen on Proceedings of the 44th Hawaii International Conference on System Sciences – 2011.

[4] Intrusion Detection Techniques in Cloud Environment: A Survey by Preeti Mishra, Emmanuel S. Pilli, Vijay Varadharajan, Udaya Tupakula Published on Journal of Network and Computer Applications, Vol.77, January 2018.

[5] A VMM-based intrusion prevwntion system in cloud computing environment by Hai Jin, Guofu Xiang, Deqing Zou, Song Wu, Feng Zhao, Min Li, Weide Zheng on the journal of supercomputing 66, 1133-1151-(2013).

[6] Cloud Computing Risk Assessment: A Systematic Literature Review by Rabia Latif, Haider Abbas, Saïd Assar, and Qasim Ali on Future Information Technology pp 285-295, 2014.