ORIENTAL JOURNAL OF
COMPUTER SCIENCE & TECHNOLOGY
An International Open Free Access, Peer Reviewed Research Journal
Published By: **Oriental Scientific Publishing Co., India.**
www.computerscijournal.org

ISSN: 0974-6471
June 2017,
Vol. 10, No. (2):
Pgs. 460-466

A Tpa-Authentication Scheme for Public Cloud Using Kerberos Protocol

ARPIT AGRAWAL and SHUBHANGI VERMA

[1]Lecturer, IET DAVV Indore, M.P.
[2]IET DAVV Indore, M.P.
Corresponding author Email: Shubhangi.verma.iet@gmail.com

http://dx.doi.org/10.13005/ojcst/10.02.29

(Received: May 08, 2017; Accepted: May 25, 2017)

ABSTRACT

Cloud computing is the new generation technology provides the way of sharing of resources, memory, software anything in the form of service using internet. Security is an important and unique phenomenon gives safe and isolated environment. Security model and principles are defined to implement security features with any applications. Confidentiality, authentication and integrity are primary principles for trust establishment. Existing work only concentrates on integrity concept and does not imposes for authentication or access control. A Kerberos based strong authentication scheme has been generated using third party auditing concept to improve the strength of authentication as well as trust on CSP. This work will implement security service architecture to create Kerberos environment and establish communication between Kerberos and CSP. The complete work will be implemented using Java technology and Open Stack serve for public cloud environment.

Keywords: Cloud computing, TPA, Kerberos, CSP.

INTRODUCTION

Cloud computing is an art of computer science which provides all the capabilities like services, platform and infrastructure. Cloud providers provide all this services. The aim of cloud computing is to have resource consumption is minimize way. The cloud computing makes desktop just an application using platform. All the services, which are available in any desktop, can be used in cloud. The profit of cloud is that it provides all the services hence one need not to install it on their machine. This will lead to minimization of memory consumption. Depends on what one will need, the services can be asked for. Some cloud gain economy just by their access whereas other cloud access can be done by having certain charges. The charges can be weekly, monthly or yearly depends on what user has selected.

The use of cloud computing can be realized at times whereas at times it is also possible

that it may not be known. In Gmail when we open any pdf within it, it is one of the cloud services. Any online editor for document creation as well as the sources for listening songs can be part of cloud. Any technology for development of websites at online level can be example of platform as a service. From government to small-owned startup everyone uses cloud services to minimize other resource utilization. Following are the facilities, which can be used in cloud:

1. Development of web services and different applications
2. Storage, retrieval and backing up of data
3. Websites hosting and blogs
4. Stream auditory and video techniques
5. On demand delivery of software

- In data mining for analysis of patterns and predictions. Performance
- Reliability

Types of cloud services

1. IaaS
2. PaaS
3. SaaS

Cloud computing can be majorly divided into three categories IaaS, PaaS, SaaS. IaaS stands for infrastructure as a service, if cloud is demanding for facility of infrastructure then it is called as Infrastructure as a service. PaaS stands for platform as a service if cloud services are used to have platform then it is called as PaaS. SaaS stands for software as a service, if software are used as a service of cloud then it can be said that it is using software as a service.

Business goals decide which protocol stack of cloud is to be used. Depends on the need the stack is formed. There may be organizations, which will just need SaaS, there may be other which need PaaS as well. After some time organization will need IaaS also.

Infrastructure-as-a-service (IaaS)

Infrastructure include virtual machine, virtual machine is having operating system virtually. There may be certain part of operating system which you may not need therefore cloud provider charge according to the need.

Platform as a service (PaaS)

Platform as a service (PaaS) provides platform for designing various applications. If one is developing web applications, the platform can be used to have its services. It is not necessary that it provide development environment only, it will also provide tools for designing, testing, support also. Hence if any person doesn't need have available resources then it can use the services of the cloud.

Platform-as-a-service (PaaS) provides the user capability of the accessing the environment without having it permanently

Software as a service (SaaS)

SaaS can be defined as software as a service, hence the cloud provide software which

Fig. 1: Cloud Computing Services

will be needed can be used by the user as per the need. It may be possible that your terminal will not have any upgraded software whereas the cloud can have the upgraded version. This software can be accessed from any devices like tablet, mobile or computer. Software can be used for retrieving data.

Types of cloud deployments

1. Public,
2. Private,
3. Hybrid

Different variety of cloud are present which are public cloud, private cloud and hybrid cloud

Public cloud

Public cloud are service provider, this are third-party cloud. Public cloud provide the facilities inside the network as well as outside the network. Microsoft Azure is one of the public network. Cloud provider managed all the services, quality and software. Web browser are used for accessing this services to have an account.

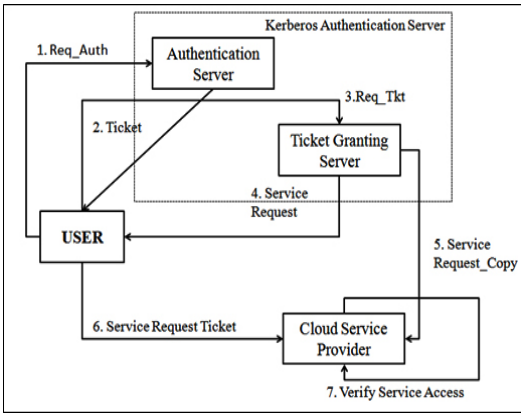

Fig. 1: System Architecture

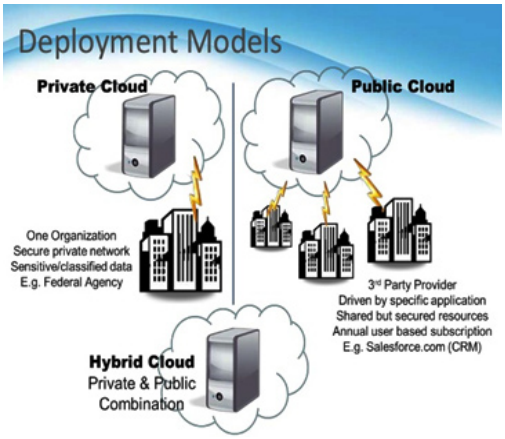

Fig. 2: Deployment Models of Cloud Computing

Private cloud

A private cloud is kind of cloud which is used inside an organization. It is possible that if the cloud is present in same site as well as it is also possible that it can be present at some other site but within the same organization. Some large organizations also have their own data centers where all the data of organization is kept. A private cloud can provide services and infrastructures.

Hybrid cloud

Hybrid cloud is combination of public and private cloud. The data can be share between public and private cloud. The flexibility of sharing services and infrastructure is present. Hybrid cloud allow to access data outside and inside the organizations hence are highly flexible the resource which can be access inside the network are used and resource which are not available in the organization can be accessed outside using public cloud.

Related Work

As the clouds are known to provide all the services, the security is never the concern in initial. Lot of work is being done in this field. Salah H. Abbdal et al. proposed the work in which cloud computing is explained as technique for resource sharing in information technology. The concept behind cloud computing is on the basis of use the resource can be used and paid. The concept lead in reducing computation cost and communication cost hence attracting the huge crowd in network. Cloud storage is remotely available servers where data can be stored and it is one of the most widely used cloud service. In such services the security is major issue as in information retrieval the only need is storage at other side. At initial cloud providers never think of the security threats which can occur while communicating data. It is possible at times services can be unreliable.

When data is stored and data centers in cloud doesn't care about security. In integrity achieving which is one of the security principle can

be achieved using third party auditor. However this idea is not always good as all the resources will rely on the one third party tool. This will degrade the performance of network as well as increase the computation overhead. The given research uses the concept of multiple integrity scheme, therefore the security maintenance is quite comfortable as the security achievement can be from multiple points. Thus overhead consumption will decrease with the time. In it the authentication is provided using linear authentication. The algorithm used in elliptic curve digital signature algorithm. For storing of data Merkle hash tree are used and the technique will be capable of gaining more security. This scheme will provide more secured data.

The given solution is described in below architecture

Amit Joshi et al combines randomized motion and hierarchical key based security in cloud architecture. It also specifies the barriers in cloud architecture and security techniques which can be used in cloud based environment. Comparison of all the security models is done in order to get the pros and cons of the architecture. The analysis of facts related to it done in the form of grid and success rate is compared.

Mehdi Hojabri et al[3] presented an architecture in which third party authentication scheme is used. In cloud based architecture entire storage and processing is performed at cloud

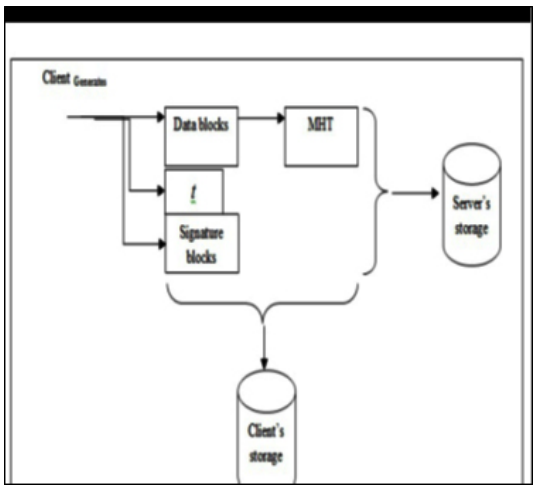

Fig. 3: Block Representation of Proposed Solution

level. Hence whenever user access any data the insertion, deletion, updation are performed using it. The correctness of data used can be checked from the security technques applied. The third party authenticator used in our scheme is Kerberos. Before having authentication the registration must be performed. In this once the registration process is performed then authentication will be done in order to have the security. The process like qualification is performed after this, which is one the step involved in Kerberos. Hence the Kerberos is step wise authentication scheme.

Kerberos Authentication Scheme

One of the well-known security protocol which will provide authentication is Kerberos. It can be used in distributed architecture as well as in centralized architecture. But it is design for distributed environment mainly. Initially the password is created by user which is called as long term secret key. Each client will have TGT which is commonly known as ticket granting ticket from authentication server (AS). This TGT can be used in multiple servers as this TGT will be used to verify client. Once the TGT is received from server then the client demands for Service granting ticket. The database stores the assigned entities of user.

Whenever we want to access any data the Service-granting –ticket will demand the password every time. The key distribution center is collection of authentication server, ticket granting server and database. The AS is responsible for ticket granting to all the user and TGS is responsible for Service granting ticket to user.

The authentication can be perform in following steps in Kerberos

a. Initial logging is perform in the workstation, the message is send to authentication server for request of granting ticket.
b. The checking in authentication server is performed, which check the data being feed by the user. If data input is correct then it assign TGT to user and also a session of user is also decide using key. In that session time the user can communicate to server.
c. Same copy of session key is also included in the ticket that AU issues to the client.

d. The key is kept by both which is client and server both.

Both TGT and session key is then encrypted using password of the user. As the encryption is performed using the key of user there are no chances that any other person can access it. As the key is known to both nobody else can access it.

Limitations

1. In an untrusted network entire operation is performed hence using an untrusted host the operation is performed it may be possible that the host itself is untrusted.
2. The password if relocated in some other place will be dangerous in Kerberos.

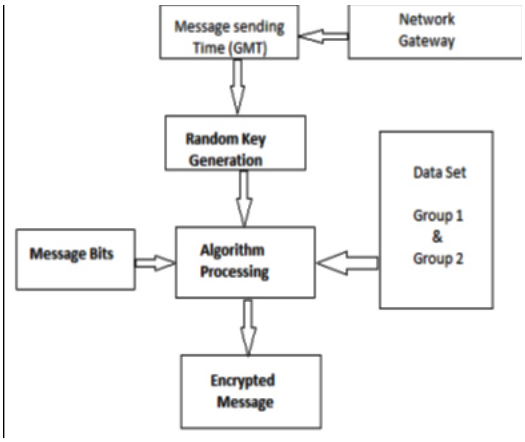

Fig. 4: Block Representation of Joshi Scheme

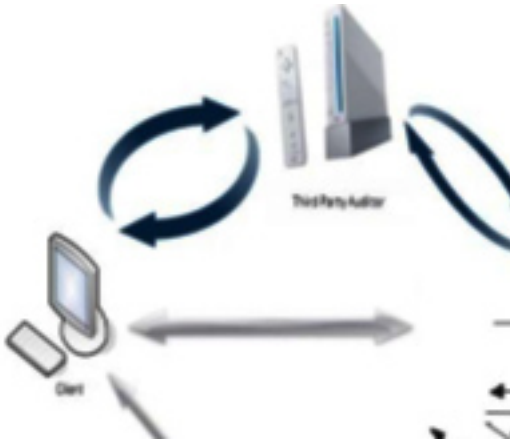

Fig. 5: Kerberos based authentication scheme

3. For using Kerberos, its libraries need to be used. The source should to be available to make such calls.
4. Kerberos never allow the unencrypted transfer of password but if required the Kerberos aware that it is just at own risk.

Problem Statement

Cloud computing is one the most widely used of network. Some use its services, while other use it platform. The accessing should be such that the servers are available at some other location. Cloud providers initially taken into account also accessing but not the security. Thus some mechanism should be their which will provide security to cloud users and servers. This security should be in the form that it provides security features like authentication, non-integrity, availability. The security should provide features like encryption.

Authentication is mechanism of assuring that the request is from the intended sender only and no interference by any intruder is performed. If sender and receiver doesn't have any way of getting the assurance of trust between both then no third party will be capable of providing as well. Authentication is the method with dependency of asset value and risk. Just authentication is no much secure. Some Weak Authentication is the authentication between third parties. In security if not provided properly is always risk to the user. With increase in risk the security threat enhances. The factor should be kept in mind of researchers and

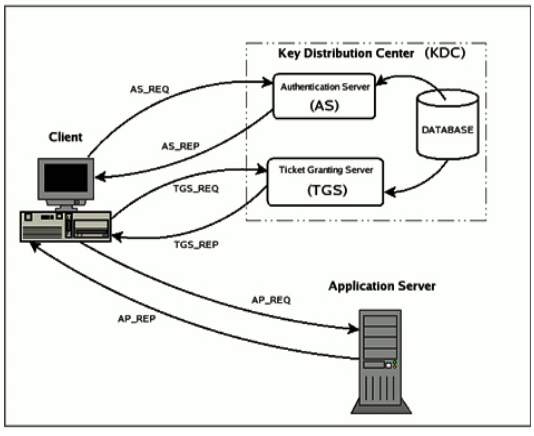

Fig. 6: Kerberos Architecture

certain protocol are designed. Hence authentication is very much required in safety of account.

There are many security mechanism applied in it. Integrity and several other security mechanisms. Certain techniques are used like password based, the password although can be tracked. Authentication mechanism involved variety of security like social security, third party security.

Our work observes that Kerberos is very good technique for enhancing the authentication, in this third party is used. The demand is to have Kerberos in cloud computing.

Solution Domain

As the need is, find that there is strong need for security. The need is that strong cloud computing policy with best authentication scheme should be present. In our solution, the Kerberos is used as authentication scheme to have better authentication then user and password. In our approach the hybrid security is used. Here KDS have AS authentication server and TGS which is ticket granting server.

Thus in our work the scheme is created which should have higher security to have authentication. In all the cloud based models the cloud server and client should have proper secure communication. The fine grain access control is the need of the architecture. Homomorphic encryption is designed along with the unique access structure. Access privilege and content which should be save form cloud servers.

Data isolation issues can be overcome in our work by avoiding the security breach of authentication. The work analyzed the resources, which can be used by multiple providers. It also lets the organization feel safe about their data against security breaches.

Our work enhance security by having TGS and AGS in it. It also provide features like accountability. The grant and revoking of request is given to user. Hence our solution is one step ahead of simple authentication. A block diagram to represent the same is shown in Figure 5.1.

CONCLUSION

As we conclude that security is basic need of the cloud. The given work implement Kerberos to achieve authentication for having better security. Kerberos can be merge with ticket granting approach in order to achieve security. Here in our work we suggest security it in cloud-based architecture. Future work on this paper can be given as calculation of computation time and other factors as well as implementation of given solution.

REFERENCE

1. Anurag Jain, Dr. Rajneesh Kumar "Confidentiality Enhanced Security Model for Cloud Environment" ICTCS '16, March 04-05, 2016, Udaipur, India.
2. Nasrin Khanezaei, Zurina Mohd Hanapi "A Framework Based on RSA and AES Encryption Algorithms for Cloud Computing Services" IEEE Conference on Systems, Process and Control (ICSPC 2014), 12-14 December 2014, Kuala Lumpur, Malaysia.
3. Deyan Chen and Hong Zhao "Data Security and Privacy Protection Issues in Cloud Computing" 2012 IEEE International Conference on Computer Science and Electronics Engineering.
4. Bokefode Jayant D, Ubale Swapnaja A, Pingale Subhash V, Karande Kailash J., Apate Sulabha S., "Developing Secure Cloud Storage System by Applying AES and RSA Cryptography Algorithms with Role based Access Control Model" International Journal of Computer Applications (0975 – 8887) Volume 118– No.12, May 2015.
5. Cindhamani.J, Naguboynia Punya, Rasha Ealaruvi, L.D. Dhinesh babu "An enhanced data security and trust management enabled framework for cloud computing systems" IEEE 5th International Conference on Computing, Communications and Networking Technologies July 11-13, 2014, Hefei,

China.

6. Shilpi Singh, Vinod Kumar "Secured User's Authentication and Private Data Storage-Access Scheme in Cloud Computing Using Elliptic Curve Cryptography" 2015 IEEE 2nd International Conference on Computing for Sustainable Global Development.
7. Kawser Wazed Nafi, Tonny Shekha Kar, Sayed Anisul Hoque, Dr. M. M. A Hashem "A Newer User Authentication, File encryption and Distributed Server Based Cloud Computing security architecture" (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 3, No. 10, 2012.
8. Rackspace Cloud: http://www.rackspacecloud.com .
9. Amit Joshi, Bhavesh Joshi, Manuj Joshi. An approach initiating security protocol towards cloud, International Journal of Computer applications -RTMC(7):-, May 2012. Published by Foundation of Computer Science, New York, USA.