JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Innovation in cloud computing

Azarooddin Shaikh[1], Moinatik Ghori[2]
[1] Lecturer,Department of Electronics Engineering Parul UniversityVadodara, 391760, India
[2] Sr. Software Engineer,Tata Consultancy Service,India
Ajhar89@gmail.com[1], moinghori.it@gmail.com[2]

***Abstract*_The cloud computing paradigm is considered as the next-generation of IT technology. It is also the internet based technology, where the users can share resources among the enormous cloud service provider, such as cloud partners and cloud vendors. Cloud computing makes high quality of service and high availability, so that users can simplyaccess to prefer cloud with internet device. This makes many advantages and drawbacks for the users to create and store data in the cloud service provider. One is the data management and software may not be fully trustworthy in the cloud, therefore the security is an important aspect of quality of service. The purpose of this article is to concentrate on cloud data storage security and to manage the user's data in the cloud by Implementation of kerberos authentication service. I believe this novel article is the background for the next opportunity of growing the cloud security.**

***Keywords*_kerberos authentication service ,Third party auditor, cloud service provider, cloud computing, cloud security.**

I. INTRODUCTION

Cloud computing is the rapidly growing branch in this era. As per the statistics, in 2019, the cloud computing market size was $266 billions which is continuously growing until todays date. Cloud computing prosperity brings many advantage along with drawbacks. Since, all the information is available on cloud, it becomes the most important to provide the security to the data. Several trends open up the era of cloud computing, which is an internet base development and use the computer technology [1].The most important service of the cloud computing as Software As A Service architecture. A user will pay only for the service being used. For instance, using Gmail to send the email to another person. Amazon Simple Storage Service and Amazon Elastic Compute Cloud are well known examples [2]-[3].In this paper , Firstly we have defined and introduced the users, their attributes, and their tasks. Secondly, we have introduced one application program as the third party auditor. Thirdly, we surveyed the Kerberos effect in cloud computing server. Finally, we examined the cloud server provider. Kerberos uses strong encryption and a complex ticket-granting algorithm to authenticate users on a network. Also, since many users are interested in Kerberos, it has the ability to distribute "session keys" to allow encrypted data streams over an IP network. Users who want to connect to the cloud, at first, they should make the profile and user ID in the third party. The information of all users such as User ID and hashed password will be saved in the large Data Base for more secure. After the registration inthe third party , it must get the user id and password. In the next race, it should be connected to the kerberos real and do this process[4]-[5].

- send the Request for ticket granting ticket to the As.
- As verifies user's access right in data base, create ticket-granting ticket and session key. Result are encrypted using keyderived from user password.
- user will send the request cloud service granting ticket to TGS.
- the TGS will send the Ticket + session key to the user. (it execute one per type of service).
- Workstation sends ticket and authenticator to cloud server provider.
- server verifies ticket and authenticator match, then grant access to service.

In this paper, we have tried to assume that each user who wants to connect and utilize the cloud server must create the profile and apply some private information for more secure in large data base. The rest of this paper is organized as the following: Section 2 discusses the Cloud providers, Section 3 discusses the problem statement Challenges and Issues, Section 4 discusses all process from connection till take cloud service provider.

II. CLOUD PROVIDERS

Cloud computing [6]-[7]-[8] systems generally divide into three course grain categories. Infrastructure as a service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS).

A. Infrastructure as a Service

Infrastructure as a Service (IaaS) provisions hardware, software, and equipment to deliver software application environments with a resource usage-based pricing model. User has to focus on application, data, Operating system, runtime and middleware. Rest of the aspects like virtualization, servers, storages and networking will be taken care by cloud vendors.

B. Platform as a Service

Platform as a Service (PaaS) offers a high-level integrated environment to build, test, configuration settings and deploy custom applications. User has to focus on application and data. Rest of the aspects like Operating system, middleware, runtime, virtualization, servers, storages and networking will be taken care by cloud vendors

C. Software as a Service

Software as a Service (SaaS) is a software distribution model in which User buys and Subscription to some software product applications and utilize that with some network typically the Internet. User can use the service without worrying about application, data, Operating system, middleware, runtime, virtualization, servers, storages and networking.

III. PROBLEM STATEMENT

A. *System Model*

A representation network architecture for cloud data storage with effect of Kerberos authentication service is illustrated in Figure 1.Seven different network entities can be identified as follows:

- *User:* User who should at the first refer to third party and created the account in the Third party data base and get the password, session which will store data in the cloud.
- *Cloud service provider:*Cloud service providers offer cloud solutions, like GoogleApps, that are delivered electronically over the internet. Unlike a managed service provider, cloud service providers do not sell or install hardware. Everything they offer is stored online and accessible securely from anywhere. There are many advantages to working with a cloud service provider like GCP when switching from your on-prem implementation to cloud services.
- *Kerberos operation:* Kerberos is an authentication mechanism that provides a secure means of authentication for network users. It prevents transmission of clear text passwords over the network by encrypting authentication messages between clients and servers. In addition, Kerberos provides a system for authorization in the form of administering tokens, or credentials[9].In the another define Kerberos is an authentication protocol for trusted hosts on untruste d networks.
- *Authentication service:* Authentication service that know the password of all user and stores in encrypted in a centralized database.In addition, the AS shares a unique secret key with each server.
- *Tickets granting service:* TGS provide and issue tickets to user who have been authentication to AS.
- *Data Base:* The database is the container the entries information related with users and services. The data base is shared between third party and Kerberos. We refer to an entry by using the principal even if often the term principal is used as a synonym for entry. Each entry contains the following information:
  - The principal to which the entry is associated.
  - The maximum validity duration for aticket associated to the principal.
  - The encryption key.
  - The maximum time a ticket associated to the principal may be renewed.
  - The attributes or flags characterizing the behavior of the tickets.
  - The password expiration date.
  - The expiration date of the principal, after which no tickets will be issued.
- *Third party*: The third party define who hasthe correctness, expertise, capabilities to access and utilize the cloud service provider.

B. *Design Goals*

To ensure the security of storage the data in cloud server we design efficient mechanisms with 4 part for achieve the following goals:

- Lightly the work: each user can perform storage and register in minimum time.
- Trustworthy: to ensure user that their data is store in trust manner and can execute their job in accurate type.

IV. IMPLEMENTATION OF PROCESS

In cloud data storage system, users store their data in the cloud and for accessing must refer to cloud provider. Thus, the correctness of the userbeing refer to the distributed cloud server must beguaranteed because the data stored in the cloud may frequently update with user including, insertion, deletion, modification, appending, reordering etc. To ensure this updating is undercorrectness user is important so in this paper we introduce one model based on kerberos. In thismodel each user for gain the cloud server must beregister and authentication with third party. After added the requirement information into the database it can get some qualification. Aftergetting the qualification it should refer to the kerberos authentication service and do this scenario:

In this scenario[5]

A. Each clientafter register in third party it shouldsend the requests access for a ticket-granting ticket on behalf of the user by sending its user's ID to the AS,together with TGS ID,indicating a request to use the TGS service.and following elements:
   - Realm:Represent realm of user
   - Option:Used to request that certain flagsbe set in the returned tickets,as explained in table 1.
   - Times:Used by client to request the following time setting in the ticket:
     - From:the desired start time for the requested ticket
     - Till:the requested expiration time forthe requested ticket
     - Rtime:requested renew-till time
   - Nonce:A random value to be repeated in message A assure that the response is fresh and has not been replayed by an opponent.

B. Get back a ticket-granting ticket,identifying information for the client,and a block encrypted using the encryption key based on the user's password.This block includes the session key to be used between the client and the TGS,times specified in message A,the nonce from message A,and TGS identifying information.The ticket itself include thesession key,identifying information for the client,the requested time value,and flags that reflect the status of this ticket and the requested option.

C. The client request a service-granting ticket on behalf of the user.For this purpose,the client transmits a message to the TGS containing the user's ID,the ID of the desire cloud service,andthe ticket-granting ticket.

D. The TGS decrypt the incoming ticket and verifies the success of the decryption by the presence of its ID. It check to make sure that the lifetime has not expired.Then it compares the user ID and network address with the incoming information to authenticate the user. If the uses is permitted access to V,the TGS issues a ticket to grant access to the requested cloud service provider.The service-granting provider ticket has the same structure as the ticket-granting ticket. Indeed,because the TGS is a server,we would expect that the same elements are needed to authenticate a client to the TGS and to authenticate a client to an application server.Again,the ticket contain a timestamp and lifetime. If the user wants access to the same cloud service at a later time,the client can simply use the previously acquired service-granting ticket and need not bother the user for a password.Note that the ticket is encrypted with a secret key(K_v) known only to the TGS and the server,preventing alteration.Finally,with a particular cloud servicegranting ticket,the client can gain access to the corresponding service with step E.

E. In this step,the client may request as an option that mutual authentication is required. The authentication include:
   - Subkey:The client's choice for an encryption key to be used to protect this specific application session.If this field is omitted,the session key from the ticket($k_{c,v}$) is used.
   - Sequence number:An optional field that specifies the starting sequence number to be used by the server for message sent to the client during this session.Message

may be sequence numbered to detect replays.The table 1 shows theimplementation of this scenario[5].

A. Authentication Service Exchange:in order to obtain ticket-granting Ticket 1) C → AS: OptionsID$_c$Realm$_c$ID$_{tgs}$Times Nonce$_1$ 2) ASC:Realm$_c$ID$_c$Ticket$_{tgs}$Ek$_c$[k$_{c,tgs}$TimesNonce$_1$Realm$_{tgs}$ID$_{tgs}$ Ticket$_{tgs}$=E$_{ktgs}$[Flagesk$_{c,tgs}$Realm$_c$ID$_c$AD$_c$Times]
B. Ticket-granting cloud service Exchange:in order to obtain cloud service-granting ticket 3) CTGS: Options ID$_v$Times Nonce$_2$Ticket$_{tgs}$Authenticator$_c$ 4) TGSC:Realm$_c$ID$_c$Ticket$_v$Ek$_{c,tgs}$ [k$_{c,v}$Times Nonce$_2$ Realm$_2$ID$_v$] Ticket$_{tgs}$=E$_{ktgs}$[Flags k$_{c,tgs}$Realm$_c$ID$_c$AD$_c$Times] Ticket$_v$=E$_{kv}$[Flags k$_{c,v}$Realm$_c$ID$_c$AD$_c$Times] Authenticator$_c$=E$_{Kc,tgs}$[ID$_c$Realm$_c$ TS$_1$]
C. client/Server Authentication Exchange:in order to obtain cloud service 5) CTGS: Options Ticket$_v$Authenticator$_c$ 6) TGSC:E$_{kc,v}$[TS$_2$SubkeySeq#] Ticket$_v$=Ek$_v$ [Flags k$_{c,v}$Realm$_c$IDcAD$_c$Times] Authenticator$_c$=E$_{kc,v}$ [ID$_c$Realm$_c$TS$_2$SubkeySeq#]

Table 1. Summary of kerberos message exchange in cloud service

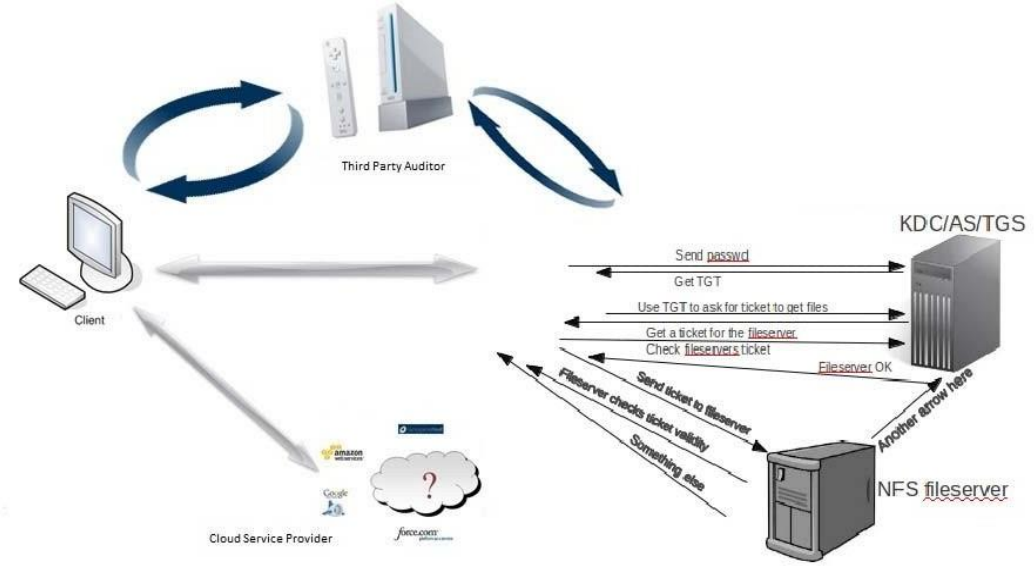

Figure 1. Cloud data storage architecture

CONCLUSION

In this paper, we have investigated the problem of data security in cloud server provider and also created one way to restrict the access to cloud server. To ensure the correctness of data users in cloud data storage and correctness of users who can access the Cloud server , we have proposed an effective and flexible distributed scheme with explicit dynamic data support, including kerberos authentication service and third party. Kerberos provides a centralized authentication server whose function is to authenticate the user to the cloudserver and the cloud server to the user. To access the cloud server ,All users should make the profile and set a password, then they can use the cloud server with some restrict which it can make by kerberos. As we know, the unique attribute of network is security, so in order to make more secure networks, we must make the way for controlling the cloud system and store the information of user’s. We want the cloud servers to be able of restricting access to authorized users and to be able of authenticating request for service. In an unprotected network environment, any client can apply to any cloud server for service ,but kerberos operation with the use of DES,in arather elaborate protocol can provide the authentication service. So in my opinion ,this task is a new strategy for enhancing the issue of security cloud computing.

REFERENCES

[1] Cong Wang,QianWang,KuiRen,”Ensuring Data Storage Security in Cloud computing”,cit by:23 IEEE International Conference on Computer and Information Technology; 2009,pp.1-9

[2] N. Gohrin “Amazon’s S3 down for several hours,” Online athttp://www.pcworld.com/business-center/article/ 142549 /amazons s3 down for several hours.html, 2008.

[3] Amazon.com, “Amazon Web Services (AWS),” Online at http://aws.amazon.com, 2008.

[4] MILL88Miller,S,;Neuman,B.;Schiller,j.;andSaltzer,j.”Kerberos Authentication and authorization System.”Section E.2.1,Project Athena Technical plan,M.I.T.Project Athena,Cambridge,MA.27 October 1998.

[5] William Stallings,”Cryptography And Network Security”,second edition,2002.

[6] John Harauz, Lori M. Kaufman, Bruce Potter, “ Data Security in the World of Cloud Computing”, IEEE Security and Privacy, July/Aug. 2009, vol. 7, no. 4, pp. 61-64.

[7] Loganayagi B, Sujatha.S., “ Cloud Computing in Stax Platform”, IEEE International Conference on Computer Communication and Electrical Technology, (IEEE-ICCCET 2011); 18-19 Mar. 2011, pp.1-5.

[8] Dawei Sun, Guiran Chang, QiangGuo, Chuan Wang, Xingwei Wang., “A Dependability Model to Enhance Security of Cloud Environment Using System-Level Virtualization Techniques”, First International Conference on Pervasive Computing,Signal Processing and Applications pcspa; 2010, pp.305-310.

[9] http://publib.boulder.ibm.com