Volume 4, Issue 3, March 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Agent Based Approach for Verification in Cloud

NAGARJUNA.T[1]
Department Of CSE, KMMITS, Tirupathi
India

KALYAN SRINIVAS C.C[2]
Department Of CSE KMMITS, Tirupathi
India

Abstract: ***Cloud computing is a new approach that brought revolution in delivering IT Services to meet ever increasing demand for computing resources and to condense ready costs. As this new way of calculation allows data and applications to be stored away from own corporate server, it brings more issues including security, such as virtualization security, distributed computing, application security, identity management, access control and authentication. However, tough user validation is the overriding requirement for cloud computing that restrict prohibited access of cloud server. By considering about facts and to support the cloud security we proposed this new agent based approach for verification in cloud (ABVC). Our approach adds one more level of security which authenticate user prior to Active Directory Server which stores qualifications and authorizes the clients to use cloud services and also reduces some of the attacks that is possible in network transit.***

Keywords: ***VCloud server, Agent, verification, Active Directory server, Generator, Time-stamp, Token***

I. INTRODUCTION

Cloud computing is a new promising computing paradigm which has developed on the base of distributed computing, grid computing, virtualization mechanisms, and efficacy computing. Cloud computing has been defined by the U.S. National Institute of Standards and Technology (NIST) as follows: " cloud computing is a model for enabling omnipresent, expedient, on-demand network access to a common pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." This cloud model promotes availability and is composed of five essential characteristics, three delivery models, and four deployment models". The cloud computing model as defined by NIST, consists of cloud providers and cloud consumers. A cloud provider is a person, organization or entity responsible for making an infrastructure, platform or software available to cloud consumers as a service (IaaS, PaaS or SaaS). The person organization that besides various services provided by cloud, the biggest problem is how to secure data and applications running in servers away from their own property. So as to guarantee the right user should use or authorized to use right resource in cloud server, we should provide stronger authentication. This is important in many services, such as e-commerce and e-banking, etc. but many other services don't require the identical strong as them, such as public information for general users. However, it is not an efficient way for cloud service providers to burden the client to enter more details every time to use the service as it not only delays but also provides opportunity for attackers. So it is better to enhance the security by using secure techniques with slight modification by adding layer to existing ones without modifying entire strategy.

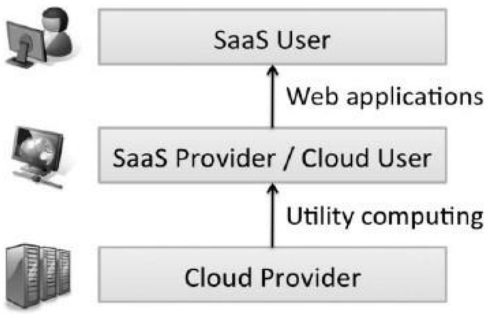

Figure 1. Users and Providers of Cloud Computing

Besides various services provided by cloud, the biggest problem is how to secure data and applications running in servers away from their own premises. So as to ensure the right user should use or authorized to use right resource in cloud server, we should provide stronger authentication. This is important in many services, such as e-commerce and e-banking, etc. but many other services don't need the same strong as them, such as public information for common users. However, it is not an effective way for cloud service providers to burden the client to enter more details every time to

use the service as it not only delays but also provides opportunity for attackers. So it is better to enhance the security by using secure techniques with slight modification by adding layer to existing ones without modifying entire strategy.

The rest of this paper is structured as follows: The related work regarding authentication is discussed in Section 2. Architecture of the proposed model Authentication based approach for Authentication in Cloud Model is discussed in Section 3. Working of ABVC and its protocols are given in Section 4. The Security analysis of the proposed ABVC is discussed in Section 5 and the paper is concluded in Section 6.

II. RELATED WORK

Cloud Computing is a kind of on-demand computing method that lets users use IT resources such as network, server, storage, service, application, and so on via Internet when needing them rather than owning them[3]. Cloud Computing can be considered as a sum of SaaS (Software as a Service) and utility computing and Figure 1 shows the roles of users or providers in the Cloud Computing under the concept[4]. A service, like any process, has a primary security identity that determines the granted access rights and privileges for local and network resources. This security identity, or security context, also determines the potential the service has for damaging local and network resources. To access these cloud services securely, cloud authentication systems are using different methods like: i) Simple text password ii) Third party authentication iii) Graphical password iv) Biometric and v) 3D password object. The weakness of textual password authentication system is that it is easy to break and vulnerable to dictionary or brute force attacks. Third party authentication is not preferred for smaller cloud deployment.

There are no concrete security technologies in Cloud Computing, however, if we regard Cloud Computing as an extension of the existing IT technologies, it is possible to divide some of them by each component of Cloud Computing and apply to. Access control and user authentication are representative as security technologies used for platforms. Access control is the technology that controls a process in the operating system not to approach the area of another process. Technologies used to authenticate a user are Id/password, Public Key Infrastructure, multi-factor authentication, SSO (Single Sign On), MTM (Mobile Trusted Module), and i-Pin. Basing on the above study we proposed this model by using Software agents which are autonomous we can use to enhance the existing authentication services in cloud.

III. ARCHITECTURE OF ABVC

Authentication is a security feature in which a client process must prove its identity to a service, and the service must prove its identity to the client, before any application traffic is transmitted over the client/service connection. Also in cloud environment user authentication is often the primary basis for access control, which keeps out unauthorized users from accessing data over the Internet. For a stronger authentication we propose this scheme Agent based approach for authentication in Cloud(ABVC) which is show in Figure-2. We have taken VMware cloud architecture to propose our scheme.

The major VMware components used in cloud environment are VMware ESX Provides a virtualization layer that abstracts the processor, memory, storage, and networking resources of the physical host into multiple virtual machines. VMware ESX install directly on the server hardware, inserting a robust virtualization layer between the hardware and the operating system. VMware ESX partition a physical server into multiple secure and portable virtual machines that can run side by side on the same physical server. Each virtual machine represents a complete system with processors, memory, networking, storage and BIOS so that an operating system and software applications can be installed and run in the virtual machine without any modification.

vCenter Server A service that acts as a central administration point for ESX/ESXi hosts connected on a network. This service directs actions on the virtual machines and the hosts. Server delivers centralized management, operational automation, resource optimization and high availability to IT environments. It provides admin to adjust the performance of physical servers, and the virtual machines they are running. It allows to access control, robust permissions mechanisms, and integration with Microsoft® Active Directory for authorized access to the environment and its virtual machines.

Active Directory Server: It provides the active directory services to the clients like authorization, privileges, user id's passwords etc. To authenticate and authorize to use cloud services.

In our proposed model ABVC, clients connecting to domain in VM's to access cloud service in ESX server are authenticated by using Active Directory Server (ADS) which provides active directory services via by an agent. vCS creates agents with agent-id (AgId) to serve the clients for authentication. The AgId is stored in database in ADS as ADC (Agent Digital Certificate) for valid agent verification which contains information regarding Agent-id, date, time of its creation by server.

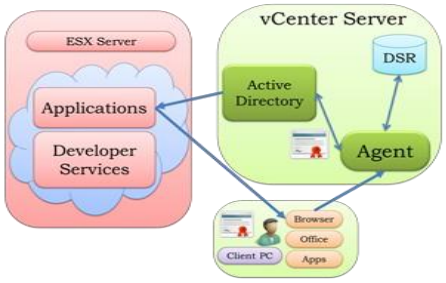

Figure-2 ABVC Model

Agent is an software agent uses data storage repository (DSR) stores data in encrypted form. DSR contains Time Stamp Table(TST) to store Time Difference T**D** for a given client Cid and Client Keys Table (CKT) to store Client Digital Certificate (CDC) which contains g,k1,k2,N,h(CST) at h(Cid) where h is a hash function.

IV. WORKING OF ABVC

While discussing the working of the ABVC for cloud some assumptions are made are not supposed to be violated while executing the scheme. The assumptions are specified below.

1. All the clients and service providers are supposed to be honest in the registration phase.
2. After registration phase is over, no client and server is trusted. The clients need to verify themselves during accessing cloud service by providing exact identification data to access services and applications in either public or private cloud.
3. Once mutual authentication is performed, the server is always trusted and it is assumed that the server never compromises with the network adversaries.

The proposed scheme works in three phases

a) Registration Phase b) Key Generation and Distribution Phase c) Authentication and Verification phase.

Table-1 Notations used in proposed scheme

Notation	Description
Cid	Cloud Identification number
ADC	Agent Digital Certificate
SDC	Server Digital Certificate
CDC	Client Digital Certificate
CSC	Client Secret Certificate
ADS	Active Directory server
vCS	VmWare Center Server
Agid	Agent Identification
CKT	Client keys table
DSR	Data Storage Repository
AST	Agent Secret Token
TST	Time Stamp Table

In Registration phase client sends credentials and TS time stamp at which the client initiates the request to vCS. Idle Agent in vCS receives the request and calculates cid from credentials, Time Difference between receiving and sending the request TD=TR-TS where TR is the time at which the server received the request. The Cid, credentials are stored in ADS.

In Key Generation and Distribution phase agent generates Client secure Token CST as given in section 4 which is based on primitive root which is and is difficult to break as it is a Discrete Logarithm problem. Part of CST which is Client Secret Certificate CSC given to Client and remaining part is retained as a hash digest with agent and stored in CKT at h(Cid) as CDC. For mutual authentication agent generates a server token(step 4 of KGDP of section 4) known as Server Digital Certificate SDC for that client and stored in ADC. SDC is sent to client along with CSC for verification.

In Authentication and Verification phase client request is authenticated to access the cloud service. When client requests the service with its Cid agent sends SDC for server authentication by client and if it is valid client sends CSC , Cid, TS to vCS where the agent will find TD=TR-TS. Agent checks the value of TD for given Cid from TST table if it matches then the CSC is accepted otherwise the Client is asked for retransmission of CSC which concludes that there is a man in middle attack. If Agent comes to conclusion that CSC is free from attack it accepts and uses it to find CDC stored in agents DSR as given in section 4. h(CST) is computed and checked for the given h(CID) in CKT if match hold good then Agent sends its Digital certificate(ADC) which contains Agent Secret Token(AST) (AST=Agid+Cid) where MSB(AST) is Agid to Active directory server. ADS will check ADC and if it matches the Agid in its data storage then agent requesting is valid and client is authenticated to access cloud service.

In this proposed scheme we propose three protocols like Client registration protocol (CRP), Key Generation and Distribution protocol(KGDP), Authentication and verification protocol(AVP) works in three phases Registration

Phase, Key Generation and Distribution Phase respectively to achieve authentication.

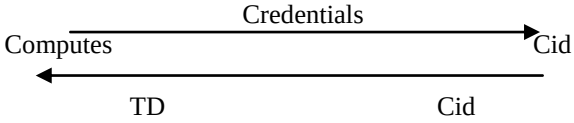

Figure-3 CRP protocol

In CRP, cloud user needs to register at the server by providing appropriate credentials details. The server process user's data and issue a client-id and computes TD which it the time difference between Time send and Time receive The procedure is as follows:

1. Client sends credentials like cname, cloc, csertype, cgrant_type, Cser_Pay , CSExptime etc., to vCenterServer(vCS) along with TimeStamp at which client has started sending data to vCServer.
2. vCS redirects the request to valid agent
3. Agent calculates Cid from its credentials and stores them in Active Directory server (ADS). ADS accept it only from a valid Agent with ADC.

4.Agent computes TD=TR-TS and stores TD,Cid in Time Stamp Table(TST) in DSR for the Agent where the TR is the time at which server receives request from client.

B. *Key Generation and Distribution protocol* This phase is used to generate Certificates for client and server which is used when client wants to access the cloud service.

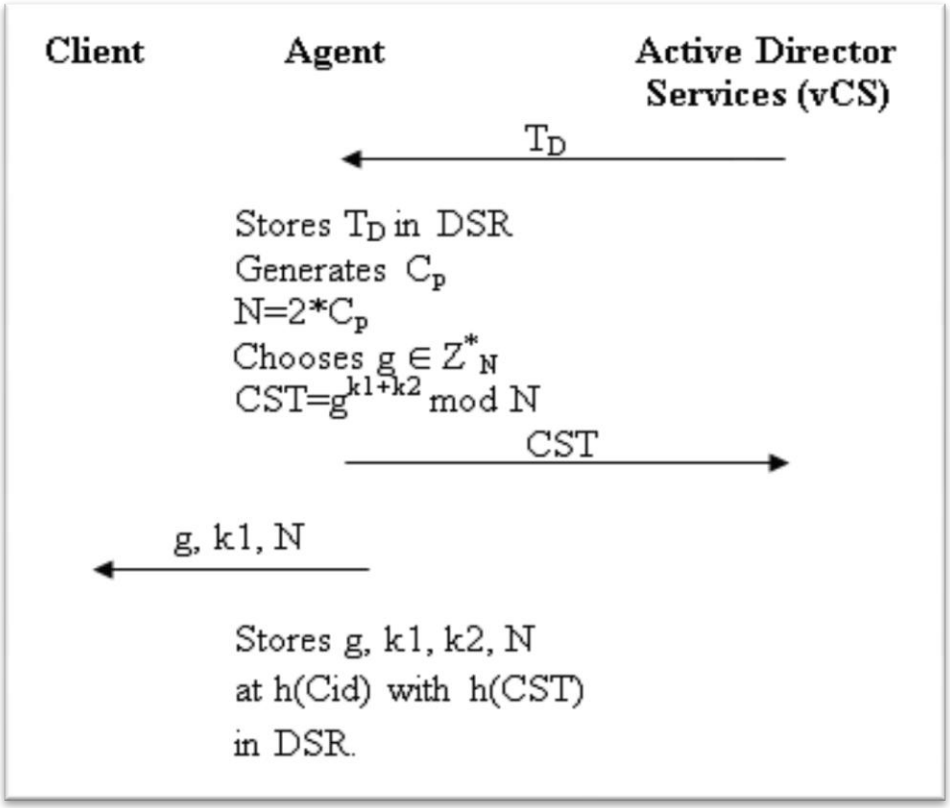

Figure-4 KGDP protocol

1. The Agent chooses large prime Cp nearer to Cid and computes N=2*Cp
2. From N,the Group ZN* is generated
3. agent chooses r1, r2,r3 ∈ ZN* such that, r1= gk1 mod N and r2=gk2 mod N r3=gk3 mod N where 'g' is the generator ie., the primitive root of ZN* and k1,k2,k3 ∈ Zǿ(N)
4. Agent computes Client Secret Token CST =r1*r2 mod N =gk1*gk2 mod N which is stored as CDC and Server Token(STk) where STk=r3*Cp*CSExpTime stored in SDC
5. Agent stores CDC,SDC for given Client in Active Directory Server (ADS) and CDC in DSR
6. Agent sends Client Secret Certificate(CSC) which contains g,k1,N(to compute CSk) and SDC to client .
7. Agent CDC at H(Cid) where H is hash function.

C. *Authentication and Verification Protocol:* At the time of Client Login or Client's access to service in Cloud this phase is used to Authenticate and verify trust for the client.

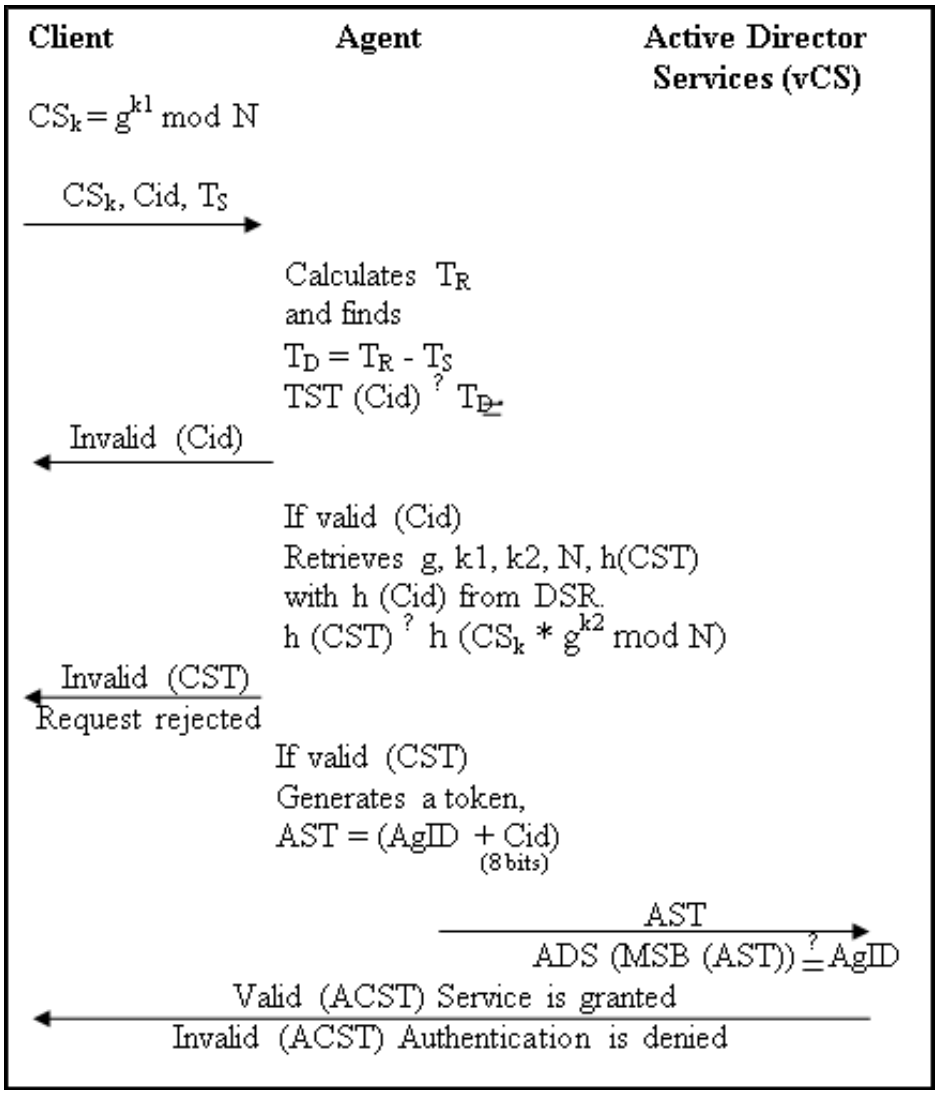

Figure-5 AVP protocol

1. Initially client validates server for STk by using SDC.
2 If above step is verified client sends CSk= g^{k1} mod N in CSC to agent in vCs
3. Agent calculates TR and computes TD=TR-TS
4. if TST(cid) <> TD then
    4.1 Client request is rejected(possible man in middle attack)
    4.2 Authentication failed and return.
5. Agent accepts CSC from client Cid and retrieves CDC for corresponding g,k1,k2,Nh(CST) from h(Cid) from KT in DSR.
6. Agent verifies CSC with CDC as h(CST) =? h(CS^{k*} gk2 mod N)
7 if the above equation holds good then
    7.1 Agent along with its ADC sends Cid to the active directory server for the access for access of service
  ELSE
    7.2 Client request is rejected by agent.(ADC contains Agent Secret Token (AST))
8. ADS verifies as If (MSB(AST)=?Agid holds good then
    8.1 Service is granted to Cid
  ELSE
    8.2 Request is rejected and authentication is denied.

V. SECURITY ANALYSIS

In our model since we are using CST =q*r=gk1gk2 mod N also CST=gk1+k2=gk mod N which gives very large value and it is difficult to find g,^{k1},^{k2} where g is a primitive root in Z* N. Also the calculation is based on DLP which is difficult to break as it is a problem of NP-Hard. Further we analysed the following.

Identity management: The vCenter Server stores all the registered clients Id's ie.. Cid in the Active Directory Server as certificate and also in Agents key table providing a unique ID in each new registration thus providing Identity.

Mutual Authentication: In the key generation phase part of the token is retained with server as in step 4 of KGDP and step 1, 6 of AVP, client and server are mutually authenticated.

Man in the middle attack: In the proposed scheme since only part of key is given to client and any change to CSk in CSC will make client unauthorized as the computation of CST is not possible if CSk is tampered in middle and request is denied. Hence MITM attack is not applicable to the proposed scheme.

Impersonation attack: In the proposed scheme Cid, CST, STk are stored in hash values in Certificates as given in step 7 in KGDP, so if any of its modification will leads to failure of authentication thus withstands this attack.

Phishing attack: Mutual authentication between the user and the server is performed (step 1,4,6 of AVP the scheme. Only the genuine server can send STk (SDC) for the requested client which will be verified by the user. Hence the scheme is also strong against phishing attack.

VI. CONCLUSION

In cloud environment user authentication is often the primary basis for access control, which keeps out unauthorized users from accessing data over the Internet. Active Directory is a flexible and scalable management platform for distributive network resources and applications which contains user's data, authorizations, privileges etc. which should be carefully accessed. As cloud provides various services with different types of users, to allow only authenticated clients to access the cloud services we have proposed this model ABVC which will give extra layer of security not only to Active directory but also to entire cloud Environment. Our model will provide an opportunity to deploy Active Directory as a Service (ADaS) in cloud with agent Security as service.

REFERENCES

[1] Peter Mell, Timothy Grance, "The NIST Definition of Cloud Computing" ,NIST Special Publication 800-145, Sep-2011
[2] Kim, J., Kim, H.,"Cloud Computing Industry Trend and Introduction Effect.", IT Insight, (2010)
[3] S. Wiedenbeck, J. Waters, J.-C. Birget, A. Brodskiy, and N. Memon, "Authentication using graphical passwords: Basic results," in Proc.Human-Computer. Interaction Int., Las Vegas, NV, Jul. 25–27, 2005
[4]. Lee, J.: "Cloud Computing, Changes IT Industry Paradigm". In: LG Business Insight, pp. 40-46 (2009)
[5]. CA Technologies cloud authentication system http://www.ca.com/us/authentication-system.aspx
[6]. Un,S.,etal.:"Cloud Computing Security Technology". In: ETRI, vol. 24, no. 4, pp. 79-88 (2009)
[7]. Armbust, M., et al.: "Above the Clouds: A Berkeley View of Cloud Computing". In: Technical Report. http://www.eeec.berkeley.edu/Pubs/TechRpts/2009/EEEC- 2009-28.html (2009)

