ZKG INTERNATIONAL ISSN: 2366-1313

A RESEARCH ON INCREASING AUTHENTICATION LEVELS IN CLOUD COMPUTING

[1]S. SUSMITHA, [2]CH.SAI LAKSHMI

[1,2]Assistant Professor, Dept of CSE, Megha institute of engineering and Technology for women, Ghatkesar (T.S)

Abstract: *Cloud computing is becoming an adoptable technology for many of the organizations with its dynamic scalability and usage of virtualized resources as a service through the Internet. Cloud computing is a way to increase the capacity or add capabilities dynamically without investing in new infrastructure, training of new personnel, or software licensing. The recent emergence of cloud computing has significantly changed everyone's opinion of infrastructure architectures, development models and software delivery. From a security perspective, several unchartered risks and challenges have been introduced from this move to the clouds, failing much of the effectiveness of traditional protection mechanisms. In cloud computing Authentication plays a very important role to provide security. Authentication protects Cloud Service suppliers against various types of attacks; here the aim of authentication is to verify a client's identity once a client needs to request services from cloud servers. There are various types of authentication technologies that verify the identity of a client before giving the access to resources.*

Keywords: *Cloud Computing, Authentication Protocol, Cloud Service Provider, Access, Environment*

I. INTRODUCTION

Introduction loud computing is a model for enabling universal, suitable, on-demand network access to a mutual pool of configurable computing resources (different networks, servers, data storage, services and applications) those may be rapidly provisioned and released with minimal management effort or service provider interaction. Today Small and Medium Business (SMB) companies are increasingly realizing that simply by tapping into the cloud they can gain fast access to best business applications or significantly boost their infrastructure resources, all at very low cost. Cloud computing applications have broadly three areas known as cloud delivery models: Infrastructure as a service (IaaS), Platform as a service (PaaS), Software as a service (SaaS). So far, there have been little scientific definitions trying to develop a

ISSN: 2366-1313

complete definition of the cloud computing phenomenon [1].

As the cloud computing is achieving popularity periodically, alarms (concerns) are being voiced about the security issues presented through the adoption of this new model. The usefulness and efficiency of traditional protection mechanisms are being reviewed, as the characteristics of this innovative deployment model, differ widely from them of traditional architectures

Authentication plays an important role in protecting resources against unauthorized use. But still the most widely used authentication system is based on the use of text passwords. Text based passwords are not secure enough for many applications that enforce security by access control mechanisms. Authentication based on text-based passwords has major drawbacks. More sophisticated authentication process is costly and may need additional equipment or hardware[2]. This paper proposes a security solution regarding secure user authentication to the cloud network and data centers, which leverages clients from the security burden, by implementing Multi-Level Authentication (MLA) technique. MLA is simple enough, cost effective and does not need any additional hardware. Thus, MLA can be used in cloud computing as well as corporate world with ease.

Cloud computing is standard architecture for providing on demand network access to a software, shared data, infrastructure and platform resources which can be quickly granted and released with minimum organizing effort or service provider interaction. It helps to improve the effectiveness of Information Technology by providing various services. Cloud computing (CC) is an architecture of computing in which dynamically expandable and often virtualized resources are granted as a service over the Internet. Cloud customers need not have proficient in, Knowledge of, or control over the technology infrastructure „in the cloud“ that supports them. Authentication, thus, becomes pretty important for cloud security. Applied to cloud computing and depending on standard X.509 certificate-based PKI authentication framework, SSL Authentication Protocol (SAP) is low efficient [3]. The researchers of Grid Security Infrastructure accepted that the current GSI technique has a poor scalability. W.B. Mao et al analysed that this scalability problem is an inherent one due to the use of SSL Authentication Protocol. Grid computing and cloud computing is so similar that grid security technique can be applied to cloud

ISSN: 2366-1313

computing. Dai et al. made great contribution to Grid security. There are basically four kinds of authentication methods: Something an individual KNOWS (e.g., password, Personal ID). Recently many security researchers are focusing on different new techniques of authentication in cloud computing that incorporate one or more of the above notified methods of authentication. Therefore, it becomes necessary to survey the various authentication methods recently proposed and implemented in the Cloud computing environment.

II. LITERATURE SURVEY

In recent times, identity-key-based cryptography (IBC) is developed very quickly. The main theme of applying IBC to grid security was basically explored by Lim et al [4].

Mao et al. [4] initiated an identity-key-based non-interactive authentication Frame work for grid. The framework is certificate-free. But the same Private Key Generator (PKG) becomes the bottleneck of framework.

Lim and Robshow [5] proposed a hybrid method for combining IBC . The method solves escrow and distribution of private key. Anyway, the non-interactive and certificate-free quality is lost.

Chen (2005) [6] revised the GSI in the GT version2 and improved the GSI architecture and protocols. It is significant to study IBC and cloud computing. Three important aspects of cloud security requirements are availability, confidentiality, and integrity. These aspects are well known as CIA. Confidentiality means keeping customers information secret in CSP and only authorized customers (computers and users) grant accessing to protected data. It depends on various aspects such as encryption methods (symmetric or asymmetric algorithm), key length (in symmetric algorithm) and Cloud Service Provider (CSP) (Sharma et al., 2011)[32]. In Cloud Computing, confidentiality has a major role in protect control on organizations‟ data situated across multiple distributed databases. Integrity means that an unofficial person is not permitted to modify, fabricate and delete sensitive data in cloud servers. By protecting unauthorized access (confidentiality), organizations can achieve greater assurance in information and system integrity. The main aim of availability is to ensure that unauthorized person cannot approach to shared data in cloud service provider (any time and any place). Cloud servers must have the ability to extend operations even in the possibility of a

ISSN: 2366-1313

security breach. Denial of Service attacks (DOS), natural disasters, as well as equipment outages can risk to availability. Cloud computing is an internet-based technology which provides various services over the internet.

These services appreciably effects on economy in terms of efficiency, scalability as well as energy, cost reducing. A service is a method that is capable of providing functionalities for using in compliance with considering rules. Cloud computing services can divide in three types by Banyal et al., 2013[7].

Platform as a Service (PaaS), Software as a Service (SaaS) Infrastructure as a Service (IaaS), Gibson and Elveleigh (Behl, 2011) [8] given various advantages of these cloud services. SaaS is an on-demand application in the first layers. It provides software as a service through the Internet such as Google Docs, Zoho, as well as Microsoft CRM. Software as a Service over comes the problem of installing and running the application on the customers end.

The second layer (outgrowth of IaaS) is PaaS. It allows users to rent database management system, operating systems, hardware, tools for design and network capacity (hosting) through the Internet (Ramgovind et al., 2010)[9].

Subashini and Kavitha (2011)[10] discussed about some security issue in this model. IaaS is bottommost layer. IaaS provides basic computing infrastructure components such as Storage, CPU and memory. It implies the combination of hosting, hardware provisioning and basic services needed to execute on cloud computing. Infrastructure is underlying physical components that are required for a system to perform its operations.

III. SECURITY IN CLOUD COMPUTING

Cloud computing paradigm has many benefits in lowering cost, sharing resources, time saving for new service implementation. While in a cloud computing model, most of the data and applications that clients use stay back on the Internet, it gets some new problems for the system, especially privacy and security of the system. Since each service may use resource from different multiple servers. The servers are geographically located at multiple locations and the services offered by the cloud may use different infrastructures with various organizations. All these characteristics of cloud computing make it more difficult to provide security in cloud computing. To provide improved security in cloud computing, various security issues like

ISSN: 2366-1313

data authentication, data integrity, data confidentiality and non-repudiation all need to be considered into account. Now days, maximum of cloud services used WS-Security service to provide security for the system. In WS-Security, XML encryption and XML signature are used to enable data integrity and confidentiality. Mutual authentication can be backed by adding Kerberos tickets and X.509 certificate into SOAP message header. As discussed in the previous section, there are three types of major clouds in general they are: private cloud, public cloud and hybrid cloud. In a public cloud, dynamically resources are provisioned on a self-service, fine-grained basis over the Internet.

Services in the cloud are given by an off-site third-party provider who shares resources and bills on a fine-grained utility computing basis. While in most private clouds, with minimum computing resources, it is very complex for a private cloud to provide all services for their clients, as some services may more resources than internal cloud can provide. Hybrid cloud is a possible solution for this issue since they can get the computing resources from external cloud computing providers. Private clouds have some advantages in managing the company and it provide reliable services, as well as they grant more management over public clouds do. For the security reasons, when a cloud environment is enabled inside a firewall, it can provide less publicity to the Internet security risks to its clients. Also in the private cloud, the services of cloud can be acquired by internal connections only, it makes easier to use existing security measures and standards. Because of these reasons private clouds more appropriate for services with sensitive data that must be protected. But in case of hybrid cloud, it combines more than one domain; it will increase the complexity of security provision, especially mutual authentication and key management.The hybrid cloud domains can be heterogeneous networks; so there may be gaps between these different networks and between the different services providers.

In the case of Public and private clouds provide well guaranteed security because of their unique network models. But in the case of hybrid clouds it is very difficult to provide guaranteed security because of its different set of network conditions and different security policies, For example, cross domain authentication can be a problem in a hybrid cloud with different domains.Although some authentication services such as Kerberos can provide multi-domain authentication, but one of the requirements for the multi-domain Kerberos authentication is that the

ISSN: 2366-1313

Kerberos server in each domain needs to share a secret key with servers in other Kerberos domains and every two Kerberos servers need to be registered with each other. The problem here is if there are N Kerberos domains and each of them want to trust each other, then the number of key exchanges is N(N-1)/2. For a hybrid cloud with a large number of domains, this will bring a problem for scalability. If different networks in a hybrid cloud using different authentication protocols, this problem can be more complex.

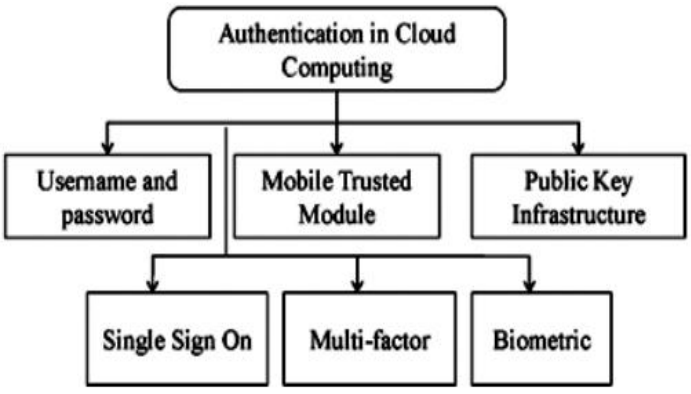
IV. AUTHENTICATION TECHNIQUES IN CLOUD

Authentication is a major criteria of each secure communication system especially in wide networks such as Cloud Computing. It guides to protect shared data from unauthorized access and it is a major technique of information security. AAA is a security organizing module for authentication, authorization and accounting. When a user tries to access cloud resources from CSP, then AAA verifies the user's authentication information. If the user is authenticated, then AAA gets the user's access level, which has been most recently pro, by inspecting the user's information in the database. In addition, authentication technique says that "Who is the authorized customer" and "Is the customer really who he claims himself to be". In addition, verification of customer"s identity is the most important aim behind an authentication. In other words, an authentication mechanism tells how customers identified and verified to access to sensitive data (Köse, 2011)[23]. Verification means confirm that demand is from the legal user. Identification implies on determining users. There are several authentication schemes (Pointcheval and Zimmer, 2008[29]) which categorized in three types as follow:

Something user know (knowledge factors) such as username and password, PIN based authentication scheme and Implicit Password Authentication System (IPAS).

- Something user has (possession factor) such as smart cards or electronic tokens and identify card such as Automatic Teller Machine card (ATM card).

- Something user is (ownership factor) such as biometric authentication



ISSN: 2366-1313

Fig.1 Authentication methods in cloud computing.

Username and Password Authentication

The most important point of authentication is to protecting the data from accessing of unauthorized person. It needs servers to reject requests from unknown visits and to manage the access of authenticated users. In this method of authentication, user should enter username and password to login to the system and can access to the information in CSP. It is extensively supposed username and password is not very secure authentication mechanism because it is difficult to confirm that the demand is from the rightful or legal owner. Moreover, commonly users choose easy passwords for a machine to guess. Even the strong password can be stolen by brute force attacks and dictionary (Karnan et al., 2011;[20]). In cloud computing the input constraints construct it hard for users to input complex passwords, often leading to the employ of short passwords and password managers. In addition, users reuse their passwords for identifying in different servers and they use weak passwords which cause to increase risks to the security of user‟s shared information.

Multi-Factor Authentication

Traditional password authentication technique does not afford ample security for information in cloud computing environment to the most modern means of attacks. A more secure scheme is the multi-factor authentication which does not only verify the username/password pair, but also needs Second factor such as biometric authentication. However, the feasibility of second factor authentication is limited by the deployment complexity, high cost. MFA technique uses combination of something you have, something you know as well as something you are to supply stronger authentication method. It is stronger user identification techniques. In fact, the trust of authenticity increases exponentially when more factors are involved in the verification process. For example, ATM transaction requires multifactor authentication, something the customer possesses (i.e., the card) clubed with something the customer knows (i.e., PIN) (Karnan et al., 2011[20]).Ziyad and Kannammal (2014)[39] proposed a multifactor biometric authentication system for cloud computing environment. These biometric methods are finger print and palm vein. The goal is to handle the biometric data in a secure fashion by storing the palm vein biometric data in multi-component smart cards and fingerprint data in the central database of the cloud security server

Mobile Trusted Module

ISSN: 2366-1313

Trusted Computing Group (TCG) introduced a group of specifications to report, store and measure hardware and software integrity through a hardware root-of-trust, which are the Trusted Platform Module (TPM) and Mobile3 Trusted Module (MTM). MTM is a security factor for employ in mobile devices. Unlike Trusted Platform Module (TPM) that is for PCs, MTM is employed in mobile devices (Sidlauskas and Tamer, 2008[33]; Sharma et al., 2011[32]). However, for high levels of protection and isolation, an MTM could be implemented as a slightly modified TPM. MTM checks all software and applications each time the underlying platform starts due to increase the security of mobile devices. Therefore, the MTM guarantees the integrity of a mobile platform. It has very constraints such as circuit area, as well as available power. Therefore, a MTM needs the spatiallyoptimized architecture and design method (Kim et al., 2010[22]). TPM provides trusted information on the internal state of the system and stores cryptographic identities and keys. It is accessed by software using a well-defined command set. Through this command set, the TPM gives cryptographic functionality such as random number generation, key generation, signing and encrypting. It could also store a limited amount of information in nonvolatile memory.

Public Key Infrastructure

The conventional authentication system is based on the secret key and is mainly support the deployment of conventional asymmetric cryptographic algorithms, such as RSA. It uses a private key to prove the user‟s identity. PKI has been used in developing security protocols such as Secure Socket Layer (SSL/TLS) and Secure Electronic Transaction (SET) with the main aim is to provide authentication. The success of PKI like as other type of cryptographic system depends on controlling access to private keys. PKI mechanism has to provide data confidentiality, data integrity, non-repudiation, strong authentication, as well as authorization.

E. Single Sign On Single Sign on (SSO) is an identity management system (Chen et al., 2011[9]; Brainard et al., 2006[8]) which user can authenticate once to a single authentication authority and then they can entrance to other confined resources without reauthenticating. In the other words, this method produces authentication information by using the different applications. The SSO is a way to access the multiple independent software system in such a way that user logs in a

ISSN: 2366-1313

system and gains the access to every system without being further to re-login in each application.

Biometric Authentication

Biometric authentication strongly supports the three important points of information security. These factors are non-repudiation, identification and authentication. It is an ancient Greek word bios = "life" and metron = "measure

V. CONCLUSION

Authentication method is main factor of preserving security and privacy of each communication in the cloud environment. In fact, the ability to perform suitable user authentication become major important issue in cloud computing where it needs to have some secure system to preserve sensitive and critical information in CSP. Authentication technique is to find out "who is the authorized customer and is the customer really who he climes himself to be. There are numerous methods of authentication in this approach which are username and password, multifactor, MTM, PKI, SSO and biometric authentication. In addition, all of this has specific sub sets.

REFERENCES

1]Acar.T,M.Belenkiy and A.Kupcu 2013 single password authentication.IACR cryptology ePrint Archive,PP:167.

[2]Akyildiz E. and M.Ashraf 2014 An overview of trace based public key cryptography over finite fields.J.Comput. Appl, Math,259:599-621.

[3]Anzaku,E.T,H.Sohn and Y.M.Ro,2010.Multifactor Authentication using fingerprints and user specific random projection.Proceding of 12th International Asia-Pacific web conference (APWEB,2010),pp:415-418.

[4] Banyal, R.K., P. Jain and V.K. Jain, 2013. Multi-factor authentication framework for cloud computing. Proceeding of 5th International Conference on Computational Intelligence, Modelling and Simulation (CIMSim), pp: 105-110.

[5] Behl, A., 2011. Emerging security challenges in cloud computing: An insight to cloud security challenges and their mitigation. Proceeding of World Congress on Information and Communication Technologies (WICT, 2011), pp: 217-222.

[6] Bhattacharyya, D., R. Ranjan, A. Farkhod Alisherov and M. Choi, 2009. Biometric authentication: A review. Int. J. uand e-Serv. Sci. Technol., 2(3):13-28. [

7]Bouayad, A., A. Blilat, N. El Houda Mejhed and M. El Ghazi, 2012. Cloud

ISSN: 2366-1313

computing: Security challenges. Proceeding of IEEE Colloquium in Information Science and Technology (CIST, 2012),pp: 26-31.

[8]Brainard, J.G., A. Juels, R.L. Rivest, M. Szydlo and M. Yung, 2006. Fourth-factor authentication: Somebody you know. Proceeding of ACM Conference on Computer and Communications Security, pp: 168-178