Additional Authentication and Authorization using Registered Email-ID for Cloud Computing

Abdelmajid Hassan Mansour Emam

***Abstract*—Cloud computing is a new computing paradigm that changes the way of information technology is provided and used. But achieving acceptable level of information security issues are an important aspect and a key factor in the cloud. This paper firstly lists some of the different security issues of the cloud computing, and then proposes additional security mechanism of authenticating and authorizing users by using registered Email-ID in the cloud computing. To ensure that only authorized persons may use the resources in the role of identity and authorizations management.**

***IndexTerms*— Cloud Computing, Authentication, Authorization, Identity management.**

I. INTRODUCTION

Cloud computing refers to the provision of computational resources on demand via a computer network. In the traditional model of computing, both data and software are fully contained on the user's computer; in cloud computing the user's computer may contain almost no software or data (perhaps a minimal operating system and web browser only), serving as little more than a display terminal for processes occurring on a network of computers far away [2]. So through the advancement of internet technology cloud computing share distributed resources via the network in the open environment, thus it makes security problems important for us to develop and use the cloud computing application. Many works are done online; this includes chatting, entertainment, information gathering and financial transactions etc. All these online activity require some type of security mechanism as the primary goal of protecting the fundamental data that powers the system and application of the cloud.

There are some security issues such as virtualization technology security, massive distributed processing technology, service availability, massive traffic handling, application security, access control, and authentication in the cloud computing service environment [1]. Authentication is to check the identity of the user, which means whether the person is same as he pretends to be [6]. Authentication assurance levels should be appropriate for the sensitivity of the application and information assets accessed and the risk involved [10]. There are many different ways to authenticate users; for example, based on what a person knows, has, or is. But the mechanisms of authentication process and the methods used to secure are a weak point in hosted and virtual services, and are frequently targeted of attackers [4], [7]. In this paper, the author propose additional safe and convenient authentication model of the users by using registered Email-ID in the cloud computing environments.

II. SECURITY ISSUES FOR CLOUD COMPUTING

Cloud computing is not secure by nature. Security in the Cloud is often intangible and less visible, which inevitably creates a false sense of security and anxiety about what is actually secured and controlled. The off-premises computing paradigm that comes with cloud computing has incurred great concerns on the security of data, especially the integrity and confidentiality of data, as cloud service providers may have complete control on the computing infrastructure that underpins the services [17].

The Security measures assumed in the cloud must be made available to the customers to gain their trust. There is always a possibility that the cloud infrastructure is secured with respect to some requirements and the customers are looking for a different set of security. The important aspect is to see that the cloud provider meets the security requirements of the application and this can be achieved only through 100% transparency. In order to have a secured Cloud computing deployment, we must consider the following areas, the cloud computing architecture, Governance, portability and interoperability, traditional security, business continuity and disaster recovery, data center operations, incident response, notification and remediation, Application Security, Encryption and Key management, identity and access management [15].

III. IDENTITY AND ACCESS MANAGEMENT

In Cloud Computing, hardware, software and services are used by many users. The role of identity and authorizations management is to ensure that only authorized persons may use the IT resources. Access to all the IT systems or services must be made secure by identifying and authenticating the users or IT systems seeking access [13].

Access control is generally a policy or procedure that allows, denies or restricts access to a system. It may, as well, monitor and record all attempts made to access a system. Access Control may also identify users attempting to access a system unauthorized. It is a mechanism which is very much important for protection in computer security. Various access control models are in use, including the most common Mandatory Access Control (MAC), Discretionary Access Control (DAC) and Role Based Access Control (RBAC). All these models are known as identity based access control models [8].

Preventing unauthorized access to information resources in the cloud is a major consideration. One recurring issue is that the organizational identification and authentication framework may not naturally extend into a public cloud and extending or changing the existing framework to support cloud services may prove to be difficult. Employing two different authentication systems, one for the internal organizational

Manuscript received on May, 2013.

Dr. Abdelmajid Hassan Mansour Emam, Assistant Professor, Department of Information Technology, King Abdulaziz University, Faculty of Computer Science and Information Technology, khulais, Saudi Arabia.

systems and another for external cloud-based systems, leads to complication that can become unworkable over time [10].

IV. AUTHENTICATION

Authentication is the process of establishing confidence in user identities. Authentication assurance levels should be appropriate for the sensitivity of the application and information assets accessed and the risk involved. A growing number of cloud providers support the SAML standard and use it to administer users and authenticate them before providing access to applications and data. SAML provides a means to exchange information between cooperating domains [10], [11]. Also strong authentication should be used, i.e. two-factor authentication as is normal, for example, in online banking. Any network access should, in principle, be made secure by strong authentication. These strict requirements apply particularly to the CSP's staff. They, too, should only gain access to the IT resources being administered via strong authentication, i.e. for example via a hardware-based authentication system using chip cards or USB sticks or via one-time passwords that can also be generated by hardware devices. This is absolutely indispensable for access via the Internet [13].

The user obtains a certificate proving his identity signed by the Certification Authority (CA). This is the basis of every trust relationship among the participants, so a strict procedure has been set up for the connection between two principals. Once the trust relationship has been established via a trusted set of Certification Authorities, participants can use this to mutually authenticate each other in a connection [8]. There are various authentication methods and techniques that organizations can choose it such as follows [14]:

A. User Password Authentication

It is the most common form of providing identification. When user accesses the resource, access control framework asks for the user name password provided to the user. The credentials are validated against the one stored in the system's repository.

B. Windows user based authentication

Usually, organizations have a list of users stored in the windows active directory. Access control framework should be able to provide authentication for the user of the Primary Domain Controller (PDC).

C. Directory based authentication

With the rising volume of business over the web, millions of users often try to access the resource simultaneously. In such a scenario, the authentication framework should be able to provide for faster authentication. One such technique is Directory Based Authentication where user credentials are validated against the one which is stored in the LDAP Directory.

D. Certificate based authentication

This is probably one of the strongest authentication techniques where the user is asked to provide his/her digital ID. This digital ID, known as digital certificate, is validated against the trusted authority that issued the digital ID. There are various other parameters that are checked to ensure the identification of the user.

E. Smart card based authentication

This is also used as a second factor authentication. Smart cards are small devices containing co-processors to process cryptographic data.

F. Biometrics

This is the strongest authentication. Known as third factor authentication, it is based on something the user is. It works after the users have provided something they know (User name password) and something they own (either a grid or token) or something they are (retina-scan, thumbprint or thermal scan). It is required in cases where data is top confidential, such as in Military/Defense.

G. Grid based Authentication

This is used as a second factor authentication. It authenticates the user based on something he knows (User name password authentication) and then asks for something he owns (grid card information). Entrust Identity Guard provides such an authentication.

H. Knowledge-based authentication

One of the simplest mechanisms for gaining additional confidence in a user's identity is to challenge the user to provide information that an attacker is unlikely to be able to provide. Based on "shared secrets", this allows for the organization to question the user, when appropriate, to confirm information that is already known about the user through a registration process, or from previous transactions.

I. Machine Authentication

Machine authentication provides validation of the user's computer in a way that secures against a variety of threats in a zero touch fashion, reducing user impact. This is an especially effective method of user authentication where users typically access their accounts from a regular set of machines, allowing for stronger authentication to be performed without any significant impact on the user experience.

J. One Time Password (OTP)

A one-time password is dynamically generated and it is valid only for once. The advantage of one time password is that if an intruder hacks it, he cannot reuse it. There are two types of OTP token generators: synchronous and asynchronous. A synchronous token device synchronizes with the authentication service by using time or an event as the core piece of the authentication process. A token device, which is using an asynchronous token generating method, uses a challenge response scheme to authenticate the user.

V. AUTHORIZATION

Authorization is an important information security requirement in Cloud computing to ensure referential integrity is maintained. It follows on in exerting control and privileges over process flows within Cloud computing.

The rights management system must ensure that each role may only see the data (including meta-data) required to achieve the task. The access control should be role-based and the roles and authorizations set up should be reviewed regularly. In general, the least privilege model should be used, with users and CSP administrators only possessing the rights that they require to achieve their tasks [13].

A. Global Authorization

In an access control decision there are several rules and policies to take into account global (e.g. organizational membership) and local (e.g. banned users). Both pieces of information have to be available in order to make the decision. Grid access is granted according to membership of Virtual Organizations. In the early versions of the Globus software, this membership information was recorded in a local grid mapfile. This required a user to have an account on all resources they wished to have access to, and their DN was mapped onto that account via the grid-mapfile [12].

VI. RELATED WORK

Authentication and Authorization is one of key security and privacy issues in the cloud computing. A lot of research discuss this problem and introduce many solutions to decrease the threat of the Authentication and Authorization. Manjea Kim, Hoon Jeong, and Euiin Choi [1], was proposed Context-aware platform that considers user's context information and profile which stored each user's personal information, preferences to provide suitable services for users. Through the Context-aware model authenticate the user and users can use Cloud computing services. In cloud computing, a grid distributed parallel authentication model based on trusted computing, was proposed by Keshou Wu, Lizhao Liu, Jian Liu and others [2]. This can realize simultaneous verification of grid authentication and grid behavior on upper layer of SSL and TLS protocols, by adaptive stream cipher heuristic code generator and heuristic behavior trust query function, plays well in authentication. The concept of face recognition was introduced by Janita S. Patel and G.B.Jethava [3], they used to provide authorization for cloud security, which play the role biometrics authentication. Additional scheme of biometrics authentication concept was proposed in [5], [10].

Multi-tier Authentication Scheme was proposed by Maninder Singh and Sarbjeet Singh, in [6] which authentication process is carried out in two levels or two tiers. First tier uses simple username and password. Second tier is pre-determined series of steps. The advantage of this scheme is that it does not require any additional hardware and software. So this can be used and accessed from anywhere across the globe.

Another scheme called An Improved Mutual Authentication Framework for Cloud Computing was proposed by Sanjeet Kumar Nayak, Subasish Mohapatra, and Banshidhar Majhi [9]. This executes in three phases such as server initialization phase, registration phase, authentication phase. They provide mutual authentication and session key agreement in cloud computing environment. The designing of N-screen based consolidated user authentication model that meets framework and protocol requirement of credentials and privacy protection requirements in a cloud computing environments was proposed by Jaejung Kim and Seng-phil Hong [16]. This provides more flexible authentication framework and also leads to safer credential management in operating various mobile devices such as smart phone and smart pad, etc.

VII. PROPOSED WORK

The proposed scheme done by authenticating users using registered Email in the cloud computing, firstly the user sends request to subscribe for specific services in the cloud before they use it. The cloud system sends to the user registration form with condition terms, one of the most important condition terms is the (Email of the user ,is compulsory which act as the ID of the user where the link of authorized service may send to it and accessed by the user mail itself), the user submit the form. The cloud system capture the details filled in the form that has chosen during registration process by the user. In order to make approval for it, then return information of successful registration. The overall working scheme is explained in 8 steps as shown in Fig.1 below.

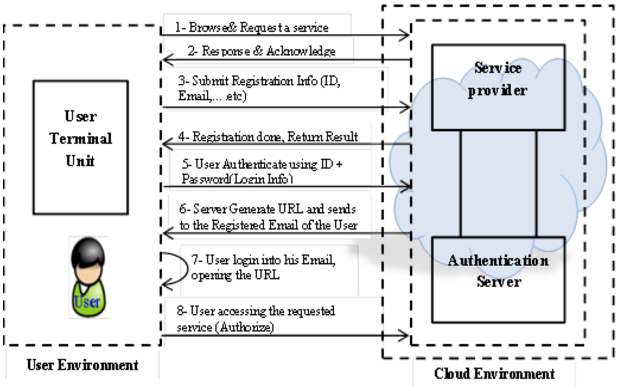
1- Browse& Request a service
2- Response & Acknowledge
3- Submit Registration Info (ID, Email,... etc)
4- Registration done, Return Result
5- User Authenticate using ID + Password(Login Info)
6- Server Generate URL and sends to the Registered Email of the User
7- User login into his Email, opening the URL
8- User accessing the requested service (Authorize)
User Terminal Unit
User
Service provider
Authentication Server
User Environment
Cloud Environment

Figure 1. Authentication and Authorization Process

These steps are marked in sequential order of their execution in the proposed scheme, as flow:

1) User browse and request for specific service from the cloud by enters URL of application.
2) The cloud system response and sends registration form to the user.
3) Upon receiving the registration form, the user fills and submits it to the cloud.
4) The Cloud checks and processes the registration from. If the details entered by the user are correct and satisfied to the condition terms, then they return information to the user of successful completion of the registration, otherwise the cloud denies.
5) The user authenticate into the cloud using registered information.
6) The cloud system after verifying the authentication of the user. They generate a dynamic link about specified service and send to the user of its registered Email-ID via text message, with notification about the process of replying.
7) The user login into his mail and enters that link received from cloud, within the threshold time, because after that the will expire and user has to login again.
8) After successful login the user is allowed and authorized to access the requested service in the cloud system, and the application is loaded.

VIII. CONCLUSIONS

Authentication and Authorization are very important for a large distributed system like a cloud system, which usually refers to determining whether an already identified and authenticated user is allowed to access information resources in a specific way. There should always be a specific security analysis for the data or applications that are to be mapped to any, so the proposed scheme ensure that only the registered user with exact Emil ID may Authorized to access the requested service by using his Mail-ID as an additional form authentication and authorization.

REFERENCES

[1] Manjea Kim, Hoon Jeong, Euiin Choi," Context-aware Platform for User Authentication in Cloud Database Computing", International Conference on Future Information Technology and Management Science & Engineering Lecture Notes in Information Technology, Vol.14, pp.170-176, 2012.

[2] Keshou Wu, Lizhao Liu, Jian Liu, Weifeng Li, Gang Xie, Xiaona Tong and Yun Lin, "Researches on Grid Security Authentication Algorithm in Cloud Computing", JOURNAL OF NETWORKS, VOL. 6, NO. 11, pp. 1639-1646, NOVEMBER 2011.

[3] Janita S. Patel, G.B.Jethava ,"Providing Authorization by Using Face Recognization for Private Cloud Computing", International Journal of Engineering and Advanced Technology(IJEAT) ISSN: 2249-8958, Volume-2, Issue-2, pp. 231-234, December 2012.

[4] B.Meena, Krishnaveer Abhishek Challa, "Cloud Computing Security Issues with Possible Solutions", International Journal of Computer Science And Technology (IJCST), ISSN:0976-8491 (Online) | ISSN : 2229-4333 (Print) Vol. 3, pp. 340-344, Issue 1, Jan. - March 2012.

[5] Himabindu Vallabhu, R V Satyanarayana, "Biometric Authentication as a Service on Cloud: Novel Solution", International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-4, pp.163-165, September 2012.

[6] Maninder Singh , Sarbjeet Singh, "Design and Implementation of Multi-tier Authentication Scheme in Cloud", International Journal of Computer Science Issues(IJCSI), ISSN (Online):1694-0814, Vol. 9, Issue 5, No 2, pp. 181-187, September 2012.

[7] Ajey Singh, Dr. Maneesh Shrivastava, "Overview of Attacks on Cloud Computing", International Journal of Engineering and Innovative Technology (IJEIT), ISSN: 2277-3754, Volume 1, Issue 4, pp. 321-323, April 2012.

[8] Abdul Raouf Khan, "ACCESS CONTROL IN CLOUD COMPUTING ENVIRONMENT", Asian Research Publishing Network (ARPN), Journal of Engineering and Applied Sciences, ISSN 1819-6608, VOL. 7, NO. 5, pp. 613-615, MAY 2012.

[9] Sanjeet Kumar Nayak, Subasish Mohapatra, Banshidhar Majhi, " An Improved Mutual Authentication Framework for Cloud Computing", International Journal of Computer Applications (0975 – 8887) Volume 52– No.5, pp. 36-41, August 2012.

[10] B.Prasanalakshmi, A.Kannammal, "Secure Credential Federation for Hybrid Cloud Environment with SAML Enabled Multifactor Authentication using Biometrics", International Journal of Computer Applications (0975 – 8887) Volume 53– No.18, pp. 13-19, September 2012.

[11] Pradnya B. Rane, Pallavi Kulkarni, Suchita Patil, Dr. B.B.Meshram, "Authentication and Authorization:Tool for Ecommerce Security", IRACST – Engineering Science and Technology: An International Journal (ESTIJ), ISSN: 2250-3498, Vol.2, No.1, pp. 150-157, 2012.

[12] Linda A. Cornwall, Jens Jensen, David P. Kelsey, A kos Frohner, Daniel Kouril, Franck Bonnassieux, Sophie Nicoud, Karoly Lorentey, Joni Hahkala, Mika Silander, Roberto Cecchini, Vincenzo Ciaschini, Luca dell'Agnello, Fabio Spataro, David O'Callaghan, Olle Mulmo, Gian Luca Volpato, David Groep, Martijn Steenbakkers and Andrew McNab, "Authentication and Authorization Mechanisms for Multi-Domain Grid Environments", Journal of Grid Computing (2004) 2: pp. 301–311.

[13] Federal office for information security, "Security Recommendations for Cloud Computing Providers (Minimum information security requirements)", White Paper, Section 114, Security Management and IT-Grundschutz, P.O. Box 20 03 63, 53133 Bonn.

[14] TRIANZ, "Authentication and Access Control- The Cornerstone of Information Security", White Paper, Vinay Purohit, September 2007.

[15] Jeon SeungHwan, Yvette E. Gelogo and Byungjoo Park, "Next Generation Cloud Computing Issues and Solutions", International Journal of Control and Automation Vol., No. 1, pp. 63-70, March, 2012.

[16] Jaejung Kim, Seng-phil Hong, "A Consolidated Authentication Model in Cloud Computing Environments", International Journal of Multimedia and Ubiquitous Engineering Vol. 7, No. 3, pp. 151-160, July, 2012.

[17] Pardeep Kumar, Vivek Kumar Sehgal , Durg Singh Chauhan, P. K. Gupta and Manoj Diwakar, "Effective Ways of Secure, Private and Trusted Cloud Computing", International Journal of Computer Science Issues(IJCSI), ISSN (Online): 1694-0814, Vol. 8, Issue 3, No. 2, pp. 412-421, May 2011.

Dr. Abdelmajid Hassan Mansour Emam, Assistant Professor, Department of Information Technology, King Abdulaziz University, Faculty of Computer Science and Information Technology, khulais, Jeddah, Saudi Arabia. Ph.D in Information Technology\ Information Security from Alneelain University, Khartoum, Sudan. **Permanent Address**: Department of Information Technology, Faculty of computer Science and Information Technology, Alneelain University, Sudan, Published two papers in National Journal and