Authentication and Authorization in Cloud : Reviewing The Trend

[1] Pratiba D, [2] Dr. Shobha G, [3] Arjun A

[1,2,3] R V College of Engineering
Bangalore, Karnataka, India

Abstract - Cloud computing is a new paradigm to deliver services over the Internet. Data Security is the most critical issues in a cloud computing environment. Authentication is a key mechanism for information security that establish proof of identities to get access of information in the system. Authorization is an important identity service to avoid unauthorized access to cloud resources. According to various researches, access control and user authentication are the most important security concerns and challenging issues in cloud-based environments. In this context, in order to prevent the unauthorized access of the distributed system components, authentication and authorization functions are to be enforced effectively. In this paper, we make an analysis of various mechanisms for access control in cloud environment and identified various issues during authentication and authorization process.

Keywords - *Cloud Computing, Access Control, Authentication.*

1. Introduction

Cloud computing, as a new paradigm of information technology, has been developed very quickly in recent years. The vast spread of Internet resources on the web and fast growth of service providers enabled cloud computing systems to become a large scaled IT service model for distributed network environments. Cloud computing is built on top of already existing Internet technologies and is delivered as a self-service utility. Three service models are: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). The main characteristics of a cloud environment are abstraction and virtualization which make the technology to be perceived and applied completely in a different manner compared with existing traditional distributed systems. Cloud environment abstracts the implementation details of services and system from users and developers.

Both cloud service providers and customers are concerned about security issues associated with the cloud environment. Although different cloud domains have different security and policy characteristics corresponding to specific functionality and usage of the system, the important aspects of secure service provisioning are generic among them. All the potential security issues associated with Identity Management, Confidentiality, Authentication, Access Control, Authorization, None-Repudiation are fatal for a cloud environment [1]. In this paper, Identity Management is considered. Identity and Access Control Service should provide identity management and access control to cloud resources for registered entities. Such entities can be people, software processes or other systems. In order to give a proper level of access to a resource, the identity of an entity should be verified first, which is the authentication process that precedes the authorization process.

2. Literature Survey

This section introduces and analyses some existing solutions about identity management and cloud authentication mechanisms, which are related to this research. The work carried out in [2] presents an attribute and role based access control (ARBAC) model. Before invoking services, requestors of various services provide their attribute information to the service providers. When the service providers receive the requests, they determine whether to permit or to deny these requests according to their access control policies.

In [3], an objected-oriented RBAC model (ORBAC) is proposed, based on which multiple domain access control is obtained. A method is presented to prevent the problem of separation of duty, and it makes sure that the domain security manager does not assign multiple exclusive roles to a user at one time. In[4], identified the various issues of identity Management in cloud computing and the privacy issues associated with cloud computing such as loss of control, lack of trust and multitenancy issues are explained. The proposed model in [5] uses one client-based agent and four cloud-based agents to establish a secure algorithm during processes, services, and communications. But maintaining the cloud agents is very challenging. In [6], a security agent-based approach is presented for solving the authorization issues in the distributed computing environment. In this work, the security agents are deployed to manage the privileges for the distributed authorization and does not consider the dynamic nature of the access control. In [7], a unified hierarchy is derived starting from an access relation between users and resources, which is used to specify the access relation that allows user queries. It is also used in cryptographic schemes that enforce the access permissions and restrictions in distributed applications. In [8], in order to simplify the administration of privileges for Internet users, a set of roles is introduced. Whenever a user want to get access to a privilege, user should enters his credentials defined in XML policy and his role, in order to authorize the privilege.

The work carried out in [9] describes dynamic access control model based on roles and trust control, giving every trust value for each user by introducing trust management to access control, each role corresponds a certain trust vale, users and systems give values for each other after operation, trust management model updates trust values, users roles will change dynamically. In [10], RBAC system can be simulated partially, it can be symbolically evaluated by using some approximations of run-time properties and finally a run-time monitor can be developed for partial step-wise verification at run-time. The work carried out in [11] proposed an authentication process which is carried in two levels or two tiers. First tier uses simple username and password. In Second tier, the user is asked to enter the code which is received on mobile phone. In [12], the proposed model identifies three phases such as server initialization phase, registration phase, authentication phase and provide mutual authentication, session key agreement in cloud computing environment.

In [13], interaction between the user and the cloud service is through the cloud API. A two stage access control mechanism is implemented at the API level using the Role Based Access Control Model (RBAC). Attributes and roles of user is validated before granting resources. The work carried out in [14], is based on biometric authentication and has two stages: Enrollment and Verification. During enrollment, the user registers his biometric data. At the verification stage, the user's biometric data is compared with the template stored in the system and decision is made according to the result. In [15], Cloud Single Sign-on (SSO), Authentication model is proposed. Through Cloud SSO a cloud provider authenticates itself with other heterogeneous cloud providers regardless of their implemented security mechanism and accesses all needed external cloud resources. The work carried out in [16] proposed an authorization process through Email-ID. The user subscribing for cloud service, register his Email-ID with Cloud Service Provider. A resource link is sent to the registered email-id by Cloud Service Provider to access the Cloud resources. Hence it ensures that only valid user access the resources. The proposed model in [17] has central authentication server, where user login once. Whenever user request to use applications, the authentication server itself supplies the user credential to appropriate server. In [18], the proposed frame-work cloud services and resources are classified into three types: low, high and medium, according to risk and security level required. The user is authenticated dynamically using Secret key, One Time Password, IMEI number factors and also uses Arithmetic captcha Expression for authenticating the user.

3. Considerations

Based on the background work, we understand that research on Identity management in cloud has retained its scope to authenticate the cloud users and reliable, scalable access control mechanism for the cloud environment. The need of extensive research in the field of trust establishment among cloud entities is an important issue. The second issue is the conflict management of organizational policies for accessing various resources. The third issue is related to provide access for cloud customers during emergency [19]. In order to establish the trust among cloud service consumers and cloud service providers, they should rely on some trusted third party usually referred as Identity Provider [19]. A mutual authentication is required among cloud entities using trusted third party.

The conflict among security policies needs to be resolved based on the type of user and their level of access to the requesting resource using strong Policy decision and enforcement mechanism. During emergency, the cloud customers should be allowed to access their resources. For example, if a user has privilege to access a file on the cloud till 5PM and if he wants to access the file around 6PM, he is not allowed to access the file. A break-glass mechanism should be used to provide access to cloud resources for its users during emergency.

4. Conclusion

This paper analyzes various proposed models for user authentication and access control mechanism in cloud environment and identifies the various issues raised during the process. The issues includes trust establishment among cloud entities, security policies conflict management and break glass mechanism for accessing cloud resources during emergency.

References

[1] David Hakobyan, “Authentication and Authorization Systems in Cloud Environments”, Master of Science Thesis, Stockholm, Sweden 2012, TRITA-ICT-EX-2012:203

[2] Yonghe Wei, Chunjing Shi, Weiping Shao, ”An Attribute and Rolebased Access Control Model for Service-Oriented Environment”, IEEE ,2010, pp. 4451-4455

[3] Chang. N. Zang, Cungang Yang, ”An Object-Oriented RBAC Model for Distributed System”, in Proc. Working IEEE/IFIP Conference on Software Architecture, 2001, pp. 24-32.

[4] Kumar Gunjan, G. Sahoo, R.k.Tiwari, ”Identity Management in Cloud Computing-A Review”, International Journal of Engineering Research and Technology (IJERT), ISSN: 2278-0181, Vol.1 issue 4, June-2012

[5] Mostafa Hajivali, Maen T. Alrashdan, Faraz Fatemi Moghaddam, Abdualeem Z. M. Alothmani, “Applying an Agent-Based User Authentication and Access Control Model for Cloud Servers”, IEEE, 2013,pp. 807-812

[6] V. Varadharajan, N. Kumar, Y. Mu, ”Security Agent Based Distributed Authorization: An Approach”, the 21st National Information Systems Security Conference (NISSC), USA, pp. 315-328(1998).

[7] J.-C. Birget, X. Zou, G. Noubir, B. Ramamurthy, ”Hierarchy-Based Access Control in Distributed Environments”, IEEE International Conference on Communication, 2001, vol. 1, pp. 229-233

[8] Cungang Yang, Chang N. Zhang,”Designing Secure E-Commerce with Role-based Access Control”, in Proc. IEEE International Conference on E-Commerce, 0-7695-1969-5/03, 2003

[9] Lingli Zhao, Shuai Liu, Junsheng Li, Haicheng Xu, Lingli Zhao, Shuai Liu,”A Dynamic Access Control model based on Trust”, 2nd Conference on Environmental Science and Information Application Technology,2010, pp. 548-551.

[10] Faith Turkmen, Eunjin (EJ) Jung, Bruno Crispo, ”Towards Run-time Verification in Access Control”, IEEE International Symposium on Policies for Distributed Systems and Networks, 2011, pp. 25-32.

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

[12] 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

[13] Avvari Sirisha , G. Geetha Kumari, “API Access Control in Cloud Using the Role Based Access Control Model”, IEEE , 2010 , pp. 135-137.

[14] Hua-Hong Zhu, Qian-Hua He, Hua-Hong Zhu, Hong Tang, Wei-Hua Cao, “Voiceprint-Biometric Template Design and Authentication Based on Cloud Computing Security “, IEEE International Conference on Cloud and Service Computing,2011,pp.302-308

[15] Antonio Celesti, Francesco Tusa, Massimo Villari and Antonio Puliafito, “Three-Phase Cross-Cloud Federation Model: The Cloud SSO Authentication”,IEEE Second International Conference on Advances in Future Internet, 2010, pp. 94-101

[16] Abdelmajid Hassan Mansour Emam, “Additional Authentication and Authorization using Registered Email-ID for Cloud Computing “ , International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-3, Issue-2, May 2013, pp. 110-113.

[17] Ashish G. Revar, Madhuri D. Bhavsar, “Securing User Authentication using Single SignOn in Cloud Computing” , IEEE , 2011, pp. 1-4.

[18] Rohitash Kumar Banyal, Pragya Jain, Vijendra Kumar Jain,” Multi-factor Authentication Framework for Cloud Computing”,IEEE Fifth International Conference on Computational Intelligence, Modelling and Simulation,2013,pp. 105-110.

[19] Manoj V. Thomas, K. Chandra Sekaran, “Agent-Based Approach for Distributed Access Control in Cloud Environments”, 2013 International Conference on Advances in Computing, Communications and Informatics (ICACCI),IEEE, pp. 1628-1633.