International Journal of Advance Foundation and Research in Computer (IJAFRC)
Volume 1, Issue 12, December 2014. ISSN 2348 – 4853

Multi-level Authentication Technique for Accessing Organization in Cloud Data.

Miss. Sneha K.Khodake*, Prof. M. S. Deshmukh
Prof. Ram Meghe Institute of Technology and Research Bandera(India)

A B S T R A C T

The purpose of this paper is to present the design for providing security and higher authentication scheme for executing secure data transaction in an Organization field over Internet. There has been incessant change in technology day by day, so security mechanisms like authentication schemes are also required to be updated. Authentication schemes that involve more than single level for authentication are moderately safer than one level authentication scheme. Numbers of multi-level authentication schemes have been proposed and implemented in various cloud computing services. In case of Cloud computing, the whole authentication control lies toward the server side. So, it is very tough to trust the third party server in Cloud Computing. This work proposes a scheme in which authentication process is carried out in two levels or multi-levels. In this system, authentication activities take place in organization, team and user levels. First activity happens at organization level. It reads the authentication password and checks to cloud access for organization and then it enters into a second level authentication. The second activity happens at team level. It reads the team login details and checks for authentication. It is a team authentication activity, once authentication done; it then enters into a user level authentication. User level activity reads the authentication information to check for the user permission and privileges.

Index Terms : Authentication, security, multi-level Authentication, Cloud Computing, Authentication services, key techniques

I. INTRODUCTION

From the past few decades, there has been very fast advancement in computing technology. Systems have been designed which have high resource handling capability, capacity and computing power. For the last decade both hardware and software improvement had been the main goal for the researchers. Through the advancement of internet technology, many works are done online. This includes chatting, entertainment, information gathering and financial transactions etc. All these online activity require some type of authentication. Authentication means to verify identity of the user, which means whether the person is same which he pretends to be. In case of financial transactions, security of information is required to carry out secure transaction. Information in case of online financial transaction includes individual authentication parameters and some other account related information etc. For authentication, various techniques are used, e.g. username-passwords, biometric face recognition, public key transportation and symmetric key based authentication schemes etc. At present, authentication is done in several ways: such as, textual, graphical, bio-metric, 3D password and third party authentication. This paper presents the strict authentication system by introducing the multi-level authentication technique which generates/authenticates the password in multiple levels to access the cloud services. In this paper, details of proposed multilevel authentication technique are presented along with the architecture, activities, data flows, algorithms and probability of success in breaking authentication. Cloud computing is an emerging, on-demand and internet- based technology. It provides variety of services over internet such as, software, hardware, data storage and infrastructure. This technology has

been used by worldwide customers to improve their business performance. However, to utilize these services by authorized customer, it is necessary to have strict authentication check. Authentication schemes are key techniques to verify the correctness of the identities of all announcement entities. Authentication is quite challenging and difficult in the case of Cloud Computing. In Cloud Computing , a third party is responsible for providing computational power, storage space and application support etc. Every data which is used by a user is stored in Cloud database. Cloud database is managed by third party Cloud provider, so user hesitates to keep his data at Cloud database. In order to utilize the resources of Cloud, user has to confirm with some identity stating that it is valid person seeking permission to use their resources. If a user requirements to use or control a remote server or process financial transactions, the user needs to pass the authentication phase first [1] [2].

The remainder of this paper is organized as follows:

Section 1 presents the introduction. Section 2 gives idea about the previous work done, the Literature Survey. Section 3 briefly provides details about Proposed System Design of authentication scheme. Results have been discussed in Section 4 and finally Sections 5 conclude the paper .

II. LITERATURE REVIEW

Dinesha H A Chori , Agrawal V K Chori [1],implemented multi-level authentication technique for cloud computing services. Provides various internet based services, on demand services like software, hardware, server, infrastructure and data storage. To provide privacy services to the intended customer, it is a better option to use multi-level password generation and authentication technique. This technique helps in generating the password in many levels of organization so that the strict authentication and authorization is possible. The security levels of cloud environment can be further improved by multi-level of authentication.

Vishal saswade [3], proposed work tried to minimize the loop holes related to the security and the authentication of the user in an organization by providing multi level authentication (User ID , Password and MAC Address) encrypted in digital certificate. “Cloud” is a virtualized pool of computing resources. Cloud computing has been around for over some years in different forms. However the third generation trend in IT industry is now ruled over by cloud computing. Cloud computing is an Internet based resource sharing methodology wherein data and resources are shared and integrity of data, resources have become prime concern. Access to intruders can be restricted by providing username and password as first level authentication Cloud computing is an Internet based resource sharing methodology where in data and resources are shared and integrity of data, resources have become prime concern. Access to intruders can be restricted by providing username and password as first level authentication.

Bo Wang, HongYu Xing [4], he mainly focused on the research of the application of cloud computing in education informatization. Firstly, the traditional computer technologies, including the virtualization, network storage technology, distributed computing, parallel computing technology, network technology and automation techniques etc. have made a tremendous development. The concept of cloud computing was jointly proposed by Google and IBM in 2007. Secondly, cloud computing is of significant importance to adapt to the development of information technology in education. Furthermore, it plays an important role in creating a flexible, unified and open platform for education information, sharing of educational resources, and alleviating the information gap between different areas of education. Finally, after the analysis of the educational information technology in today's China, throught the study of the basic concepts of cloud computing technology, core technology and system architecture, they discusses cloud computing applying in education informationalization.

Tanvi Naik, Sheetal Koul [5], Current authentication schemes suffer from many weaknesses. Textual passwords are widely used; however users tend to choose meaningful words from dictionaries. This makes textual passwords easy to break and vulnerable to dictionary or brute force attacks. Many available graphical passwords face lack of space. Smart cards or tokens can be lost or are prone to theft. Many biometric authentications have been proposed but users tend to resist using them because of their intrusiveness on their privacy. The three dimensional (3-D) password is a multifactor authentication scheme i.e. it combines most of the existing authentication schemes such as textual passwords, graphical passwords, and biometrics into a single virtual three-dimensional environment. Users navigate through this virtual environment and interact with the objects placed in it. The combination of all the actions and inputs towards the virtual three-dimensional environment constructs the user's 3D password. Simple approach for a secure authentication is to use one or more of the above mentioned authentication techniques in combination for multi-level authentication, so that , the probability of breaking such a password is reduced to a large extent. Hence multi-level authentication technique can be used for ensuring a more stringent authentication.

J. Kim, Z. Kim, and K. Kim[6], proposed, the security is the most important thing in the pervasive environments. The personal information's are identified by the malicious user. Some of the drawbacks are involved in the UPnP architecture. They are user authentication, and service access control. These are all not suitable in the pervasive environments. And also the integrated heterogeneity of the pervasive environments provides the different security and pervasive environments depending upon the services and the environment provided. In our proposed concept we not only provide the multilevel user authentication but also providing the flexible security approach that adapt to the network. For security purpose we use the multi level negotiation protocol. In our proposed concept first the user registered into the network for the securely accessing the network. Because in our proposed concept the only authorized person can access the networks. After that the registration process the key will be send through their mobile. With the help of the password we can enter into the site. In this stage the authentication and authorization process is performed. We can access the system in secure manner. In our concept we can control the system via the mobile phones in secure manner because the authorized person can only access the system .

Cavoukian [7], implemented security as a service in the Cloud using a discretion algorithm and also implementing an intrusion detection system for the Cloud. To protect and mitigate the privacy and security attacks on the Cloud. Currently, there is on-going research on how to protect the confidentiality and security of data stored in the Cloud.

Sabahi f [8] argues the need for a flexible and user-centric identity management such that in the future a user will not have to re-enter credentials for a website and can rely on an identity service to manage website access. In order to protect a user's data confidentiality, some form of access control needs to be implemented in the Cloud. Access control should allow a user to choose who can view his data and who shouldn't.

Li J, Zhao G, Chen X, Xie D, Rong C, Li W, Tang L, Tang Y[9], Access Control Lists (ACLs) were originally used however, it was not effective as it was too coarse-grained and was not scalable; one of the primary features of the Cloud. An alternative and effective access control technique is encryption.

Huang R, Gui X, Yu S, ZhuangW [10], states that encryption must occur in transit, at rest and on backup media. Symmetric and asymmetric encryption, the symmetric encryption, a key is used to encrypt the data to make it virtually unreadable. The same key is also used to Secure Data Sharing in the Cloud convert the unreadable ciphertext to its original plaintext. This key must be kept confidential with the

data owner. In asymmetric encryption, a public and private key is used to encrypt and decrypt data. A user encrypts the data using another person's public key. The other person then uses his private key to decrypt the data. The public key can be broadcast to the world but the private key must remain confidential with the user. When involving data in the Cloud, encryption thus becomes crucial. Many works in literature suggest the need for encrypting data in the Cloud in some form or another.

Yao J, Chen S, Nepal S, Levy D, Zic J [11] proposed a system called 'TrustStore' which encrypts and partitions data on the client side and sends each partition to different Cloud storage providers. This greatly enhances the confidentiality of data as the chance of compromising two or more storage providers is low. However, it doesn't handle the case of data sharing and collaboration, which is the focused in that project . When considering data sharing and collaboration, simple encryption techniques do not suffice, especially when considering key management. To enable secure and confidential data sharing and collaboration in the Cloud, there needs to first be proper key management in the Cloud.

Yogesh Patel , Nidhi Sethi [12], The proposed work aims to enhance authorization and authentication process by using multilevel authentication to protect cloud from malicious user and unauthorized access, implement security measure to protect data of users stored in cloud environment. It will also provide service level security. Also user based access control is applied over user's data so that user can grant, revoke sharing permission at any point according to individual user. The data is removed completely along with access permissions as soon as owner of file request's to remove the file. The web application is HTTPS enabled. The proposed scheme is resistant to security attacks in cloud computing environment. The scheme provides multilevel authentication and service level security i.e. user needs to enter credentials sent to user when requested first time for each type of service request once per session. Here user based access control is applied over user's data like user can grant, revoke sharing permission at any point. The data is removed completely along with access permissions as soon as owner of file request's to remove the file. The site is HTTPS enabled.

III. PROPOSED SYSTEM DESIGN

In this proposed system we are going to implement the technique authenticates data at multiple levels so, generates passwords at multiple levels and then concatenates them into one single password. Authentication activities take place in organization, team and user levels. User has to go through different levels of the authentication, First authentication will ask for the user id and password which defines that user is authenticated or not, second level will assign the number of resources for team member and last one defines the access rights for the resources. It reads the authentication password and checks to authenticate the organization for cloud access. Providing different password at different levels of management, developer and user according to their accessing rights. Also providing data sharing , symmetric key(AES) & asymmetric key(RSA) and its combination for data encryption technique for the purpose of improving data security.

A. System Architecture

1. Detailed design of multi-level authentication process:

This technique authenticates the cloud access in multiple levels. It generates the password and concatenates the generated password at multiple levels. Based on the leaf level concatenated password, one can access the cloud services provided that the password authentication is successful in all the previous levels. Fig. 1 shows that the architecture of multilevel password generation technique.
This technique has two separate entities: i) Cloud service provider, who provides the cloud services and ii) Authenticated client organizations that access the cloud services (Before using cloud services,

company authentication confirms with service agreement and other formal procedure from cloud vendors).

This architecture helps in checking the authentication against the services and privileges. It also helps to ensure which customer has what kind of privileges to use cloud services. This is evaluated by multiple levels authentications. First level of authentication is organization level password authentication/generation. It is for ensuring the cloud access authentication from cloud vendor. If unauthenticated organization or hackers tries to access the cloud services, they are going to terminate in this level itself. Second level of authentication is a team level password authentication/ generation. It is to authenticate the team for particular cloud service. Like this, authentication system can have third, fourth, fifth etc level. Finally, the last level will be the user level password authentication/generation, which ensures that customer/end user has particular privileges and permission.

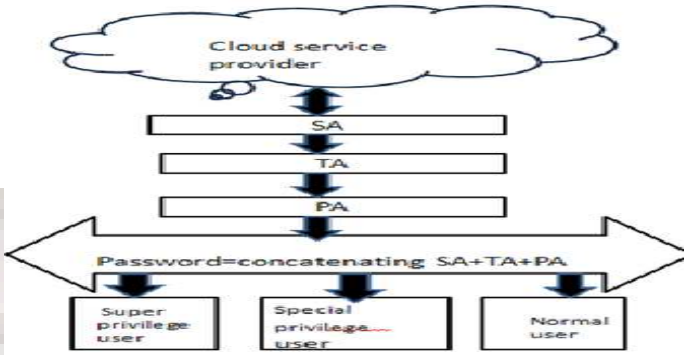

Figure 1. Architecture diagram of multilevel authentication

IV. CONCLUSION

Cloud computing provides various internet-based, on demand services like software, hardware, server, infrastructure and data storage. To provide privacy services to the intended customer, it is a better option to use multi-level password generation and authentication technique. This technique helps in generating the password in many levels of organization so that the strict authentication and authorization will be possible. The security levels of cloud environment can be further improved by multi-level of authentication. As here we are going to accept different types of password like SA, TA and PA then it will going to provide different types of data services and data access to user. Here we are also providing different level of securities to data like encryption of data using standard encryption techniques.

V. REFERENCES

[1] Dinesha H. A. CORI, Agrawal V. K. CORI "Multi-level Authentication Technique for Accessing Cloud Services," IEEE - 978-1-4673-0270-8, Feb 2012.

[2] Wen-Shenq, Juang, Sian-Teng Chen, and Horng-TwuLiaw,"Robust and efficient Password-Authenticated Key Agreement Using Smart Cards", IEEE, Transaction on Industrial Electronics, Vol. 55, No. 6, June 2008

[3] Vishal Sasawde, "Technologies Cloud Authentication System", http://www.ca.com/us/authentication system.aspx

[4] Bo Wang, HongYu Xing, "The Application of Cloud Computing in Education Informatization", IEEE Modern Educational Tech. center.

[5] Tanvi Naik ," Multi-Dimensional and Multi-Level Authentication Techniques ", International Journal of Computer Applications (0975 – 8887) Volume 75– No.12, August 2013.

[6] J. Kim, Z. Kim, and K. Kim, "A lightweight privacy preserving authentication and access control scheme for ubiquitous computing environment", Proc. of The 10th International Conference on Information Security and Cryptology, Berlin, Heidelberg: Springer-Verlag, 2007, pp. 37–48.

[7] Cavoukian " Privacy in the clouds" ,Identity Inf Soc 1(1):89-108, 2008

[8] Sabahi F (2011)" Cloud computing security threats and responses",IEEE 3rd international conference communication software and networks (ICCSN) 2011, pp 245–249.

[9] Li J, Zhao G, Chen X, Xie D, Rong C, Li W, Tang L, Tang Y " Fine-grained data access control systems with user accountability in cloud computing ", IEEE second international conference on cloud computing technology and science(CloudCom) 2010, pp 89–96.

[10] Huang R, Gui X, Yu S, Zhuang" Research on privacy preserving cloud storage framework supporting cipher text retrieval", International conference on network computing and information security 2011:93–97, 2011

[11] Yao J, Chen S, Nepal S, Levy D, Zic J " TrustStore: making Amazon S3 trustworthy with service composition", 10th IEEE/ACM international conference cluster, cloud and grid computing (CCGrid) 2010, pp 600–605,2010.

[12] Yogesh Patel1 , Nidhi Sethi2:"Enhancing Security in Cloud Computing Using Multilevel Authentication" ,International Journal of Electrical Electronics & Computer Science Engineering Volume 1, Issue 1 (February 2014), ISSN : 2348 2273.

AUTHORS PROFILE

Miss.Sneha Khomeshwar Khodake persuing Master of Engineering degree From Sant Gadge Baba Amravati University , India

