International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

An Adopted Multi-level Authentication Framework in Cloud Environment

Shaik Mujafar[1], K. B. V. Rama Narasimham[2]

[1, 2] Computer Science Engineering, Guntur Engineering College, Guntur, India

Abstract: ***Cloud Computing provides vast types of services by means of internet connectivity. Cloud has been an vast area of research since its inception, one such area is authentication of the user to cloud securely. Authentication is a process of verify the right entity and granting the permission to enter into the system and function. Thus authentication is a crucial part of any system to protect its data integrity and security. So far, the moated trusted forms of authentication are text based passwords. this form of passwords are most likely to fall short of performance due to factors as easy guess, human memory involvement, and with today's era of computation easy computable or breakable due to which many researchers in the past has been argued to provide alternative method of authentication, such as mnemonic password, graphical password, and biometrics. 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 a represented along with the architecture, activities, data flows, algorithms and probability of success in breaking authentication.***

Keyword: Bio-metric, Cloud Computing Authentication, Graphical password, Multi-level Authentication.

1. Introduction

Cloud computing since its inception has seen vast growth in its adoption by IT-Industry. Cloud computing is a paradigm of computing that aims at providing dynamically scalable computing resources over the Internet as a service. Users do not need to bother about the management of technology infrastructure. They simply use the resources on a pay-per-use basis, commissioning and decommissioning as many instances of computing resources as needed.

1.1 Types of Cloud Services

Cloud service providers provide services such as software, hardware, data storage and infrastructure. Cloud Computing Services are grouped into 4sections: they are, Software as a Service(SaaS), Data as a Service(DaaS),Infrastructure as a Service(IaaS) and Platform as a Service(PaaS)[3] [4]. SaaS (Software as a Service) is an on-demand application service. It delivers software as a service over the Internet. It eliminates the need of installing and running the application on the customer's own computers [3] [4]. PaaS (Platform as a Service) is an on-demand platform service to host customer application. Authentication is quite challenging and difficult in the case of Cloud Computing. In order to utilize the resources of Cloud, user has to prove with some identity stating that it is valid person seeking permission to use their resources. If a user needs to use or control a remote server or process financial transactions, the user needs to pass the authentication phase first [2].

2. Literature Review

Denial of Service (DoS) attacks – It has been argued that a cloud is more susceptible to a DoS attack; because more than one client can access cloud at the same time, which makes DoS attacks much more damaging. Twitter has suffered a devastating DoS attack in 2009[7].To access these cloud services securely, cloud authentication systems are using different methods like: i) Traditional text password ii) Trusted Third party authentication iii) Various Graphical password methods iv) Limited Biometric systems and v) 3D password objects. 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 [5] is not preferred for smaller cloud deployment [6]. Graphical passwords have memory space that is less than or equal to the textual password space. Graphical passwords are based on the idea that users can recall and recognize pictures better than words. However, some of the graphical password schemes require a long time to be performed [4] [5]. Bio-metric authentications such as, finger prints, palm prints, hand geometry, face recognition, voice recognition, iris recognition, and retina recognition, have been proposed in literature. Each bio-metric recognition scheme has its own advantages and disadvantages based on many factors such as consistency, uniqueness, and acceptability. One of the main drawbacks of applying biometrics is its intrusiveness upon a user's personal characteristic. In addition, most bio-metric systems require a special scanning device to authenticate users, which is not applicable for remote and Internet users. 3D- password does not support the multiple levels of authentication [6]. Another simple approach is to use one/combination of the above techniques in multi-level authentication, so that, probability of breaking such a password is reduced to a large extent. Hence it has motivated us to introduce a multi-level authentication technique in secure cloud transmission for ensuring the strict authentication. Fig 2 briefs the activities of multi-level authentication 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 authenticate the organization for cloud access 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.

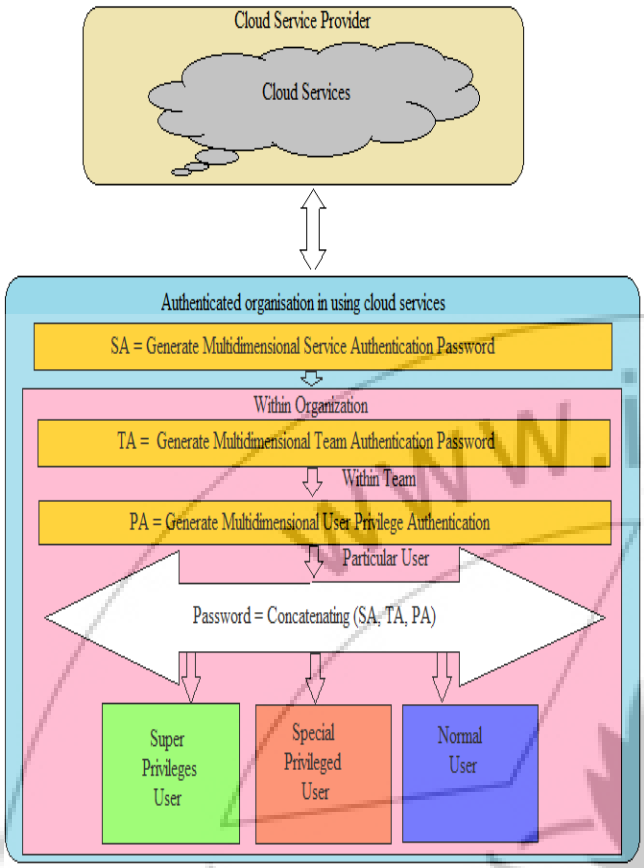

Figure 1: Framework diagram of multi-level authentication system

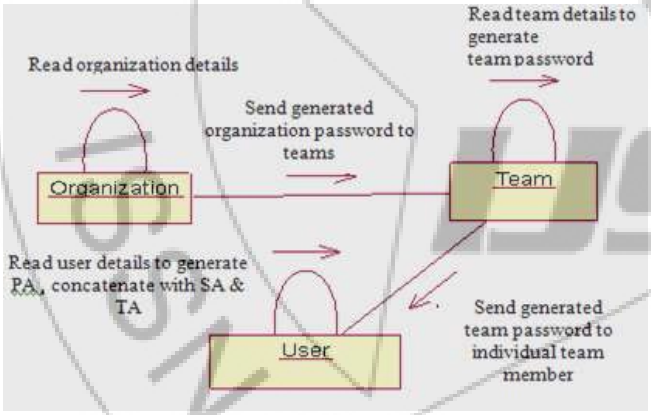

Figure 2: Activity diagram to generate multi-level password

3. Adopted Multi-Level Authentication Framework

The proposed Framework generates the unique password and combines the phased password at multiple levels. Based on the successful password verification on phases, access to cloud services is granted. Fig. 1 shows that the architecture of multilevel password generation technique. This framework 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.

4. Show case of Multi-Level Authentication Framework

This section presents the data flow diagram and algorithm of multi-level password generation technique discussed in section2. Fig 3 shows the DFD Level 0 for multi-level password generation and authentication system. Password generation will happen between the cloud service provider and cloud customer and then the password gets authenticated while accessing the cloud service. Fig 4 shows the DFD level 1 for the multi-level authentication system. This DFD describes detailed flow of password authentication process.

Figure 3: Data Flow Diagram Level 0 to shows the Overview of multi-level authentication

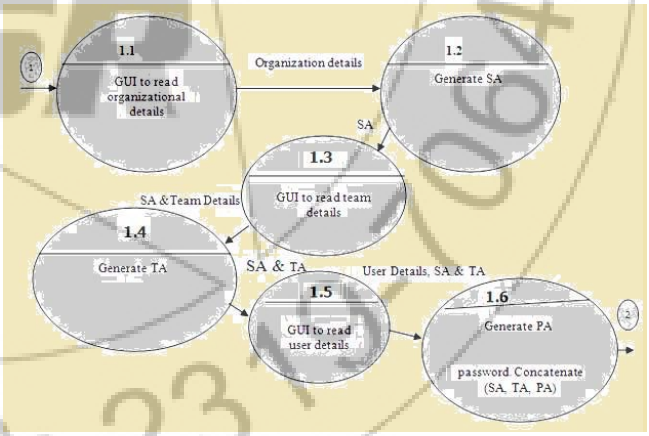

Figure 4: Data Flow Diagram Level 1 to shows the multi-level authentication process

A. Proposed Algorithm

Section below presents the algorithm of complete multi-level password authentication/generation technique. Important notations being used in the algorithms are: SA-service authentication, TA- team authentication and PA- privilege authentication. Multi-level authentication system reads the details given by organization, team and user and produces the password output at different levels.

Algorithm: Multi-Level Authentication

Step 1: SA - Organization level password generation
If SA is authenticated organization then
TA - Team level password generation
If TA is authenticated then
…
PA – User level password generation
If PA is authenticated user then
Password = Concatenate SA, TA (...) and PA
If password privileged authenticated then

Provide cloud service
Else
Go to step 2
End
Step 2: Exit

B. Probability of Breaking Multi-Level Authentication

In multi-level authentication system, to be successful, one has to know the password of all the levels. Example: Let us take three levels (as shown in architecture) such as organization level, team level and user level and two outcomes such as success and failure to determine probability of breaking.

Let S be the sample space. Two outcomes of event are success S and failure F. To break this one has to succeed in three times repeatedly. Hence, Sample Space S = {SSS, SSF, SFS, SFF, FSS, FFS, FFF, FSF}

=> n (S) =8 where n(S) is the cardinality of set S.

Assuming
i. Success and failure probability at each level is independent and
ii. The Probability of success at each level 'p' Then
Success of breaking multilevel authentication given by probability of the event SSS, defined as P (E) and is equal to P (E) = p3.

Failure in breaking the multilevel authentication system is1-P (E) = 1- p3.

For Instant, If probability of success at any level p=0.1 (say) then the probability of breaking the multi-level (three level) authentication is 0.001. Therefore, we conclude that by using multi-level authentication technique, we can improve the security folder. Multi-level technique is a simple technique. Even though it has multiple levels of authentications, at every stage, every user has a burden to remember only one password. Based on the above discussion, we expect the use of multi-level authentication to provide better security for accessing the cloud services.

5. Conclusion and Future Enhancement

Cloud authorized access has to be defined to perfection as users data security plays an vital role in the cloud architecture, we designed and elaborated an unique multi level authentication framework successfully which can enhance the security framework indeed thus the security levels of cloud environment can be further improved by multi-level of authentication. Further we can lead research over multidimensional password generation method to multi-level authentication technique.

References

[1] Kundu, C. D. Banerjee, P. Saha, "Introducing New Services in Cloud Computing Environment", International Journal of Digital Content Technology and its Applications, AICIT, Vol. 4, No. 5, pp. 143-152, 2010.
[2] DoD Directive 3020.40, Defense Critical Infrastructure Program, 19 Aug, 2005, p. 13, http://www.dtic.mil/whs/directives/corres/pdf/302040p.pdf.
[3] Cloud Computing services & comparisons http://www.thbs.com/pdfs/Comparison%20of%20Cloud%20computing%20services.pdf
[4] A User Identity Management Protocol for Cloud Computing Paradigm Safiriyu Eludiora1, Olatunde Abiona2, Ayodeji Oluwatope1, Adeniran Oluwaranti1, Clement Onime3,Lawrence Kehinde apered in Int. J. Communications, Network and System Sciences, 2011, 4, 152-163
[5] CA Technologies cloud authentication system http://www.ca.com/us/authentication-system.aspx
[6] . X. Suo, Y. Zhu, G. S. Owen, "Graphical passwords: A survey," in Proc.21st Annual Computer Security Application. Conf. Dec. 5–9, 2005, pp. 463–472.
[7] S. Wiedenbeck, J. Waters, J.-C. Birget, A. Brodskiy, and N. Memon, "Authentication using graphical passwords: Basic results," in Proc.Human-Comput. Interaction Int., Las Vegas, NV, Jul. 25–27, 2005.
[8] Fawaz A. Alsulaiman and Abdulmotaleb El Saddik, "Three-Dimensional Password for More Secure Authentication," IEEE, http://ieeexplore.ieee.org., Last Updated – 6 Feb 2008
[9] Cloud Computing services & comparisons http://www.thbs.com/pdfs/Comparison%20of%20Cloud%20computing%20services.pdf
[10] A User Identity Management Protocol for Cloud Computing Paradigm Safiriyu Eludiora1, Olatunde Abiona2, Ayodeji Oluwatope1, Adeniran Oluwaranti1, Clement Onime3,Lawrence Kehinde apered in Int. J. Communications, Network and System Sciences, 2011, 4, 152-163
[11] Protection against Denial of Service and Input Manipulation Vulnerabilities in Service Oriented Architecture. Alwyn Roshan Pais, Deepak D. J. , and B. R. Chandavarkar. Chennai,India : Springer, 2011. Advances in Network Security and Applications. pp. 331–343.

Author Profile

Shaik Mujafar Obtained M.Sc degree in Computer Science from Andhra University College of Engineering, Visakhapatnam. At present pursuing the M.Tech in Computer Science and Engineering (CSE) at Guntur Engineering College, Guntur.

K. B. V. Rama Narasimham obtained the M.C.A Degree from Madras University in 1999 and M.Tech (CSE) from JNTU, Kakinada in 2013. At present pursuing Ph. D (CSE) in K. L. University. He has 8 years of teaching experience and working in Computer Science and Engineering (CSE) Department at Guntur Engineering College, Guntur.