Multi-Level authentication in Cloud Computing using 3D security

Jeena Jha
jeenajha22@gmail.com
Jalak Pansuriya
B.Tech, Computer Science, Jaipur National University, Jaipur, India
jalakpansuriya1995@gmail.com

ABSTRACT

Cloud computing is an emerging, on-demand internet- based technology. It provides variety of services over internet such as, software, hardware, data storage and infrastructure. The 3D security checking system by using the multi-level authentication technique generates the password in multiple levels to access the cloud services. This system is able for thwarting Shoulder attack, Tempest attack, and Brute-force attack, dictionary attacks and many more which are present at client side, with the use of strong techniques in the Graphical password.

Keywords—Cloud Computing, Authentication, Graphical password, 3D security, multi-level authentication

I. INTRODUCTION

Cloud computing is internet based technology which provides variety of services over internet such as software, hardware, data storage and infrastructure. Within the cloud computing systems environment, the virtual environment lets user's access computing power that exceeds that contained within their own physical worlds. Fundamentally, abundant security issues arises as it comprises many technologies including networks, virtualization, operating systems, resource scheduling, transaction management (when user query about some secure data), load balancing(preventing the cloud from crashing when the user demand increases),concurrency control(many users simultaneously requesting or accessing the same data on the cloud) and memory management. It also encompasses scheduling data backup and safe storage of the backup media. Security is implicit within these capabilities, but moreover elementary concerns exists that need attention. Cloud computing is becoming a tempting target for cybercrime. If not all cloud providers supply adequate security measures, then these clouds will become high-priority targets for cybercriminals. As cloud systems are inherited architecture so a single cyber attack offers opportunity to the attacker to influence a large number of sites through a single malicious activity. There are many security issues are arises for accessing these services in cloud. To remove these issues the 3D security system is provided with powerful and more secure authentication techniques. This system is responsible to categories the files or confidential data on cloud. Categorization is depends on 3 important factors: Confidentiality, Integrity and Availability.

II. SECURITY ISSUES IN CLOUD

The cloud security and privacy is a big concern now a day. Security, privacy and secure storage of data are two barriers which are preventing the organizations and users from adopting the cloud computing. Emphasis must be given on security, privacy and stability on the cloud based technologies and computing to make them admirable among the corporate multitenant environment. Malicious and Abusive attacks are proliferating cloud security. The data leakage and security attacks can be caused by insufficient authentication, authorization, and audit (AAA) controls, inconsistent use of encryption and software keys, operational failures, persistence and reminisce challenges: disposal challenges, risk of association, jurisdiction and political issues, data center reliability, and disaster recovery. Some of the risks in cloud computing are well known in traditional computing models.

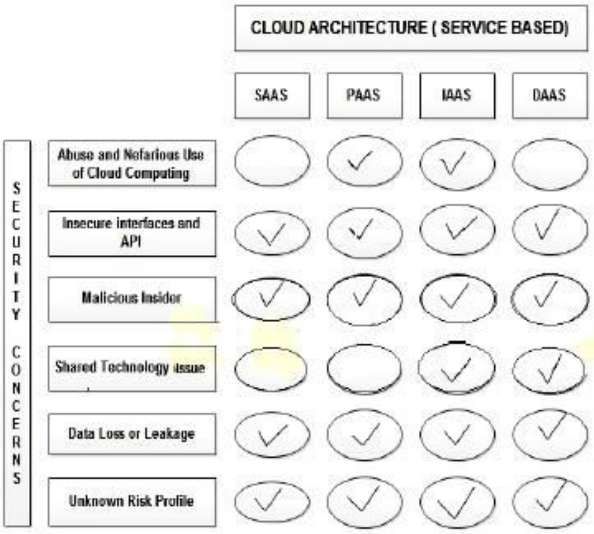

Figure 1.1: Security concerns in various Clouds Architecture

These risks include, for example, malicious insiders, insecure user authentication (such as usage of weak passwords), malicious code running on the cloud, vulnerabilities of the shared resources leading to information leakage, or account hijacking by phishing methods, unknown risk profile, data loss (no stability in data storage on cloud).

III. 3D SECURITY TECHNIQUE

The 3D security system is provided with powerful and more secure authentication techniques. This system is responsible to categories the files or confidential data. It is a multi-level authentication system. It removes the time complexity issue.

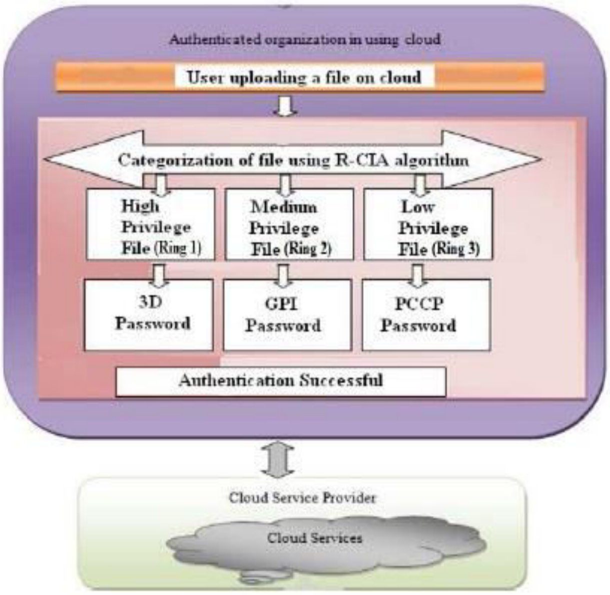
Authenticated organization in using cloud
User uploading a file on cloud
Categorization of file using R-CIA algorithm
High Privilege File (Ring 1)
Medium Privilege File (Ring 2)
Low Privilege File (Ring 3)
3D Password
GPI Password
PCCP Password
Authentication Successful
Cloud Service Provider
Cloud Services

Figure1. 2: Architecture of 3D security system

In 3D security system, User accesses the cloud services. User is going to upload a file on the cloud. There are 3 Protection rings. The inner most ring is most secure. The file categorization is done using Revised- CIA algorithm. The R-CIA divides the files into ring 1, ring 2 and ring 3. 3D password is used for ring1. GPI (Graphical password with icons) password is used for ring2. PCCP (Persuasive clued click point) password is used for ring3. At the time of downloading, this password should be match. If it is matched, then the authentication is successful. The user can access the cloud services.

1) Ring-1:-

The 3-D password is a multifactor authentication scheme. For the authentication, it is require to presents a 3-D virtual environment where the user navigates and interacts with various objects. The sequence of actions and interactions toward the objects inside the 3-D environment constructs the user's 3-D password. The 3-D password can combine most existing authentication schemes such as textual passwords, graphical passwords, and various types of biometrics into a 3-D virtual environment. The design of the 3-D virtual environment and the type of objects selected determine the 3- D password key space.

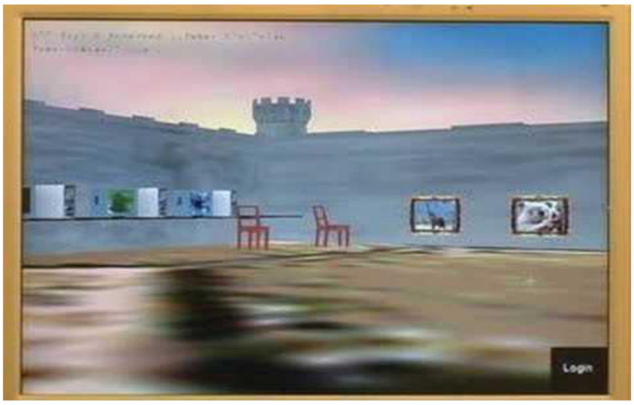

Figure 1.3: 3D password

2) Ring-2:

GPI (**G**raphical **P**assword with **I**cons) is the first graphical password scheme we propose in this paper. In GPI, to mitigate the hot spot problem users may click on a subset of displayed icons as their passwords instead of selecting specific locations on a background image. Experimental results show that the use of icons in GPI makes possible to evenly distribute possible click-points to a certain extent.

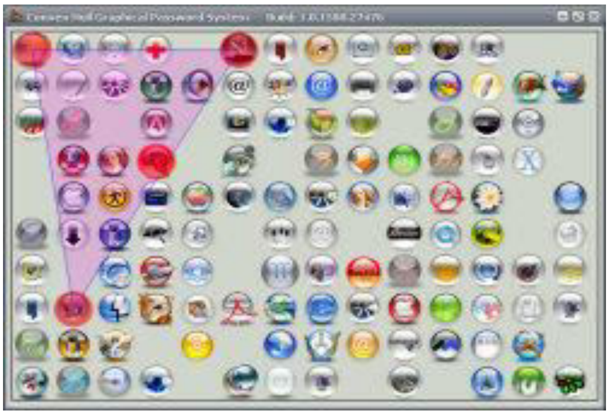

Figure 1.4: GPI interface

3) Ring-3:

To address the issue of hotspots, Persuasive Clue Click Point (PCCP) was proposed. As with Clue Click Point, a password consists of five click points, one on each of five images. During password creation, most of the image is dimmed except for a small view port area that is randomly positioned on the image as shown in Fig 1.5 Users must select a click-point within the view port. If they are unable or unwilling to select a point in the current view port, they may press the Shuffle button to randomly reposition the view port. The view port guides users to select more random passwords that are less likely to include hotspots. A user who is determined to reach certain click-point may still shuffle until the view port moves to the specific location, but this is a time consuming and more tedious process.

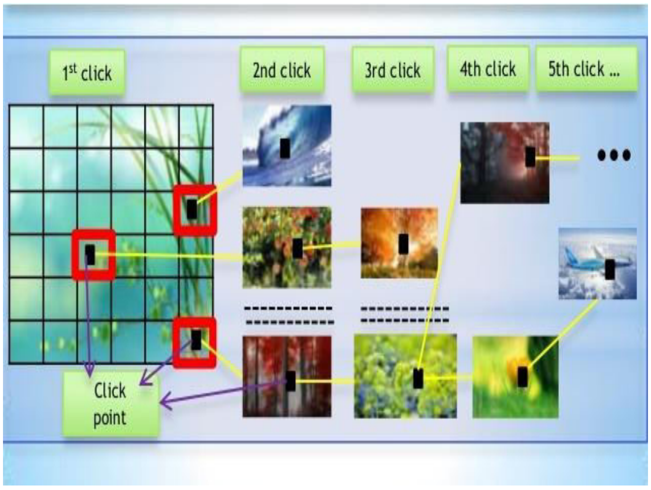

Figure 1.5: Persuasive Clue Click Point

IV. PROPOSED MULTI-DIMENSIONAL PASSWORD GENERATION TECHNIQUE

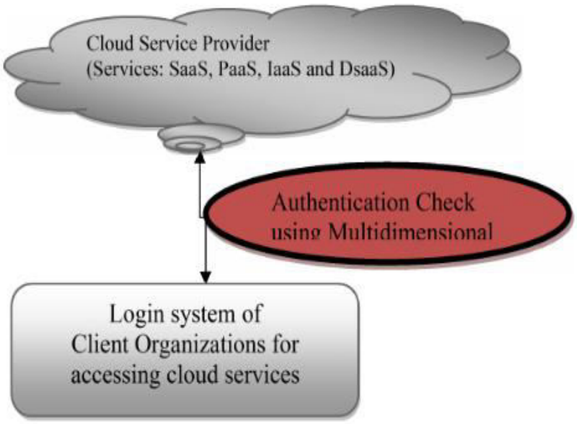

Fig 1.6: Architecture of multidimensional authentication system

According to our proposed theory, access to the cloud is authenticated using a multi-dimensional password. It generates the multi-dimensional password by considering the many parameter of cloud paradigm such as: vendor details, consumer details, services, privileges and etc. These parameters considered as input dimension. These many dimensions (input) combined together and produces multidimensional password. Fig. 1.6 depicts the architecture diagram of multi-dimensional authentication system. This has two separate entities i) cloud service provider which provides variety of cloud services and ii) Authenticated client organization to use cloud services (Before using cloud services, company authentication confirms with service agreement from cloud vendors). This architecture helps in checking authentication against the services and privileges. The multi-dimensional password is generated by considering many aspects and confidential inputs such as logos, images, textual information and signatures etc. This is portrayed in figure 1.7. With the help of this technique, the probability of brute force attack for breaking the password is greatly reduced.

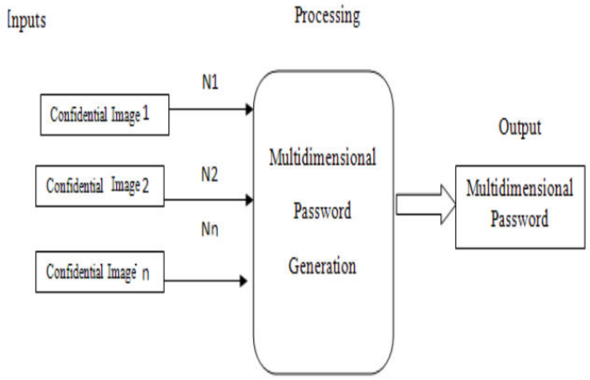

Fig 1.7: Multi-Dimensional password generation technique

V. CONCLUSION

To provide Cloud services to the intended customer, it is a better option to use 3D Security system rather than multi-level 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 level of cloud environment is much stronger by using multi-level security system. Depending on rings, levels of multilevel security system increases for secure access of cloud services. This system is able for thwarting Shoulder attack, Tempest attack, and Brute-force attack, dictionary attacks and many more which are present at client side, with the use of strong techniques in the Graphical password.

Thus, according to our proposed theory, to provide secured services to intended customer, we have used multi-dimensional password generation technique. The multi-dimensional password gets generated by considering many aspects and inputs such as, logos, images, textual information’s and signatures etc. By doing so, the probability of brute force attack for breaking the password can be reduced to a large extent.

VI. REFERENCES

[1] www.wikipedia.com
[2] www.slideshare.com
[3] Rupal Rawat, Sreeja Nair “ A novel graphical password approach for accessing cloud and data verification”
[4] Jaidep sen “Security and privacy issues in cloud computing”
[5] Vaishnavi Deokar, Sayali Deshpande, Radhika Devkar “Password Generation Techniques For Accessing Cloud Services”
[6] "Database as a Service," MIT-CSAIL-TR-2010-014.
[7] M. Riccuiti. Stallman: Cloud computing is stupidity. Available: http://news.cnet.com/8301-1001_3-10054253-92.html

[8] N. Antonopoulos and L. Gillam, *Cloud Computing*: Springer-Verlag London Limited, 2010.

[9] K. JACKSON, "Secure Cloud Computing: An Architecture Ontology Approach," Defense Information Systems Agency 2009.

[10] R. Raja and V. Verma, "Cloud computing: An overview," Research Consultant, IIIT Hyderabad.

[11] D. Rowe. (2011, The Impact of Cloud on Mid-size Businesses. Available: http://www.macquarie telecom.com/hosting/blog/cloud-computing/impact-cloudcomputing-midsize-businesses

[12] S. Hanna, "Cloud Computing: Finding the Silver Lining," Juniper Networks2009.

[13] NIST Definition http://www.au.af.mil/au/awc/ awcgate/nist/cloud-def -v15.doc

[14] Cloud Computing services & comparisons http://www.thbs.com/pdfs/Comparison%20of%20Cloud%20cmputing%20services.pdf

[15] Safiriyu Eludiora1, Olatunde Abiona2,Ayodeji Oluwatope1, Adeniran Oluwaranti1, Clement Onime3,Lawrence Kehinde "A User Identity Management Protocol for Cloud Computing Paradigm" appeared in Int. J. Communications, Network and System Sciences, 2011, 4,152-163

[16] 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.

[17] 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.

[18] Fawaz A. Alsulaiman and Abdulmotaleb El Saddik,"Three-Dimensional Password for More Secure Authentication", Instrumentation and Measurement, IEEE Transactions , 03 April 2008, 57, Issue:9, 1929–1938