# Enhancing User Security in Cloud Computing using Colour Palette Scheme (CPS)

**Dr.S.HariGanesh, S.Ananthi**

***Abstract* -- Cloud computing is one of the most exciting technologies in recent trend. This technology not getting that much impact because of its limitations. At present cloud user authentication is done by many ways like password authentication, Graphical and 3D password etc. In this paper we proposed the robust strong authentication generation technique by authentication and session management in cloud computing environment. User authentication executes in several modules like user registration, user login, user authentication, and password modification using Colour palette.**

***Index Terms*--Cloud computing, Colour palatte scheme Password change, Session management.**

## I. INTRODUCTION

The success of any technology is purely depends upon the effectiveness. Cloud Computing is a service based mostly on the safe, convenient and knowledge storage service in web computing [1]. Cloud computing model for enabling convenient on demand for network access to a shared pool of configurable computing resources like networks, servers, storage and release with minimum management efforts or service providers [2]. Cloud computing models are divided into non-public cloud, public cloud and hybrid cloud according to the various service objects. Public clouds are virtualizes data centers outside of firewall and service provider makes resources available for client or demand over web [3]. The non-public cloud is deployed within the company and security will be created simply. Non-public clouds virtualized cloud data centred within firewall and it's non-public area dedicated to system among cloud data centre. Non-public cloud refers to internal data center of business or different organization [4]. Hybrid cloud is that the combination of two or more clouds. Hybrid cloud combines each non-public additionally as public clouds [5]. Software as a Service (SaaS):- within the SaaS model cloud provider installed and operates application software within the cloud and cloud users access software from cloud client [7]. Cloud users do not manage the cloud infrastructure and platform on that application is running. This eliminates ought to installed and run the appliance on the cloud. Platform as a service (PaaS):- In PaaS model cloud supplier deliver a computing platform usually as well as OS, programming language execution environment, database and internet server [8]. Application developer will develop and run their software resolution on a cloud platform while not the cost and complexity of shopping for and managing the hardware and computer code layers [9]. Infrastructure as a Service (IaaS):- Primary objective of an organization is to reduce time and cash needed to provide provision and install new hardware system [10]. IaaS fulfil the first objectives i.e. instrumentation is outsourced to supports operation. The service providers are accountable for housing, running and maintenance of equipment. Several companies and organization are placing their data into cloud. As cloud computing are concerned reliability, ownership, data backup and plenty of additional things like security [11]. The application security and identity management, access control and Authentication [12]. Confidentiality doesn't guarantee of security. It's to think about authentication and authorization features [13].

## II. LITERATURE SURVEY

Cloud server architecture play a dominant role in user authentication. For this, we prefer some existing authentication scheme. Most of the popular remote authentication procedure was recommended by Lamport in 1981[14]. In this server stores each User_Id and password in hash table for verification. The password generation uses hash functions that generate service of password. Existing some password authentication schemes are proposed [15]. Smartcard is employed to prevent from the attack. so as to create a secure usage of services provided by the cloud. Cloud user authentication systems may be use completely different password techniques like 1) simple text password 2) Graphical password authentication 3) 3D password object. The weakness of password authentication



ISSN: 2278 – 1323 

system is, it may be break and extremely a lot of liable to attack. Graphical password needs memory area that is found less or equal area to matter password. Whereas graphical password need massive area and time [16]. 3D countersign having its own limitations. Some systems have proposed authentication supported sending the SMS, however it doesn't guarantee to delivery of SMS on time. Therefore as review of higher than mentioned existing systems, in this paper I proposed some technique to access the computing resources hope all these technique makes the computing security more stronger.

## III. PROPOSED WORK

This work consist of the following phase: User registration, User login, password generation phase and finally the generated session password is send to the registered email-id. With this access user enjoy the utmost security.

### *A. User Registration*

Whenever user wants to access cloud resources, user has to register first on to the cloud. The way to register on the cloud are as follow

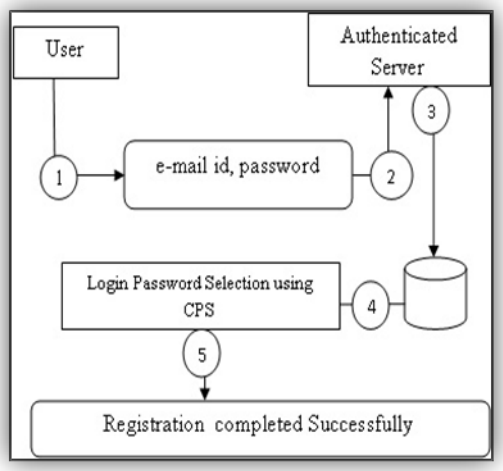


Fig.1. Registration phase

The way to register is as follow like steps:

1. User want to register in the cloud he should give valid email_id along with the password to the Authenticated server.
2. Then the Authenticated server store the user email_id and password in the database, for further verification.
3. After storing the user information, the server switch the user access to the Login Password Selection phase.

Login Password Selection phase is a sub-phase in the registration phase. In this phase user must select the login password this is for give more security to the user access. In this user select the four colours from the palette it will automatically fix in the corresponding box in sequential order. The below figure show that


.

Fig.2. Login Password Selection phase

The selected colour in order is considered as a another password to access the cloud resources. Selected password is also store in the database. If user selects the password the user registration is successfully completed.

### *B. Login Phase*

In this phase user undergo many verification process to access their own resource. All these process to provide the utmost security to the user. Login phase comprise the following steps are

1. User give valid email_id along with the password not the login password.
2. The server authenticate the user given details with the details which are already given at the time of registration.
3. If the given details are matched then the server insist the user to undergo the CPS test.
4. If the user pass in the test, he is allowed to access the resource. Unless he repeat the test till the user succeed. In other word user have only three times to participate in that CPS test in a day.

Colour Palette Scheme is comprising the following steps are as

- User select the colour from that scheme in those order which is in already registered scheme.
- If user complete the step1, then user move to the next step i.e. user should fill the textbox by numbers which is randomly displayed on the screen. Those numbers in screen are arranged in the



ISSN: 2278 – 1323 

order of rows and column. User choose the number from rows corresponding to the column.

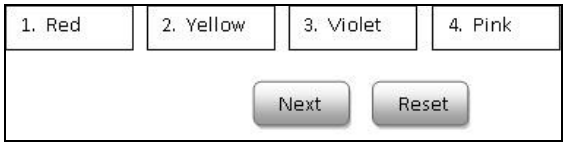


Fig.3.1 User entries for Login Password

The above figure show the completed entry for login password.

| | Violet | Orange | White | Black | Pink | Yellow | Green | Blue | Red |
|---|---|---|---|---|---|---|---|---|---|
| Red | 9 | 8 | 6 | 4 | 3 | 2 | 5 | 1 | 7 |
| blue | 6 | 8 | 7 | 4 | 5 | 3 | 1 | 2 | 9 |
| Green | 3 | 2 | 1 | 5 | 7 | 8 | 9 | 4 | 6 |
| Yellow | 3 | 8 | 4 | 9 | 2 | 1 | 5 | 6 | 7 |
| Pink | 1 | 8 | 7 | 6 | 9 | 3 | 2 | 5 | 4 |
| Black | 6 | 2 | 1 | 3 | 5 | 4 | 8 | 7 | 9 |
| White | 8 | 7 | 3 | 2 | 5 | 4 | 6 | 1 | 9 |
| Orange | 6 | 2 | 6 | 4 | 1 | 5 | 3 | 8 | 7 |
| Violet | 1 | 4 | 6 | 3 | 5 | 8 | 7 | 2 | 9 |

Fig.3.2. User entries for Login Password

The user must fill the box with number select from the above table. For e.g. user select red, yellow, violet, and pink. Then the user choose number from red to red in rows and column and the selected number is "7". The selected number corresponds to both rows and column. Like wise he choose the numbers "7119". And the final step is user are not supposed to fill as such as, he should reverse the number like"9117" and then fill it in the login box.

After this the server authenticate the user access, it send the password (token) to the user valid email-id.

### *C. Password Generation Phase*

Authentication server generates the dynamic token from hash table and sends it to the user's Email_Id for authentication. User checks his Email for obtaining the dynamic token for more authentications. User has to enter the token value for authentication. Authentication server matches the token with the dynamic token that was send by itself. When matching the token authentication, user will Authenticate and server provides access of resources to the user.

## IV SECURITY ANALYSIS

In this system security is provided by authentication and dynamic token send to user's Email_Id. There area unit some security measures that satisfy this proposed system.

### *A. Authentications*

By providing dynamic token on to the user's Email_Id no attacker will receive the dynamic token which can be helpful for authentication.

### *B. Session Management*

Session key i.e. dynamic token is generated from hash table. This token can remain valid up to the actual session only. When the logout or some amount of time it'll get expired.

Apart from this other dreadful attacks like Dictionary Attacks, Guessing, Shoulder surfing, Bruteforce attacks and Complexity are eradicated.

## V CONCLUSION

Cloud computing provides the variety of internet based on demand services. To provide secure services to the client, I have used authentication technique with several security features like authentication, session management. These technique provide a high security to the server to resist the attacks like password stolen attacks, replay attacks.

## VI REFERENCES

[1] Center Bo Wang, HongYu Xing "The Application of Cloud Computing in Education Informatization, Modern Educational Tech..." Computer Science and Service System (CSSS), 2011 International Conference on IEEE, 27-29 June 2011, 978-1-4244-9762-1, pp 2673 – 2676

[2] Mell P. and Grance T., "The NIST Definition of Cloud Computing", vol 53, issue 6, 2009.

[3] A Platform Computing Whitepaper, enterprise cloud computing: Transforming IT. Viewed 13 March 2010

[4] Dooley B 2010, „Architecture requirement of The Hybrid Cloud". Information Management Online, Viewed 10 February 2010

[5] Global Netoptex Incorporated, 2009, Demystifying the Cloud. Important opportunities, choices, Viewed 13 December 2009.

[6] Lofstrand M, „The VeriScale Architecture: Elasticity and Efficiency for Private Clouds", Sun



ISSN: 2278 – 1323 

Microsystems, Sun Blueprint, Online, Part No 821-0248-11, Revision 1.1, 09/22/09

[7] S. Roschke, et aI., "Intrusion Detection in the Cloud," presented at the Eighth IEEE international Conference on Dependable, Chengdu, China, 2009.

[8] Leavitt N, 2009, „Is Cloud Computing Really Ready for Prime Time?" Computer, Vol. 42, pp. 15-20, 2009.

[9] Brodkin J, 2008, „Gartner: Seven cloud-computing security risks", 13 march 2009 from http://www.infoworld.com/d/security-central/gartner-seven-cloudcomputing

[10] Reddy B. ET. Al., "Cloud computing security issues and challenges", 2009.

[11] Almulla S. A., Yeun C. Y., "Cloud Computing Security Management", Engineering Systems Management and Its Applications (ICESMA), Second International Conference, 2010.

[12] Lamport L., "Password authentication with insecure communication," Communications of the ACM, vol. 24, issue 11, Nov 1981.

[13] Hwang M.S., and Li L H., "A New Remote User Authentication Scheme using Smart Cards", IEEE Transactions on Consumer Electronics, vol. 46, issue 1, 2000.

[14] 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.



ISSN: 2278 – 1323 