Design And Implementation of an Optimized Way of Multi-Phase Grid And Color Based Password Authentication System in Cloud Computing

Teshu Gaurav Singh **Miss Sarita Sharma** **Mr. Gurpreet Singh Chhabra**

Abstract— **Human being can remember graphical notations & signs, very easily & for a long time. The main aim of this paper is to build a mechanism for password so that our password become more secure, remembering durability & easy to create. We have implemented for multi-tier authentication system, because multi-tier authentication system is more secure than single level authentication system. We are using graphical symbols as password, So that user can remember multiple passwords for a long time. Obviously, if we are giving more facility to the user then we must more concern towards the security of the passwords. This is a mechanism to optimize between facilities & securities. Our main concern about security is to protect the user from Shoulder Surfing attack & Dictionary attack.**

Index Terms— **Graphical password, Password optimization, Secure Cloud authentication, ease to remember, Shoulder Surfing, Dictionary attacks.**

I. INTRODUCTION

Now a day's security is a big concern in the age of cloud computing. Recently there has been a great emphasis to offer more security for passwords. The 21st century is definitely the more advancing age of world-wide-web as well as related contents, highly exposing data which innovated before an additional or say in respect of many just a few seconds. Probably the traditional opportunity for authentication is textual Security password. Most of the users prefer to choose short and simple password to be able to be easily memorized and it is usually recalled on the login-time. In common many experts have surveyed that the normal users is necessary to memorize at the very least 3 account points. again in addition for this the user needs to remember password for banking, e-commerce, online community sites together having email accounts. Limited and uncomplicated textual passwords are simple remember, but might end up being easily hacked although random and lengthy passwords are attached but hard to take into account. To overcome that matter graphical authentication systems were proposed. And also in today's changing world they were easily prone to be able to shoulder surfing catches. Many others authentication strategies was proposed to be able to overcome against humeral joint browsing on attacks but a real can at least assist in improving the overall performance of graphical information authentication scheme.

***Teshu Gaurav Singh**, Computer Science & Engineering Department , DIMAT(CSVTU,), Raipure, Raipur, India, 8269982648*
***Miss Sarita Sharma**,Computer Science & Engineering Department, DIMAT(CSVTU) Raipur India, 8109453812.*
***Gurpreet Singh Chhabra** , Computer Science & Engineering Department , KITE(CSVTU), Raipur,.,9826142436*

II. LITERATURE REVIEW

A. Secure User Authentication in Cloud Computing Management Interfaces-Liliana F. B. Soares et.al.-

This report proposed variable factor authentication. The convergence to help Single Sign-On (SSO) models is being used to eradicate or decrease account password management complexity.Such mechanisms could be based on public-key cryptography and might resort to several technologies to boost user knowledge, specifically Quick Response (QR) limits, Short Message Services (SMS), Honest Program Modules (TPMs), as effectively as contactless Near Industry Connection (NFC). Another trend leans towards adoption of risk-based authentication. Efforts for locking down authentication are mainly being undertaken with the Initiative for Open up Authentication (OATH) with the Fast Identity On the world wide web(FIDO) alliance. Security is offered from proxy gateway level.

Advantages-
authentication could be evolving to device-centric and user-centric.

Disadvantages-
Phishing attack & spam attack can be possible in this technique.

B. Multi-level Authentication Technique for Accessing Cloud Services-

This paper provides the rigid authentication system by introducing the particular multi-level authentication technique which generates/authenticates the particular

password in multiple levels obtain the cloud solutions. In this particular report, details of offered multilevel authentication technique are presented as well as the architecture, activities, information flows, algorithms in addition to probability of accomplishment in smashing authentication.

This method has two distinct entities:
i) Cloud service provider,and
ii) Authenticated customer corporations thatgain access to the particular cloud solutions.

Cloud service corporation, provides the solutions & Authenticate users develop the effect of checking the understanding before using cloud.
Various levels connected with password authentication/generation are-
(1) Organization level.
(2) Team level.
(3) User Level.

There can be multiple levels involving level two & level 3.

Advantages-
• This method gives multiple advanced of security, which is much better then previous methods.
• Hacker need to help break the password in any respect level.

Disadvantages-
• It's really tedious work not to ever forget multiple passwords.

C. Grid Based Scheme-Authentication Using Graphical Password in Cloud, Ming-Huang Guo et.al.-

A grid contain multiple number connected with blocks. User have to select a routine blocks. Back ground of grid is going to besome images. User think that he is choosing the sequence connected with images, but actually he's planning to select a routine of grid prevents.That selected sequence will possibly be user's all occasion password.

Advatage-
• Very simple remember.

Disadvantage-
• Shoulder Searching, Thesaurus attacks. may be possible with this structure.

D. Multi-factor Authentication Framework for Cloud Computing- Rohitash Kumar Banyal et.al.

Security at static occasion is hack ready. Suppose if all of us blocked any user by 10, 000 static indicates, then a creative hacker can just find a new opportunity intended for hacking. So security from dynamic time is very much required. Giving security from dynamic time is very difficult task, but this report gives an algorithm to present security dynamically. Suggested a shared authentication structure between user& impair.

This method offered three steps-

(1) Sign up Phase.
(2) Get access Stage.
(3) Impair Authentication Phase.

User ought of do their sign up honestly. Then mutual authentication is conducted between user & cloud.

Advantages-
• Multi-level dynamic protection provide greater advanced of security.

Disadvantage-
• User identification vary. Its very trial to identify appropriate user accurately.
• Spoofing attack can be possible in this technique.

E. Graphical Password Authentication- Shraddha M. Gurav et.al

This paper proposed very easy method and that is simple to remember. In the offered method user should get into their username. On the basis of user name some pictures are caused. user selects any one of these that will be his in history password.

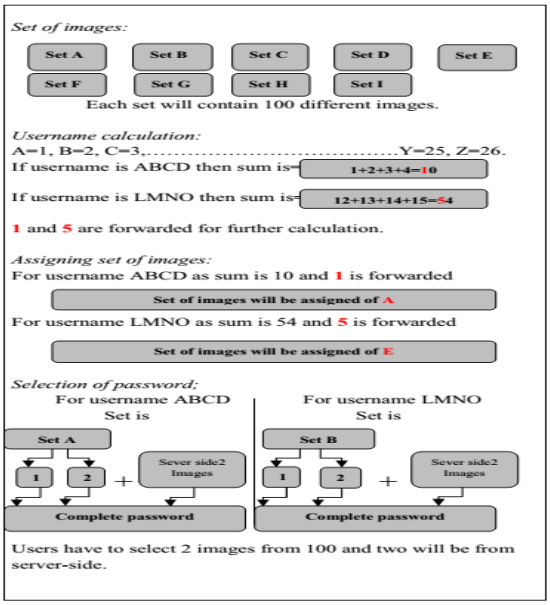

Fig .1 Previous System Flow Chart

F. Design and Implementation of Multi-tier Authentication Scheme in Cloud- Maninder singh et. al.

The purpose of this paper is to present the design of a secure and more advanced authentication scheme for executing secure financial transactions over Internet. Systems have been designed which have high resource handling capacity and computing power. Submit your manuscript electronically for review. This paper presents the design and implementation of a multi-tier authentication scheme in Cloud. The proposed authentication scheme is divided into two tiers. First tier authentication uses the encryption decryption mechanism as followed in normal authentication schemes. The second tier authentication requires the user to perform a sequence of predetermined

ISSN: 2278 – 1323

activities on the fake screen. This fake screen is loaded by the Cloud server in order to capture second tier authentication details from the user.

Advantages-

1.In proposed scheme, the data is stored at Cloud side in hashed form, so it is safer from insider attack.

2. The emphasis of this work is on the design and implementation of multi-tier authentication scheme, which is free from any hardware or software requirements.

Disadvantage-

Shoulder surfing attack is possible.

.

III. PROPOSED SCHEME

The proposed authentication scheme is divided into three tiers. These are-

1. Alphanumeric Password.
2. Grid Password.
3. Sequence of activities.

First tier authentication uses the encryption decryption mechanism as followed in normal authentication schemes. The second tier authentication requires the user to draw a pattern on grid. According to the drawn pattern user's are provided particular three colours. User needs to select sequence of colures as his third level password. During login phase if user is authenticated for first two level then, on third level user's are provided with same set of colours again he has to select same sequence of colours, he has selected during registration phase.

Step wise working of proposed scheme is explained below:

Step 1: User enters URL of application in his browser. Login GUI is loaded in the browser.

Step 2: User enters his first tier credentials (username and password). These credentials are passed to the Cloud server for validation as shown in Figure 2.

Step 3: Cloud checks for first tier credentials. If the username and password are correct then Cloud sends validation reply to observer (this is application program) at client side through step 3.

Step 4: Upon receiving validation reply from Cloud server, observer initiate the code to load Grid Authentication Scheme. The

pattern from Grid Line Drawn is taken during this step.

Step 5: Once the pattern is drawn from user from it is fetched to the database.

Step 6: A value is calculated against drawn pattern.

Step 7: According to the calculated value a set of three colours is given to the user.

Step 8: User needs to select the sequence of those colours. These sequence of colours will be his/her third level password.

Step 9: After completion of registration phase an acknowledgement screen is displayed. Now user is ready to login.

Step 10: User needs to fill his/her respective passwords in three levels, as he/she has selected during registration phase.

Step 11: Upon successful completion of step 10, original screen is loaded in the browser.

Step 12: The direct communication between client and Cloud server is established in this step.

screen in the browser to check for second tier authentication credentials. These second tier credentials are some sequence of registered activities. Observer checks for these activities continuously.

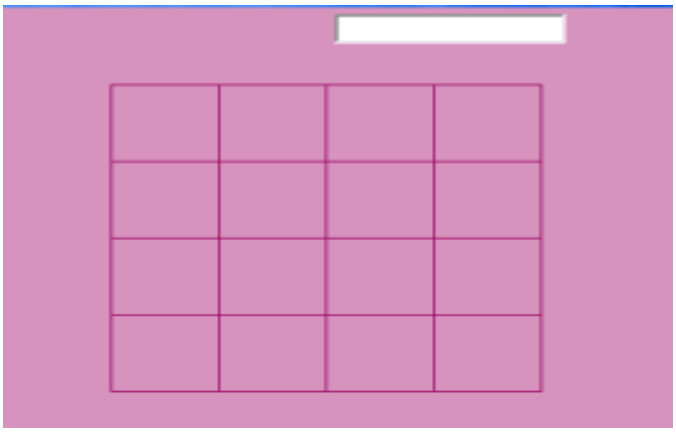

Fig. 2- Level 2

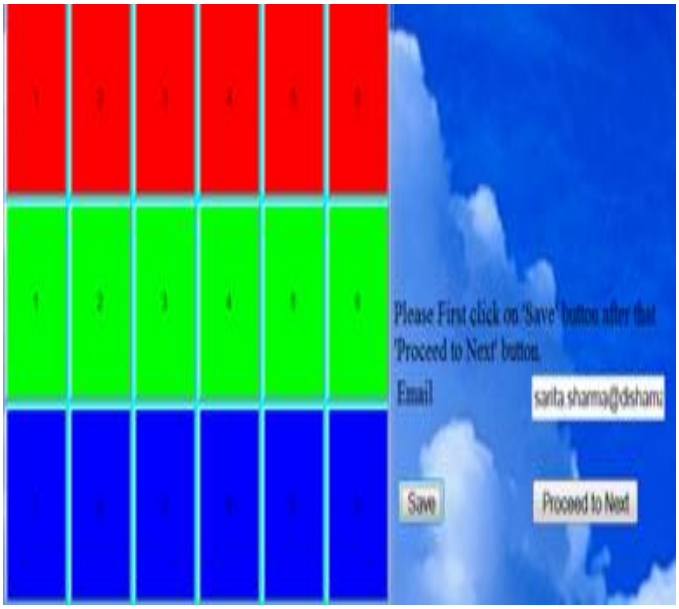

Fig. 3 – Level 3

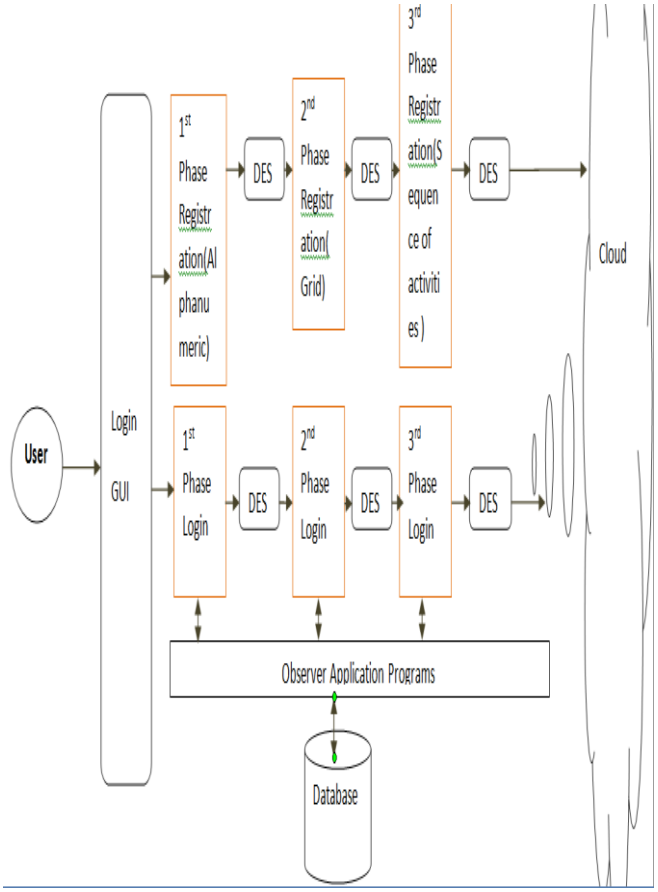

Fig 4. Flow Chart of proposed system

Sequence of Activities:

N*N Grid is divided in different spaces, each space is set with particular alphabetic symbols. Like first space is named with A, next with B,C,D….& consequent. Given in Fig 3.

A	B	C	D
E	F	G	H
I	J	K	L
M	N	O	P

Fig. 5 Grid Naming

We have set value for each space like

A=0, B=1, C=2, D=3…….p=15.

& we have 15 set of different colors or name of eminent personalities. In set 0 is set of three colors RED,GREEN & BLUE. If user selects A as his/her 2nd level password (Shown in Fig 4) then RED,GREEN & BLUE color is given to the user on 3rd level (shown in Fig 5). User needs to set sequence of colors & that set of color will be his/her third level password. Next time when user login & will select A same set of colors (RED, GREEN, BLUE) is given to the user. User needs to select the same of colors in sane sequence as he/she has set it during registration phase. Likewise we have Different set of colors or name of actors or cricketers on set 1,2,3,4,5……User can draw a pattern instead of selecting any one space. Against the drawn pattern value is calculated. As for example :User select ADM as his/her pattern then value will be calculated as:

A=0,D=3 & M=12.

So A+D+P = 0+3+12=15 =1+5(add unit & tens place) =6.

Answer is 6 so set number 6 is given to the user. Set 6 can be names of football players. User needs to choose the sequence as he/she like.

IV. RESULTS

The three-tier graphical password authentication technique proposed in section 4 has been implemented on cloud using Google App Engine platform and Eclipse IDE (Integrated Development Environment). Various necessary details required for developing the cloud application using GAE is discussed in www.developers.google.com. The analysis of various parameters of results has been checked on Google's Dashboard, on the basis of which following analysis has been made. The multi-tier authentication technique proposed has been implemented on cloud using Google App Engine platform and Eclipse IDE (Integrated Development Environment). Various necessary details required for developing the cloud application using GAE is discussed in [8-11]. Development of application on cloud server has been made using Eclipse IDE by installing GAE plugin package [12-14].

A. Security Analysis

In proposed scheme, the data is stored at Cloud side in hashed form, so it is safer from insider attack. This technique can be extended to any levels, but here, it is only three levels. In each level we are taken care about remembering durability of passwords & their security. Let the two outcomes of the registered events as success and failure be S and F respectively. Then outcome of two levels is {SS, SF, FF, FS} and n(S) = 4, in this case. If probability of success at each level is p, then breaking multilevel authentication for success SS, denoted by P(E), is equal to p^2. Now failure of multilevel authentication is 1-P(E) =1-p^2. If probability at each level for success is p= 0.1 (say) then probability of breaking multilevel authentication is 0.01 (p^2). For first factor authentication, if encryption key is of length 128 bits then there are 2^{128} different combination for a particular key.

In the proposed scheme, the strength of second & third tier authentication is as follows:

Grid Authentication System:

Probability of breaking code = (N!*N!)/(2N)!

Where N is for N * N grid system.

Selecting Sequence of colors:

Obviously by increasing level, probability of breaking code also decreased by 10 times . If we take total 10 set of activities then again it will decreased by 10 times. There is another point that is sequence of activities. It helps us to prevent shoulder surfing attack. If attacker come to know about any single set then rest 9 sets will be remains safe from attacker. In other words we can say that 9 set will always hidden from attacker.

ISSN: 2278 – 1323

So for overall probability of breaking will be = (N!*N!)/(2N)!

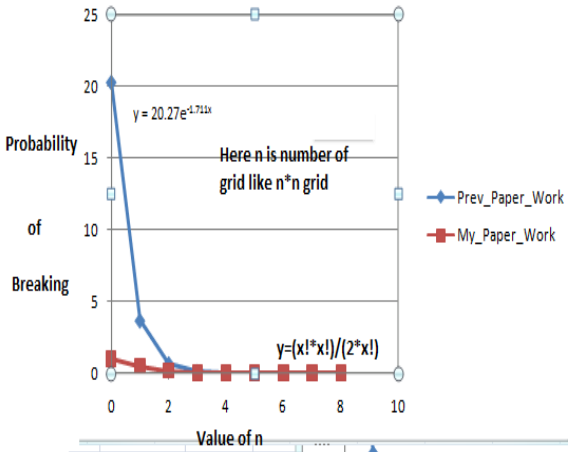

Fig. 6 Probability of failure

B. *Space Requirements*

Since we are dealing in cloud environment space is not a big deal. We are provided with a large number of space in cloud. Space requirement is calculated for both two tier authentication scheme in cloud and Three Tier Grid Authentication system. Three tier authentication scheme consumes more space than two tier authentication scheme. It is clear from the graph that as the data entries are increased in three tier grid authentication scheme, the space consumed also increases linearly. On an average, three tier grid authentication scheme uses 332 bytes to store one user's credential and two tier authentication technique requires 253 bytes to store one user's credential. If at any time 100000 users are registered, then server would need 100000*(332-253) = 7900000 (7.53 MB approx) bytes of additional storage, which is not a big issue in comparison to more security provided by three tier grid authentication technique.

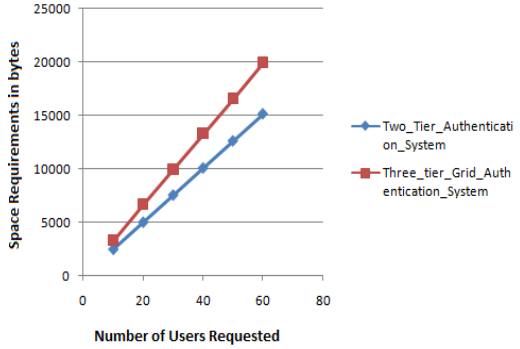

Fig 6 Space Requirement

C. *Performance Analysis*

The performance is evaluated on the basis of CPU processing time. To evaluate performance two tier and three tier grid authentication techniques are compared. They are tested on the basis of same parameters. Three tier grid authentication scheme uses only 0.0011429s more than two tier. In terms of Cloud Computing, which provides us unlimited, scalable resource, this difference is negligible. So it can be said that three tier grid authentication system is highly beneficial & memorable durability than two tier authentication scheme.

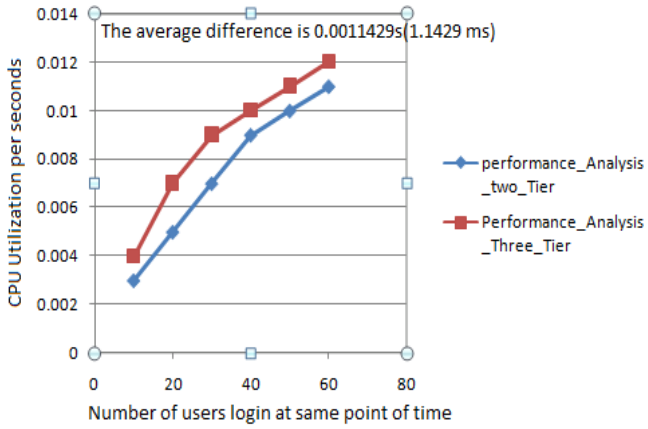

Fig 7 Performance Analysis

D. *Remembering Passwords*

We have analyze the password remembering capacity on 10 users weakly & on the completion of 8th weak we found that on an average 90% users can remember the password for a long time.

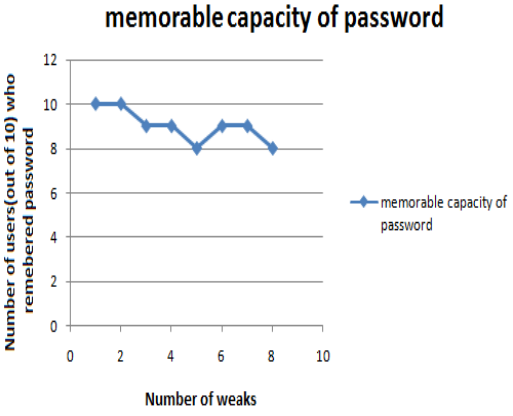

Fig 8 Remembering durability of password

E. *Comparisons with other methods*

On the basis of Literature Review we have some observations from the attacking point of view. Observation shown in table 1.We observed that most of the existing system does not work for shoulder surfing attack. But three phase grid & colour based authentication system is designed & implemented for shoulder surfing attack. This system does not give an option to change user password, but it can be implemented in future. Another thing not implemented is session key agreement else everything is implemented for this system.

Table 1:-Comparison table of literature review

Performance Matrices	**Asib Hasan khan et al [7]**	**Rohitash Kumar Banyal et al [2]**	**Dinesha H A et al[6]**	**Ming-HaungGuo et al [5]**	**Maninder Singh et al[4]**	**Shradha M. Gurav et.al[3]**	**Teshu Gaurav Singh et.al**
Shoulder Surfing Attack	No	No	No	Yes	Yes	No	Yes
Identity Management	YES	YES	YES	YES	YES	YES	Yes
USER Privacy	YES	YES	YES	YES	YES	YES	Yes
Mutual Authentication	YES	YES	YES	YES	YES	YES	Yes
Password Change	NO	YES	N0	YES	YES	YES	No
Session Key Agreement	NO	YES	YES	YES	NO	NO	No
Replay Attack	YES	YES	NO	YES	YES	YES	Yes
MITM	NO	YES	YES	YES	NO	YES	Yes
DOS	NO	NO	NO	NO	YES	NO	Yes
Impersonation Attack	NO	YES	NO	YES	NO	YES	Yes
Password Guessing Attack	NO	YES	NO	YES	YES	YES	Yes
GUI	NO	YES	YES	YES	YES	YES	Yes
Dynamic Security	NO	YES	YES	YES	YES	YES	Yes
Phishing Attack	YES	YES	NO	YES	NO	YES	Yes
Ease to Remember	NO	NO	YES	YES	YES	YES	Yes

ISSN: 2278 – 1323

V. CONCLUSION

The strength of any authentication technique depends upon the probability of breaking that technique & remembering durability of password. As we have seen the probability of breaking code is very less. One problem arises with multi tier authentication system is remembering the multiple password for a long time. We have tried a lot to solve this problem, so we have implemented with grid password & a sequence of activities. As we shown in graph we tried it for 10 people. Now it became easy to remember on an average 90% user can remember the password for at least two months. One drawback of three tier password grid based cloud authentication system is that it takes more apace than single level & two level password authentication systems. Since we are dealing with cloud, so we have enough resources available with us. It is not a big problem. Our main goal is to protect the password from unauthenticated user. We have resolved the problem & overcome from the shoulder surfing attacks & other attacks. There is very less chance to break the code because in third phase if one will know one set he will be unaware about remaining sets. It is independent of additional hardware and software requirements. In terms of performance, multitier authentication technique no doubt takes slightly higher CPU time, but this slight difference is in milliseconds, which is negligible.

VI. FUTURE WORK

We have not given any option to change the password. In future it can be implemented. Instead of multiple colors multiple images can be used which is much beneficial then existing system. Cryptography algorithm can be applied for images protection. By rethinking on methodology we can optimize the process, so that password can be more secure from unauthenticated user. We can add new features so that password is more memorable.

REFERENCES

[1] Graphical Password Authentication system in an implicit manner, SUCHITA SAWLA*, ASHVINI FULKAR, ZUBIN KHAN Department of Computer Science, Jawaharlal Darda Institute of Engineering & Technology, Yavatmal, MS, India. March 15, 2012.

[2] Multi-factor Authentication Framework for Cloud Computing Rohitash Kumar Banyal *Dept. of Computer Engineering* Rajasthan Technical University Kota, Rajasthan, Iindia. e-mail: rkbayal@gmail.com, Pragya Jain, *Computer Services Center* Indian Institute of Technology New Delhi, India e-mail: pragya@cc.iitd.ac.in, Vijendra Kumar Jain *Dept. of EIE* SLIET Longowal Punjab, India. e-mail: vkjain27@yahoo.com Fifth International Conference on Computational Intelligence, Modelling and Simulation Dept. Of Computer Engineering Rajasthan Technical University Kota, Rajasthan, India.

[3] Graphical Password Authentication ,Cloud securing scheme - ShraddhaM. Gurav Computer Department Mumbai University RMCET Ratnagiri , India. guravsm292@gmail.com, Leena S. Gawade Computer Department Mumbai University RMCET Ratnagiri ,India.lgleena90@gmail.com, Prathamey K. Rane Computer Department Mumbai University RMCET Ratnagiri ,India.prathamey@gmail.com, Nilesh R. Khochare Computer Department Mumbai University RMCET Ratnagiri,India, nileshkhochare@gmail.com, 2014 International Conference on Electronic Systems, Signal Processing and Computing Technologies.

[4] Design and Implementation of Multi-tier Authentication Scheme in Cloud , Maninder Singh Computer Science and Engineering, UIET Panjab University, Chandigarh-160014, India , Sarbjeet SinghComputer Science and Engineering, UIET Panjab University, Chandigarh-160014, India, IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 5, No 2, September 2012.

[5] Authentication Using Graphical Password in Cloud Ming-Huang Guo, Horng-TwuLiaw, Li-Lin Hsiao, Chih-Yuan Huang Department of Information Management Shih Hsin University Taipei, Taiwan.

[6] Multi-level Authentication Technique for Accessing Cloud Services Dinesha H A Agrawal V K CORI CORI Bangalore, Karnataka Bangalore, Karnataka.

[7] Open ID Authentication As A Servicein Open Stack asib Hassan Khan, JukkaYlitalotand Abu Shohel Ahmed* Aalto University, School of Science and Technology, Finland t Ericsson Research, Finland Royal Institute of Technology(KTH), School of ICT, Sweden 117th International Conference on Information Assurance and Security(IAS).

[8] Daniel Guermeur and Amy Unruh, "Google App Engine Java and GWT Application Development", Packt Publication, Chapter 1, November 2010.

[9] Fay Chang et al., "Bigtable: A Distributed Storage System for Structured Data", Google Incorporation, Available at:http://research.google.com/archive/bigtable.html.

[10] "Google Web Toolkit Get Started", Available at: https://developers.google.com/webtoolkit/doc/latest/FAQ_GettingStarted.

[11] Daniel Guermeur and Amy Unruh, "Google App Engine Java and GWT Application Development", Packt Publication, Chapter 2, November 2010.

[12] "Google Plugin for Eclipse 3.7 Installation Instructions", Available at: https://developers.google.com/eclipse/docs/install-eclipse-3.7

[13] "Google Web Toolkit: Organize Projects", Available at: https://developers.google.com/webtoolkit/doc/latest/DevGuideOrganizing Projects.

[14] "Create a GWT Project", Available at: https://developers.google.com/web-toolkit/doc/latest/tutorial/create

Author Profile

Teshu Gaurav Singh completed my Engineering Degree with Computer Science & Engineering Branch from Guru Ghasidas University, Bilaspur in the year of 2007. I completed C-DAC (DAC) from MET, Mumbai in 2009. Recently I am M. Tech Scholar at Disha Institute of Management And Technology , Raipur (C.G.). My Research area is Cloud Computing & Neural Network. I am M. Tech Scholar student under the guidance of Miss Sarita Sharma . She is working as Assistant Professor at Disha Instute of Management & Technology (Chhattisgarh Swami Vivekanand technical University) , Raipur.

Miss Sarita Sharma Is an Assistant Professor in Computer Science & Engineering branch at Disha Institute of Management And Technology , Raipur. Her Research interest include Digital Signal Processing & Image Processing , Neural Network, Artificial Intelligence, Information & Network Security, Analysis & Design of Algorithm.

Mr Gurpreet Singh Chhabra having Master degree in Computer Science & Engineering and is a member of CSI (Computer Society of India) and is pursuing PhD in Wireless Sensor Network(WSN). He has a credit of many national and international papers. His qualifications are fortified with a great deal of creativity and problem solving skills. He has also a proven record of teaching for the last 9 years.

