# Implementing Graphical Password and Patternlock Security using MVC into the Cloud Computing

V. Sulochana
Research Scholar
Karpagam University
Coimbatore

R. Parimelazhagan
Department of Mathematics
Karpagam College of Engineering
Coimbatore

## ABSTRACT

This article presents secure authentication system by using sequence level authentication technique which creates/authenticates the password in sequence levels to access the cloud services. The article includes graphical survey and details of proposed sequence authentication technique are presented along with the architecture, data flows, algorithms and implementation, probability of success in breaking authentication.

## Keywords

Cloud Computing Authentication, Graphical Password, Sequence Level Authentication

## 1. INTRODUCTION

Cloud computing is an emerging, on-demand and internet based technology. This technology is used by global customers to improve their business performance. To utilize the cloud services by authorized customer, it is necessary to have secure authentication system. Cloud computing is an internet based model which provides variety of services over internet such as data storage, hardware, software and infrastructure. Bo Wang [3] stated that to utilize cloud services by authorized user and to secure cloud data, it is necessary to use secured authentication system.

Cloud authentication systems use different methods like i) Simple text password ii) Third party authentication iii) Graphical password iv) Biometric v) 3D password object. According Wixted [7] users choose short, simple passwords which is vulnerable to dictionary or brute force attack. Third party authentication is not preferred for smaller cloud deployment by K.Venkataramana [12]. Graphical password schemes require long time to be performed by V.K.Agrawal [6]. Dinesha H.A [5] stated that biometric authentication requires a special scanning device to authenticate users which is not applicable for remote and internet users. According to F.A.Alsuaiman [1], 3D-password which is secure, support the multifactor authentication. Another simple approach is to use one/combination of the above methods in sequence level, so that probability of breaking such a password is reduced to large extent. Sequence level authentication technique is introduced to secure cloud transmission for ensuring the strict authentication. Tanvi Naik, Sheetal Koul [11] discussed about the techniques for multi-dimensional and multi-level authentication. Multi-dimensional authentication is the combination of the existing authentication techniques into one virtual environment. Multi level authenticates data at multiple levels. Prasad.P [9] applied 3D security in cloud computing, mainly focused on problem of data leakage and proposes a frameworks in two phases. In the first phase, data classification is done by client before storing the data. After the completion of the first phase the data, which is received by cloud provider for storage uses three dimensional techniques for accessibility.

Sneha Vasant Thakare [10] presents 3D security cloud computing using graphical password. The 3D security have 3 protection ring in which file categorization is done by R-CIA algorithm, divides the files into ring1, ring 2, ring 3. 3D password used for ring1, Graphical password with icons used for ring 2, Persuasive clued click point used for ring 3. Depending on the rings, multi level security system increases for secure access of cloud services. 3D password is time consuming process and needs large amount of memory space and so multi-level authentication is taken for consideration. In the technique proposed by Dinesha H.A [5], each authentication activity takes place in organization, team and user levels. Each level reads password and checks for authentication.

In this paper, the sequence level authentication techniques generate passwords at five levels and then concatenates into one single password. The distinctive features of the technique makes the security measures of the cloud computing more stringent. Even if intruder is aware of the particular password, it will not be helpful to him as password to any new level is the concatenation of the new password with all the passwords belonging to the previous levels.

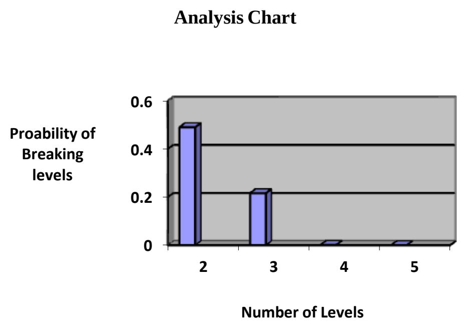


**Table 1: Comparative Analysis**

| Number of levels | Probability of Breaking levels |
|---|---|
| Two | 0.49 |
| Three | 0.216 |
| Four | 0.0016 |
| Five | 0.00032 |

The comparative analysis is made between number of levels of authentication technique and probability of breaking levels. For two levels, probability of breaking is 0.49. For three levels, probability of breaking is 0.216. For four levels, probability of breaking 0.0016. For five levels, probability of breaking is 0.00032. In this paper, sequence level technique uses five levels in which breaking level or success rate is very low compared to other levels [13][10][9][5]. To provide better security to the intended customer, it is better option to use sequence level authentication technique for accessing cloud services.

To overcome the problems of authentication methods, an idea of graphical password was introduced by Greg Blonder [G.Blonder, Graphical Passwords, United States Patent 5559961 (1996)]. Partha Pratim Ray [8] added that graphical password uses pictures instead of textual password because human can remember pictures more easily than sequence of characters. In the first level, password based authentication used, where user presents userID and a password to the sequence authentication technique. Weinshall and Kirkpatrick [4] authentication schemes applied to second level which includes picture recognition, object recognition and pseudo word recognition. The analysis of this level shows that pictures are most effective than textual password. Third level includes Jansen et al., graphical password mechanism in which matrix pattern is used instead of theme and creates patternlock password. Passface technique is applied to fourth level, beanie babies are used instead of human faces because human recall the beanie babies than the pictures [2]. In fifth level, OTP is created and sent to the registered E-mail and redirect the user to the cloud based application or PaaS environment.

This technique authenticates the cloud access in sequence level. At each level, password is created, the cloud user can access the services provided that password authentication is successful in all the previous levels. This technique has two separate entities i) cloud service provider who provides cloud services, ii) Authenticated cloud user who access the services (Before using cloud services, cloud user authentication confirms with service agreement and other formal procedure from cloud vendors). This architecture helps checking authentication for accessing the cloud services.

The first level is the password based authentication which validates userID and password and the cloud user gets authenticated, enter next level or unauthenticated. Second level is the image authentication which validates the single choosen image from the desktop with previous choosen image of registration phase of authorized user and get authenticated, enter the next level. If hackers tries to access the cloud services, they can terminate in this level itself. Third level is the patternlock authentication which validates the choosen patternlock with previous choosen patternlock of registration phase of authorized user and get authenticated, enter the next level. Fourth level is the image sequence authentication which validates the choosen beanie babies with previous choosen beanie babies of registration phase of authorized user and get authenticated, enter the next level. In fifth level one time password is validated and sent to the registered E-mail and redirect user to the cloud based application or PaaS environment.

## 2. DESIGN OF SEQUENCE LEVEL AUTHENTICATION TECHNIQUE

Password authentication happens between cloud user accessing cloud services and cloud service provider. Figure 1 shows the DFD level 0 for sequence level password creation and authentication Technique. Figure 2 shows the DFD level 1 for sequence level authentication Technique. This DFD describes detailed flow of password authentication process.

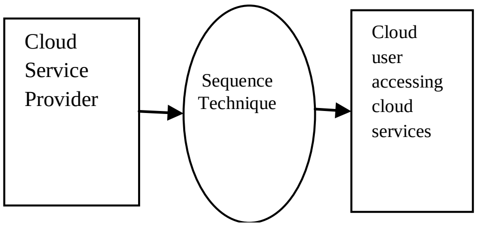


**Figure1. Data flow diagram Level 0**

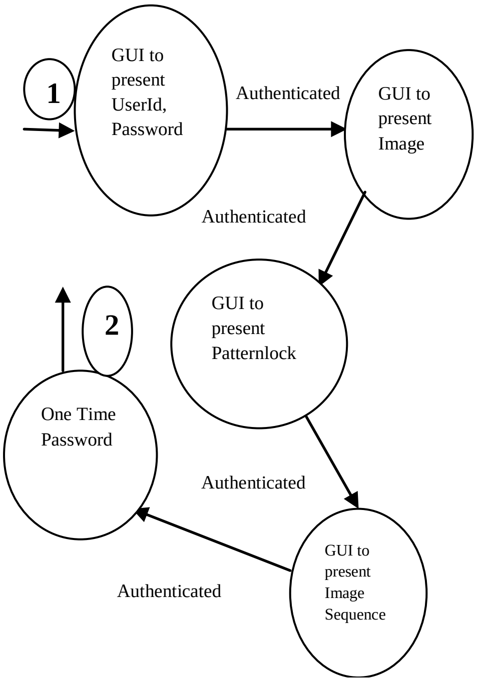


**Figure2. Data flow diagram Level 1**

The algorithm for sequence level password creation/authentication technique is given below. Important notations used in the algorithms are PA-Password authentication, Reg_PA-Registered Password, IA-Image authentication, Reg_IA-Registered Image, PL-Patternlock Authentication, Reg_PL-Registered Patternlock, IS-Image Sequence Authentication, Reg_IS-Registered Image Sequence, OTP-One Time Password, Reg_OTP-Registered One Time Password.

```
Step1: If (User = New)
        New User register with Sequence Level Authentication Technique
        Go to Step 2.
Else
If (User = Registered)
```

```
          Registered User presents PA password authentication
If (PA=Reg_PA) then authenticated, presents IA
 If (IA=Reg_IA) then authenticated, presents PL
 If (PL=Reg_PL) then authenticated, presents IS
 If (IS=Reg_IS) then authenticated, presents OTP
 If (OTP=Reg_OTP) then authenticated
          Provide Cloud Service
     Else
          Go to Step 2.
    End
Step2: Exit
```

The next level is implementation of technique, can be done by Model-View-Controller (MVC) pattern. The MVC is a software architecture pattern which separates the representation of information from the user's interaction with it. The technique developed using software packages like Java, MySQL, jdk, jsp, Tomcat Server and divided into three kinds of components. The model component implements application data, business rules, logic and functions, View component display output representation of data such as chart or a diagram. Controller component mediates input and converts to command for the Model and View. The separation helps to manage complexity when application is built, because it enables to focus on one aspect of implementation at a time.

The system state and business logic javabeans uses view for JSP pages and presentation component and uses controller for Action Servlet and Action Mapping. The bean uses service and access the database using DAO Figure 3. Some screen shots for registration, creating graphical password and patternlock are given in Figure 4,5.

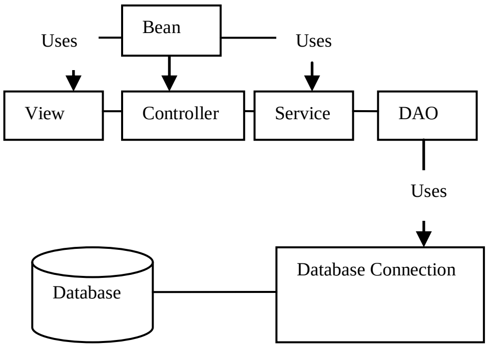
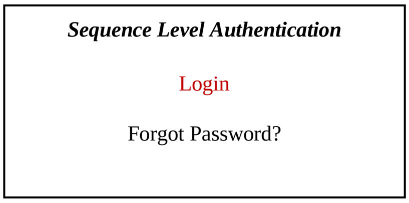
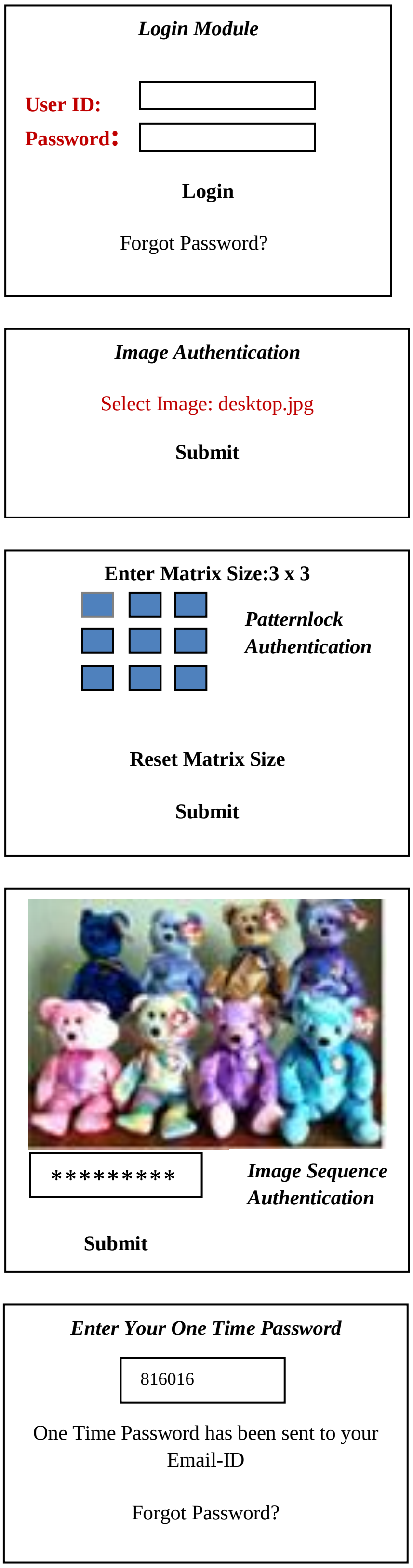


**Figure 3. Implementation**


*Sequence Level Authentication*

Login

Forgot Password?


*Login Module*

User ID:

Password:

Login

Forgot Password?

*Image Authentication*

Select Image: desktop.jpg

Submit

Enter Matrix Size:3 x 3

*Patternlock Authentication*

Reset Matrix Size

Submit

*********

*Image Sequence Authentication*

Submit

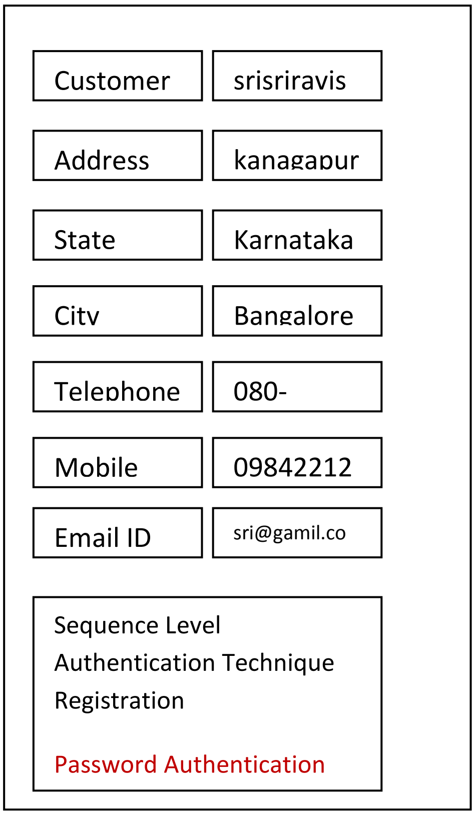
*Enter Your One Time Password*

816016

One Time Password has been sent to your Email-ID

Forgot Password?

**Figure 4: Graphical Password, Patterlock Screen Shots**



| | |
|---|---|
| Customer | srisriravis |
| Address | kanagapur |
| State | Karnataka |
| Citv | Bangalore |
| Telephone | 080- |
| Mobile | 09842212 |
| Email ID | sri@gamil.co |

Sequence Level
Authentication Technique
Registration

Password Authentication

**Figure 5: Registration Screen Shots**

The next level of technique is the probability of breaking sequence level technique in which the cloud user should recall the password at each level of the authentication technique. Five levels are taken and two outcomes such as success and failure to determine probability of breaking. Let S be the sample space. To break this one is succeeded in five times repeatedly. Hence sample space S={ SSSSS,SSSSF,SSSFS,SSFSS,SFSSS,FSSSS,SSSFF,SSFSF,SSFFS,SFSSF,SFSFS,SFFSS,FSSSF,FSSFS,FSSS,FFSSS,SSFFF,SFSFF,SFFSF,SFFFS,FSSFF,FSFSF,FSFFS,FFSSF,FFSFS,FFFSS,SFFFF,FSFFF,FFSFF,FFFSF,FFFFS,FFFFF} n(S)=32 where n(S) is the cardinality of set S.

Binomial distribution is used in this technique, the probability of getting success is 0.4096 then the probability of breaking the sequence level (five level) authentication is 0.00032. Based on the above discussion, the use of sequence level authentication provides better security for accessing cloud services.

## 3. CONCLUSION AND FUTURE ENHANCEMENT

The technique is developed by integrating text passwords with images to strengthen the security of cloud. The sequence level authentication technique is more secure, reliable & robust and there is always drastic improvement in future. This technique helps in generating the password in sequence level so that the strict authentication and authorization is possible. The technique can be further improved to enhance security. The next step for future work is to rebuild the technique for the SaaS and IaaS service models.

## 4. REFERENCE

[1] F.A.Alsuaiman, A.El Saddik 2008 Three Dimensional password for more secure authentication, IEEE Transactions on Instrumentation and Measurement Vol. 57, 1929-1938.

[2] Ashwini Fulkar, Suchita Sawla, Zubin Khan and Sarang Solanki 2012 A study of graphical passwords and various graphical password authentication schemes,World Research Journal of Human Computer Interaction Vol.1,04-08.

[3] Bo Wang, HongYu Xing 2011 The Application of Cloud Computing in Education Informatization, International Conference on Computer Science and Service System(CSSS).

[4] Daphna Weinshall, Scott Kirkpatrick 2004 Passwords you'll never forget, but can't recall, ACM,1399-1402.

[5] Dinesha H.A 2012 Multilevel Authentication Technique for Accessing Cloud Services, International Conference on Computing, Communication and Applications (ICCCA), 1-4.

[6] Dinesha H.A, V.K.Agrawal 2012 Multi dimensional password generation technique for accessing cloud services, International journal on cloud computing: Services and Architecture (IJCCSA), Vol.2, 31-39

[7] Machha.Narender,M.Y.Babu,M. Mohan Rao 2010 Towards secure design choices for implementing graphical passwords, Global journal of Computer science and Technology,Vol. 10, 24.

[8] Partha Pratim Ray 2012 Ray's scheme: Graphical password based hybrid authentication system for smart hand held devices, International journal of computer trends and technology,Vol.3, 235-241.

[9] Prasad.P, Ojha.B, Shahi.R.R, Lal.R, Vaish.A, Goel.U 2011 Three Dimensional Security in Cloud Computing, Computer Research and Development (ICCRD), 3 rd International Conference, Vol 3, 198-201

[10] Sneha Vasant Thakare, Deipali.V.Gore 2013 3D Security Cloud Computing Using Graphical Password, International Journal of Advanced Research in Computer and Communication Engineering, Vol 2, 945-949.

[11] Tani Naik, Sheetal Koul 2013 Multi-dimensional and Multi-level Authentication Techniques, International Journal of Computer Applications, Vol 75, 17-22.

[12] K.Venkataramana, M.Padmavathamma 2012 Agent based approach for authentication in cloud, IJCSITS,Vol. 2,598-603.

[13] http://simulation-math.com/VideoEL/(6B)BinomialDistribution.pdf