A Puzzle Based Authentication Scheme for Cloud Computing

Sulochana.V[1], Parimelazhagan.R[2]

[1]*(Research Scholar, Karpagam University, India)*
[2]*(Department of Mathematics, Karpagam College of Engineering, India)*

ABSTRACT : *This article presents puzzle based authentication scheme in which cloud user registers and solves the puzzle, puzzle solving time and sequence of image block is stored and validated by local server and the cloud user get authenticated and start accessing the cloud services. The article includes details of puzzle based authentication scheme are presented along with design, algorithm, security and implementation.*

Keywords -Cloud Computing, Cloud Services, Graphical Password, Puzzle, Security

I.   INTRODUCTION

Cloud Computing is emerging technology which consist of existing techniques combined with new technology paradigms. Recently the cloud computing paradigms has been receiving significant excitement and attention in the media and blogosphere. This technology is used by global customer to improve their business performance. To utilize the cloud services by authorized customer, it is necessary to have secure authentication system. Authentication is a process that ensures and confirms a cloud user's identity and form a base for information assurance. Cloud user authentication is mandatory, because it eliminates the attacks/risks to enter into cloud service provider environments[1]. Cloud authentication systems uses different methods like i) text password ii) 3D password object iii) Third party authentication iv) Biometric v) Graphical password by Sulochana.V[2]. According to Dinesh.A, text password is easy to break and vulnerable to dictionary or brute force attacks[3]. 3D password object is a multifactor authentication scheme which combines all existing authentication schemes into a single 3-D virtual environment by Grover Aman[4]. According to Dinesh.H.A[5] presents third party authentication is not preferred for smaller cloud deployment and biometric requires a special scanning device to authenticate users, which is not applicable for remote and internet users. Graphical password have been proposed as possible alternative to traditional text based password, proved that human brain is better in recognition and recalling the image or pictures.

In the survey, 83% people use image as password to protect their account[6].

The idea of graphical password was pioneered by Greg Blonder holds US patent 5559961 in 1996. The ubiquity of graphical user interfaces and input devices, such as the mouse, stylus and touch screen that permit other than typed input, has enabled the emergence of graphical passwords[7]. In graphical password human beings have the ability to remember faces of people, places visited and things seen for a longer duration which make more user-friendly and increases the level of security[8]. John Charles Gyorffy[9] presents token based graphical authentication which uses a graphical password deployed from a trojan and virus resistant embedded device. Graphical password utilizes a personal image to construct an image hash which is provided as a input to cryptosystem returns the password. The graphical password require user to select small number of points on the image and embedded device stretch the points into a long alphanumeric password. Ahmad Alomari[10] applied puzzle encryption in the on-demand routing protocols in mobile ad hoc networks (MANETS). The main goal is to promote and improve the authentication between the nodes in the MANETs by applying the puzzle encryption before they start exchange the data packet between them. Sanjay K.Dhurandher[11] designed authentication mechanism in which malicious nodes present in the network is identified, measures to oust the identified malicious node from the network and provides the transmission of the encrypted data to the base station which is collected by the deployed sensor nodes. Dinesh.H.A[5] presents strict authentication system by introducing multi-level authentication technique which generates/authenticates the password in multiple levels to access the cloud services. Sulochana.V[2] presents secure authentication system by using sequence level authentication level authentication technique which creates/authenticates the password in sequence levels to access the cloud services. Rachhna[8] developed graphical password authentication system with a puzzle to increase the remembrance of the password. The system consists of puzzle in which user select and change the image block for

log on process. This article propose graphical password system with puzzle, puzzled image are arranged in rows and columns, cloud user moves the puzzled image to form the complete puzzle and its solving time and sequence of image block is stored and validated by local server and the cloud user get authenticated and start accessing the cloud services.

In this article puzzle play an important role which is used to authenticate cloud user. The puzzle solving is a purely mental activity and it is presented in some physical form with solutions relying on manual actions and tests for legal moves requiring visual inspection. A puzzle tests the ingenuity of the user, moves pieces together in a logical way to find desired solution. The new cloud user presented with registration form and puzzled image which are arranged in rows and columns. Cloud user starts moving the puzzled image to form complete puzzle. Puzzle solving time is difference between the start time of moving puzzled image block and ending time of forming a complete puzzle and the track of the sequence of image block is updated in the local server. For registered cloud user, the puzzle solving time and sequence of image block is validated with local server and cloud user get authenticated start accessing the cloud services. This scheme provides enough security to protect against online attacks and may be used as a building block for future user authentication systems. The major advantage of the scheme is that level of confidentiality is very high which leads to higher level of security.

II.   DESIGN OF PUZZLE BASED AUTHENTICATION SCHEME

This scheme developed as graphical based authentication mechanism by using puzzle strategy which is attracted by the cloud users. In this scheme, puzzle are developed and merged with the authentication of the cloud user. The authentication scheme happens between the cloud user accessing cloud services and cloud service providers. Fig 1 shows the DFD level 0 for puzzle based authentication scheme. Fig 2 shows the DFD level 1 for puzzle based authentication scheme. This DFD describe the detailed flow of puzzle authentication scheme.
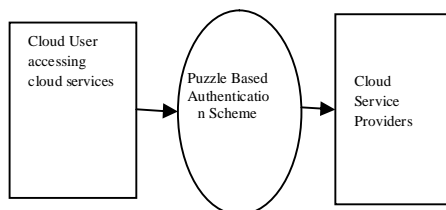

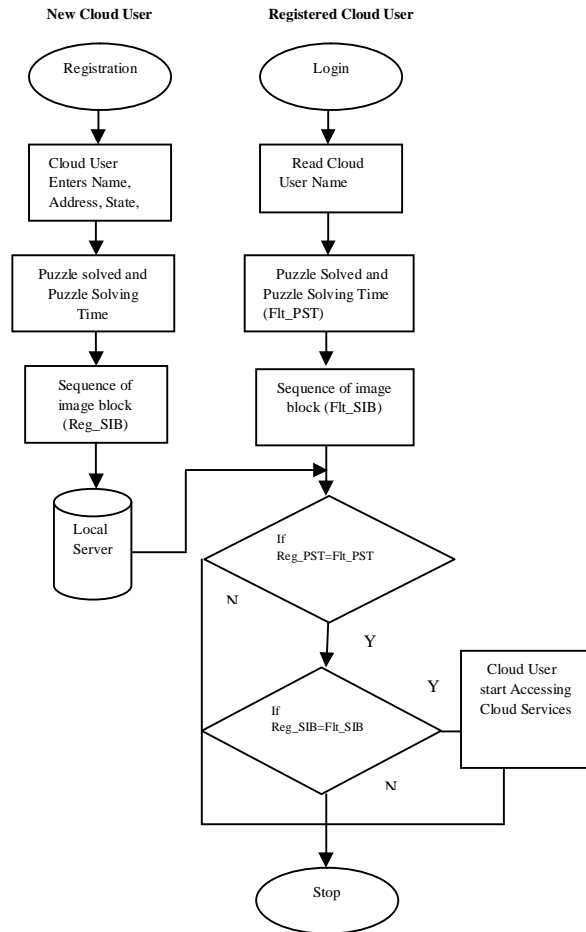**Figure1. Data flow diagram Level 0**

Figure2. Data flow diagram Level 1

The fig 3 shows the overall working of the puzzle based authentication scheme, initially cloud user connect with local server wirelessly and acknowledgement sent to the cloud user after successful connection establishment. After this process if the cloud user is not registered, registration form and puzzled image are presented to the cloud user. After registration, cloud user starts moving the puzzled image to form complete puzzle. Puzzle solving time is difference between the start time of moving puzzled image block and ending time of forming a complete puzzle, track of the sequence of image block is updated in the local server. The local server stores the puzzle solving time and track of the sequence of image block in the database. If the cloud user is registered, puzzle solving time and track of the sequence of image block is validated with local server. After successful, local server will establish connection

between the cloud user and service providers. Cloud user start accessing the cloud services.
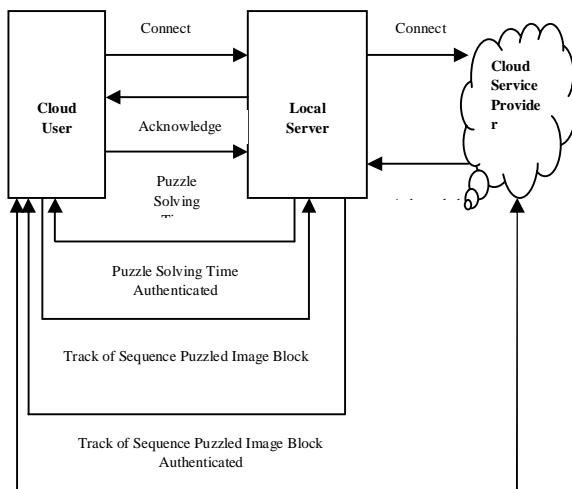

Figure3. Puzzle based authentication scheme

The algorithm for Puzzle Based Authentication Scheme are given below: Important Notations used in the algorithms are: Reg_PST-Registered Puzzle Solving Time, Reg_SIB- Registered Sequence of Image Block, Flt_PST-Float Puzzle Solving Time, Flt_SIB-Float Sequence of Image Block.
Step 1: If (User=New)

New Cloud User registers the Details, solves the puzzle and Reg_PST and Reg_SIB is Stored in local server

Go to Step 2.
Else
If (User=Registered)

Registered User solves the Puzzle where Flt_PST, Flt_SIB are presented for validation

If (Reg_PST = Flt_PST) then authenticated

If (Reg_SIB=Flt_SIB) then authenticated

Provide Cloud Service
Else
Go to Step 2

Step2: Exit

The next level is implementation which can be done by using software packages like ASP.Net AJAX, SQL, photoshop. The main puzzle or pictures divided into different pieces and stored as image. In the registration form cloud user presents the details start importing the image and

arrange the image block in rows and columns. The next step is to initiate drag and drop of image block moved from drag source to drop target. The cloud user moves image block from drag source to drop target to form the complete puzzle with the efficient solving time. The puzzle solving time is the difference between the start time of moving puzzled image block and ending time of forming a complete puzzle. The puzzle solving time and track of sequence of image block is validated with local server, cloud user get authenticated and start accessing the cloud services. Some screenshots for Implementation, Registration, Puzzle, Puzzled Image, Sequence of Image Block are given in Fig 4,5,6,7,8
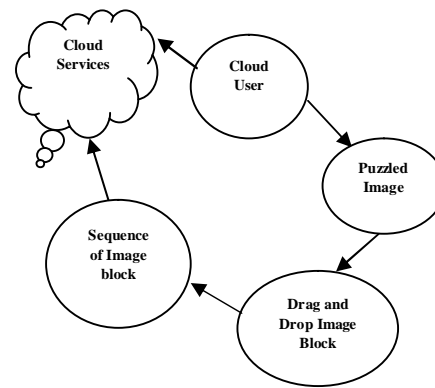

Figure 4. Implementation

Figure 5. Registration screen shots

Figure 6. Puzzle

**Figure 7. Puzzled
image**

**Figure 8. Sequence of
image block**

The sequence of independent and identical Bernoulli trails are applied to the puzzled based authentication scheme. The trails are independent with two possible outcomes (1 represent success or 0 represent failure). The geometric probability model for Bernoulli trials.

$$P(X = x) = p\ q^{x-1}$$

Where p-probability of success, q=1-p=probability of failure, X=Number of trials until the first success occurs.

In the first round of moving image block from drag source to drop target, attacker trials 20 times to get one success. After first success, attacker needs to trails 210 times to get 20 successes for moving image block to form

complete puzzle. The overall success rate of attackers is 0.095 which has minor effect on the security. The results shows that puzzle based authentication scheme would be strong enough to withstand online attack, where the system is able to detect and stop or throttle the attack after the fixed number of failed login attempts.

III.   CONCLUSION

The puzzle authentication scheme is reliable, more secure and robust and there is always drastic improvement in future. The analysis of the scheme shows that there is great opportunity to develop new ways to protect the confidentiality of cloud user data and information. The security levels of cloud environment can be further improved by using puzzle based scheme which overcome the loopholes present in the traditional authentication methods.

REFERENCES

[1].Daniela Elena, Popescu, Alina Madalina Lonea, *An Hybrid Text-Image Based Authentication for Cloud Services, International Journal of Computer Communicaiton,CCC Publications, Vol 8(2), 2013,pp.263-274.*
[2].Sulochana.V and R.Parimelazhagan, *Implementing Graphical Password and Patternlock Security Using MVC into the Cloud Computing, International Journal of Computer Applications, Vol 79, Number 8,2013,pp.7-10.*
[3].Dinesh.H.A and Dr.V.K.Agarwal, *Multi Dimensional Password Generation Technique for Accessing Cloud Services, International Journal on Cloud Computing: Services and Architecture(IJCCSA), Vol.2,No.3,2012,pp.31-39.*
[4].Grover Aman, Naran Winnie, *4-D password : Strengthening the Authentication Scene, International Journal of Scientific & Engineering Research, Vol.3,2012,pp.1-6.*
[5].Dinesha H.A *Multilevel Authentication Technique for Accessing Cloud Services, International Conference on Computing, Communication and Applications (ICCCA),2012, pp.1-4.*
[6].Navnath D.Kale, Megha M.Nalgirkar, *A Ample-Range Survey on Recall Based Graphical Password Authentication Based On Multi-Line Grid and Attack Patterns, International Journal of Science and Modern Engineering (IJISME),Vol.1,2013,pp.32-36.*
[7]Rachna Singh Thakur, Shubham Pathak, Rupali Patil, Neha Kate, Aditi Badkul, *Graphical Password (Puzzles) Authentication System, International Journal of Computer Architecture and Mobility(0082-0169),2012,Vol 1.*
[8].Wazir Zada Khan, Mohammed Y Aalsalem and Yang Xiang, *A Graphical Password Based System For Small Mobile Devices, International Journal of Computer Science Issues, Vol.8,No.2,2011,pp.145-154.*
[9]John Charles Gyorffy, Andrew F.Tappenden, James Miller , *Token Based Graphical Password Authentication, International Journal of Information Security, Vol 10,2011,pp.321-336.*
[10].Ahmad Alomari,*Appling Puzzle Encryption In the On-Demand Routing Protocols in Mobile Ad Hoc Networks (manets),Journal of Information Systems & Operations,2012.*
[11].Sanjay K.Dhurandher, Mohammed S.Obaidat, Ankit Mahendru, Lakshaya Agnani, *Puzzle Solving Based Authentication Method for Enhanced Security in Spins and Its Performance Evaluation, Proceedings of the 14th Communications and Networking Symposium,2011,pp.5-10.*