COMPARISON OF DATA SECURITY IN GRID AND CLOUD COMPUTING

Harmeet Kaur

Research scholar, Department of Computer Application Guru Kashi University Talwandi sabo (Bathinda), Punjab, India
Kaurharmit41@gmail.com

Abstract

In the current era, Grid computing and cloud computing are the main fields in the research work. This thesis define which are the main security issues to be considered in cloud computing and grid computing, and how some of these security issues are solved. Comparative study shows the grid security is tighter than the cloud. It also shows cloud computing is less secure and faced security problems. This research work is based on main security problems in cloud computing such as authentication, authorization, access control and security infrastructure (SLA). Cloud infrastructure is based on service level agreement; simply cloud providers provide different services to cloud's users and organizations with an agreement known SLA. So the security and privacy of user's data is the main problem, because unauthorized person can't access the data of cloud user. Hacking and data leakage are the common threats in cloud computing. As the security due to hackers increase over internet and the cloud computing is totally on internet. At this time, cloud computing demand the tight password protection and strong authentication and authorization procedure. For an increased level of security, privacy and password protection, we provide a new strong authentication model named "Two factor authentications using graphical password with pass point scheme". This authentication model includes the login procedure, access control that is based on service level agreement (SLA) in cloud computing.

Index Terms: *Cloud computing, Authentication, login, Recognition, Recall, Pass point, security, Cloud Provider, Service level Agreement, Two Factor Authentication*

----------***----------

1. INTRODUCTION

This section briefly describes the Grid and cloud computing paradigm, and a comparison between Cloud and Grid Computing security solutions. It presents security risks to the cloud user .Here we have proposed a new graphical password based system "Two factor authentications using graphical password with pass point scheme" in cloud computing.

1.1 What is Grid Computing?

Grid Computing defined combination of computer resources from multiple administrative domains, connection of potentially unlimited number of machines to reach common goal and tackle a same problem such as in science, industrial research, engineering, and commerce. It also provides highly scalable, highly secure, and extremely high performance mechanisms for discovering to remote computing resources.
Mary R. Thomson: "A Computational Grid is a collection of heterogeneous computers and resources spread across multiple administrative domains with the intend of providing users easy access to these resources." [1]

Main characteristics of Grid computing are:-
1).Large scale: A grid deals with a number of resources ranging from just a few to millions of resources.
2).Geographical distribution: Grid's resources may be located at geographically.
3).Heterogeneity: Grid belongs to different type of data like scientific instruments, display devices, personal computers, super-computers and networks.
4) Resource sharing: Grid belongs to many different organizations which allow other organizations to access them.
5). Multiple administrations: Each organization may establish different security and administrative policies under which the resources owned by can be accessed and used.

1.2 What is Cloud Computing?

Cloud computing is current buzzword in the market. Cloud computing is a technology that uses the internet and central remote servers to maintain data and applications. Cloud computing allows consumers and businesses to use applications without installation and access their personal files at any computer with internet access. This technology allows for much more efficient computing by centralizing storage, memory, processing and bandwidth. [2]

Cloud computing is basically cost effective and on demand service offered to the clients. The resources in the cloud are rented according to the needs and budget of the client. As the

cloud has involvement of many parties and resources its security remains a major issue. [3]

1.2.1 Cloud Service Models:

Cloud computing have three services models like Saas, Paas, and Iaas etc. Spinola (2009) explains the three service models of cloud namely:-

- **Cloud Software as a Service (SaaS),** where software hosted by the cloud vendors are rented to the end users;
- **Cloud Platform as a Service (PaaS)**, where infrastructure and programming tools supplied by the vendors are rented to the customers. It allows the customers to create their own applications; [4]
- **Cloud based Infrastructure as a Service (IaaS)**, where storage, networking and other fundamental computing resources for all purposes, are rented to the end users. Consumers can get services from the perfect computer infrastructure through the Internet. [5]

1.2.2 Cloud Deployment Model

Cloud provides the three types of deployment models.

- **Public:** Services and resources are reachable to the public by using the internet. The main concern in this type of cloud environment is the security; since this environment is accessible to the public and user data in one stage is hosted by a third party. [6]The cloud infrastructure is available to the general public. [5]
- **Private:** Services and resources are reachable within a private institute. Security is not a main issue compared to the public cloud as the services are reachable only through private and internal networks. [6] The type of the cloud, that is available solely for a single organization .[5]
- **Hybrid:** This type combines the methods from the private and public clouds, where resources can be used either in a public or a private cloud environment. The advantages and the concerns are a mixture of the earlier type.[6]

1.2 A COMPARISON BETWEEN GRID AND CLOUD COMPUTING SECURITY SOLUTIONS

Our main objective is to know the difference between Cloud and Grid computing and compare them from the point of view of security. We will see which security provides the better security. The main scope of my thesis is authentication, authorization and security infrastructure. We present the security difference from the analysis of the previous research papers. Here we have a list of differences between Grid and Cloud in order to clarify what are the main differences between Cloud and Grid computing:-

Cloud computing is a developing area and its ultimate strengths and weaknesses have not been fully researched yet. **Grid computing** is a much more mature technology than Cloud computing and grid security is better than the cloud security. Many facts could be given which shows that better security of grid computing and the cloud computing face same problems. **IoanRaicu and Shiyong Lu [7]** said that "The cloud computing security model seems to be relatively simpler and less secure than the security model adopted by Grids. " The strict security approach given by Grid computing adds security, helping to prevent unauthorized access, while Cloud computing does not. Grid computing needs to have multiple IDs, while Cloud computing only needs one. [7] The public-key based GSI (Grid Security Infrastructure) protocols are used for authentication, communication protection, and authorization. Furthermore, CAS (Community Authorization Service) is designed for advanced resource authorization within and across communities. Cloud infrastructure's typically rely on Web forms to create and manage account information for end-users, and allows users to reset their passwords and receive new passwords via Emails in an unsafe and unencrypted communication.

In grid computing, accounts and passwords requires also a person to person conversation to verify the person, perhaps verification from a sponsoring person who already has an account. The Grid approach to security might be more time consuming, but it adds an extra level of security to help prevent unauthorized access. [8] Security is one of the largest concept which is adopted from the grid Computing into the cloud computing.

Grid is based on proper key management. Grid use totally Public Key Infrastructure (PKI) in mostly methods of authentication such as SSL authentication, PKI authentication, and Mutual authentication. **Cloud** used simple ID and password techniques which is less secure. Mostly techniques of cloud authentication are under proposed work. Cloud computing is mostly using OTP (One Time Password) authentication; Two factor authentication, multifactor authentication Many cryptography techniques are adopted from the Grid computing.

Gruber (A Grid Resource Usage SLA Broker) is an example that has distributed policy enforcement points to enforce both local usage policies and global SLAs (Service Level Agreement) which allows resources at individual sites to be efficiently shared in multi-site. When grid one communicates to grid two then they used trust base relationship.

SLA is actually a service contract between customer and service provider where service's level is formally defined. Currently, the security model for Clouds (SLA) seems to be relatively simpler and less secure than the security model adopted by Grids. Broker (Gruber) works as a TPA in grid computing.

The Grid Security Infrastructure (GSI) is totally developed, which provide tight security for grid infrastructure. Nowadays, and knowing that Grid Computing is a much more mature technology than Cloud computing is, we agree that the security is better in Grid than in Cloud Computing. This thought is shared by Ian Foster, Yong Zhao, IoanRaicu and Shiyong Lu. [7]

Here we show the comparison of security at different level in tabular form.

Table 1: Security comparison at different level

Level of security	Grid computing	Cloud computing
Authentication	Full	Half
Authorization	Full	Half
Infrastructure	Trust Base Relationship /Service Level Agreement (SLA)	Service Level Agreement (SLA)

1.3 SECURITY RISKS TO CLOUD USER

In this research paper we outline some risks that are faced by a Cloud user:

1) Privileged user access: Data is accessible for only privileged users. Enterprise companies need to privacy and secure data. [9]

2) Insufficient authentication and authorization: Cloud providers should think beyond the customary security practices like restricted user access, password protection etc. Restricted user can access from simple user name / password protection. [10] Unauthorized parties access to sensitive data. Examples: Insufficient authentication, authorization and audit (AAA) controls Steve Mansfield mainly points out that we need to have a great deal of trust in the design of system with good authentication and authorization capabilities. [11]

3) User interface attacks: A Web browser is used for accessing Web applications. Thus, browser's user interface becomes an important security factor. Example: An attacker tries to fool the user into thinking that she is visiting a real website instead of a forgery. Techniques used here include fake HTTPS lock icons. [12]

4) Data leakage and Hacking: There are issues from hackers or attackers where they might get access to the base system and data in cloud. As the security due to hackers increase over internet and the cloud computing is totally on internet. [13] Here we find out the main risks in cloud environment. This thesis research is focused on identity-security solutions for cloud environments.

To overcome the previous Papers problems then I need to design the protocol that will cover all the problems. For solving the main risks in cloud, proposed a new strong authentication model named "**Two factor authentications using graphical password with pass point scheme".** This authentication model includes the login procedure, access control (authentication, authorization) that is based on service level agreement infrastructure (SLA) in cloud computing.

1.4 TWO FACTOR AUTHENTICATION USING GRAPHICAL PASSWOED WITH PASS POINT SCHEME

Passwords provide security mechanism for authentication and protection services against unwanted access to resources. I have proposed a new graphical password based scheme "Two factor authentications using graphical password with pass point scheme" in the cloud computing. This scheme is based on recognition technique and pure recall based technique and that offers many advantages over the existing systems and may be more convenient for the user. Our scheme is proposed for smart devices (like smart phones i.e. PDAs, iPod, Iphones, laptops and desktop computer systems etc) which are using the cloud services. [14]Three main things in our authentication model have been introduced:-

What type of authentication is used in this procedure?
Which types of techniques are used?
Which types of schemes are used under these techniques?

Our authentication model is used two factor authentication type. It is a combination of two techniques such as recognition technique and pure recall based technique. Then it uses the Pass Point Scheme, which comes under the recall based technique.

1.4.1 Two-Factor Authentication

Two factor authentications enable users to secure their logins and transactions. The two-factor system of authentication provides a much greater security shield against phishing and identifies theft. There are many two-factor authentication solutions on the market today. [15]

How it Works

First, users type in their usernames and passwords as usual. If primary authentication succeeds, then you enter the secondary authentication they are offered a choice of authentication method. It allowing users to authenticate with whatever method is best for them such as use pin code, ID card and smart card etc. Then user login securely**.** [16]

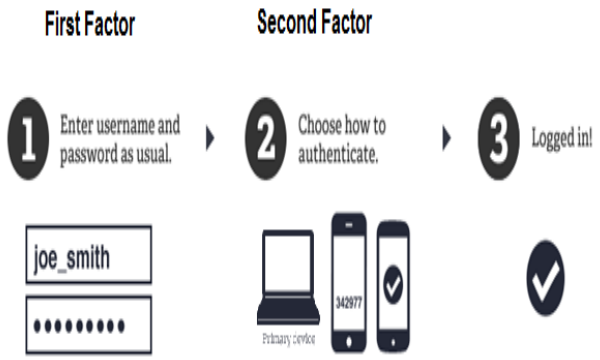

Fig- 1: working with two factor Authentication

Here we present image based and graphical password with the help of pass point scheme in the second factor. It provides the more tight security to user.

1.4.2 Recognition Technique and Recall Technique

In graphical password based system, we use the two techniques named recognition technique and recall technique. We combine the both techniques and that offers many advantages over the existing systems and may be more convenient for the user. In recognition technique a set of images is presented to a user from the cloud provider and the user is recognized and identified the images he selected during the registration stage. In recall based technique a user is to reproduce something that he created or selected earlier during the registration stage. In this procedure we used the pass point scheme, which is under the recall technique. According to this scheme user select a specific location on the image. [17]

1.4.3 "Pass Point" Scheme

I used the recall based technique. In this technique user is asked to reproduce something that he created or selected earlier during the registration stage. This technique provides many types of authentication schemes such as Draw-A-Secret (DAS) Scheme, Pass Point Scheme and Grid Selection Scheme etc. I pick up the pass point scheme for our authentication procedure, which is used with two factor authentication. In pass point scheme user click on any place on an image to create a password. A tolerance around each chosen pixel is calculated. In order to be authenticated, user must click within the tolerances in correct sequence. [17]

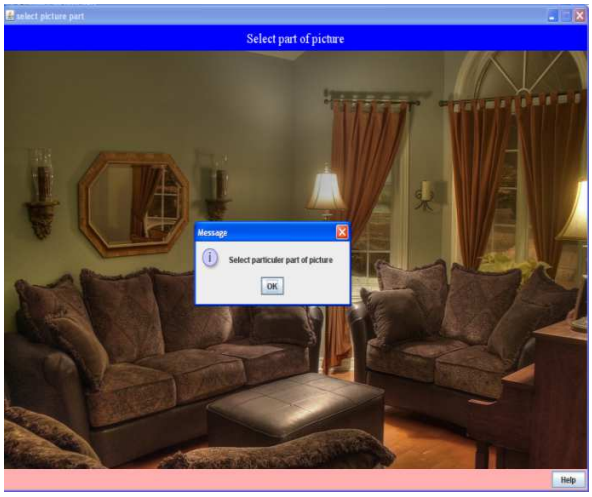

Fig-2: using pass point scheme

Pass point is based on the number of pixels or smallest units of a picture. In this technique the numbers of pixels are calculated as the password. It is hard to remember the specific location of the picture that provides the strong security.

2. OVERVIEW OF PROPOSED GRAPHICAL PASSWORD AUTHENTICATION SCHEME

The proposed procedure "Two factor authentications using graphical password with pass point scheme" is based on SLA (Service Level Agreement) that is an agreement between cloud user and cloud provider. First here we designed the TPA (Cloud provider) who provides the authentication services to cloud user from its database storage in graphical password authentication model.

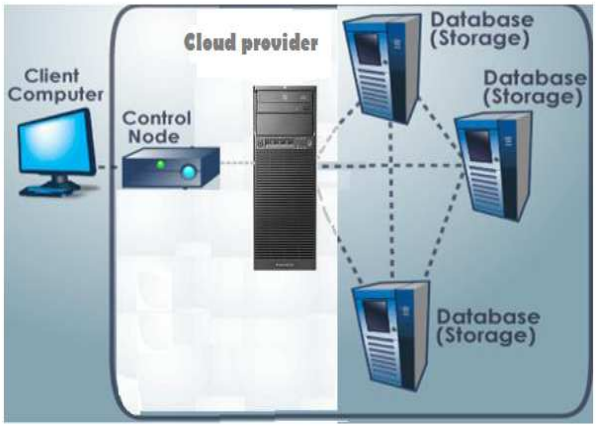

Fig- 3: Graphical password authentication model with SLA

Entire services provided by the Cloud Provider such as PaaS, SaaS, IaaS etc. Cloud service provider will be the responsible for maintenance and deliveries the software, infrastructure and storage over the internet.

2.1 Three-Level Defence System Structure

The proposed graphical password authentication model used three-level defence system structure:-primary password authentication, graphical authentication and authentication with pass point technique. Show figure 3:

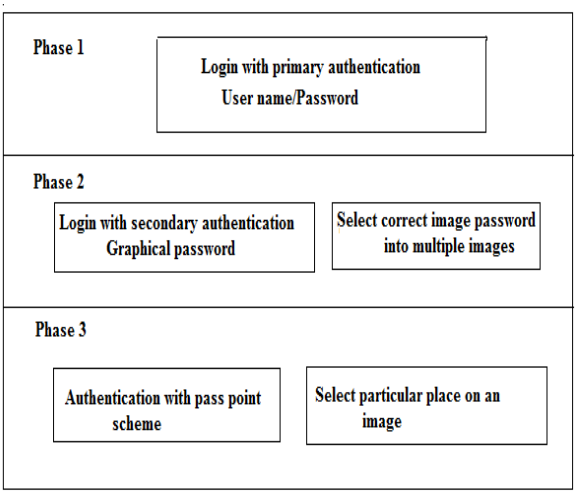

Fig- 4: Proposed Graphical password authentication model in cloud computing

The first phase: Primary authentication is achieved by using user name and password.

The second phase: In graphical authentication we can say it secondary authentication, multiple images shows. Select a correct image, which is selected by you as a password.

The third phase: It includes the pass point scheme authentication. If you select correct image as a password, then click on particular place into that image which is your password.
If you select the correct location you login successfully.

3. DESIGN AND IMPLEMENTATION

We present design security system architecture for a cloud environment, which aims to deliver two identity services, such as authentication and authorization in a secure and interoperable manner, which is called "Two factor authentications using graphical password with pass point scheme". The following flow chart describes the procedure of Graphical password authentication with pass point scheme:-

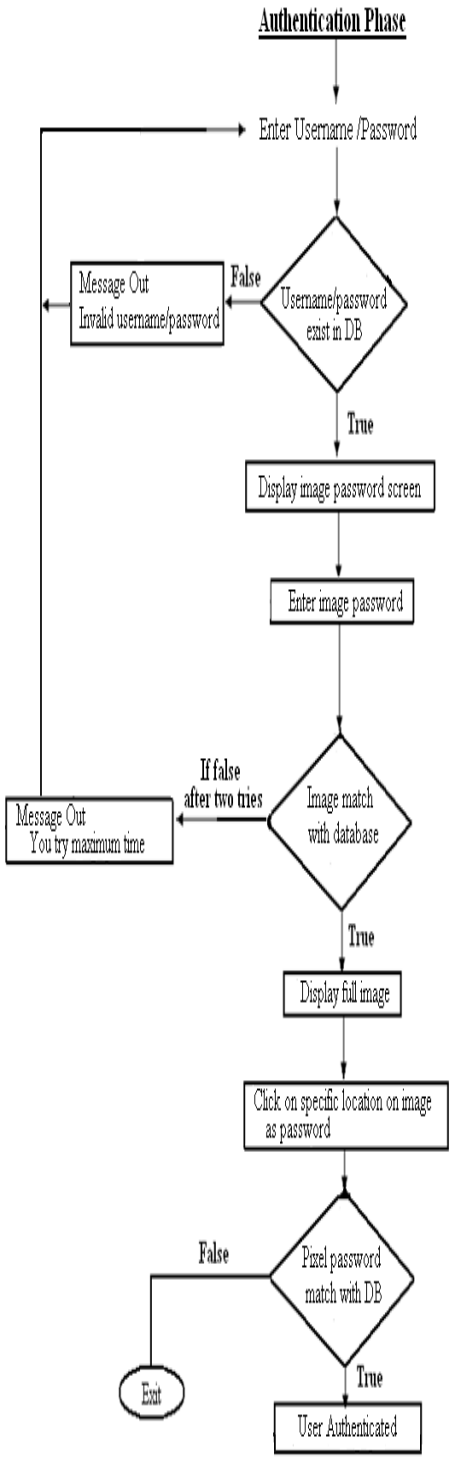

Fig- 5: Flow chart of Graphical password authentication scheme

4. SIMULATION RESULTS OF GRAPHICAL PASSWORD AUTHENTICATION SCHEME IN CLOUD ENVIONMENT

In this section, we describe the simulation results of the proposed authentication model.The cloud user select company for cloud using which company provides better facilities to the users. [18]

In the starting, user opens the cloud, and then loading page is showed for opening the cloud environment.

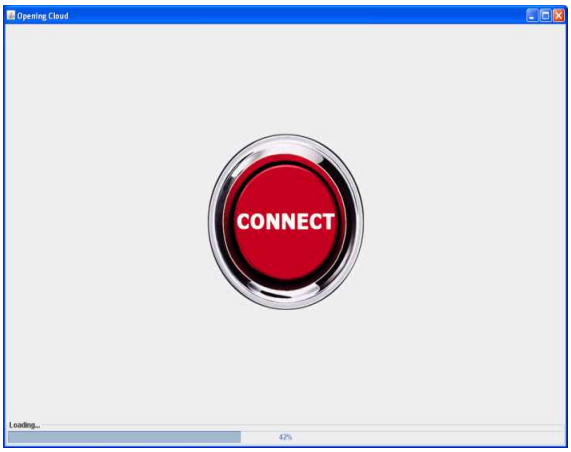

Fig- 6: starting the cloud environment

4.1 Registration phase

The first phase is the registration phase.The cloud provider displays login screen, which welcomes you in cloud.

Fig- 7: user login page

Then user create an account, user click on create new account button in login page. Display the registration form. Enter your basic information in the registration form.

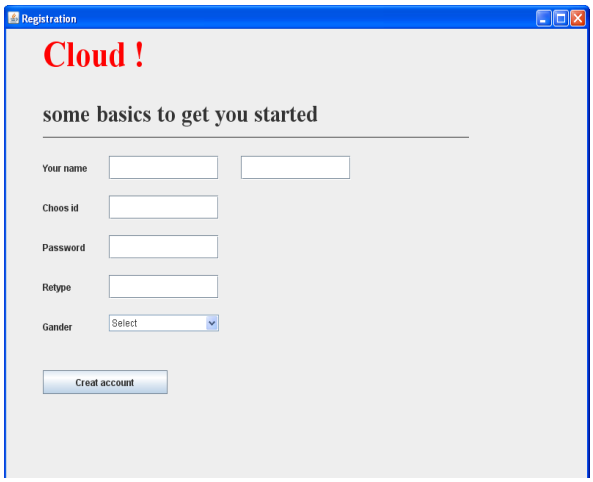

Fig- 8: user registration form

Cloud provider upload user information in DB in cloud storage. Cloud Provider confirms user with his username and password. Then cloud user registers his picture password from the multiple pictures. Then display the full picture, which selected by user as a password.

User registers his/her particular place on the picture password. Cloud provider uploads user's information into the cloud database storage, and goes to the page.

4.2 Authentication Phase

When a cloud user requests his/her data, cloud provider provides him login page. User authenticates with the graphical password authentication scheme. Here we describe the authentication steps:-

In first phase, Authentication: -This is password based or primary authentication. When a cloud user requests his/her data, cloud provider provides login page. Cloud user login with username and password. Cloud provider check is valid username and password by searching in DB in cloud storage. If user information not valid display error message as show figure

Fig- 9: user login page with error message

Else display second phase of authentication.

In second phase authentication steps: Then user enters the graphical password authentication. Cloud provider displays graphical login screen, which contain multiple pictures.

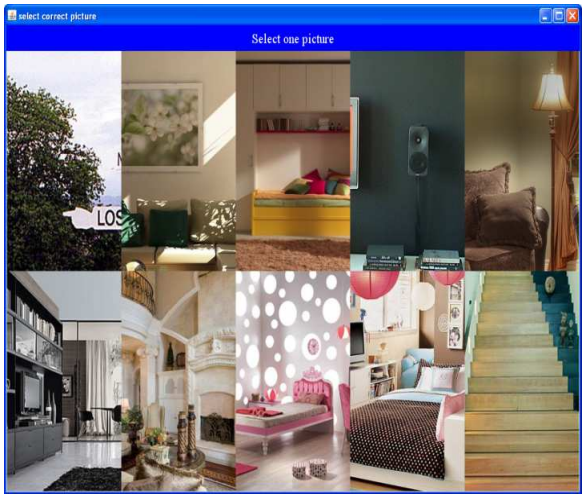

Fig- 10: select picture password

The cloud user selects his/her picture password into the multiple pictures. Cloud provider check is valid graphical picture by searching in DB in cloud storage. If user image is not valid display error message else display the full picture, with the message

"Select particular part of the picture". Show figure 10.

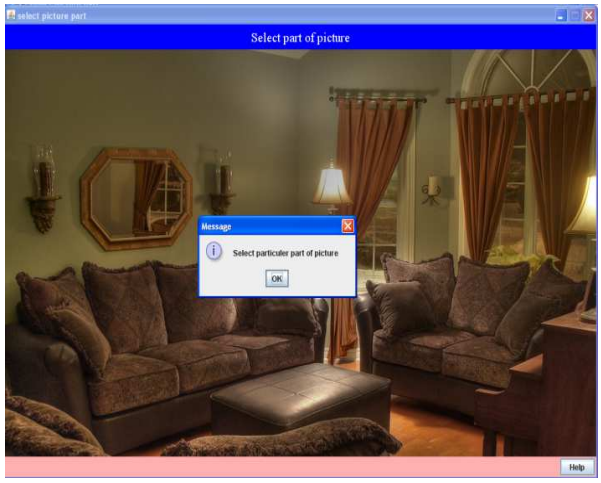

Fig-11: Select picture part password with message select particular part of picture

Then user clicks on the specific place (location) on the image. Cloud provider check is valid graphical image location password by searching in DB in cloud storage.

If user password is not valid exit the system. Otherwise you will successfully authenticate with cloud server, goes to cloud home page.

4.3 Change Password

If user wants to change the password, then he/she easily changes their password after authentication procedure. In cloud home page, click on change password option, and then it provide a dropdown menu list. Change main password and change picture password. Show figure 11.

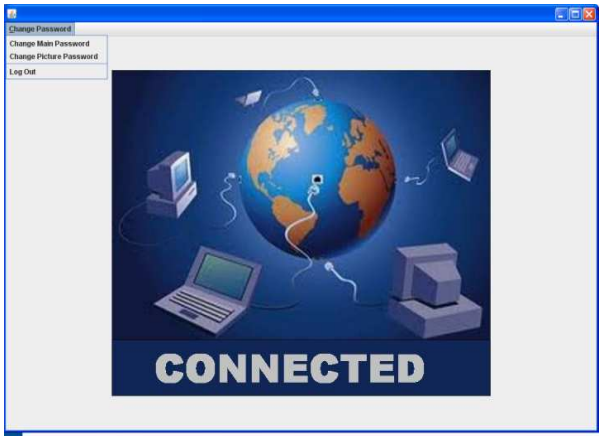

Fig- 12: Change password

If user want to change main password click on change main password option. It also provide the confirm password option.

Fig- 13: change the password

First fill old password and new password .It also provide the confirm password option, then click on next button, it comes back to home page. Your password is changed. Then click on change picture password. Provider display multiple pictures screen to change the password.

You can select any picture as password and click on next button. Display the change location password of picture screen. This screen displays the red labels as passwords. You can select any red part of picture as password. Your picture part is also changed.

4.4 Forget Password

If you forget your password, TPA provide you option forget password. In the login page, a link is provided you "Forget your password?" click on this link, cloud provider display the recover the password window.

Fig- 14: recover the password

If you enter the right username, then it displays the next question screens. Show figure14.

Fig-15: recover the password with question screen

Then some questions will ask to user, which were selected by user at the time of registration phase. If user gives the right answers to those questions, then he/she recover the password. User also chooses the new password as the main password, picture password and picture part password.

4.5 Administration Login

In admin login cloud provider checks the information and record of the users. It is only use for cloud provider. For admin login cloud provider use the Administrator login option. Cloud provider login with username and password. It provides the detail of the users, which are connected to the cloud provider. After login display the admin home page. All user which are connected to the provider, show on the right hand side.

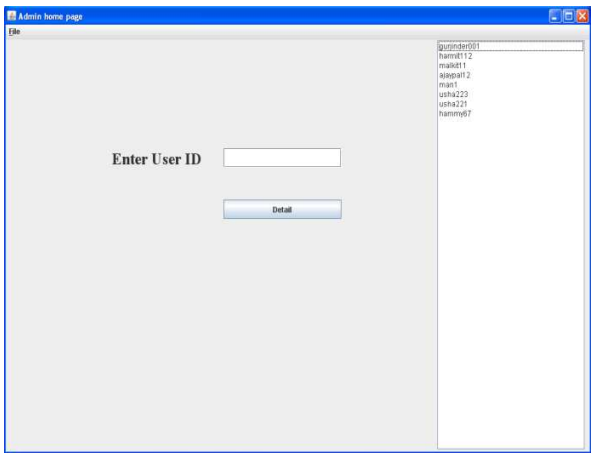

Fig- 16: admin home page

When you double click on any user ID in the right side, it provides the all detail of the users.

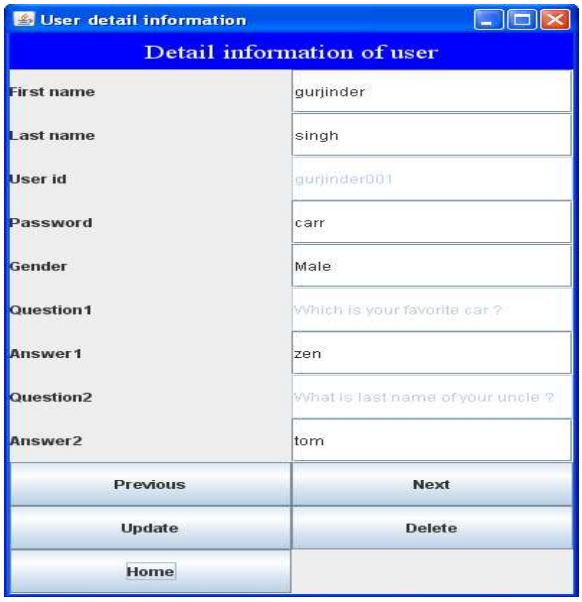

Fig- 17: user information detail

You can view the previous and next user ID with the previous and next buttons. You can update the user record the update button. You can delete the user record the delete button. Click on home button and come back on the admin home page
In this research paper, we successfully implemented authentication procedure, which is based on the image base processing.

CONCLUSIONS AND FUTURE WORK

In this research paper, for solving cloud authentication risks, we proposed a new strong authentication model named "Two factor authentications using graphical password with pass point scheme". This is image-based authentication procedure. This procedure provides more protection for cloud environment. This authentication model includes the login procedure, access control that is based on service level agreement (SLA) in cloud computing.

We implement the graphical password authentication procedure for cloud computing.People is better at memorizing graphical passwords than text-based passwords. It is more difficult to break graphical passwords using the traditional attack methods. Graphical password used the more storage location instead of textual password. In future image compression technique also applied this procedure. You can decrease the storage space for compression technique and it provides the more powerful protection for graphical password.

ACKNOWLEDGEMENTS

All praise and glory is due to God for blessing, God is always here for me whenever I needed help and guidance. It is a contribution of many persons that make a work successfully. My deepest gratitude to my supervisor, Dr. R K Bansal (Research Dean of Guru Kashi University) whose ceaseless support, encouragement, and flexibility I shall never forget.
As I proceed in my life, Dr. R K Bansal will always be my mentor and a model of how a successful supervisor should be.
Special thanks to Er. Manjit Singh for useful discussions during early stage of my work. This thesis would not have been possible without the support of my family specially my brother Gurjinder Singh.

REFERENCES

[1]. Harish Vepuri, Moshin Rahman "IMPLICATIONS OF CLOUD COMPUTING IN IT ORGANIZATIONS" MASTER THESIS 2011
[2]. Pankaj Arora, Rubal Chaudhry Wadhawan, Er. Satinder Pal Ahuja "Cloud Computing Security Issues in Infrastructure as a Service" ijarcsse ISSN: 2277 128X January 2012
[3]. Richa Chowdhary, Satyakshma Rawat "One Time Password for Multi-Cloud Environment" Department of Computer Science Engineering Amity School of Engineering and Technology Noida March 2013
[4]. Spínola, Maria. (2009). "An Essential Guide to Possibilities and Risks of Cloud Computing - A pragmatic, effective and hype-free approach for strategic enterprise decision making."Computing. Available at: http://www.mariaspinola.com/CloudComputing.php (Acc. 2011-9-15)
[5]. Rehan Saleem "CLOUD COMPUTING'S EFFECT ON ENTERPRISES" school of Economics and management Lund university January, 2011
[6]. Hosam AlHakami, Hamza Aldabbas, and Tariq Alwada'n "COMPARISON BETWEEN CLOUD AND GRID COMPUTING: REVIEW PAPER" Software Technology Research Laboratory (STRL), De Montfort University 2012
[7]. David Munoz Sanchez "Comparison between security solutions in Cloud and Grid Computing" Helsinki University of Technology 2010
[8]. DAVIT HAKOBYAN "Authentication and Authorization Systems in Cloud Environments" Master of Science Thesis, Stockholm, Sweden 2012
[9]. Ian Foster, Yong Zhao, 1Ioan Riau, Shiyong Lu "Cloud Computing and Grid Computing 360-Degree Compared" Department of Computer Science, University of Chicago, Chicago, IL, USA 2008
[10]. PROF: ASHA MATHEW "SECURITY AND PRIVACY ISSUES OF CLOUD COMPUTING; SOLUTIONS AND SECURE FRAMEWORK" Welingkar Institute of Management Development and Research, BangaloreVol.2 Issue 4, April 2012.

[11]. Steve Mansfield-Devine, "Danger in Clouds", Network Security (2008), 12, pp. 9-11.
[12]. Ankit Singh "The security and privacy threat to cloud computing" Frankfurt am Main, Germany April 23, 2012
[13]. Anurag Porwal, Rohit Maheshwari, B.L.Pal, Gaurav Kakhani "An Approach for Secure Data Transmission in Private Cloud" International Journal of Soft Computing and Engineering ISSN: 2231-2307, Volume-2, Issue-1, and March 2012
[14]. Partha Pratim Ray "Ray's Scheme: Graphical Password Based Hybrid Authentication System for Smart Hand Held Devices" Department of Computer Science and Engineering, Surendra Institute of Engineering and Management, Dhukuria
[15].http://www.entrust.com/two-factor.html
[16].https://www.duosecurity.com/product
[17]. M.Bhargavi Graphical password Authentication /www.slideshare.net/akhilrocker143/558-11294069
[18]. Eman M.Mohamed, Hatem S.Abdelkader "Data Security Model for Cloud Computing" Department of Computer Science, Menofia University Faculty of computers and information Egypt 2013

BIOGRAPHIES

Harmeet kaur received the Post Graduation diploma in Computer Application from Guru Nanak Dev University Amritsar, Punjab in 2008. She has been received the Msc degree in Information Technology from Punjab Technical University Jalandhar, Punjab in 2009, and the M.C.A degree from the same university, in 2010. She is currently working towards the M.Phil Degree in the Department of Computer Application at the Guru Kashi University Talwandi Sabo, (Bathinda) Punjab. Her main research interests include Network Security and Cloud computing.