IARJSET
ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
ISO 3297:2007 Certified
Vol. 3, Issue 11, November 2016

Title: Graphicos Parasynthima Security

Auti Mohini[1], Jadhav Pratiksha[2], Auti Sayali[3], Gadge Meghana[4]
Dept of Computer Engineering, SGOI COE, Maharashtra, India[1, 2, 3, 4]

Abstract: This project is a new graphical password scheme. This increases the security. User can set the password in the form of image. User presents this image to a system camera and then enters their password as a sequence of selection on live video of object. In existing system cloud data storage and its access in done by using text password which is combination of numbers, characters and special symbols that why these password are the easily guessable and easy to hack. Because of this drawback we are propose to a new solution and that is graphical password security. In that we are going to use the image processing concept for login purpose. To achieve that goal we store one sample image of object and password as the part of that image.

Keywords: Loci metric Password Schemes, Multifactor Authentication Schemes, Live face, PassBYOP, Feature extraction, Physical tokens, click points, Security

1. INTRODUCTION

Now a day security is important issue. Text password is most useful authentication method. But it has many security usability related problems. Authentication is a process of identifying whether a particular individual or device should be allowed to access a system or not. Text password requires to remembering it and recalling at time of login operation. It is use to provide security to system & resources.

User authentication is most important for providing security. It provides accountability & access control to user. There are various types of authentication systems in market. In that text password that is alphanumeric password. This password are easy to remember & easy to use. But if this password is too short then, it easily guess by attacker & if password is strong it is hard to remember. To solve the problem which occurred due to text password i.e. easily guess & difficult to remember.
The market was provide a technique OTP (One Time Password). OTP passwords provided by token devices are very expensive.

Another proposed solution is to use Graphical password. In which graphical images are used for provide security. But graphical password has some disadvantages that are shoulder surfing attack and intelligent guessing. Such attack are more powerful because of area selected by user on image is observed or guess by attacker.

1.1 Existing system

Password is used for user authentication. It is used to prove identity or access approval to gain access to a resource. Two conflicting requirements of alphanumeric passwords-

1) Easy to remember
2) Hard to guess
Many people tend to ignore second requirement, which lead to weak passwords. So many solutions have been proposed one of them is graphical passwords.

1.2 Architecture of existing system:

1. User Registration process:

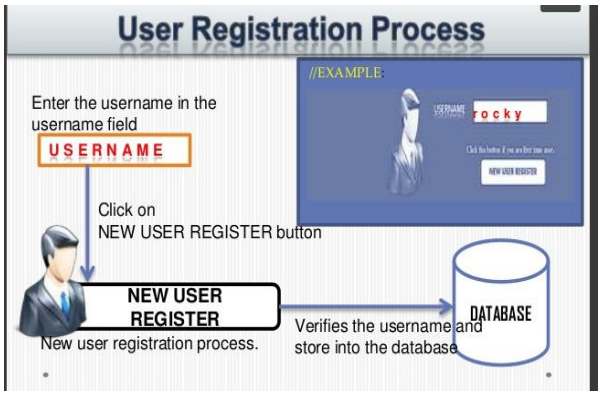

Fig 1.1: User Registration process.

In registration phase user enter user name. If username is already existing in database then it does not accept this username otherwise username is stored in database.

2. Picture Selection Process:

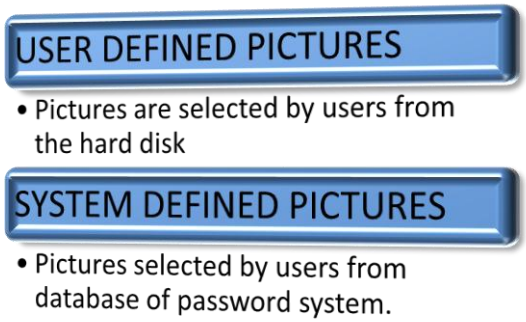

Fig 1.2: Picture Selection Process.

In Picture selection process user can give its own pictures or system defined pictures.

IARJSET
ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
ISO 3297:2007 Certified
Vol. 3, Issue 11, November 2016

3. User Verification Process:

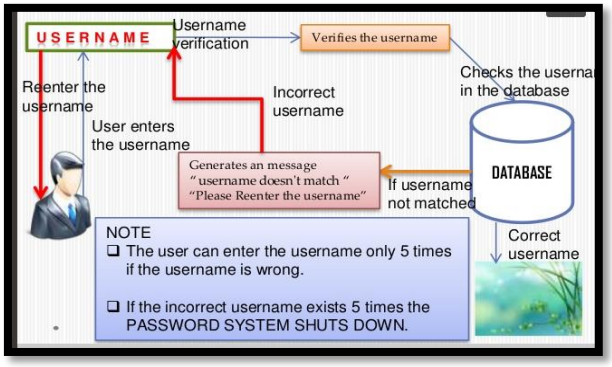

Fig 1.3: User Verification Process.

In this phase user entered the username then verifies the username. If the user name is correct then login operation is performed. If username is incorrect then generate a message" User Name Doesn't Match. Please re-entered username".

4. Click Point Verification:

If Username is correct then it goes to next step.
That is click points selection. Then it verifies the click points. After verification login operation is performed

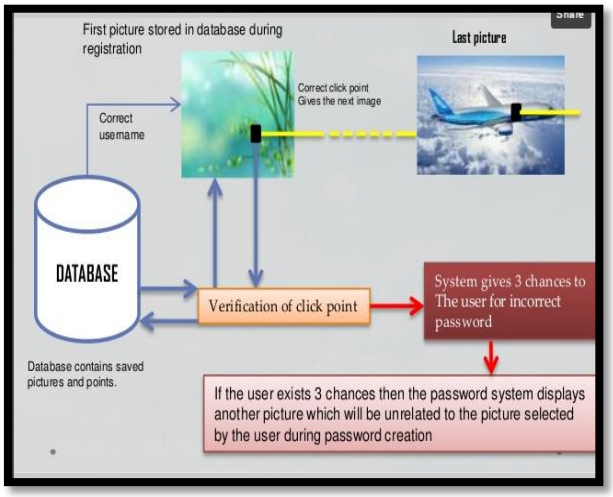

Fig 1.4: Click Points Verification.

In this phase click points are selected and stored in database and verified.

1.3 Literature Survey:

Ethan Rublee, Vincent Rabaud, Kurt Konolige, Gary Bradski proposed a new technique ORB. ORB is used for object matching algorithm. As compare to SIFT & SURF this algorithm work efficiently & faster. [1].
Raikoti Sharanabasappa, Sanjaypande M. B proposed a " Real Time Multiple Face detection from Live Camera". In this system author proposed a face detection and segmentation for automatic attendance. Segmented faces use to recognise student. In the system, camera is static and periodically takes the snap of class and after that each snap is process to extract the face. [2]

Priti C. Golhar, Dr. D.S. Adane developed a " Graphical Knowledge Based Authentication Mechanism". In that Cude click points was use to reduce different patterns and to reduce the usefullness of hot spot for attackers. Rather than all click points on same image CCP uses one click point on different image which are used for password. If click points location on first image is correct then only second image will appear. If it creates a path through an images Number of images in equal to number of click points. But if click points are more than it is difficult to remember. [3]

Hu Han, Brendan F. Klare, Kathryn Bonnen, Anil K. Jain, designed a "Matching Composite Sketches to Face Photos: A Component-Based Approach" The problem of automatically matching sketches of facial photograph is address in this paper .Author propose component based representation(CBR) approach to measure the similarities between a composite sketch and mugs hot photograph.[4]
V. Bhusari designed an approach"Graphical Authentication Based Techniques". In this approach creates a password by selecting an image at the time of registration .During login time, this image is retrive from data base as a password chooses multiple point-of-interest area in the image. After registration user select a record signature. Due to this it provides better security. But user need to upload image at the time of login by own. Also remember to area points otherwise fails to perform login. [5]
Iranna A. M., Pankaja Patil proposed that "Graphical Password Authentication Using Persuasive Cued Click Point". This paper focuses on the integrated evaluation of the Persuasive Cued Click Points graphical password authentication system, including usability and security. An important usability goal for authentication systems is to support users in selecting better passwords, thus increasing security by expanding the effective password space. They use persuasion to influence user choice is used in click-based graphical passwords, encouraging users to select more random, and hence more difficult to guess, click-points. [6]

G. Akhila Goud, B. Hemanth proposed that "Face Recognition using Edge Detection of Layer". This paper developed a new technique for human face recognition in crowd. Here face recognition in crowd is done by using canny edge detection algorithm. But this system is less efficient when crowd is vast. [7]
Fei Zuo Peter H. N. de, developed a "Real-time Face Recognition for Smart Home Applications". This technique automatic replace a face in photograph. In this system input face will be replace with one selected image from large collection of face images. the system for face replacement can be use for face identification, personalize face replacement. [8]

Dmitri Bitouk, Neeraj Kumar, Samreen Dhillon, Peter Belhumeur, Shree K. Nayar designed an approach "Face Swapping: Automatically Replacing Faces in Photographs". For increasing security system face

IARJSET
ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
ISO 3297:2007 Certified
Vol. 3, Issue 11, November 2016

recognition (FR) technology has been applied but in this technology there is one problem that is attach with spoofing with faces to guard from this attcks & to improve relialibility of FR system anti spoofing approches have been developed. In this paper various face liveness detection method are discussed.[9]Dhananjay Garud, Dr. S.S. Agrawal proposed an" A Review: Face Liveness Detection. In this system author proposed face detection and segmentation for automatic attendance. Segmented faces use to recognise student. In the system, camera is static and periodically takes the snap of class and after that each snap is process to extract the face. [10]

2. PROBLEM STATEMENT:

Design a system which provides a better authentication to cloud. Traditional system uses text, numeric or some pattern passwords which is not the good way. Because by using the shoulder surfing techniques anyone may guess the passwords. To overcome this problem we will introduce the new way to unlock the Cloud Account which is the face recognition technique.

3. PROPOSED SYSTEM:

Now a day security is very important issue in terms of cloud computing. To authenticate the system text passwords are mostly used. But it has many security & usability related problems.

Basically Authentication is a process of identifying whether a particular individual or device should be allowed to access a system or not. Text passwords are easy to memorize & recall it at the time of access a system. To address this issue, we proposed a new technique "Graphicos Parasynthima Security". Graphical password system is a technique that depends on selecting click points on image. This technique resistance to brute force attack and shoulder surfing attack. Such attacks are more powerful because attacker can easily hacked a system.

3.1 Architecture of Proposed System:

It contains two phases:
1. Registration Phase
2. Login Phase

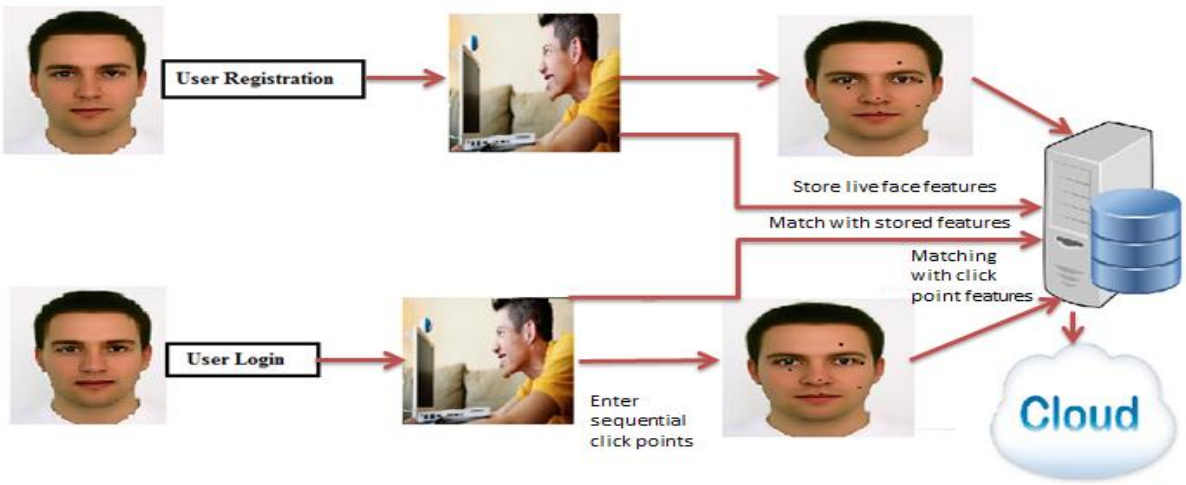

Fig 3.1: Architecture of Proposed system

In this, we use Live Face detection & Recognition technique to authenticate the system. User present live face to a camera & select the click points as a portion of an image. Highly distinctive features extracted from this live face & click points are saved in database & used as a password. At the time of login user again gives live face and sequential click points. The extracted features from this live face and click points are match with stored features in database. We have set some threshold value to match extracted features .If features are match then successful authentication to cloud otherwise authentication denied. Graphicos Parasynthima Security shows better security while maintaining the usability of current graphical password technique.

3.2 Advantages of proposed system:

1. This system seeks to make graphical passwords more secure against intelligent guessing and shoulder-surfing attacks.
2. This system does not place additional burdens on users.
3. Overcome the Shoulder surfing attack.
4. Secure way to authenticate the cloud.

3.3 Goals and Objectives:

1. Secure Authentication using the Face Recognition.
2. Provide security to cloud access.
3. Overcome Shoulder surfing attack.

4. TECHNIQUES USED:

There are two types of techniques used for face detection and click points verification.

These techniques are:
1. Haar like feature
2. ORB (Oriented FAST and Rotated BRIEF)

IARJSET
ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
ISO 3297:2007 Certified
Vol. 3, Issue 11, November 2016

1. Haar like feature:

Haar like features work with face detection. It uses Positive images (Image of face) and Negative images (images without faces) to train the classifier. After that extract feature from these images. Haar like features work on four techniques:

1. Edge Features
2. Line Features
3. Center Surround
4. Diagonal Line

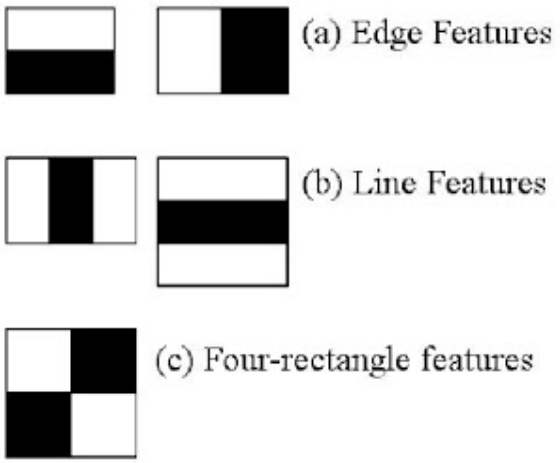

Fig 4.1: Techniques of Haar algorithm

2. ORB (Oriented FAST and Rotated BRIEF)

ORB is used for object matching. As compare to SIFT and SURF this algorithm is efficient and faster. ORB is a combination of FAST key point & BRIEF descriptor.

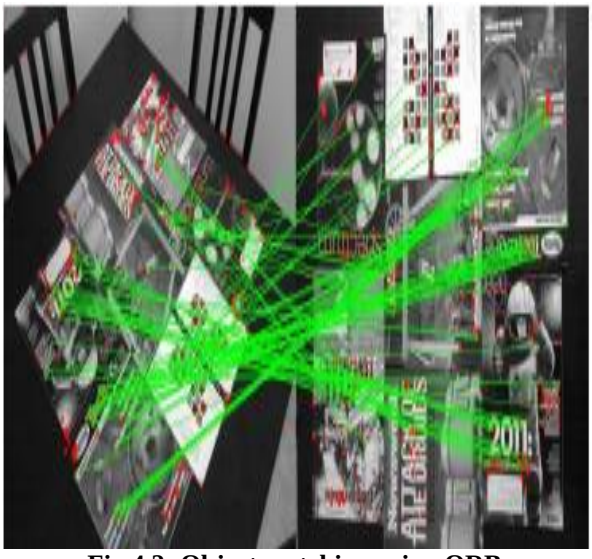

Fig 4.2: Object matching using ORB

5. CONCLUSIONS

We conclude that, our system provide secure authentication to cloud. It vanish the shoulder surfing attack. It resistance to brute force attack & guessing attack.

6. ACKNOWLEDGEMENT

The authors would like to thank computer department HOD Prof. Shimpi M.R and Prof. Devokar M.S, Prof. Ingale S.E. in Samarth Group Of Institutions Belhe (Bangarwadi) Savitribai Phule Pune University for their kind support and assistance during the course of this research.

REFERENCES

[1] Ethan Rublee, Vincent Rabaud, Kurt Konolige, Gary Bradski, "ORB: an efficient alternative to SIFT or SURF" 2010.
[2] Raikoti Sharanabasappa, Sanjaypande M. B "Real Time Multiple Face detection from Live Camera, a Step towards Automatic Attendance System" International Journal of Computer Applications (0975 8887), Volume 45 No.4, May 2012.
[3] Priti C. Golhar, Dr. D.S. Adane " Graphical Knowledge Based Authentication Mechanism". International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 10, October 2012.
[4] Hu Han, Brendan F. Klare, Kathryn Bonnen, Anil K. Jain, "Matching Composite Sketches to Face Photos: A Component-Based Approach," in IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 8, NO. 1, JANUARY 2013.
[5] V. Bhusari " Graphical Authentication Based Techniques" in International Journal of Scientific and Research Publications, Volume 3, Issue 7, July 2013. [6] Iranna A. M., Pankaja Patil, "Graphical Password Authentication Using Persuasive Cued Click Point", International Jousrnal of advanced research in Electrical, Electronics and Instrumentation Engineering Vol. 2, Issue 7, July 2013.
[6] Iranna A. M.,Pankaja Patil,"Graphical Password Authentication Using Persuasive Cued Click Point" International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering Vol. 2, Issue 7, July 2013
[7] G. Akhila Goud, B. Hemanth,"Face Recognition using Edge Detection of Layer", IJSRSET,VOL 1,2015.
[8] Fei Zuo Peter H. N. de, "Real-time Face Recognition for Smart Home Applications".
[9] Dmitri Bitouk, Neeraj Kumar, Samreen Dhillon, Peter Belhumeur, Shree K. Nayar" Face Swapping: Automatically Replacing Faces in Photographs", 2015.
[10] Dhananjay Garud, Dr. S.S. Agrawal " A Review: Face Liveness Detection" in International Journal of Advanced Research in Computer and Communication Engineering, Vol. 5, Issue 1, January 2016.