Shoulder Surfing Resistance Using Message Digest 5 Algorithm (MD5)

Namitha M.S [1], S.Shanmuga Priya [2]

[1]Department of Computer Science and Engineering, New Horizon College of Engineering,Bengaluru-560103,Karnataka ,India

2Senior Assistant Professor, Department of Computer Science and Engineering, New Horizon College of Engineering,Bengaluru

***Abstract*-Nowadays authentication is been used for all the application for the security purpose .Humans have a mindset of always choosing a short password or the password which is been easy for them to remember. As the mobile application pilling up, people can use their application anytime and anywhere they need it. This is the convenient way of using but this may lead to the shoulder surfing attacks, because as the person whoever is standing behind you can view your password typing or they can record it by any camera.**

So instead of using only textual password for authentication we can also use the graphical password for the second authentication for unlocking the application. This graphical password will resist shoulder surfing resistance by one time valid login password along with the horizontal and vertical bars covering the entire scope of the pass-matrix images. This authentication can avoid the shoulder surfing attacks when there is a proper usability

***Keywords*- Shoulder surfing Resistance, Authentication, one time login password, pass matrix.**

I INTRODUCTION

Textual passwords are now been replaced by the graphical authentication which overcomes all the problems of textual password. Human brain has a better memorization in remembering the images than the alpha numeric passwords and the chances of forgetting the images is also less.

As a result humans can remember any complicated image password for a longer time Even though they are not using their application frequently there graphical password will be remembered

II LITERATURE SURVEY

Sharddha, M.Gurav and Leena[1] told that graphical passwords are the solution for the textual password as it is easy to remember .When the application have a user friendly authentication it becomes easy for the user to use this application .According to the psychology studies it is told that the human brain can easily remember images than the alphabets or digits as visual reorganization is more in humans.it will be more secure when an application will have textual password and graphical image password .here graphical security is by mean of pass matrix images.

A .Paivio and T.Rogers and P.Symthe [2] told that pictures as the objects were recalled better than the alphabets in the trials recalling of alphabets for two times did not differ organization but striking in the input serial order differed it. But the recalling of the images in both the trials were recalled easily which is been recognized as verbal and non -verbal memory code.

P.C Van Oorschot and Jalie Thorpe [3] in a lab survey of 43 users and 17 images and 223 user accounts we explore the use of human computation to predict the hot-spot which is needed they generated two humans-seeded attacks based on some methods one based on first-order markov mode, another based on independent probability models present. Within some 100 guess the first method was able to find 4% of the password in the first data set and the 10% in the second data set, in the second method we were able to find out 20% in the first data set and 36% in the second data set from this we were able to evaluate that our first method of markov mode-based attack with the cross –validation of the field study the average of 7-10% of the user passwords were guess within 3 guess then we should also found that the should be an improvement in the second method .Then in our results we suggested that the graphical scheme are vulnerable for both online and offline attack

T.Kwon and S. Shin[4] when the user interacts with the computer system for entering their secret password shoulder surfing attacks are more nowadays. There was assumption that human eye cannot capture the things easily but this assumption was put down ,in this paper they have even show that human adversaries, even without a recording device, can be more effective at eavesdropping than expected by training themselves by the training even the difficult pin also would be hacked because of shoulder surfing attack.so this proved that than expected humans adverserires are powerful.

Huanyu Zhao and Xiaolin Li [5] the vulnerability of the textual password are well known to us as human always choose the short password or a meaningful password which is been easy to remember for them, which makes the hackers or the person standing behind him can easily hack the account or the hackers can use an hidden camera or a recording device to hack the account so we propose a system of scalable shoulder surfing password authentication in which we include a textual authentication with graphical password and provide a perfect resistance to the shoulder surfing resistance even if there is a hidden cameras or a recording devices

Tetsuji Takada[6] Peeping attack is the tread for the authentication nowadays the worst part is the hackers started using the cameras or video recording for capturing the passwords this paper has the unique authentication called the fake pointers as it uses the methods of fake pointers the hacking becomes difficult when there is a camera and a recording devices fake pointers provide the double layered input screen This interface makes it difficult for attackers to identify a legitimate user's secret even if they have a video record showing a target user's authentication action. This fake pointer use two feature’s in the second method fixed secret and a disposable secret this enables in changing the secret input operation in each and every authentication this and all makes the user difficult to understand the password even if there any recording cameras

III Proposed System

In this system we introduce a graphical authentication system called pass matrix it consist of pass-square per pass images user can select one pass images as the password and a hash code will be generated for it using the MD5 algorithm this type of authentication will overcome the naked eyes attack as the one type password is been generated even the video capturing does not work here as the password can be used only for the one time.

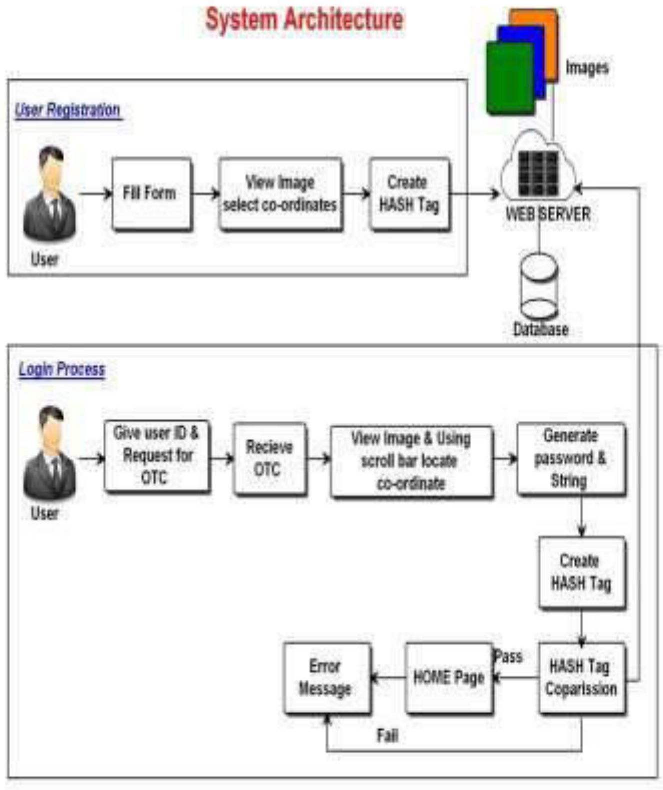

Fig.1 System Architecture

In the fig 1 it represents the system architecture .At the first user has to register by filling the form then a random pass matrix images will be randomly generated then the user has to select the image coordinates as the user wish and the user needs to remember the image coordinate which he has selected then a hash code will be generated for it using the MD5 algorithm and that hash code will be stored in the database and the same hash code is been compared with the login hash code.

When the user logins the user will request for the OTC(one time code) after receiving the OTC the user will map the code according to the password with the help of horizontal and vertical bars and for that particular pass matrix a hash code will be generated and that hash code generated during login time and registration time is been compared if it matches it will go for the home page of the user else error message will be displayed.

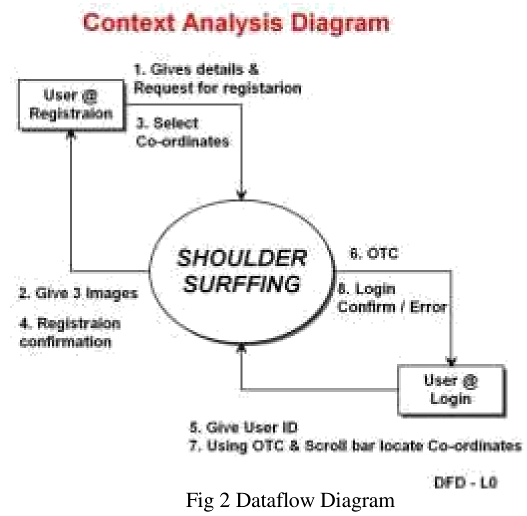

Fig 2 Dataflow Diagram

In the fig 2 it represents the dataflow diagram in this the user needs to register by giving user id of its own and some basic information of the user then three pass-images will be given for the user to select the coordinates pass matrix images as the password and for that then the registration will be confirmed while login to the application the OTC is be sent to the registered email id and the OTC which is been generated should be mapped with the help of the vertical and horizontal bars accordingly for all the three images, if the mapping is correct then the home page of the user is been displayed .

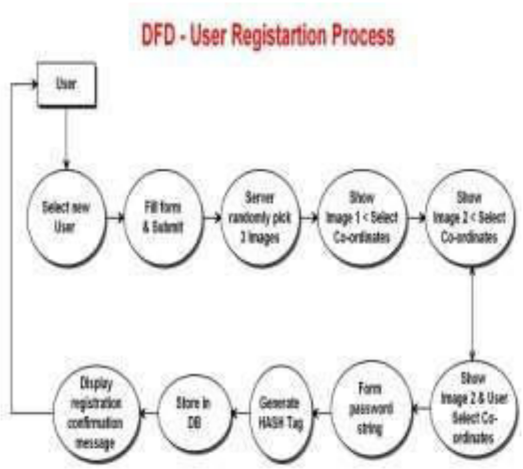
DFD - User Registartion Process
User
Select new User
Fill form & Submit
Server randomly pick 3 images
Show Image 1 < Select Co-ordinates
Show Image 2 < Select Co-ordinates
Show Image 2 & User Select Co-ordinates
Form password string
Generate HASH Tag
Store in DB
Display registration confirmation message

Fig 3 DFD User Registration

Fig 3 represents DFD user Registration in this if the user is making use of the application for the first time then he needs to undergo the registration steps for the then the user needs to fill the user form and submit it later then the Server generate three pass-matrix images to select the coordinates pass-matrix images and those pass matrix images Coordinate is also been stored in the database and hash code is generated for the selected coordinate images and will be stored in the database. In fig 4 it represents the user login process in this the user first needs to undergo the textual authentication later the email is been sent to the users email id then the horizontal and vertical bars around the parse matrix is been displayed and according to the mail id received the user needs to set the password string accordingly then on click of the submit button the hash code generated during the registration time and the login time is unique then the users application can be unlocked

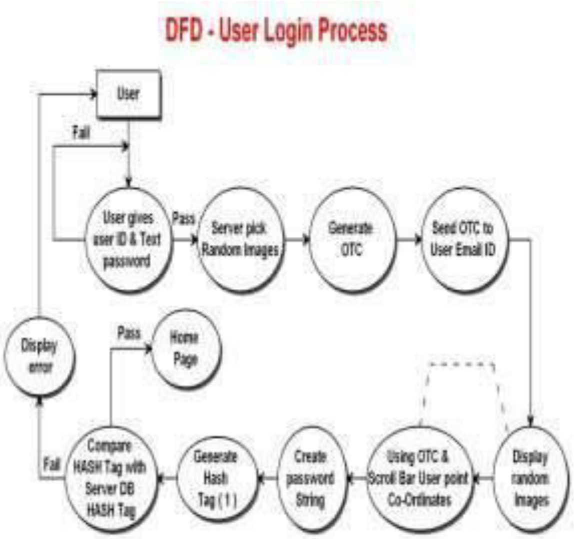
DFD - User Login Process
User
Fail
User gives user ID & Text password
Pass
Server pick Random Images
Generate OTC
Send OTC to User Email ID
Display error
Pass
Home Page
Fail
Compare HASH Tag with Server DB HASH Tag
Generate Hash Tag (1)
Create password String
Using OTC & Scroll Bar User point Co-Ordinates
Display random Images

Fig 4 DFD User Login

Algorithm

MD5 (Message Digest 5):-the MD5 algorithm is also been called as hashing algorithm which is mainly used for the secure cryptographic hash algorithm for the authentication purpose .this algorithm takes the input of arbitrary length here for this authentication it is been taking the arbitrary length of the image chunks and this input string is been broken down into two half and a bit logical operation is been done and a output of 128 bit is been generated..

Split images into chunks:-This algorithm helps to split a big images in to small chunks this algorithm takes the input of image in which path it has been present and then we need to select in how many rows and columns it should be divided then it calculates the chunk width and height then the image is been spited into chunks

IV Conclusion

With the increase in the application use and shoulder surfing attack this authentication method will help in overcoming of the shoulder surfing attacks as the login process is according to the one time login password and pass- matrix image coordinates and the OTC password to be unique happens only 36000 times once as the horizontal and vertical bar uses the first six alphabets and first six numbers the combination of them is 36000 ,Hence hacking of the account becomes very difficult.

REFERENCES

[1] Graphical Password Authentication: Cloud Securing Scheme in the year 2014.

[2] Why are pictures easier to recall than words? Psychonomic Science in the year 1968

[3] Exploiting Predictability in Click-based Graphical Passwords in the year 2011

[4] Covert attentional shoulder surfing: Human adversaries are more powerful than expected in the year 2014

[5] A Scalable Shoulder-Surfing Resistant Textual-Graphical Password Authentication Scheme in the year 2010

[6] Fake Pointer: An Authentication Scheme for Improving Security against Peeping Attacks Using Video Cameras in 2008