Advances in Computational Sciences and Technology
ISSN 0973-6107 Volume 10, Number 10 (2017) pp. 3015-3031

http://www.ripublication.com

A multi-phase authentication system for data protection with the assistance of graphical password and fingerprint authentication system against shoulder surfing attacks

Shums Tabrez
M.Tech (software engineering)
Department of Information Science and Engineering
Ramaiah Institute of Technology, Bangalore, Karnataka, India

Jagadeesh Sai D
Assistant Professor
Department of Information Science and Engineering
Ramaiah Institute of Technology, Bangalore, Karnataka, India

Abstract

In today's world of quick growing technologies, security play's a prominent role in the protection of people's vital information from varied system attacks. So as a solution to these problems there should be some form of authenticated protection. Most of the system user prefer textual password in the application of security and privacy for their computer system. However there will always be a risk of human's selecting a bad or small password or either inputting them in an insecure manner which is said to be "the weakest process" in the authentication chain. Rather than selecting a powerful character set, user tend to select the password which is easier, less complicated, short, or a type of password which is easy for memorization. With new web technologies and mobile application pilling up, individuals can easily access their application anywhere with various devices such as mobiles. This transformation brings nice convince but also increase the risk of exposing password to shoulder surfing attacks. The observation by the attacker can be done directly with naked eyes or indirectly by using some recording devices to collect's individual's confidential data.

We introduced a multiple phase authentication system where the phase 1 is graphical authentication system called as Pass Matrix, In PassMatrix password which is formed graphically in which, we select only single pass-square block per pass-image for a sequence of n images. The number of images (i.e., n) is user-defined. In Pass Matrix, users choose one pass-square block per image for a sequence of n images rather than n pass-squares blocks or points in one image. Then we next tend to add another phase of protection with the help of fingerprint authentication where the users need to match the correct finger details for authentication. Here we are considering features such as minutiae intersection and minutiae Endpoint. Once both authentication is done we proceed to the final phase where user is capable of uploading the file in cloud storage which is encrypted and can only access if he enters the right key that is been send to his registered email id. If an individual enters thrice the wrong key then a file will be downloaded which will be fake and also the user who is trying to access the file with trial and error method will be blocked ,which in term defines the better solution for the protection of user data. As a result we found that the proposed system has a better resistive solution to shoulder surfing attacks while maintaining usability.

Keywords*:* Authentication,shoulder surfing attacks,graphical password,finger print authentication,data protection.

INTRODUCTION

In most of the authentication scenarios, password based on text which includes lowercase, uppercase letters and numerical are used from many years for the authentication process. Such passwords are very much strong against the brute-force attacks. But it is quite difficult to remember, memorize and recollect [1] those strong password. For these reasons user either chooses a shorter password or something which he is easily capable of remembering rather than a strong character string. To make it even worse in most of the cases, user uses the same password for multiple account login [2].An article from computer world writes that, a company to check their employee's security tried a brute force algorithm [trial-and error] method on their company network, for everyone's surprise 70-80% of their passwords were cracked within 30 seconds. Passwords based on text are often insecure due to difficult to memorize strong one. To address the limitation of textual password method, various authentication schemes based on graphical password method were developed [4].A studies such as in say that human being are very much capable of recollecting images with long term memory rather than textual representation or character string.

Many research paper's [6][7] says that password with images or graphically

represented are easy to remember and to recollect. As a conclusion, we are able to say that user can use complicated word with the graphical illustration and might be easily recollected within a protracted time. But these kind of authentication method are substantially susceptible to attacks like shoulder surfing attacks, wherever associated in nursing aggressor will directly see together with his naked eyes or either often recorded with any external recording device's to collect individual's PIN, Password or any necessary information. However there will always be a risk of individual choosing a foul, small or inputting word in an exceedingly wrong method are same to be the weakest cycle within the authentication method. Therefore for individual's, it is necessary to create or style a brand new authentication method to beat all the limitation expressed here in our document, We tend to style and gift a stronger and secured authentication system supported with graphical login system known as PassMatrix wherever the system facilitate the individual get shielded from being the victim of shoulder Surfing attacks. With the help of one time password [OTP] which terminates and can't be used again whenever the session is over. As it provides better protection as individual can use dynamic pointer to check the position rather than inputting password directly. Once the phase of authentication is over with Pass Matrix, we next tend to add another phase of protection with the help of fingerprint authentication[14] where the user need to match the correct finger details in our project for authentication we are considering features such as minutiae intersection and minutiae Endpoint .Once both authentication is done we proceed to the final phase where user is capable of uploading the file in cloud storage which is encrypted and can only access if he enters the right key that is been send to his registered email id. If an individual enters thrice the wrong key then a file will be downloaded which will be fake and also the user who is trying to access the file with trial and error method will be blocked ,which in term defines the better solution for the protection of user data.

Motivation

As the details provided and explained by the "denial" a statistician about the statistics of mobile production and marketing, in the year 2011, the mobile shipment have overtaken the pc shipment and also the number of user of mobile device has been raised to 2 billion which has overtaken computer user as of 2014. Since due to huge usage of mobile devices in public places, it has caused a great threat to individual's privacy, confidenality and security by the shoulder surfing attacks. As the individual's will access the application and web service anywhere in public for which the attackers can observe and creates problem to individual's privacy either by observing directly or by using any external recording devices.

A secure process should be build which must be capable of protecting or securing us

from various attacks and should be work fine with all the devices such as personal computer, tablets, mobile etc .The scheme such as [4],[8],[9],[10],[11] are good but have some limitation's such as usability or small password or few cannot be used on all types of device or the process can recorded by external recording devices such as Google glasses or take more time for login or has complex password of the process authentication is too complicated for user.

To overcome this problem a scheme called as Pass Points [7] has been proposed by wiedneck in 2006, in which he made use of graphical system where he selected several blocks (2 to 6) blocks from a single image during the registration phase and applied same during the login phase every time he logged in .It was good scheme compare to basic password and pin entry system but, it was quite insecure and vulnerable to shoulder surfing attack's. Hence based on above process, we included or added an idea of one time password system and a sequence of images(n=3) rather than using single image and developed a process called as pass-matrix authentication system that is better resistant to shoulder surfing attacks. And also the fingerprint authentication system.

Organization

The paper is arranged as follows, existing techniques and its connected work are explained in section Two. Different attack model are explained in section three. And the proposed system of the project is represented in the section four. Section five will be the conclusion of the result.

BACKGROUND AND ASSOCIATED WORK

In the field of authentication and specifically in password authentication, a lot of work is been carried out from past many years it will be no wrong saying from past many decades by researchers, scientist and software engineers. Among all the approaches, here we are focusing only the approaches which are related with graphical authentication chain.

Draw-a-secret [4] which is proposed by Jermyn et.al in the year 1999 which describe that individual has to redraw the already defined picture of 2d graph as defined earlier during registration. If the both the images are same. Then the authentication is true and valid. This was the one of the first approach in the development graphical authentication which after there was the improvement in science and technology.

NY Roth et.al proposed a new approach in the year 2004 which defines a robust approach of PIN entry [15] by decreasing the noise to observer. Here the binary numbers [0&1] are in black and white colour randomly and same to be selected again in the same described format .it may disturb the attacker while capturing using

recording devices. Also if the attackers observe the process of authentication then the process can be attacked.

T.Takada proposed a scheme in year 2008 called as Fake pointer [12], which we can called it as double authentication in which along with the basic pin number entry the user will get again a new answer indicator each time the person authentication process at the atm system. Here the interface will display user an image of numerical with 10 numbers with each key on top of randomly picked shape. The numbers can me moved circularly but not the shapes. Using the right left arrow keys. This approach was described to protect individual being the shoulder surfing attackers with the help of video capturing.

David Kim et.al [11] proposed a scheme in the year 2010 called as "color rings" which is visual authentication process where the system user will be given I keys which will be any of one color ring red, blue, green and pink. During login phase 72 icons will be displayed for each color grid out of only one ring is ours selected during registration phase which the user must drag all the four colors rings and placed them correctly. If correctly done authentication is valid. But it is very much vulnerable for brute force attack.

PassPoints [5] has been proposed by wiedneck in 2006, in which he made use of graphical system where he selected several blocks (2 to 6) blocks from a single image during the registration phase and applied same during the login phase every time he logged in .It was good scheme compare to basic password and pin entry system but, it was quite insecure and vulnerable to shoulder surfing attack's. Hence based on above process, we included or added an idea of one time password system and a sequence of images(n=3) rather than using single image and developed a process called as pass-matrix authentication system that is better resistant to shoulder surfing attacks.

PROBLEM STATEMENTS AND ATTACK MODELS

As discussed in the introduction, there is a huge generation or production of mobile phones, web technologies. As an individual or mobile user's will be accessing their personal details such as internet banking social media application etc anywhere, anytime. When using of these things through application can expose their password to the unknown people unknowingly, people with bad mind set could see and the password and may also collect full Login process by using the recording devices. Once they collected, they will surely cause threat, problem to individual's confidentiality. Shoulder surfing attack has been in recent trend for hacker in past few decades. Here we are trying to describe some of the problem we would like to understand.

- How to have or perform secure authentication in public?

- How to decrease noise and increase the password security in traditional pin method?
- How to memorize and remember the very much complexes password?
- How to reduce the complexity of this type of scheme?
- How to solve the problem of usability that can be used to some devices only.

Attack Model's

As described earlier and survey done in research done previously [10][11]][12] we basically classified two type of attack model they are

Shoulder Surfing Attacks

The individual while using or adding password may disclose their password. People with bad intention will access and cause threat to you. Then according to study we can classify shoulder surfing in two types as follows

Type A: People who see the password and process through naked eyes.

Type B: Capturing password or authenticated process one or more than once using recording devices.

So we need to work on scheme which will protect us from any such type of attacks.

Smudge attacks:

This is another classification where the attackers will collects the password or data by seeing individual screen by observing the smudge left on the screen[the marks of fingers on mobile screen.

Assumption

Here we try to make out some assumption which will be helpful in our proposed scheme.

- The communication is protected in client and server side by secured system login [ssl] by which user will be unable to collect our data or information.
- The system must be trustworthy.
- As full screen of mobile or system is difficult to protect but a small part can be protected.
- The scheme must protect the user from attacks in public.
- The data or file which are stored in the cloud are encrypted and can only access if correct decrypted key is provided.

Existing System

In the Existing System Users' actions such as typing from their keyboard or clicking on the pass-images or pass-points in public may reveal their passwords to people with bad intention. Existing approaches are defenseless to shoulder surfing attacks.

Disadvantages of the Existing System

Existing system is defenseless to shoulder surfing attacks.

Type-I: Naked eyes.

Type-II: Video captures the entire authentication process only once.

Type-III: Video captures the entire authentication process more than once.

Proposed System:

To overcome with

- The security limitation of the basic PIN entry technique.
- The easy way of obtaining password by shoulder surfing attacker's in public.
- The with the process of getting the data by hackers with the help of trial and error method.
- The complexity and adaptability issues to different devices.

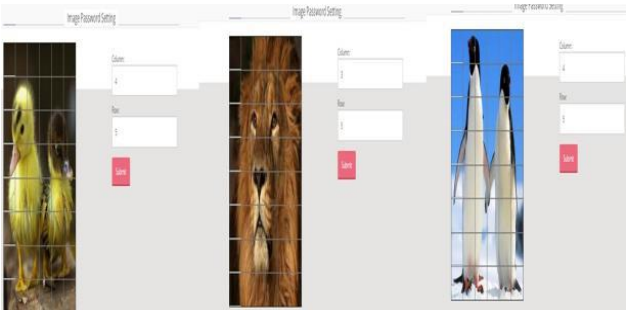

Fig 1: Pass-matrix images which describing the location

Selected during registration phase

We introduced a multiple phase authentication system where the phase 1 is graphical authentication system called as PassMatrix. In PassMatrix password which is formed graphically in which, we select only single pass-square block per pass-image for a sequence of n images. The number of images (i.e., n) is user-defined. In PassMatrix, users choose one pass-square block per image for a sequence of n images rather than

n pass-squares blocks or points in one image as that in the PassPoints scheme. Then we next tend to add another phase of protection with the help of fingerprint authentication where the user need to match the correct finger details in our project for authentication we are considering features such as minutiae intersection and minutiae Endpoint .Once both authentication is done we proceed to the final phase where user is capable of uploading the file in cloud storage which is encrypted and can only access if he enters the right key that is been send to his registered email id. If an individual enters thrice the wrong key then a file will be downloaded which will be fake and also the user who is trying to access the file with trial and error method will be blocked ,which in term defines the better solution for the protection of user data.

Advantages of the Proposed System

Proposed system is invulnerable to the all types Shoulder Surfing Attacks such as,

- Type-I: Naked eyes.
- Type-II: Video captures the entire authentication process only once.
- Type-III: Video captures the entire authentication process more than once.
- It overcomes the security weakness of the traditional PIN method.
- It overcomes the easiness of obtaining passwords by observers in public.
- Full secured way to overcome trial and error method for obtaining the useful data of the individual by the hackers.

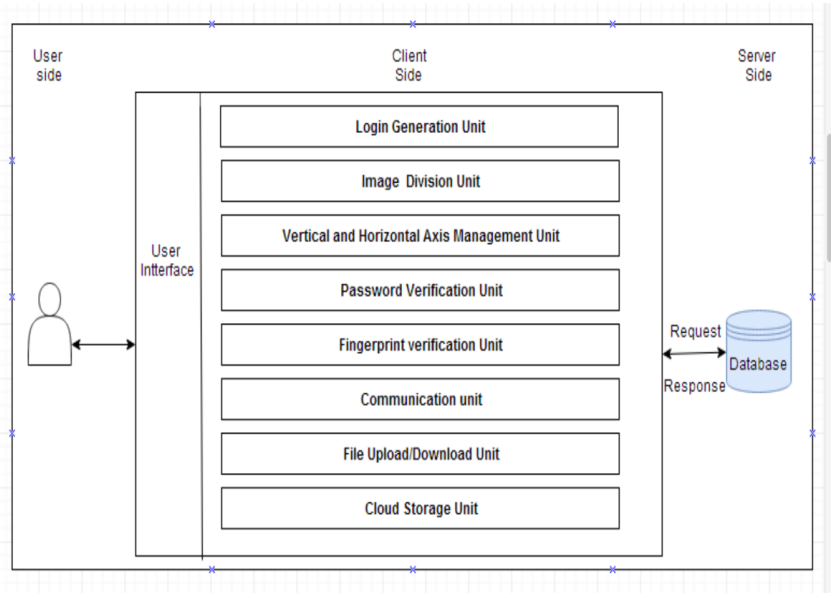

Fig 2: block diagram of proposed system

PassMatrix is composed of the following components

- **Login generation unit**: Here the with help of Gmail or sms a random generated otp [both letter's and number's] are sent to registered Gmail account or mobile number using which the individual will authenticated to the application. The otp will be useless once the procedure is over.
- **Image –division unit**: Here in this unit every picture [image] is divided into small squares or blocks from which user can select one-pass-block as described in figure .The image used is divided into 6*8 blocks. As large number blocks describe strong password space.
- **Vertical and horizontal management unit**: The system is meant where along with the random elected images a vertical and horizontal bars are placed .in that vertical bar consist of numbers and horizontal bars consist of letters. This unit provide fill and drag function for user to control the bar's based on otp generated. We must drag and shift bars as per otp and requirement.
- **Password verification unit**: Since the block details are stored in the database and the otp generated .using both we need to enter it. The password will be verified if each-pass square block is correctly matched with the obtained otp or login indicator.
- **Fingerprint verification unit**: The finger details which are added during registration phase either physically or dynamically with the help of biometric device. Here we are considering minute intersection and end to end points of the finger print details.
- **Communication unit**: This unit is helpful for data transmission between secured server and the client system .the communication is secured by secured socket layer.
- **File Upload/download Unit:** This is the phase where the user who is working on the application called as honey pot process application follows the algorithm for uploading and downloading the files in the cloud storage.
- **Cloud storage Unit:** Here we are using DRIVEHQ service provider which is one of the type of cloud storage service provider for uploading the file with the encrypted key and when the user wanted to download the key need add the decryption key for downloading the files. We can store up to the 15 GB of data for free of cost.
- **Database**: The information (database) unit incorporates numerous details such as username; email id, password, and block used throughout registration in pass images with relevancy to username also the hash code associated to user.

Modules Description:

- **User Registration:** In this module user has to register by giving his information such as userid, user name, password, valid e-mail id etc, and after giving this information, randomly three images will be assigned to the user, in those images he has to select the coordinate squares of the images as the graphical password. The details of coordinates of all images will be stored in the database with respect to the specific user.
- **Hash code generation:** After successful setting of the coordinates of the images ,those details will be stored in the database, concatenating all the three images coordinates and generate hash code for that and store in the database with respect to the user.

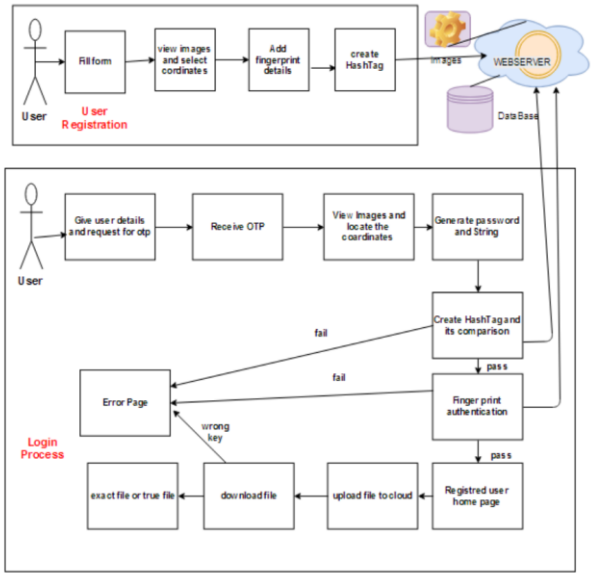

Fig 3: System architecture for proposed system

- **Finger Print Authentication:** The finger details which are added during registration phase either physically or dynamically with the help of biometric device. Here we are considering minute intersection and end to end points of the finger print details.
- **User Login Process:** Registered user will be login to the application by using his userid and password, if the userid and password is valid One Time Password (OTP) will be sent to the user's e-mail, whereas OTP contains the random pair of vertical and horizontal slider coordinate points of all the three images. After successful login, three assigned images will be displayed to the

user with horizontal and vertical sliders; user has to set the horizontal and vertical sliders for all the three images, where the OTP coordinate value should be equal to the coordinates chosen by the user at the time of password setting. The hash code will be generated for all OTP coordinates by concatenating .if the hash code is matched with the existing hash code user can successful enter in to the home page , else process ends and login page will display.

- **Admin:** Admin has to login to his account by the authenticated user name and password. Admin can able to view all the users' details, which are successfully registered.

ALGORITHMS

- **Randomized Image Selection Algorithm**

This algorithm is invoked when user is registered with our system for each user our system has to pick 3 distinct random images from Password image database for this purpose this algorithm is used.

- Step 1: Let the number of images be represented as "N" in Image DB
- Step 2: Step 2: Let M represent the number of Password Images Required
- Step 3: Initialize Integer Array RAN[M]
- Step 4: C =1
- Step 5: Generate a Random number between 1 to N and let it be R
- Step 6: if R is in RAN array then Go to step 5
- Step 7: RAN[C] = R
- Step 8: C = C + 1
- Step 9: if C <= M then go to step 5
- Step 10: Stop.

- **Click Based Pixel to Co-ordinate conversion**

When a user clicks on the image x and y co-ordinate pixel he retrieved. These pixel locations has to convert into column offset, row offset coordinates which makes user friendly selection process.

- Step 1: Let C be the Column offset [ex: C = 200]
- Step 2: Let R be the Row offset [ex: R = 200]

- Step 3: Let P(X,Y) is the user clicked Pixel on Image
- Step 4: Let RV = CEILING(Extract Row value from P(X,Y) / R)
- Step 5: Let CV = CEILING (Extract Column value from P(X,Y) / C)
- Step 6: (RV, CV) is the Co-ordinate value for password image
- Step 7: Stop.

➢ **Password string creation and hash code generation**

As per the system user has to select 3 locations on 3 images (1 location per image). Using previous algorithm the pixel location converted into co-ordinate. Concatenating all the co-ordinates we get a password string. By using hashing technique on generate password string system produce secret hash code which has to stored in database for password verification.

- Step 1: Let M be the number of password images
- Step 2: C = 1, *password* = ‘’;
- Step 3: Let P(X,Y) is the user clicked Pixel on Image
- Step 4: Pass P(X,Y) to Pixel to Co-ordinate function and get (RV,CV)
- Step 5: *password* = *password* + RV + “,” + CV
- Step 6: C = C + 1
- Step 7: if C<= M then goto Step 3
- Step 8: Use Hashing function on *password* and get Secret Code
- Step 9: Store Secret Code in DB
- Step 10: Stop.

➢ **One Time Code (OTC) Generation & Email Sending**

There is a different between OTC and OTP. OTP is one time password which act as a password itself, OTC one time code it is not a password, it a clue for the user to select password image co-ordinate, this algorithm is used to generate OTC.

- Step 1: Let M be the number of password images
- Step 2: C = 1, *OTC* = ‘’;
- Step 3: Let K be number of Columns in the image
- Step 4: Let L be number of Rows in the image

- Step 5: Random number Is generated between 1 to K and let it be R1
- Step 6: Generate Random number is generatedbetween 1 to L and let it be R2
- Step 7: Convert R1 into Alphabet (AR1), ex; 1 -> A, 2->B
- Step 8: OTC =OTC + AR1+R2
- Step 9: C = C + 1
- Step 10: If C<=M then goto Step 5
- Step 11:Pick User EmailId from D
- Step 12: Email OTC to user Email ID
- Step 13**.**

➢ **OTC & Scroll Bar Mapping and Co-ordinate Generation**

Once the user receives the OTC he has to move the vertical scrollbar and horizontal scroll bar on password image to point the co-ordinate. We need the system based on scroll bar movement co-ordinates has to be generated.

- Step 1: Let K be number of Columns in the image
- Step 2: Let L be number of Rows in the image
- Step 3: Let RA1 is Column value in OTC of image
- Step 4: Let R2 is Row value in OTC of image
- Step 5: Assume user positioned the both the scroll bar and press submit button
- Step 6: Let XR1 is the current column position of RA1
- Step 7: CV = XR1
- Step 8: Let XR2 is the current Row position of R2
- Step 9: RV = XR2
- Step 10: (RV,CV) is the OTC mapped co-ordinate
- Step 11: Stop.

➢ **Secret Code Comparison**

Once co-ordinates are generated the hash code has to be extracted on the co-ordinate string. The extracted hash code verified with secret hash code which is stored in data base. If both are same these algorithms allow the user to login home page.

- Step 1: Let M be the number of password images
- Step 2: C = 1, *password* = ‘’;

- Step 3: Let (RV,CV) is the co-ordinate generated for the Image(C) using scroll bar mapping.
- Step 4 : Password=password +RV+"."+C
- Step 5: C = C + 1
- Step 6: if C<= M then goto Step 3
- Step 7: Use Hashing function on *password* and get SecretCode(1)
- Step 8: From the DB fetch the user's SecretCode (2)
- Step 9: if SecretCode(1) != SecretCode(2) then goto Step 11
- Step 10: Navigate to Home page
- Step 11: Stop**.**

➢ **Message Digest 5 Algorithm**

The MD5 algorithmic rule could also be a large used hash perform producing a 128-bit hash value. Although MD5 was at the beginning designed to be used as a science hash perform, it has been found to suffer from intensive vulnerabilities. it'll still be used as a substantiation to verify data integrity, but alone against unintentional corruption.

- Step 1: Get the Message
- Step 2: Convert message in to the bits.
- Step 3: Append whole Bits (Make the message bit length got to be the actual multiple of 512 bits furthermore as sixteen word Blocks).
- Step 4: Divide total bits in to 128 bits blocks each
- Step 5: Initialize MD Buffer. A four word buffer (A,B,C,D) is used to reckon the message digest , total 128 bits.
- Step 6: Do AND,XOR,OR,NOT operations on A,B,C,D by giving three inputs and obtain one output.
- Step 7: Do the Step 6 until get the 128 bits hash(16 bytes).
- Step 8: Stop.

➢ **Fingerprint Feature Extraction**

- Step 1 : Get width and height of image.
- Step 2: Get the packed pixel content of whole image as an array
- Step 3: Transform the array into a gray scale array

- Step 4: Extract Feature Minutiae Intersection
- Step5: Extract feature Minutiae Endpoints.
- STEP 6: Store the Feature value in variable
- STEP 7: Return Feature Value Variable.
- Step 8:Stop

CONCULSION AND FUTURE WORK

As from the beginning of our discussion, we have been seeing there is huge increase the application and web services, individual are capable of using this anywhere with varieties of device. So to maintain confidentiality, authentication is must to the personal assessment data .As a threat to application someone may check out our data from the shoulder surfing attack. Though the basic process of authentication in most of the device is textual password but they are very vulnerable to the system because of basic selection of password.

We tend to style and gift a stronger and secured authentication system supported with graphical login system known as pass-matrix wherever the system facilitate the individual get shielded from being the victim of shoulder Surfing attacks. With the help of one time password which terminates and can't be used again whenever the session is over. As it provides better protection as individual can use dynamic pointer to check the position rather than inputting password directly. Once the phase of authentication is over with Pass Matrix, we next tend to add another phase of protection with the help of fingerprint authentication where the user need to match the correct finger details in our project for authentication we are considering features such as minutiae intersection and minutiae Endpoint .Once both authentication is done we proceed to the final phase where user is capable of uploading the file in cloud storage which is encrypted and can only access if he enters the right key that is been send to his registered email id. If an individual enters thrice the wrong key then a file will be downloaded which will be fake and also the user who is trying to access the file with trial and error method will be blocked ,which in term defines the better solution for the protection of user data. We also experimented the authentication prototype on different system and tried a real –time experiment to check its usability and. As a result we found that the proposed system a better resistance solution to shoulder surfing attacking while maintaining its usability. Based on my survey and experimental result we can conclude, Pass-Matrix is a very much easy-to-ease and novel system which will protect us from shoulder surfing attacks.

REFERENCES

[1]. S. Sood, A. Sarje, and K. Singh, "Cryptanalysis of password authentication schemes: Current status and key issues," in Methods and Models in Computer Science, 2009. ICM2CS 2009.Proceeding of International Conference on, Dec 2009, pp. 1–7.

[2]. S. Gurav, L. Gawade, P. Rane, and N. Khochare, "Graphicalpassword authentication: Cloud securing scheme," in ElectronicSystems, Signal Processing and Computing Technologies (ICESC), 2014International Conference on, Jan 2014, pp. 479–483.

[3] R. Dhamija and A. Perrig, "Deja vu: A user study using imagesfor authentication," in Proceedings of the 9th conference on USENIXSecurity Symposium-Volume 9. USENIX Association, 2000, pp. 4–4.

[4] I. Jermyn, A. Mayer, F. Monrose, M. Reiter, and A. Rubin, "Thedesign and analysis of graphical passwords," in Proceedings of the8th conference on USENIX Security Symposium-Volume 8. USENIXAssociation, 1999, pp. 1–1.

[5] S. Wiedenbeck, J. Waters, J. Birget, A. Brodskiy, and N. Memon,"Passpoints: Design and longitudinal evaluation of a graphicalpassword system," International Journal of Human-Computer Studies,vol. 63, no. 1-2, pp. 102–127, 2005.

[6] S. Brostoff and M. Sasse, "Are passfaces more usable than passwords?a field trial investigation," PEOPLE AND COMPUTERS,pp. 405–424, 2000.

[7] A. De Angeli, M. Coutts, L. Coventry, G. Johnson, D. Cameron,and M. Fischer, "Vip: a visual approach to user authentication," inProceedings of the Working Conference on Advanced Visual Interfaces.ACM, 2002, pp. 316–323.

[8] D. Hong, S. Man, B. Hawes, and M. Mathews, "A passwordscheme strongly resistant to spyware," in Proceedings of Internationalconference on security and management, 2004.

[9] D. Tan, P. Keyani, and M. Czerwinski, "Spy-resistant keyboard:Towards more secure password entry on publicly observabletouch screens," in Proceedings of OZCHI-Computer-Human InteractionSpecial Interest Group (CHISIG) of Australia. Canberra, Australia:ACMPress.Citeseer,2005.

[10] M. Kumar, T. Garfinkel, D. Boneh, and T. Winograd, "Reducingshoulder-surfing by using gaze-based password entry," in Proceedingsof the 3rd symposium on Usable privacy and security. ACM,2007, pp. 13–19.

[11] D. Kim, P. Dunphy, P. Briggs, J. Hook, J. Nicholson, J. Nicholson,and P.

Olivier, “Multi-touch authentication on tabletops,” inProceedings of the 28th international conference on Human factors incomputing systems. ACM, 2010, pp. 1093–1102.

[12] T. Takada, “fakepointer: An authentication scheme for improvingsecurity against peeping attacks using video cameras,” in MobileUbiquitous Computing, Systems, Services and Technologies, 2008. UBICOMM’08.The Second International Conference on. IEEE, 2008, pp.395–400.

[13] “Android 2.2 platform highlights,” http://developer.android.com/sdk/android-2.2-highlights.html

[14] K. Gilhooly, “Biometrics: Getting back to business,” Computerworld,May, vol. 9, 2005.

[15] V. Roth, K. Richter, and R. Freidinger, “A pin-entry method resilient against shoulder surfing,” in Proceedings of the 11th ACM conference on Computer and communications security, ser. CCS ’04. New York, NY, USA: ACM, 2004, pp. 236–245