A Shoulder Surfing Resistant Graphical Authentication System

Deore Chetan[1], Beloshe Pankaj [2], Wasim Akram [3], Adekar Vikas [4], Prof.V.N.Dhage[5]
Department of Computer Engineering
[1,2,3,4] Student, P K Technical Campus, chakan ,Tal. Khed , Dist. Pune, Maharashtra, India.
[5] P K Technical Campus, chakan ,Tal. Khed , Dist. Pune, Maharashtra, India.

Abstract- *When users input their passwords in a public place, they will be in peril of attackers stealing their secret. associate attacker can capture a secret by direct observation or by recording the individuals authentication session.|this can be often noted as shoulder-surfing and should be a known risk, of special concern once authenticating in public places. until recently, the only defence against shoulder-surfing was the alertness on the a section of the user.*

Shoulder surfing resistant secret authentication mechanism assure shoulder-surfing resistant authentication to user. It permits user to authenticate by coming into pass-word in graphical approach at insecure places as a results of user never need to click directly on secret icons. Usability testing of this mechanism showed that novice users were ready to enter their graphical secret accurately and to recollect it over time. However, the protection against shoulder-surfing comes at the value of longer time to hold out the authentication

Keywords- Security, Experimentation, Human Factors

I. INTRODUCTION

The shoulder aquatics attack in an attack that will be performed by the antagonist to get the user's secret by observing over the user's shoulder as he enters his secret. As typical secret schemes area unit liable toshoulder aquatics, Sobrado and Birget planned three shoulder surfing resistant graphical secret schemes. However, most of this graphical watchword schemes ar liable to shoulder-surfing a known risk where anattacker can capture a watchword by direct observation or by recording the authentication session.Due to the visual interface, shoulder-surfing becomes Associate in Nursing exacerbated downside in graphical passwords. A graphical secret is less difficult than a text-based word for many people to recollect. Suppose Associate in Nursing 8-character word is very important to understand entry into a specific network. durablepasswords will be created that ar proof against idea, wordbook attack. Key-loggers, shoulder-surfing and social engineering. Graphical passwords ar used in authentication for mobile phones, ATM machines, E-transactions.

Although the graphical password method is beneficial, but shoulder-surfing attack is the main concerns in this authentication mechanism. Shoulder-surfing attack is referred to capturing the password by direct watching or recording the user's authentication session while selecting or producing the images as the password. In this project, a recognition-based graphical password technique based on the false image which is resistance to shoulder-surfing attack is suggested. In this way, the false image within the authentication step can confuse a hacker who tries to capture the password using shoulder-surfing attack.

II. LITERATURE SURVEY

Sr. No	Paper Name	Year	Description	Advantages	Disadvantages
1	Multi-touch passwords for mobile device access	2012	Draw-a-Secret password schemes, like the Google Android Pattern Lock, entail stroking out a shape on a	To increase password entropy	to utilize the novel functionalities provided

			touch screen.		
2	The doodb graphical password database: Data analysis and benchmark results	2013	We present DooDB, a doodle database containing data from 100 users captured with a touch screen-enabled mobile device under realistic conditions following a systematic protocol.	high intra-user vari-ability in the production of doodles	the analysis of the impact of doodle complexity in the performance against skilled forgeries
3	Graphical Password-Based User Authentication With Free-Form Doodles	2015	User authentication using simple gestures is now common in portable devices. In this work, authentication with free-form sketches is studied.	High variability between capture sessions increases the error rates.	he GMM system has better performance against skilled forgerie
4	Covert attention shoulder surfing: Human adversaries are more powerful than expected	2013	When a user interacts with a computing system to enter a secret password, shoulder surfing attacks are of great concerne	human performance modeling tool for security analysis and improvement.	secure authentication method based on the abundant evidence
5	The doodb graphical password database: Data analysis and	2013	We present DooDB, a doodle database containing data from 100 users	performance against forgeries is analyzed using state-of-the-art algorithms	to an improvement in their verification performance which would become closer to pseudo-signatures

	benchmark results		captured with a touch screen-enabled mobile device under realistic conditions following a systematic protocol.		

III. EXISTING SYSTEM

Using traditional textual passwords or PIN method, users need to type their passwords to authenticate themselves and thus these passwords can be revealed easily if someone peek over shoulder or uses video recording devices such as cell phones shoulder surfing attacks have posed a great threat to users' privacy and confidentiality as mobile devices are becoming indispensable in modern life. In the early days, the graphical capability of handheld devices was weak; the color and pixel it could show was limited. With the increasing amount of mobile devices and web services, users can access their personal accounts to send confidential business emails, upload photos to albums in the cloud or remit money from their e-bank account any time and anywhere. While logging into these services in public, they may expose their passwords to unknown parties unconsciously.

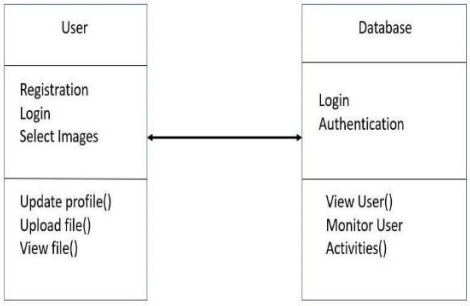

Fig 1: Class diagram of the process

IV. PROPOSED SYSTEM

To overcome this disadvantage, we projected a shoulder aquatics resistant authentication system supported graphical passwords, named Pass Matrix. using a one-time login indicator per image, users can entails the location of their pass-square whereas not directly clicking or touching it ,which is an action vulnerable to shoulder aquatics attacks .Because of the planning of the horizontal and vertical bars that cowl the complete pass-image, it offers no clue for attackers to thin the parole area although they need over one login records of that account .In Pass Matrix, a word consists of only one pass-square per pass-image for a sequence of images. the number of images (i.e., n) is user-defined. In Pass Matrix, users take one sq. per image for a sequence of n images rather than n squares in one image as that within the Pass Points theme Pass Matrix's authentication consists of a registration section and an authentication section as described below :At this stage, the user creates associate account that contains a user name and a word. The password consists of alone one pass-square per image for a sequence of n images. the quantity of images (i.e., n) is decided by the user once considering the trade-off between security and price of the system .At this stage, the user uses his/her username, password and login indicators to log into Pass Matrix.

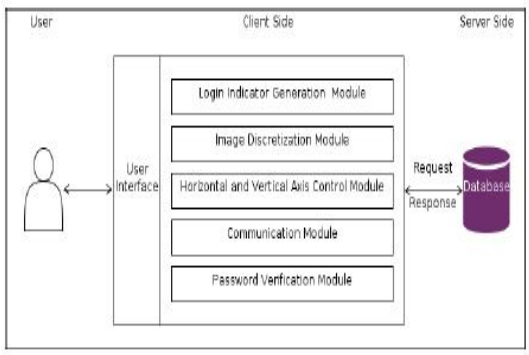

Fig2. Proposed System Architecture

V. REGISTRATION

Since registration is the first step, each user needs to input his full name, email address and username. In addition, he requires to select minimum 3 and maximum 9 image categories from giving options. After the information is submitted to the database, selecting graphical password process will start. In this case, a user can select one image

from each category per page, depends on the length of his Password (minimum 3 and maximum 9 image) but this selection must be done by typing the alphanumeric character, which is attached to each image. In addition, the alphanumeric characters which belong to each image and the position of images in each category are selected to be randomized.

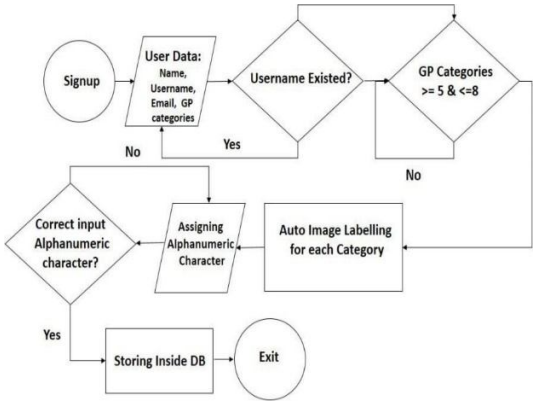

Fig 3. Registration Flowchart

VI. CONCLUSION

Proposed a shoulder surfing resistant authentication system supported graphical passwords, named Pass Matrix. using a one-time login indicator per image, users can point out the location of their pass-square while not directly clicking or touching it, that is an action at risk of shoulder surfing attacks. because of the planning of the horizontal and vertical bars that cowl the complete pass-image, it offers no clue for attackers to slenderize the password space although they need over one login records of that account. moreover, we have a tendency to implemented a Pass Matrix image on android and distributed user experiments to judge the memorability and worth. The experimental result showed that users can log into the system with a mean of 1:64 tries (Median=1), and also the Total Accuracy of all login trials is 93:33% even time period once registration. the full time consumed to log into Pass Matrix with an average of 3:2 pass-images is between 31:31 and 37:11 seconds and is taken into account acceptable by 83:33% of participants in our user study. supported the experimental results and survey information, Pass Matrix may be a novel and easy-to-use graphical parole authentication system, which can effectively alleviate shoulder-surfing attacks. to boot, Pass Matrix is applied to any authentication state of affairs and device with simple input and output capabilities. The survey information in the user study to boot showed that Pass Matrix is sensible within the real world

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, "Graphical password authentication: Cloud securing scheme," in Electronic Systems, Signal Processing and Computing Technologies (ICESC), 2014 International Conference on, Jan 2014, pp. 479–483.

[3] K. Gilhooly, "Biometrics: Getting back to business," Computerworld, May, vol. 9, 2005. R. Dhamija and A. Perrig, "Deja vu: A user study using images for authentication," in Proceedings of the 9th conference on USENIX Security Symposium-Volume 9. USENIX Association, 2000, pp. 4–4.

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

[5] A. Paivio, T. Rogers, and P. Smythe, "Why are pictures easier to recall than words?" Psychonomic Science, 1968.

[6] D. Nelson, U. Reed, and J. Walling, "Picture superiority effect," Journal of Experimental Psychology: Human Learning and Memory, vol. 3, pp. 485–497, 1977.

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