International Journal of Trend in Scientific Research and Development (IJTSRD)
International Open Access Journal
ISSN No: 2456 - 6470 | www.ijtsrd.com | Volume - 2 | Issue – 3

A Game Based Graphical Password Authentication System to Prevent Shoulder-Surfing

C. Asvin Parthasarathy, R. Purushothaman
Department of Computer Science and Engineering,
G.K.M. College of Engineering and Technology, Chennai, Tamil Nadu, India

ABSTRACT

In order to prevent intruders from looking into sensitive data in smartphones users will have their own security measures, but those security measures are traditionally available measures one among them is finger based pattern doodling which became quite popular among users, also studies show that it is easy to remember and use than alphanumeric text based passwords. But these patterns are static in nature which can be stolen using shoulder-surfing attack. Shoulder-surfing refers to attack which is made based on observation of attacker either directly, or indirectly using applications to record such as camera or key logger. In this paper we have introduced a concept of dynamic patterns which when user records his input for the first time the positions will remain same but the next time the positions of each pattern is changed dynamically, also there is one more concept called image falsification is used. Image Falsification means deceiving the attacker to the false image pattern instead of exposing the true image pattern and the true pattern remains known only to the user.

Keywords: *Graphical Password, Shoulder-Surfing, Dynamic Pattern, Image Falsification*

I. INTRODUCTION

Passwords are widely being used by the users to protect sensitive data from being misused or stolen. Traditionally passwords are believed to provide security to user's sensitive data and there is lot of methods available in the modern technology to provide security. In these days even biometrics are used as passwords to provide security to user's data. But the need and use of traditional techniques are so inevitable such that the technologies we use in today's world are only here to further enhance the security of the existing methodology. In that case it is necessary to provide proper security to the existing system itself. The alphanumeric passwords are used for a long time from now and known for providing security to some extent. But the use of alphanumeric passwords has a problem, even though existing system has different password policies to measure the strength of the password and also provides stringency in keeping passwords user's find it difficult to remember them. So it is a tradeoff between Stringency and simplicity, further if the user keeps predictable patterns such as their name or date of birth or most commonly used words it is a lot easier for the attacker's to crack them. The idea of graphical passwords was originally proposed by blonder in1996 Supporting the fact that humans can remember images more than the text's. The authentication of graphical password mechanism is simple, users will have to choose their images from the number of duplicate images available. The graphical passwords became quite famous then because of the Déjà Vu effect that works well with human minds. Since people adopted with graphical passwords number of methods are proposed for providing authentication to user's. In this paper we have introduced a concept of graphical authentication scheme which works like a game to deceive attackers mind. The advantage of this method is user won't be clicking on the pass image directly, also we have added a feature called time where within that limit user has to authenticate otherwise the permission will not be granted. Also we have introduced a concept called pattern shuffling where for each successive

authentication the image pattern shuffles dynamically. This system can prevent shoulder-surfing and helps user to authenticate in public places without the fear of password cracking.,

II. RELATED WORKS

Andrew Lim Chee Yeung, Bryan Lee Weng Wai and Cheng Hao Fung together designed a graphical password scheme which is resistant to shoulder-surfing. They designed a falsification technique which allows hackers to capture the false image where the original image is hidden. S. Weidenbeck, J. Waters, L. Sobrado, J.C. designed a convex hull pattern scheme where the pass icons are selected by drawing a convex hull over the edges of the pattern for each rounds authentication number of pass icons appear in the screen like a game where the authentication is done based on user's pattern drawing. Swale ha Saeed, M. Sarosh Umar designed a method called pass neighbor technique which allows users to select neighbor image as password instead of original image to create the delusional effect for attackers. Hung-Min Sun, Shiuan Tung Chen, Jyh-Haw Yeh and Chia-Yun Cheng designed a graphical password where for each authentication the pass-matrix of the image varies so that each image is valid for only one time.

III. PROPOSED SYSTEM

The proposed system is designed to avoid shoulder-surfing problem. It has two phases, registration and authentication. In between these two phases there is password selection process where user has to select his pass icon.

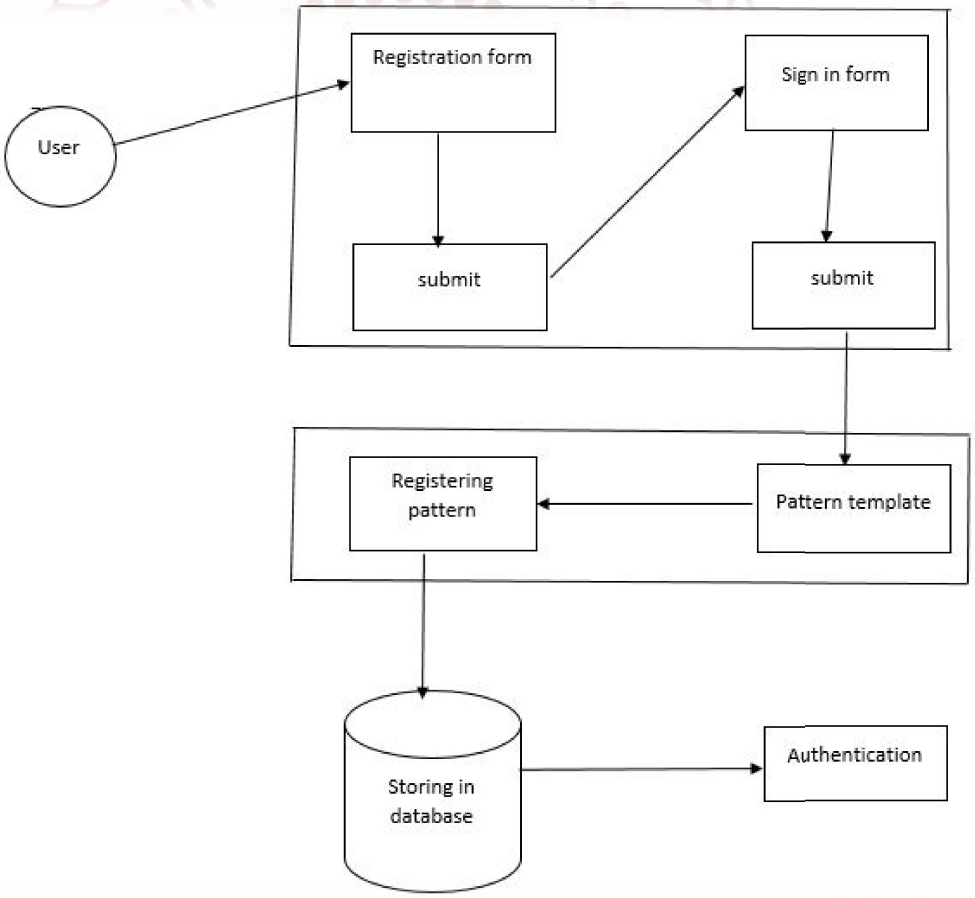

Fig. 1 Architecture diagram

The above diagram explains two traditional phases of a graphical password system but it also includes one more phase where users has to choose their image pattern to keep it as their password security. The first module explains how users have to register their details and second module explains about choosing their pattern how the process works and third module is about authenticating the user. This whole process has to be verified first with number of devices in order to check if there are any variations in functioning of the process. The number of successful attempts of the user is noted.

A. Registration phase

In this module users will have to provide input to the system. The registration module works for each device only once so that only true owner of the phone will be able to access this system. Suppose if the registration phase accepts more than one users detail in one device then any person who is not intended can also register their details in that device and can set up their own authentication system and can use their device to their free will. Also current pattern locking systems does not support this feature, which in case will be so annoying for the users to register their details each time and have to authenticate themselves. Once the registration of details is over then user can authenticate themselves as an existing user so that they can enter their email and password again for verification. If the details are entered and the system says already exists then the registration process is done successfully, then this phase will work as a onetime phase.

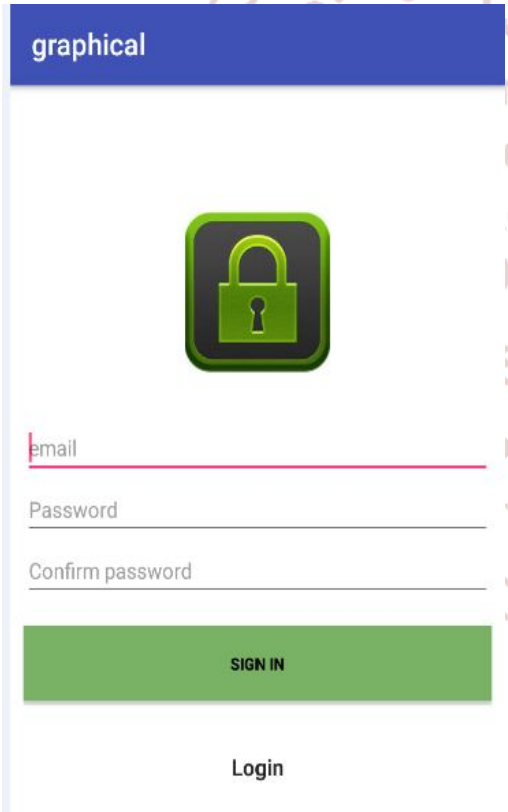

Fig. 2 Registering user details

The fig .2 explains user registration process, first user will be prompt to give his e-mail id and password, password can be of any character not necessarily your e-mail's password also the password you are registering have to be given again for confirmation sake. When u give sign in your details will be stored in the cloud, so that the next time when u give login instead of sign in u have to enter your e-mail id and password once again if it shows already registered then your id and password is synced in cloud the registration process is done successfully.

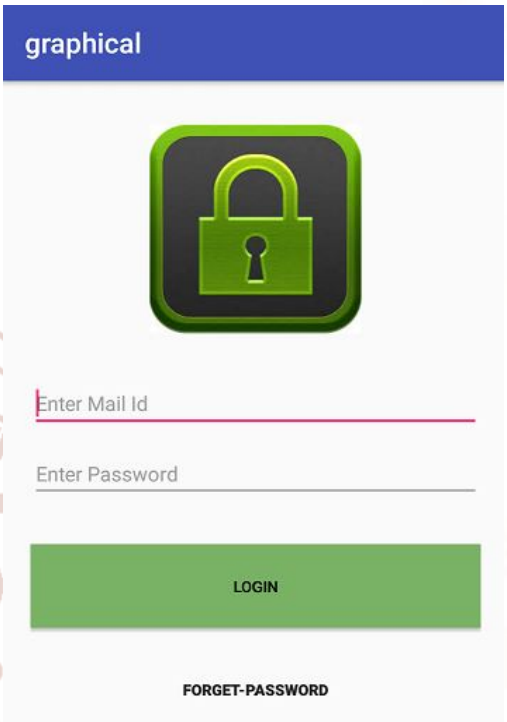

Fig. 3 login page

The fig. 3 shows login page where user has to provide their registered e-mail id and password in order to go to pattern selection phase.

B. Pattern selection phase

In this phase user has to select a pattern image from the number of patterns available predefined. Those are the pattern which will be repeating in the pattern template from which user has to select the right pattern.

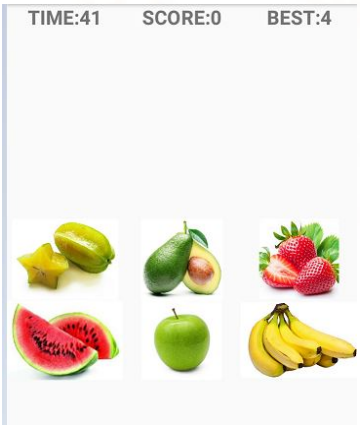

Fig. 4 selecting pattern

The fig. 4 shows the available patterns from which users have to select one for their authentication phase. It is to be noted that user has to confirm their pattern selection because in authentication phase each image will have their replicas so that user need to be careful on their pattern selection and also to note its position.

C. Authentication phase

In this phase users have to input their password image for each round so that the system will authenticate user based on their image selection. If user inputted wrong password then the page itself will show password failed, if the user has given correct password then the system will shuffle the positions of the image for each successive time and finally within the given time if the user was able to complete his authentication in all rounds then then the following application connected with this system will open by itself.

Fig 5. Authenticating the user

The fig. 5 shows user authentication page. Here time represents within the given time user has to authenticate himself, best represents number of attempts and score represents the successive authentication attempts.

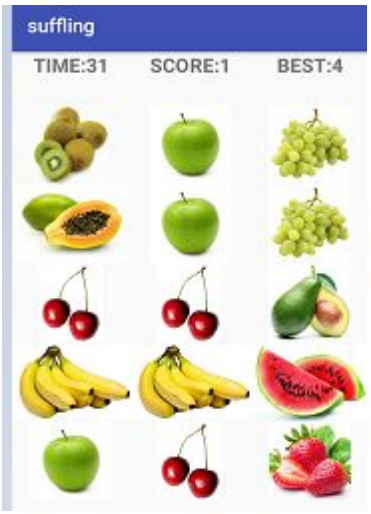

Fig 6: Shuffling

The fig 6 explains the pattern shuffling. You can see the difference between the pattern positions in the previous fig 5 and this fig 6. The shuffling of images takes place because of the implementation of shuffling algorithm on these images.

D. Conclusions

This game based graphical authentication system helps us to authenticate even in public without the fear of attackers attacking our device and stealing personal data. It works as a simple game even if the attacker tries to observe our pattern he won't be able to see the true password because of this method. In future we can add one more feature to our existing system which acts as a theft protection mechanism. If a thief steals your phone and try to access the personal data, this pattern within the given time will authenticate users with the correct pattern. However, if the attacker tries to access the system and failed to do so the proposed system will send an alert message to the phone number which will be registered by the user stating that your phone is in the danger of being stolen.

REFERENCES

1. Shukun Yang, Shouling Ji, Raheem Beyah, 2017. "DPPG: A Dynamic Password Policy Generation System". *IEEE Transactions on Information Forensics and Security (*Volume:13, Issue:3).

2. Hung-Min Sun, Shiuang-Tung Chen, Jyh-Haw Yeh and Chia-Yun Cheng, 2016. "A Shoulder Surfing Resistant Graphical Authentication System". *IEEE Transactions on Dependable and secure Computing (*Volume PP, Issue:99).

3. Swaleha Saeed, M Sarosh Umar, 2016. "Pass Neighbor: A shoulder surfing resistant scheme". *Next Generation Computing Technologies (NGCT),2016 2nd International Conference.*

4. Andrea Bianchi, Ian Oakley, Hyoungshick Kim, 2015. "PassByop: Bring Your Own Picture for Securing Graphical Passwords". *IEEE Transactions on Human-Machine System (Volume:46, Issue:3).*

5. Andrew Lim Chee Yeung, Bryan Lee Weng Wai, Cheng Hao Fung, Fiza Mughal, Vahab Iranmanesh, 2015." Graphical Password: Shoulder-surfing resistant using falsification". *Software Engineering Conference(MYSEC),2015 9th Malaysian.*

6. Haichang Gao, Xiang Liu, Sidong Wang, Honggang Liu, Ruyi Dai, 2009." Design and Analysis of Graphical Password Scheme". *Fourth International Conference on innovative Computing, Information and Control(ICICIC).*

7. Huanyu Zhao, Xiaolin Li, 2007." A Scalable Shoulder-Surfing Resistant Textual-Graphical Password Authentication Scheme". *Advanced Information Networking and Application Workshops, 2007 21st International conference*