International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 03 | Mar 2020 www.irjet.net p-ISSN: 2395-0072

TTL: TAP TO LOGIN

Prof. Shimpli Dhale[1], Bhakti Murdio[2], Ankita Bhoyar[3], Sajid Sheikh[4], Vaishnavi Rithe[5] Reena Wagh[6]

[1]Assistant Professor, Dept. of Computer Science & Engineering, Datta Meghe Institute of Engineering Technology & Research, Wardha, Maharashtra, India
[2,3,4,5,6]Student, Dept. of Computer Science & Engineering, Datta Meghe Institute of Engineering Technology & Research, Wardha, Maharashtra, India

---

Abstract - *User authentication is the most important procedures required to access secure and confidential data. Authentication of users is usually achieved through textual password schemes. Attackers through social engineering techniques can easily hack the text based password of a user. Apart from being vulnerable to social engineering attacks, text based passwords are either weak and memorable or secure and difficult to remember. Image based authentication allows user to create graphical password which has several advantages over text based passwords. Graphical passwords have been designed to make passwords more memorable and easier for people to use. In this project, TTL is a new graphical password scheme for public terminals that replaces the static digital images typically used in graphical password systems that allows users choice password and simultaneously influences users to select stronger password is proposed. To add a layer of security, user is asked to input own digital picture and select sequence tokens from the picture used during registration phase. The user has to reproduce the same tokens by input the same image during his login phase. This proposed system offers reasonable security and usability and appears to fit well with some practical applications for improving digital security.*

Key Words: **Authentication**, **Passwords**,**TTL**, **Static, token, Security, terminal.**

1. INTRODUCTION -

A graphical password is an authentication system that works by having the user select from images, in a specific order, presented in a graphical user interface (GUI). For this reason, the graphical-password approach is sometimes called graphical user authentication (GUA). Some types of graphical passwords are, Multifactor authentication, based on the combination of two or more independent processes, can boost security. In typical multifactor authentication schemes, physical tokens are used to generate and store secrets for user authentication. For example, One-time password generation, user snapping a picture of QR code. Biometrics is one of the various alternatives to increase the security but it requires lot of investments.

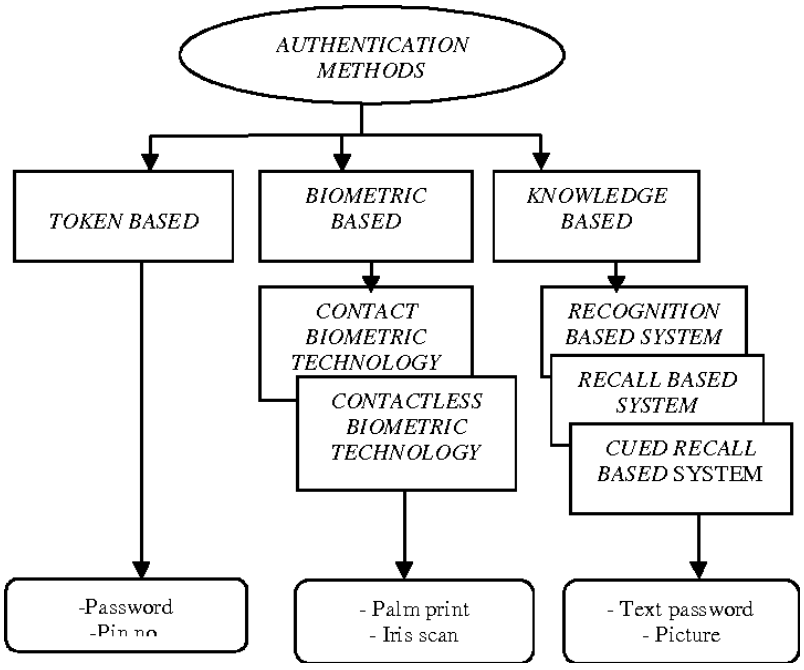

Fig.-1: Taxonomy of different authentication methods.

Fig-2: User snapping a picture of QR code.

Fig.-3: Token based authentication method.

Fig.-4: Biometric based authentication method.

Tap to Login make graphical passwords more secure against intelligent guessing and shoulder surfing attacks. Graphical password schemes have been proposed as a possible alternative to text based schemes, motivated partially by the fact that humans can remember pictures better than text. People select predictable passwords. This occurs with both texts based and graphical passwords. Users tend to choose passwords that are memorable in some way, which unfortunately often means that the passwords tend to follow predictable patterns that are easier for attackers to hack. While the predictability problem can be solved by disallowing user choice and assigning passwords to users, this usually leads to usability issues since users cannot easily remember such random passwords. This proposed system allows user choice while attempting to influence users to select stronger passwords. It also makes the task of selecting a weak password more easy , in order to discourage users from making such choices.

1.1 Problem Statement

Text passwords and personal identification numbers (PINs) are the dominant authentication method are simple and can be deployed on systems including public terminals, the web, and mobile devices. Here focus on the authentication problem. The most common computer authentication method is to use alphanumerical usernames and passwords. This method shown to have various drawbacks. Most of the graphical password authentication uses static image to login and store the image on server side which can be vulnerable to database hacker. To address this issue, present a new point click graphical password system, TTL- Tap to Login that increase resistance to observation attack by coupling the user's password to an image.

1.2 Objective

- To use gaussian blur algorithm to remove noise in captured image
- To use SIFT algorithm to detect and describe local features in digital images
- Storing TTL selections on authentication server as a set of optical features computed with the SIFT image processing algorithm.
- Using blob detection algorithm to extract the number and size of matching regions

2. System Architecture

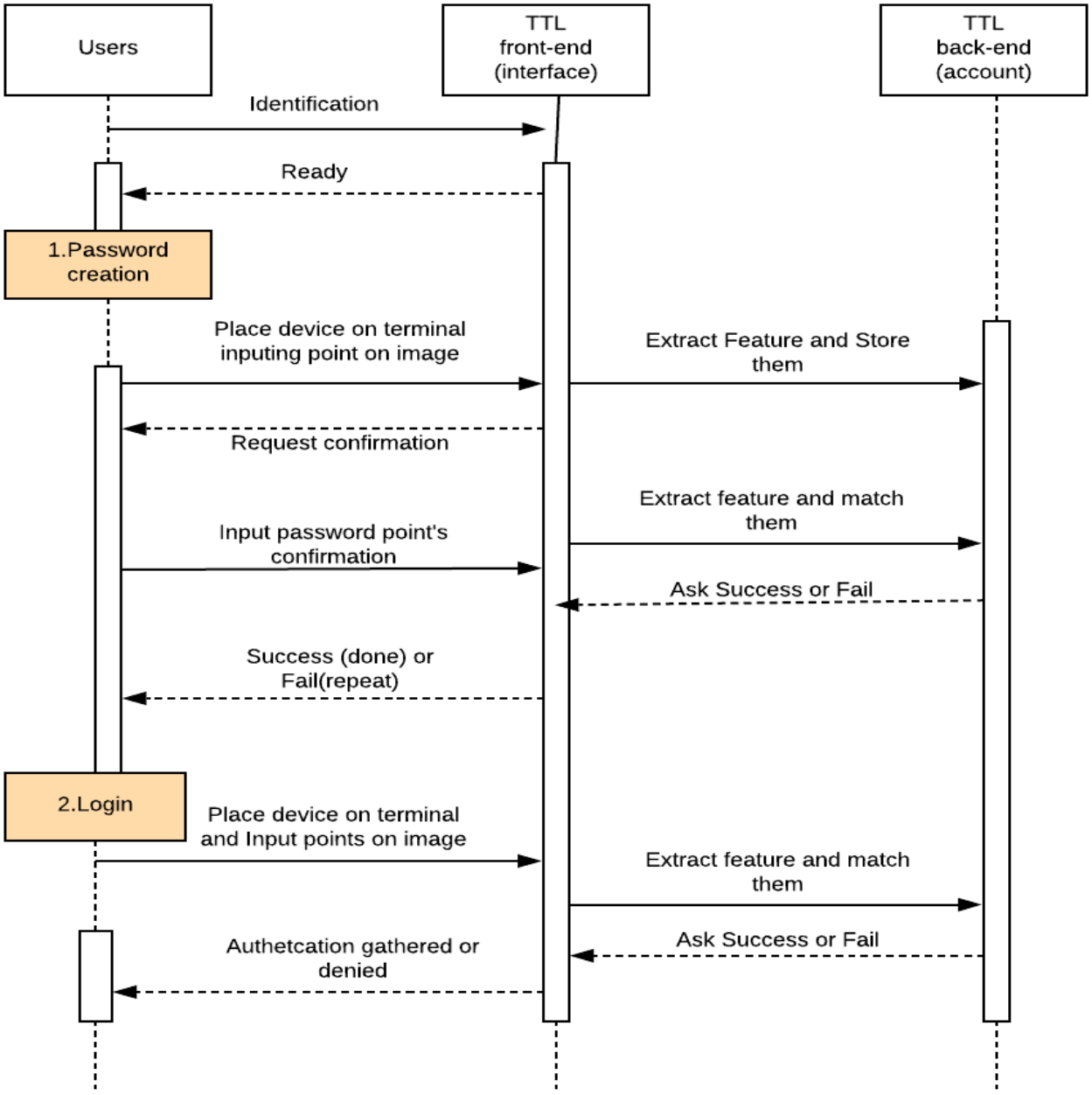

Fig.- 5: System Architecture

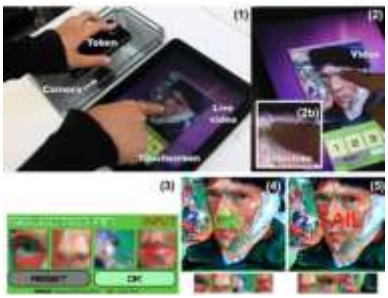

Fig.-6: (1) Overview of the TTL system.

(2)Input selection and closeup.

(3)Input selection that make up a password.

(4)Successful authentication and

(5)denied authentication.

Implementation:

TTL authentication takes place as follows (See Fig.-6):-

- Assuming users have previously created a password, login involves users identifying themselves at a TTL terminal.
- For example, user ID might be used on a public computer, and higher security applications such as bank ATM, will likely rely on a physical token such as an ATM card. TTL can be integrated in any of these scenarios.
- Second, users place a previously chosen password image or object they possess on top of a camera unit in the terminal. This is captured and displayed live on an adjacent touch screen.
- Third, they tap on the image locations that correspond to their password. This way, authentication requires both the physical token and the password simultaneously.
- In Fig. 5.2, Users must input a total of four items and then press an OK button in order to enter a complete password. They can also press a reset button to clear the entered password items at any time.

3. CONCLUSIONS

This project propose for improving the security of graphical password system by integrating live video of physical token that a user carries with them. It first demonstrate the feasibility of the concept by building and testing a fully functional prototype. It then illustrates that user performance is equivalent to that attained in standard graphical password system through a usability study assessing task time , error rate and subject workload. Finally, a security study shows that TTL substantial increases resistance to shoulder surfing attacks compared with existing graphical password scheme. Ultimately this project demonstrate that TTL conserve the beneficial properties of graphical password while increasing their security. While this approach was simple and effective, greater speed and efficiency would be attained with a native application.

By taking advantage of users' ability to recognize images and the memory trigger associated with seeing a new image, TTL has advantage over other system in terms of usability. But in proposed system user verification process is not achieve high level security so focus on verification process and proposed feature points with order evaluation approach i.e. not only verify feature points but also verify the order of feature points. During the registration the feature points are stored in the server with its order sequence and match the feature points and its sequence thus achieve high level security and also provide better usability.

REFERENCES

[1] Adams and M. Sasse "Users are not the enemy," Commun. ACM, vol. 42, pp. 40-46, 1999.

[2] S. Chiasson, P.C. van Oorschot, and R. Biddle, "Graphical password authentication using cued click points," in Proc. 12th Eur. Symp. Res. Comput. Security, 2007, pp. 1-12.

[3] Arash Habibi Lashkari , Azizah Abdul Manaf , Maslin Masrom, "A Secure recognition based graphical password by watermarking " in IEEE 11th International Conference on Computer and Information Technology,164-170 , 2011.

[4] William Stallings, Lawrie Brown, "Computer Security: Principles and Practice," in Pearson Education Limited , Jan 2012.

[5] Harinandan Tunga, "Graphical User Authentication Techniques for Security: a Comparative Study," in Journal of Surface Engineered Materials and Advanced Technology , June 2015

[6] Andrea Bianchi, Ian Oakley, and Hyoungshick Kim, "PassBYOP: Bring Your Own Picture for Securing Graphical Passwords" in IEEE Transactions on HUMAN-MACHINE SYSTEMS, 2017.