IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 6, May 2023

Emoji Code – A Graphical Way of Authentication

Piyush Garg
Student, Department of Computer Science Engineering
Dronacharya College of Engineering, Gurugram, India

Abstract: *There are many ways to perform the authentication, be it password, image, pattern, security key, security pin, etc. But all these ways are difficult to remember and therefore people tend to choose shorter and easy to remember passwords like name, date of birth, etc. which can be guessed easily. Therefore, to overcome these challenges, we can use a graphical way of authentication which uses emojis as the passcode. These emojis can be arranged in a story-based manner to make it easy to remember the sequence of emoticons.*

Keywords: Graphical Password, Emoji-based Password, Story-based Password, Authentication.

I. INTRODUCTION

User authentication is the process of proving the identity of the user trying to access the system. Username and passwords are most used method of authentication. These passwords comprise of alphabets, digits, symbols & special characters. Ideally, a user must choose secure password wisely and different for different websites. But strong & hard to crack passwords are difficult to remember and therefore, users tend to choose passwords related to them like initials from their family member name or any other personal detail. This makes the password susceptible to the attack and being compromised. Also, users generally use the same password across multiple websites. To avoid such problems, we are presenting a graphical authentication system.

II. PROPOSED SYSTEM

This article [1] by YusmadiJusoh discusses the existing graphical ways of authentication along with their pros and cons. Another paper [2] discusses the use of Emojis in mobile authentication. Mohammed Abbas Fadhil Al-Husainy wrote a research paper [3] on using the emojis to strengthen the immunity of passwords against attackers. Here we propose an emojis & story based graphical way of authentication which provides user an easy way to authenticate themselves. It is scientifically proven that people can remember more than 2,000 pictures with at least 90% accuracy and it takes only 13 milliseconds for the human brain to process an image. Moreover, graphical approaches are more secure because they are resistant to brute force and dictionary attack.

The proposed technique works in 2 phases -

A. Registration Phase

During the registration phase, the users are required to create a graphical password. At time of creation of password, the users are suggested some short stories to remember their password. Now after deciding a story, the users select images to complete the story. Similarly, user selects images for 2nd story out of various available and fill the images in the provided grid.

B. Login Phase

During the login phase, the users are required to select the same images that were selected at time of registration. If the sequence & images matches, then user is logged in. The story helps the user in selecting the images in correct sequence and reduce the authentication failures.

DOI: 10.48175/IJARSCT-10092

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 6, May 2023

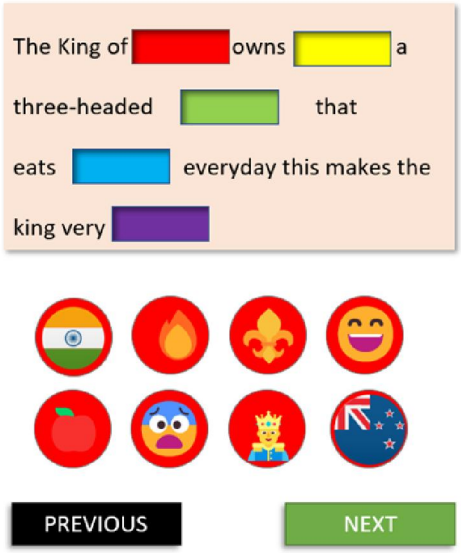

Fig. 1: Sample story filling during Registration Phase

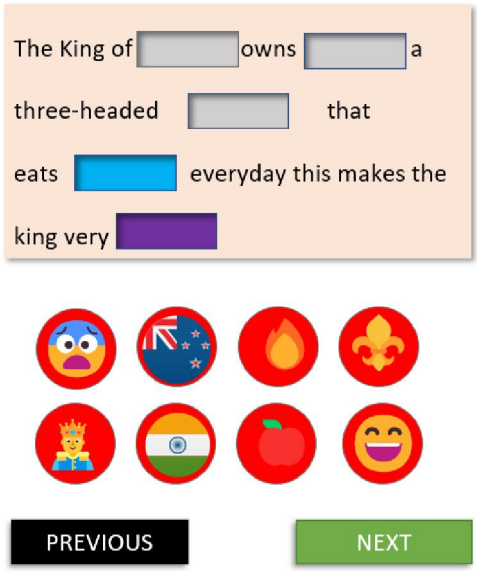

Fig. 2: Sample story filling during Login Phase

III. ATM USE CASE

The proposed technique is well suited for use at ATMs as a replacement for numeric PIN. The user can set the images/emojis initially and while entering the PIN, user must select the emojis based on the emojis set at time of registering. It can be integrated with existing ATMs without much changes. The user can select the emojis by pressing the corresponding numeric value. After pressing, the screen will show new emojis/images mapped to different numbers. This way, the numeric PIN is always changing and it also prevents the shoulder surfing attack. The fig.3 shows a sample screen for ATM.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 6, May 2023

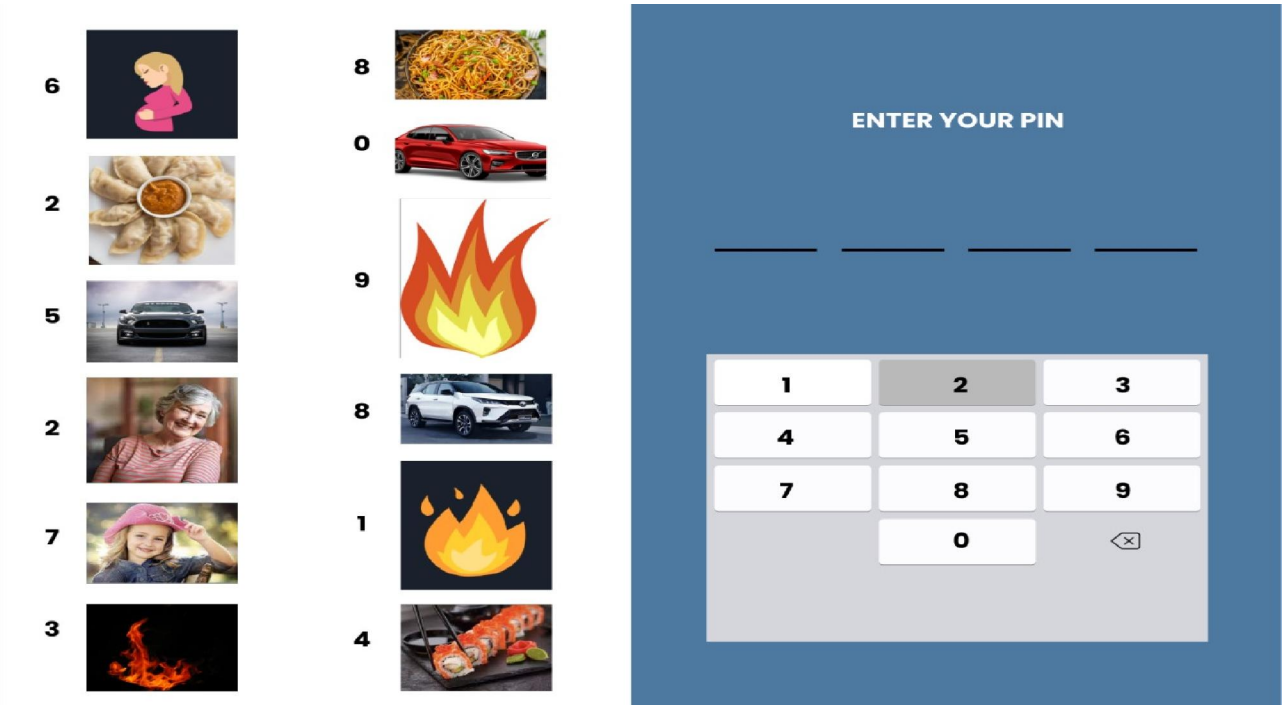

Fig. 3: Sample screen of ATM while entering PIN

IV. CONCLUSION

The proposed technique is efficient in terms of remembering the code and providing more security since we can add any number of emojis/images. Also, the proposed technique works very well in case of ATMs and possess the ability to eliminate the need of remembering numeric PIN. Also, if someone watches the PIN, then also that person cannot use that PIN directly and cannot know the emojiCode also.

REFERENCES

[1] EjikeEkeke Kingsley Ugochukwu, and YusmadiJusoh, "A Review on the Graphical User Authentication Algorithm: Recognition-based and Recall-based" in International Journal of Information Processing and Management 4(3):238-252, May 2013.

[2] Lydia Kraus, Robert Schmidt, Marcel Walch, Florian Schaub, Sebastian Möller., "On the Use of Emojis in Mobile Authentication" in 32th IFIP International Conference on ICT Systems Security and Privacy Protection (SEC), May 2017, Rome, Italy. pp.265-280, 10.1007/978-3-319-58469-0_18 hal-. 01649025.

[3] Dr. Mohammed A. Fadhil Al-Husainy, and Raghda Ahmed Malih, "Using Emoji Pictures to Strengthen the Immunity of Passwords Against Attackers" in European Scientific Journal October 2015 edition vol.11, No.30 ISSN: 1857 – 7881 (Print) e - ISSN 1857- 7431.