Graphical Password Authentication

Vishal Pednekar, Sayli Tawhare, Arundhati Pradhan, Nidhi Shettigar, Bharati Singh, Amisha Sahu

Department of Computer Engineering
Excelssior Education Society's K.C. College of Engineering & Management Studies & Research
Kopri, Thane (E) – 400603, India

Abstract – With cyberattacks rising exponentially, there is a need for protection of our digital data. Based on various studies which suggest that human brain has a greater capacity to remember what they see, to overcome the limitations of text-based passwords, we have introduced the concept of Graphical Password Authentication. The proposed system uses a 3 X 3 grid of 9 randomly selected images which when selected in a particular order makes a password. The proposed system, will also increase the level of security provided by today's traditional passwords by eliminating the chances of brute-force attacks, dictionary attacks and shoulder surfing.

I. INTRODUCTION

Passwords are ubiquitous in today's digital world. Password authentication systems usually comprise of a text-based password. Such passwords are prone to various cyberattacks such as brute-force, shoulder surfing, dictionary attacks and phishing attacks. According to various studies, many users also tend to forget their passwords [1], apply weak passwords [2] or write it down insecurely to remember it which may cause the passwords to get compromised. To overcome such challenges, we designed a graphical password authentication system which is based on recalling concept. Research conducted by various institutions show that human brain has a greater capacity to remember what they see [3] which gives idea to the concept that graphical passwords may be easier to remember than traditional alphanumeric passwords [4][5]. It uses images instead of alphanumeric characters. Users will be presented with a grid of different images and patterns to choose from. Such systems will simplify the authentication process and save time in the long run.

II. LITERATURE SURVEY

Cyberattacks have been rising exponentially since the past decade. Data is very precious today than it ever had been. This data ranges from a user's personal data to a country's highly confidential data. This data must be protected from going into wrong hands at all costs. Cyber criminals use various methods to gain illegal access and steal this data, some of the most common methods being phishing/social engineering, compromised/stolen devices and credential theft [6]. Passwords are one of the ways to authenticate users who have the rights to create, access, modify or delete the data. Traditional passwords consist of a string of alphanumeric characters of varying length. One of the challenges of using such passwords is that, users tend to forget them. According to a study, 78% of users forget their passwords and go for reset [1]. Some of the methods that users resort to overcome this challenge are to write down the password somewhere or set an easy password [7]. Easy to remember passwords are also prone to brute-force and dictionary attacks. A study conducted by Avast – a multinational cybersecurity software company, shows that 83% of the users in the United States apply weak passwords [2]. Phishing attacks where an attacker asks for user's credentials by posing as a legitimate website or application can also be carried out for alphanumeric passwords.

Research conducted by various institutions show that human brain has a greater capability to remember what they see [3][7]. This gives rise to an idea that graphical passwords are easier to remember than traditional alphanumeric passwords [8][6]. So, to overcome the limitations of alphanumeric passwords, we introduced a Graphical Password Authentication System. The proposed system uses a random set of images from which the users select some of them in a

specific order to form the password. Such a password is easier to remember and more secure than the traditional alphanumeric passwords.

III. METHODOLOGY

In the traditional authentication method involving alphanumeric passwords, the plain text password created during the registration phase is hashed using hashing algorithms like SHA256 or MD5. Hash makes sure that the data is unchanged. Slightest change in the data changes its hash as well. During the authentication phase when a user attempts to sign in to an application or website, he/she enters the plain text password in the field provided. The entered password appears as dots, stars or dashes to prevent the characters from being read by anyone else watching the screen. This plain text password is sent to the server and hashed. This hash is now compared with the hash calculated during the registration phase. If the hash matches, the password is correct and authentication is successful.

Our proposed system is an extension of the existing system wherein instead of hashing alphanumeric characters, image data is hashed in a specific order. Even the slightest change in the image data will make the authentication fail, thus making it very difficult to crack the password. Shuffling the images at each attempt will also make shoulder surfing difficult. Our proposed algorithm is discussed in the next section.

IV. PROPOSED ALGORITHM

The proposed authentication system is divided into two phases – Registration and Authentication. Following events occur during the Registration phase of the system:

A. Registration phase

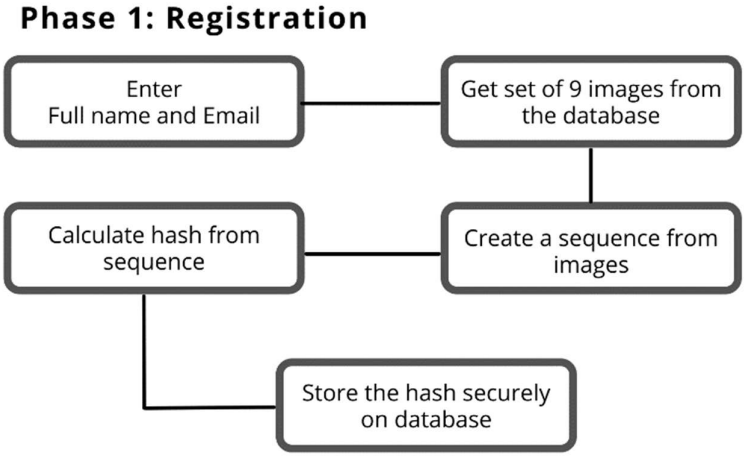

Fig 1. Flowchart of the registration phase

a. Users enter their credentials as required by the application or website.
b. A set of nine images is selected randomly from the database based on a seed created at the time of registration. These images are pre-processed using a special function to make them unique for each user.
c. The image IDs in the set are encoded using the seed and stored securely in the database for retrieving them in the future. The encoding uses a custom mathematical function.
d. User has to select 4 or more images (repetition allowed). The order of selection creates a sequence of images which is used as a password.

e. The images in the sequence are converted to binary and the data is added up before hashing. The sequence of binary images is hashed using SHA256 algorithm and stored securely in the database.

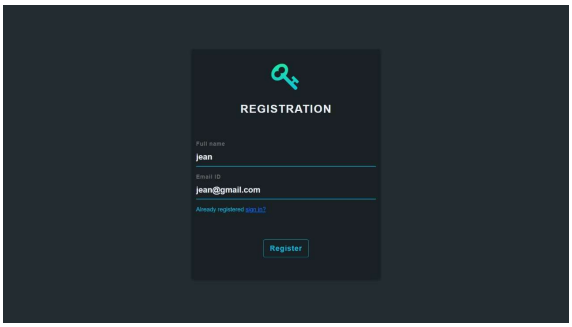

Fig 2. Registration page

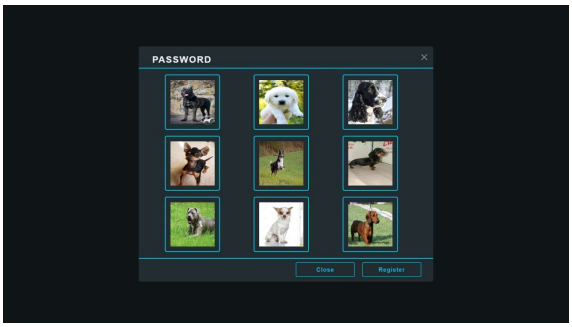

Fig 3: Set of 9 images for registration

One registration is completed and password is set, user can authenticate to that application or website. Following events occur during the authentication phase of the system:

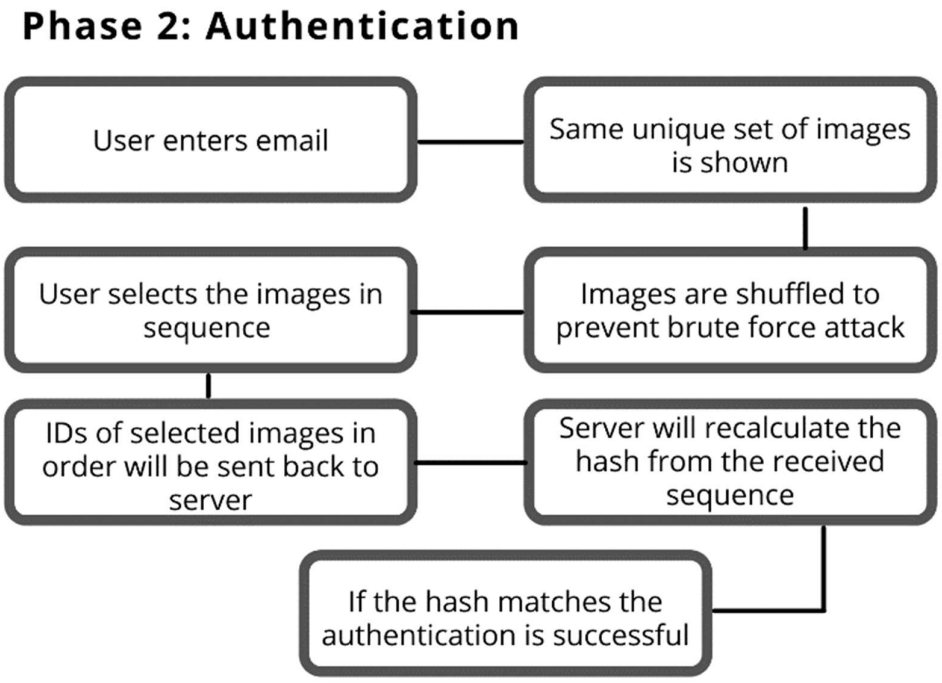

Fig 4: Flowchart of the authentication phase

a. Users enter their email address.
b. The encoded image IDs linked to this email address are decoded using the seed to obtain real IDs.
c. Once we get real IDs, we fetch the same set of 9 images from the database and apply pre-processing function to generate the unique images.
d. These images are presented to the user after shuffling them randomly at each login attempt.
e. User selects the images in the same order as in the registration phase.

f. The selected sequence is sent back to the server and their binary form is hashed with SHA256. This hash is then compared with the hash in the database. If it matches, then authentication is successful.

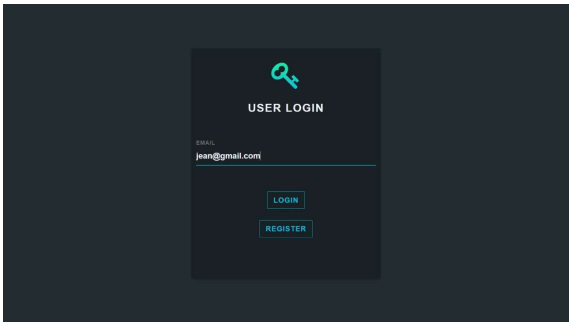

Fig 5. Login page

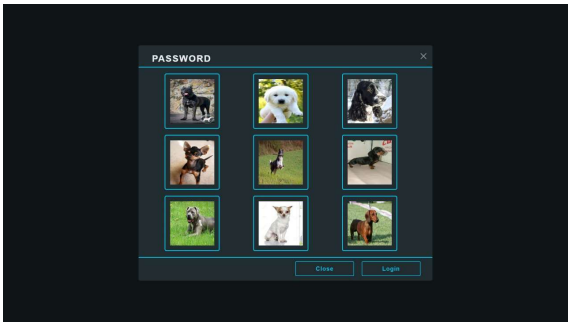

Fig 6. Set of 9 images for authentication

V. COMPARISON BASED ON ATTACK RESISTANCE

Category of schemes	Schemes	Attacks			
		Shoulder Surfing	Guessing and Dictionary	Spyware	Social Engineering
Recognition based	Passface	×	×	✓	E
	Déjà vu	✓	✓	×	D
	Triangle	✓	✓	×	M
	Movable frame	✓	✓	✓	D
	Picture Password	✓	✓	✓	M
	Proposed system	✓	✓	✓	D
	WIW	✓	✓	×	D
	Story	×	×	✓	E
	CHC		✓	✓	D
	Image Pass	×	✓	✓	E
	S-Passface		✓	✓	M
Pure recall based	DAS	×	×	×	M
	PASSDOODLE	×	✓	✓	M
	SYUKRI	×	✓	✓	E
Cued Recall Based	Blonder	×	×	×	M
	PassPoints	×	×	✓	D
	CCP	×	✓	×	D
	PCCP	×	✓	✓	D

E – Easy, M – Medium, D – Difficult

VI. CONCLUSION

Through the proposed graphical password authentication system, we overcame the limitations of the existing text-based passwords. Thus, graphical password authentication is quite user-friendly and secure as compared to other authentication methods. Random image selection, making slight modification to images for each user and shuffling them renders most of the widely used cyber-attacks useless. Efficient image compressing techniques also make this type of authentication suitable for offline authentication systems as well as devices with low memory.

VII. FUTURE SCOPE

1. We can provide an option for the user to use their own unique set of images.
2. We can ask the user to select a theme for the images displayed, making it even easier to remember the patterns.
3. We will attempt to develop image-based cryptography techniques which will use image(s) as a key to encrypt/decrypt the data.

REFERENCES

[1] https://www.digitalinformationworld.com/2019/12/new-password-study-finds-78-of-people-had-to-reset-a-password-they-forgot-in-past-90-days.html

[2] https://press.avast.com/83-of-americans-are-using-weak-passwords

[3] https://www.vox.com/the-highlight/22716264/memory-science-memorability

[4] Ali Mohamed Eljetlawi; Norafida Ithnin - Graphical Password: Prototype Usability Survey - 2008 International Conference on Advanced Computer Theory and Engineering

[5] Liew Tze Hui; Housam Khalifa Bashier; Lau Siong Hoe; Goh Kah Ong Michael; Wee Kouk Kwee - Conceptual framework for high-end graphical password - 2014 2nd International Conference on Information and Communication Technology (ICoICT)

[6] https://www.forbes.com/sites/chuckbrooks/2022/01/21/cybersecurity-in-2022--a-fresh-look-at-some-very-alarming-stats/?sh=730bcd146b61

[7] Jaffar Abduljalil Jaffar; Ahmed M. Zeki - Evaluation of Graphical Password Schemes in Terms of Attack Resistance and Usability - 2020 International Conference on Innovation and Intelligence for Informatics, Computing and Technologies (3ICT)

[8] Gi-Chul Yang - PassPositions: A Secure and User-Friendly Graphical Password Scheme – 2017 4th International Conference on Computer Applications and Information Processing Technology (CAIPT)

[9] Khazima Irfan, Agha Anas, Sidra Malik, Saneeha Amir - Text based Graphical Password System to Obscure Shoulder Surfing - 2018 15th International Bhurban Conference on Applied Sciences and Technology (IBCAST)

[10] Ali Mohamed Eljetlawi; Norafida Ithnin - Graphical Password: Comprehensive Study of the Usability Features of the Recognition Base Graphical Password Methods - 2008 Third International Conference on Convergence and Hybrid Information Technology

[11] M. Arun Prakash; T.R. Gokul - Network security-overcome password hacking through graphical password authentication - 2011 National Conference on Innovations in Emerging Technology