WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Visual Key-A Multi-Layer, CNN Image Derivation Based Graphical Authentication System

Riddhi Zavare[1], Shreyash Jadhav[2], Priyanshu Sharma[3], Akshaya Prabhu[4]

[1, 2, 3]Final Year Student, Computer Engineering Department, VIVA Institute of Technology, India
[4]Assistant Professor, Computer Engineering Department, VIVA Institute of Technology, India

A B S T R A C T

Authentication techniques have seen tremendous advancement, innovation, and thus success in the real world. It has moved its way up from rudimentary ciphers to complex authentication techniques which would require thousands of years even for the most powerful computers to crack. Today Alpha-Numeric Passwords, in User ID and Password combination are the most used type of authentication format in the world. However, researchers have shown that while alpha-numeric passwords are good, and often very hard to crack, they are vulnerable to many attacks such as phishing, social engineering, malware, dictionary attack, offline cracking, spidering, Brute force attack, shoulder surfing, guessing, etc. All these attacks are possible due to either human error, or the blazing fast speed that a computer can interact with the authentication system while deploying its password cracking technique. Thus, in order to counter these to drawbacks of alpha-numeric passwords, researchers have been coming up with new methods of authentication which does not use any alpha numeric inputs, or any other qualities which cause the drawback in said system. In order to accomplish this goal some researchers have started on various variations of graphical based passwords, as these systems are much more sophisticated as compared to alphanumeric passwords. In this paper, we showcase a new type of graphical authentication system which allows the user to use images as passwords by using the VGG16 algorithm, this system is also fully backwards compatible with alpha numeric authentication systems, It is either equivalent or more efficient, easy to use, robust and user friendly than the current alphanumeric authentication systems.

Keywords: Alphanumeric password, , Graphical password, Graphical password authentication, Password, Security, Text-based password

1. Introduction

In today's digital world, almost everyone has access to a personal computer that is connected to the internet. To access various online services on the internet, users need to create a username and password. A password is unequivocally one of the most important words a user has to choose in their lifetime [14]. The password needs to be in a format where users are required to add at least one capital letter, small letters, numbers, and a special character. But according to a survey by Digital Guardian [24], users experience 'password overload' as complex passwords are now a requirement on most websites. Also, these passwords are hard to remember, and more than 30% of the users online write down the password on a piece of paper [24]; and 81% of hacking-related breaches involved either stolen or weak passwords [25].

The proposed method provides the user with the ability to authenticate any application, website login page, and similar instances of authentication by allowing the user to select random images which they set as the password. The proposed model is easy to remember while also being secure and hard to crack. In the proposed system, users are required to upload a fixed number of images in the application to create a pool of images which will be displayed at the time of login. The user chooses a certain number of pictures from this pool to be used as a password in a particular order. The software creates a queue of photos when the images are chosen, processes them, and then feeds the images to an image detection model. This model consists of a convolutional neural network (CNN) as well as a recurrent neural network (RNN). CNN is used to extract features from images, and RNN is used to generate sentences. The output of this model is meaning sentences for each image, which is our unencrypted password, so the next step is to encrypt this text using a hashing method. The resulting hash is then encrypted, ensuring that even if this particular password is leaked, it cannot be used to reverse-engineer our image detection model. Because, if left unencrypted, one can reverse-engineer the data set and forecast what it would output when given a certain image by using 100k photographs, or an amount equivalent to the one used in the data set. The proposed technique is more secure than alphanumeric-based authentication schemes and is also simpler to use and memorise [6].

2. Related Work

This section describes the various methodologies and techniques used in prior studies for graphical password authentication. Haichang Gao, et.al [1] provided a comprehensive security overview of published research of existing graphical password. Gi-Chul Yang, et.al [2] compared PassPositions and PassPositions-II, which are recently announced graphical password authentication systems, and shows experimental results on usability and security of implemented systems. Sung-Shiou Shen, et.al [3] proposed a new graphic pattern protection mechanism for enhance authentication level in the keypad

lock screen app field. Nida Asmat, et.al [4] proposed system allowed the user to divide a picture into multiple chunks and while unlocking it selecting the previously defined chunks results successfully in unlocking the device. Herv Chabannne, et.al [5] introduced a new wallet recovery pro-cess. They proposed visual passwords which is a photograph of a secretly picked object with the help of ImageNet classifiers that transforming images into binary vectors and, obfuscated fuzzy matching for storing visual passwords/retrieving wallet seeds. Touraj Khodadadi, et.al [6] A novel recognition-based graphical scheme with enhanced usabcility characteristics is presented in this study. The suggested scheme's prototype was created and made available to users for testing. Teoh joo Fong, et.al [7] proposed Authentication Model which is a hybrid graphical password mobile authentication scheme.

Jaffar Abduljalil Jaffar, et.al [8] comprised of comprehensive research in the graphical password schemes and evaluates each of the available schemes at two main areas that are attack resistance and usability. Zach Parish, et.al[9] discussed about recent advancements in password assaults employing publicly released passwords, personal information, and sophisticated guessing techniques, password security which has become a critical problem. By utilising people's better memory for visual cues, graphical passwords have the potential to increase password memorability and maybe provide ideas for additional methods to make text passwords more memorable. Sonia Chiasson, et.al[10] proposed a new click-based graphical password scheme called Cued Click Points (CCP). It can be also viewed as a combination of PassPoints, Passfaces, and Story. Wazir Zada Khan, et.al[11] proposes a new hybrid graphical password based system that combines recognition and recall based techniques to make it more convenient for the user. Xiaoyuan Suo, et.al[12]says that the most common computer authentication method is to use alphanumerical usernames and passwords, but this has been shown to have drawbacks. To address this, some researchers have developed authentication methods that use pictures as passwords. O.J Elugbadeboa, et.al[13] says most authentication systems use passwords, which are strings of secret texts requested from the user to access computing resources. However, these passwords are susceptible to dictionary attacks, brute force attacks, shoulder-surfing attacks etc. Rahul Shrivastava, et.al[14] says user authentication is a basic part of laptop security, with alphamerical username/passwords being the most common style. However, they are prone to lexicon and brute-force attacks, making them difficult to remember. J. Thorpe, et.al[15] studies the impact of named parameters on the size of the word space for " Draw-A-Secret "(DAS) graphical passwords. They examine the part of and connections between the number of compound strokes, grid confines, and word length in the DAS word space. M. Anwar, et.al[16] shows mobile devices are frequently used for sensitive activities such as banking, healthcare, and shopping. Z. Zhao, et.al[17] says picture gesture authentication (PGA) is a new login experience for touch-screen devices that Microsoft Windows 8TM operating system uses. P.K. Dokhale, et.al[18] says, Traditional text-based or biometric authentication methods for computer systems have drawbacks. S. Wiedenbeck, et.al[19] says, The article discusses the development of PassPoints, a graphical password system where users click on images to authenticate themselves. H. Parmar, et.al[20] says, Phishing is a serious security threat that aims to gather personal and financial information of the receiver through fraudulent emails.

3. Research Objectives

Alphanumeric, biometric, and rudimentary graphical or image-based authentication systems are effective in providing decent security, utilizing sophisticated methods to make authentication difficult to crack. However, to further enhance security, this research aims to implement advanced encryption algorithms, including SHA-256 and AES-256, along with the VGG16 model and a customized dataset tailored to the user's specific requirements. This unique authentication system is designed to resist various password-cracking methodologies, offering stakeholders a much higher level of security that is significantly more difficult to breach than traditional authentication methods. Ultimately, this system greatly improves the user's security posture, providing greater peace of mind.

4. Proposed System & Methodology

4.1 Algorithm

The algorithm for the proposed system is as follows:

Step 1: Import all necessary packages. (hashlib, pycrypto, keras)

Step 2: Display GUI to the user.

Step 3: If the user selects Register, go to Step 5.

Step 4: Else if the user selects Login, go to Step 11.

Step 5: User creates a username.

Step 6: 25 Images needed to be uploaded from the user's system. These images are stored on the server.

Step 7: From the uploaded images, 9 images should be sequentially selected by the user. These images will be used for the password.

Step 8: The images are processed and passed on to the image recognition program. The program outputs a meaningful sentence out of the images.

Step 9: The sentences are then hashed, encrypted and stored safely in the database.

Step 10: After storing the password, the user is prompted as 'Registration successful' and then redirected to the login page.

Step 11: The user is required to provide their username in the login page.

Step 12: All 25 Images which were already selected by the user are displayed.

Step 13: The correct images with their sequence are needed to be selected. After selecting the images, the user submits them.

Step 14: On the server side, the images are processed and meaning sentences are derived from them by the image detection program. The hashing and encryption are also carried out.

Step 15: The output from Step 13 is checked with the password stored in the database. If they are the same, the user is logged in, else the user is again required to submit the password.

Step 16: After certain no. of tries or if the user doesn't remember the sequence of images, a Reset password link to provided. If the link is clicked then go to Step 5.

4.2 System Block Diagram:

The Fig.1 depicts the block diagram of the proposed system for registration process in which the principal parts and functions are represented by blocks which are connected by lines that show the relationships of the said blocks. User activities are shown in one block and backend activities are shown in another block. Fig. 2 depicts the block diagram for login process.

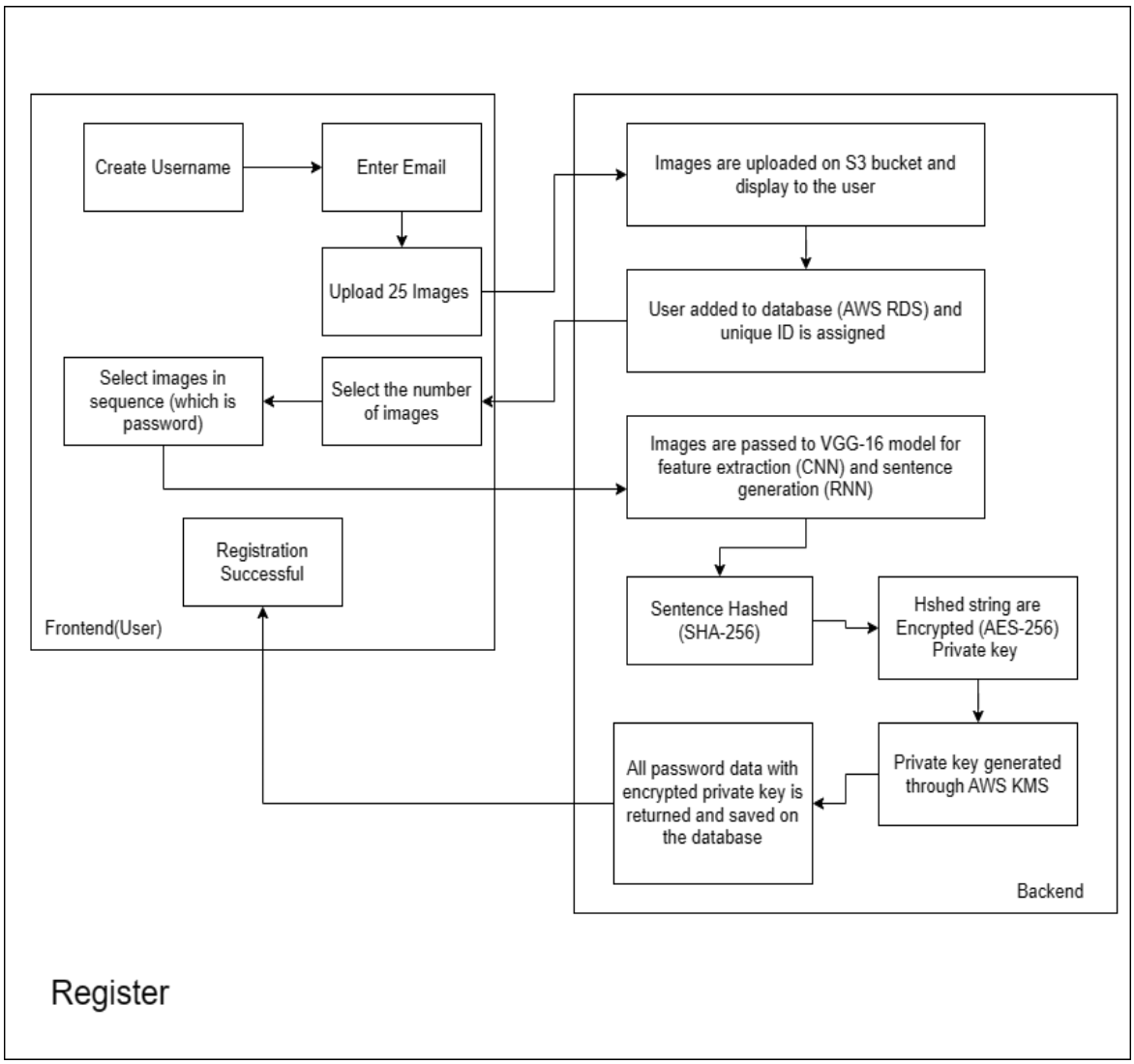

Fig. 1 Block Diagram for Registration

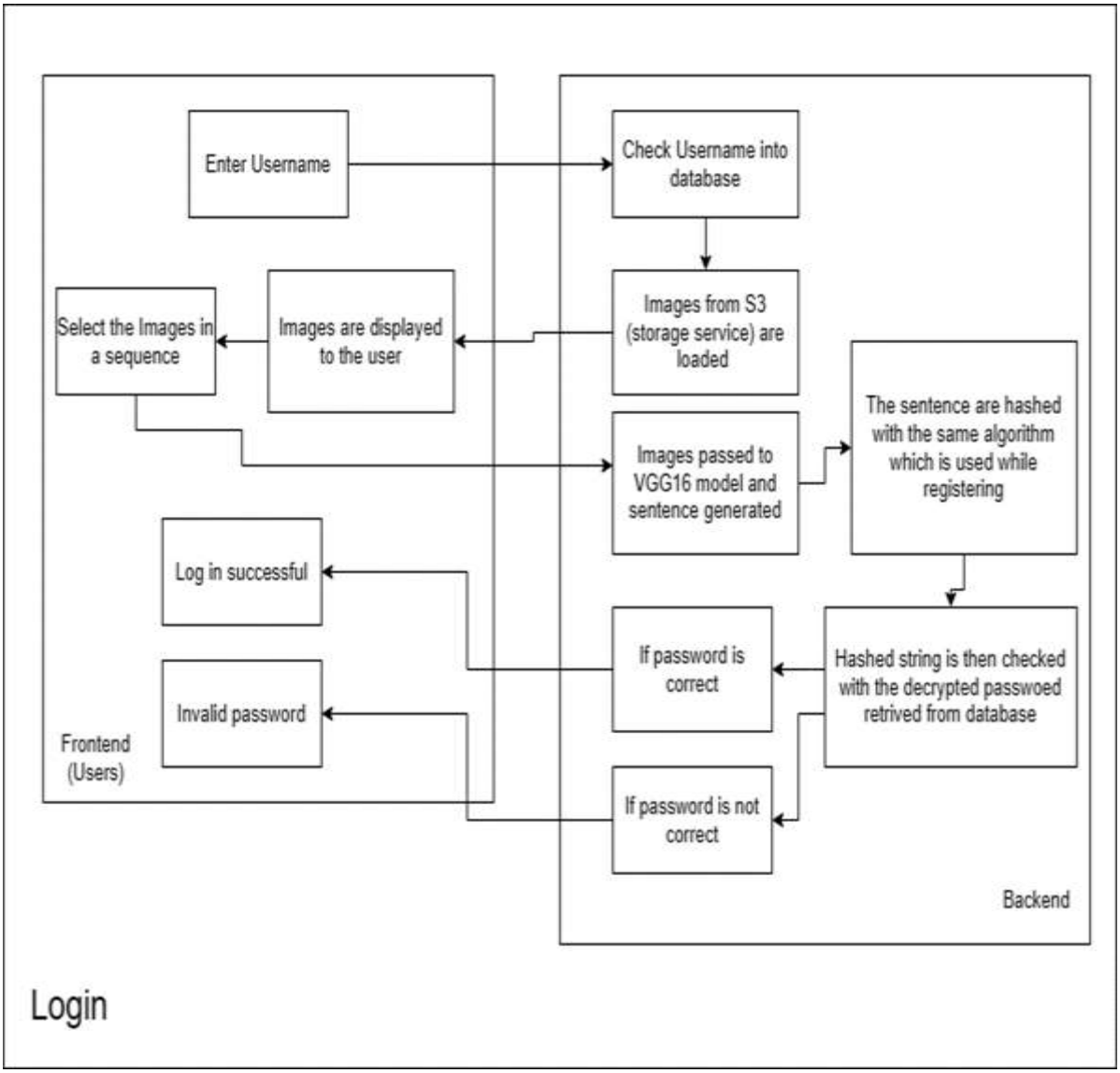

Fig. 2 Block diagram for Login process

4.3 System Flow Chart

The Fig.3 is the system flow diagram of the proposed system that visualizes the sequence of actions, movements within the proposed system and decision points. The figure shows the detailed process of the system that how the images are uploaded, where the hashing and encryption is done etc.

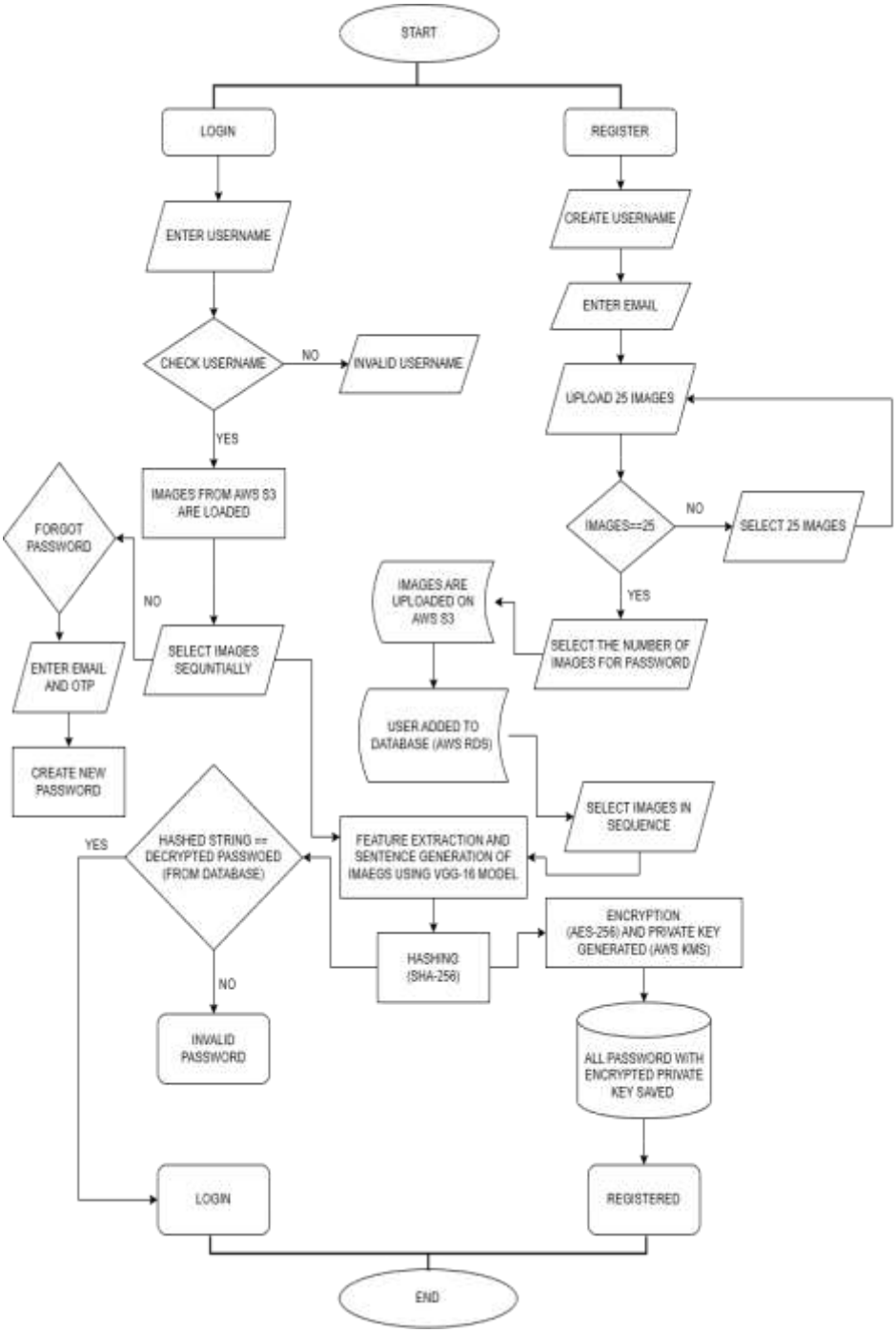

Fig.3 Flow chart of proposed system

4.4Methodology

In the proposed system, the user chooses randomly selected photographs from their computer to upload to the software, building a pool of images that will be shown when they log in next time. From this pool, the user selects a certain number of images to be used as passwords in a specific order. When a photo is selected, the software generates a queue of it, analyzes it, and then passes it to the VGG16 model. VGG16 is composed of 13 convolutional layers, 5 max-pooling layers, and 3 fully connected layers. Therefore, the number of layers with tunable parameters is 16 (13 convolutional layers and 3 fully connected layers). That is the reason why the model name is VGG16. The number of filters in the first block is 64, then this number is doubled in the later blocks until it reaches 512. This model is finished by two fully connected hidden layers and one output layer. The two fully connected layers have the same number of neurons, which is 4096. The output layer consists of 1000 neurons corresponding to the number of categories in the dataset. Convolutional neural networks (CNN) and recurrent neural networks (RNN) are elements of this model. The RNN is used to create phrases, whereas the CNN is used to extract characteristics from images. The VGG16 model generates meaningful sentences for each image, which serve as our unencrypted password.

The next step is to encrypt this text obtained from the VGG16 model using a hashing method. The SHA-256 algorithm is used for hashing. The SHA-256 algorithm, like other hash functions, takes any input and produces an output (often called a hash) of fixed length. It doesn't matter if the input is a single word, a full sentence, a page from a book, or an entire book, the output of a hashing algorithm like SHA256 will always be the same length. Specifically, it will be 256 bits, which is 32 bytes, and is displayed as 64 alphanumeric characters. All outputs appear completely random and offer no information about the input that created it. There is no way to reverse engineer an input from knowledge of the output.

The final hash from the SHA-256 algorithm is encrypted to ensure that even if this specific password is exposed, it cannot be used to decipher our picture detecting algorithm. AES-256 is used for encryption. AES (or Advanced Encryption Standard) is referred to as a block cipher where the information to be encrypted is categorized into sections called “blocks”. AES-256 has a key length of 256 bits and is considered unbreakable by brute force attacks. The larger the key size, the more combination possibilities there are. AES-256 has become the market standard to protect important data against unauthorized users. Finally, the encrypted password from AES-256 is saved in the database. To log into their account, the user needs to enter their username, which is verified by the server, and after that, the 25 images uploaded by the user during registration are displayed. Nine pictures from this set must be chosen sequentially. These 9 images are then again processed and checked with the password stored in the database. The user can log into their account if they are correct; otherwise, they can try again or reset their password.

5. Results

Here are results of the proposed system. Fig.4 depicts the Log in page of the system where the users have to enter their username which is created at the time of registration. If the users are new than they have to click on Register here tab and register themselves.

Fig.4 Log in page

Fig.5 depicts the window which shown after entering the username correctly. Here by checking the username from database, the images are loaded from database. These images are same as selected while creating the password by users from their system. Here users must select the images sequentially as selected while creating the password. If users forgot their password than they can reset their password by clicking on Forgot password tab.

Fig.5 Loading images from database

In Fig.6, it shows the successful message after selecting password sequentially.

Fig.6 Successfully login

Fig. 7 depicts the forget password window. If the users forgot their password than by clicking on forgot password tab (while login) these window is shown. Here for reset the password, users have to enter their email id and the OTP is send on entered email id. So the users can easily reset their password.

Fig.7 Forgot password

Fig. 8 depicts the registration page where the users have to create their username and enter their email id. So these information will saved into database. If users already registered than they can directly click on log in page and can enter their log in details.

Fig.8 Registration page

Fig. 9 depicts a password creation page which is shown after entering username and email by users. Here, firstly users have to upload the 25 images from their system. After that they have to select the number of images (minimum 3 number of images) for creating a password from the slide bar. Next they have to make the sequence of images which is their password.

Fig.9 Create password

In Fig.10, it shows the successful message after creating password.

Fig.10 Successfully register

6. Conclusion

With an increase in the digitalization of the world, the use of authentication systems has only increased, while alphanumeric passwords have proven to be hard to crack, many tools and techniques have been developed that can be used to bypass or crack such systems. Thus, we have developed a new authentication system that is either equivalent or more secure, robust, and accessible to users, this authentication system is called 'Visual Key' it is a Graphic based authentication system.This system works on the basis or replacing the alpha numeric passwords with a password that is graphical in nature and thus much harder to crack using traditional cracking methods in most cases. The 'Visual Key' system allows users to set their password using images from their system and create a sequence of a images at the time of registration. If the users are already registered, then they can login by entering their username. After entering the username, images are retrieved from the database, which are selected at the time of registration. The system is made up of using the VGG-16 model, the Advanced Encryption Standard, and Secure Hash Algorithm Techniques. So, in conclusion, the proposed system is more secure than the alphanumeric authentication scheme as it uses images as a password and it will be easy to remember.The implications of implementing such a system in the authentication industry are highly positive. By deploying this system, the authentication process will become simplified, robust, and resilient to various types of attacks, including phishing, social engineering, malware, dictionary attacks, offline cracking, spidering, brute force attacks, shoulder surfing, and guessing, among others. These attacks are usually possible due to human error or the high speed at which computers can interact with the authentication system, enabling them to use password-cracking techniques. Thus by implementing this system, security can be enhanced, while maintaining ease of access.

References

[1] Gao, H., Jia, W., Ye, F., & Ma, L. (2013). A survey on the use of graphical passwords in security. J. Softw., 8(7), 1678-1698.

[2] Yang, G. C., & Oh, H. (2018). Implementation of a graphical password authentication system 'PassPositions'. Journal of Image and Graphics, 6(2), 117-121.

[3] Shen, S. S., Kang, T. H., Lin, S. H., & Chien, W. (2017, May). Random graphic user password authentication scheme in mobile devices. In 2017 International conference on applied system innovation (ICASI) (pp. 1251-1254).

[4] Asmat, N., & Qasim, H. S. A. (2019, March). Conundrum-Pass: A New Graphical Password Approach. In 2019 2nd International Conference on Communication, Computing and Digital systems (C-CODE) (pp. 282-287). IEEE.

[5] Chabanne, H., Despiegel, V., & Guiga, L. (2022, December). One Picture is Worth a Thousand Words: A New Wallet Recovery Process. In GLOBECOM 2022-2022 IEEE Global Communications Conference (pp. 1801-1806). IEEE.

[6] Khodadadi, T., Javadianasl, Y., Rabiei, F., Alizadeh, M., Zamani, M., & Chaeikar, S. S. (2021, December). A novel graphical password authentication scheme with improved usability. In 2021 4th International Symposium on Advanced Electrical and Communication Technologies (ISAECT) (pp. 01-04). IEEE.

[7] Fong, Teoh joo, Abdullah, A., Jhanjhi, N. Z., & Supramaniam, M. (2019). The Coin Passcode: A Shoulder-Surfing Proof Graphical Password Authentication Model for Mobile Devices The Next Generation Swift and Secured Mobile Passcode Authenticator. INTERNATIONAL JOURNAL OF ADVANCED COMPUTER SCIENCE AND APPLICATIONS, 10(1), 302-308.

[8] Jaffar, J. A., & Zeki, A. M. (2020, December). Evaluation of Graphical Password Schemes in Terms of Attack Resistance and Usability. In 2020 International Conference on Innovation and Intelligence for Informatics, Computing and Technologies (3ICT) (pp. 1-5). IEEE.

[9] Parish, Z., Salehi-Abari, A., & Thorpe, J. (2021). A study on priming methods for graphical passwords. Journal of Information Security and Applications, 62, 102913.

[10] Chiasson, S., Van Oorschot, P. C., & Biddle, R. (2007, September). Graphical password authentication using cued click points. In ESORICS (Vol. 7, pp. 359-374).

[11] Khan, W. Z., Aalsalem, M. Y., & Xiang, Y. (2011). A graphical password based system for small mobile devices. arXiv preprint arXiv:1110.3844.

[12] Suo, X., Zhu, Y., & Owen, G. S. (2005, December). Graphical passwords: A survey. In 21st Annual Computer Security Applications Conference (ACSAC'05) (pp. 10-pp). IEEE.

[13] Orunsolu, A. A. (2022). An Efficient And Secured Graphical Authentication System. Acta Informatica Malaysia (AIM), 6(1), 17-21.

[14] Prof. Krupi Saraf , Rahul Shrivastava, Ram Patidar, Rajesh Patidar & Pranit Ghate (2022). A Graphical Password Authentication System. International Journal of Research Publication and Reviews, 3(11), pp. 2361-2365

[15] Thorpe, J., & Van Oorschot, P. C. (2004, December). Towards secure design choices for implementing graphical passwords. In 20th Annual Computer Security Applications Conference (pp. 50-60). IEEE.

[16] Anwar, M., & Imran, A. (2015, April). A Comparative Study of Graphical and Alphanumeric Passwords for Mobile Device Authentication. In MAICS (pp. 13-18).

[17] Zhao, Z., Ahn, G. J., & Hu, H. (2015). Picture gesture authentication: Empirical analysis, automated attacks, and scheme evaluation. ACM Transactions on Information and System Security (TISSEC), 17(4), 1-37.

[18] Dharane, S. R., Kakade, P. N., Gaikwad, S. P., Dokhale, P. K., & Bhamare, A. Y. (2015). A novel method for graphical password mechanism. International Journal on Recent and Innovation Trends in Computing and Communication, 3(1), 156-161.

[19] Wiedenbeck, S., Waters, J., Birget, J. C., Brodskiy, A., & Memon, N. (2005, July). Authentication using graphical passwords: Effects of tolerance and image choice. In Proceedings of the 2005 symposium on Usable privacy and security (pp. 1-12).

[20] Parmar, H., Nainan, N., & Thaseen, S. (2012). Generation of secure one-time password based on image authentication. Journal of Computer Science and Information Technology, 7, 195-206.

[21] https://viso.ai/deep-learning/vgg-very-deep-convolutional-networks, last accessed on: 4/10/2022.

[22] https://datagy.io/python-sha256, last accessed on: 2/10/2022.

[23] https://www.n-able.com/blog/aes-256-encryption-algorithm, last accessed on: 4/10/2022.

[24] https://digitalguardian.com/blog/uncovering-password-habits-are-users-password-security-habits-improving-infographic, last accessed on: 03/09/2022.

[25] https://www.connections.com/blog/why-secure-passwords-are-important, last accessed on: 02/09/2022.