ASET JOURNAL OF MANAGEMENT SCIENCE
A Bi-Monthly Peer Reviewed Journal

Aset Journal Of Management Science
Volume 1/ Issue 3/ pg: 23-31

GRAPHICAL PASSWORD AUTHENTICATION SPECIFICALLY FOR SHOULDER SURFING ATTACKS,(EMAIL PASSWORD AUTHENTICATION)

Mr B. Sanjaikumar[1], Mr S. Suriyaprakash[2], Mr R. Thirupathi[3], Dr.T. Loganayagi[4]

[1,2,3]B.E Student B.E Student of Cyber Security Department
[4] Professor of Electronic And Communication Engineering Department

[1,2,3,4]Paavai Engineering College, Pachal, Namakkal, Tamil Nadu

ABSTRACT

The importance of security in the authentication process as well as the increase in threat level posed by such malware has attracted many researchers to the field. Many attacks are successful in accessing social network accounts since the current password-based authentication paradigms are not efficient and robust enough as well as vulnerable to automated attacks. The traditional two-factor authentication mechanisms are not applicable to online social networks because physical token or biometric data cannot be easily used to log into users' profiles. The selection process ensures that each user's password is unique and virtually impossible to guess or replicate by an attacker. The system will be designed with user-friendliness in mind, offering an intuitive and engaging interface for symbol selection. The goal is to create a secure and memorable authentication system that mitigates the risk of unauthorized access.

Keywords: Graphical Password, Shoulder Surfing, Authentication Scheme,Passwords, Graphical Authentication,Password Attacks.

1.INTRODUCTION

Current authentication systems suffer from many weaknesses. The vulnerabilities of the textual password have been well known. Users tend to pick short passwords or passwords that are easy to remember, which makes the passwords unprotected for attackers to break.

Passwords possess many useful properties as well as widespread legacy deployment; consequently, we can expect their use for the foreseeable future. As well as when a user enters information using a keyboard, mouse, touch screen or any traditional input device, a malicious observer may be able to acquire the user's password credentials. This is a problem that has been difficult to overcome.

2.TYPES OF AUTHENTICATON

Cyber security is the process of taking precautions to guard against unauthorised access, misuse, malfunction, modification, destruction, or improper disclosure of the underlying networking infrastructure. Undoubtedly, the Internet has occupied a significant portion of our lives. In today's generation, a large portion of people's professional, social, and personal activities are conducted online. How secure is your network, though? Many people try to break into our computers that are connected to the Internet, invade our privacy, and prevent us from using the Internet services. Network security has emerged as a key issue in the field of cyber security due to the frequency, variety, and threat of new and more destructive attacks in the future. By putting network security measures in place, computers, users, and programmes can operate in a secure environment while performing their authorised vital functions.

2.1 Password Authentication

While password authentication is the most common way to confirm a user's identity, it isn't even close to the most effective or secures method. Anyone with your credentials could access your account without your permission, and the system wouldn't stop them. Most passwords are weak, and hacking techniques can breakthem in less and less time.

2.2 Email Authentication:

Email authentication is a password less option that allows users to securely log in using just an email address. The process is very similar to signing in with a Facebook or Twitter account, but this method offers a universal approach.

- The user clicks the login button. This opens a mail to link that directs the person to pre-written email that includes an encrypted token.

- The user sends the email. The message already comes with a recipient address, so the user doesn't need to enter any information.

- The server verifies the request. Using a combination of token-based security checks, the user's identity is verified.

2.3 Biometric Authentication:

Biometric authentication includes any type of authentication method that requires a user's biology. While this may seem like new-age technology, you're probably already using it to unlock the screen on your smartphone. Fingerprint scanning is the most well-known form of biometric authentication, but face recognition tools are an increasingly popular choice for developers.

3.PASSWORD AUTHENTICATION METHOD

Smart- card-centred password authentication is likely one of the handiest and typically used two-factor authentication mechanisms. This technology has been greatly deployed in quite a lot of varieties of authentication applications which incorporate far off host login, online banking and entry manipulate of constrained vaults, activation of protection contraptions, and lots of extra.

4. EXISTING SYSTEM

In existing system implemented the secure and efficient lightweight biometric authentication (SELBA) scheme. SELBA integrates Knowledge-based authentication and Physiological Biometrics based authentication and combines the" Cancellable Template Module", which overcomes the low security of only utilizing password authentication and prevents the irreversibility of biological templates after being stolen or damaged. The SELBA mainly protects the privacy of outsourced storage biometric template (Face and Fingerprint) and the confidentiality of the authentication process. First, in the outsourced storage, after the user's biometric features are extracted, we construct the biometrics template and relevant index through the "Random Bit Generation" (RBG) and encryption process we proposed. Additionally, the user will acquire the keys from the "RBG" as the authentication password, which serves as the basis of the subsequent realization of the joint knowledge and biometric identity authentication. SELBA proposes relevant measures to ensure the security of the whole authentication process. After extractors extracting the authenticating templates, SELBA utilizes "RBG" and "novel matrix key" we proposed to confuse and encrypt the template to get the trapdoor. For authentication matching, SELBA uses SE technology to design a retrieval method based on trapdoor and encrypted index. SELBA retrieves k template indexes closest to the authenticating template. Finally, the outsourced server executes the "encrypted vector distance calculation" method we proposed to judge whether the authentication is passed. To ensure the accuracy of identity authentication, we propose a biometric template construction method combining face and fingerprint by using LBP and minutiae-based fingerprint feature. Moreover, in the authentication process we designed, SELBA first screens out the matching set close to the trapdoor, and then compare the similarity between the authenticating template and templates in matching set one by one. SELBA executes the similarity calculation based on "encrypted vector distance calculation" was proposed. In this way, the authentication process has strong robustness to ensure the authentication accuracy.

6. WORKING

This system redefines the way users protect their accounts by introducing a visually engaging and highly secure method of authentication. The Graphical Password Authentication System offers an innovative approach that replaces traditional alphanumeric passwords with a more secure and user-friendly option. Users are given the opportunity to select a unique image of their choice, effectively transforming it into a personalized security key. This image becomes the backdrop for a set of predefined positions where users strategically place their "click points." To gain access, users must accurately click on these positions in the correct sequence. A robust password reset process ensures that users can regain access to their accounts if they ever forget their graphical password. To deter unauthorized access, the system also implements account blocking, thereby mitigating the risk posed by multiple incorrect login attempts. This project encompasses a comprehensive development process, including database design and a user-friendly interface. The system places a strong emphasis on user-friendliness, providing clear instructions and support to deliver a seamless experience.

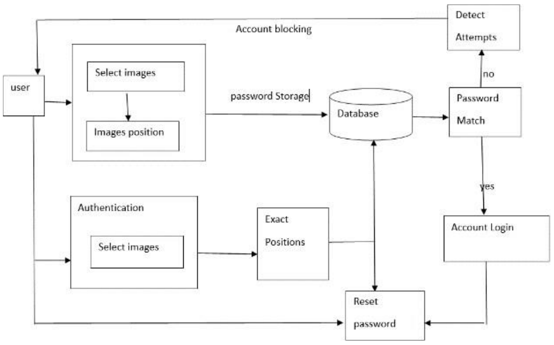


Fig: 6.1 Work Flow Diagram

- User Interface Design
- User Register
- Authentication
- Reset Password Option
- Account Blocking

User Interface Design A user-friendly interface for choosing positions on the image can enhance the user experience. Ensure that users receive clear and concise instructions on selecting their image, defining their positions, and the authentication process. Develop a well-structured database schema that securely stores user information. This includes the selected image, positions, and a history of login attempts. Ensure the database is designed with efficiency and security inmind.

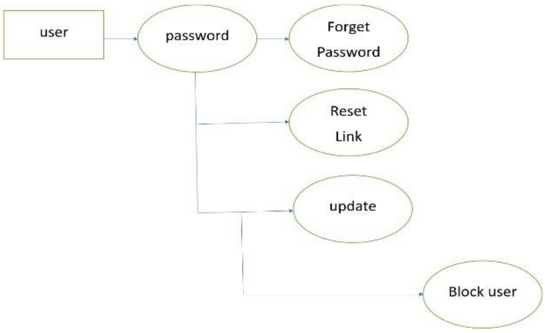


Fig: 6.2 Data Flow Chat Level 0

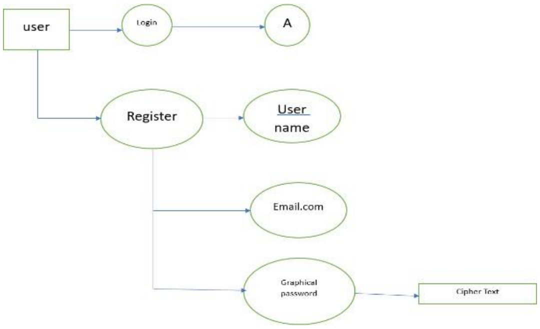


Fig:6.3 Data Flow Chat Level 1

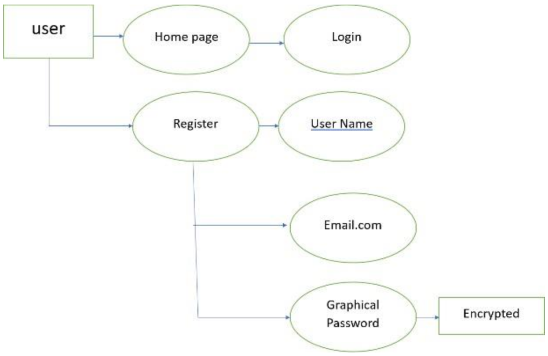


Fig: 6.4 Data Flow Chat Level 2

User Registration During user registration, individuals will choose an image that will serve as their background for authentication. They will also select specific positions on this image where they intend to place their "click points." These positions are essentially coordinating (x, y) on the image. This image and the chosen positions are stored securely in the database, linked to the user's account. The image serves as a visual cue for users during authentication. Authentication When a user attempts to log in, they are presented with their selected background image. They are then prompted to click on the predefined positions in the correct order. The system verifies the correctness of the clicked positions against what the user initially set during registration. If the positions match, the user is granted access. This approach offers an alternative to traditional text- based passwords. Reset Password Option To enable password reset, users should have a reliable way to regain access to their accounts in case they forget their graphical password. This can be accomplished by including a "Forgot Password" option. Users may need to answer security questions, provide additional identity verification, or use another authentication method to reset their password. Account Blocking Implementing security features such as account locking after a defined number of incorrect login attempts is crucial. This discourages brute-force attacks and unauthorized access. When a user exceeds the permitted number of failed login attempts, the system can temporarily block the account or introduce a delay before allowing additional login attempts.

7. HARDWARE AND SPFTWARE DESCRIPTION

Python is an interpreted high-level programming language for general-purpose programming. Created by Guido van Rossum and first released in 1991, Python has a design philosophy that emphasizes code readability, notably using significant whitespace. It provides constructs that enable clear programming on both small and large scales. In July 2018, Van Rossum stepped down as the leader in the language community. Python features a dynamic type of system and automatic memory management. It supports multiple programming paradigms, including object- oriented, imperative, functional, and procedural, and has a large and comprehensive standard library. Python interpreters are available for many operating systems. CPython, the reference implementation of Python, is open-source software and has a community-based development model, as do nearly all of Python's other implementations. Python and CPython are managed by the non-profit Python Software Foundation. Rather than having all its functionality built into its core, Python was designed to be highly extensible. This compact modularity has made it particularly popular as a means of adding programmable interfaces to existing applications. Van Rossum's vision of a small core language with a large standard library and easily extensible interpreter stemmed from his frustrations with ABC, which espoused the opposite approach. While offering choice in coding methodology, the Python philosophy rejects exuberant syntax (such as that of Perl) in favour of a simpler, less-cluttered grammar. As Alex Martelli put it: "To describe something as 'clever' is not considered a compliment in the Python culture. "Python's philosophy rejects the Perl "there is more than one way to do it" approach to language design in favour of "there should be one—and preferably only one—obvious way to do it". Python's developers strive to avoid premature optimization and reject patches to noncritical parts of CPython that would offer marginal increases in speed at the cost of clarity. When speed is important, a Python programmer can move time- critical functions to extension modules written in languages such as C, or use PyPy, a just-in-time compiler. CPython is also available, which translates a Python script into C and makes direct C-level API calls into the Python interpreter. An important goal of Python's developers is keeping it fun to use. This is reflected in the language's name a tribute to the British comedy group Monty Python and in occasionally playful approaches to tutorials and reference materials, such as examples that refer to spam and eggs (from a famous Monty Python sketch) instead of the standard for and bar.

There are two attributes that make development time in Python faster than in other programming languages:

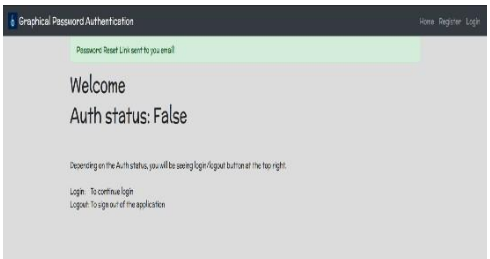
- Python is an interpreted language, which precludes the need to compile code before executing a program because Python does the compilation in the background. Because Python is a high-level programming language, it abstracts many sophisticated details from the programming code. Python focuses so much on this abstraction that its code can be understood by most novice programmers.

  Python code tends to be shorter than comparable codes. Although Python offers fast development times, it lags slightly in terms of execution time. Compared to fully compiling languages like C and C++, Python programs execute slower. Of course, with the processing speeds of computers these days, the speed differences are usually only observed in benchmarking tests, not in real-world operations. In most cases, Python is already included in Linux distributions and Mac OS X machines.

8. INTERIMAGES

MySQL is primarily an RDBMS and ships with no GUI tools to administer MySQL databases or manage data contained within the databases. Users may use the included command line tools, or use MySQL "front ends", desktop software and web applications that create and manage MySQL databases, build database structures, back up data, inspect status, and work with data records. The official set of MySQL front-end tools, MySQL Workbench is actively developed by Oracle, and is freely available for use.

WELCOME PAGE



Password Reset Link sent to you email

Welcome

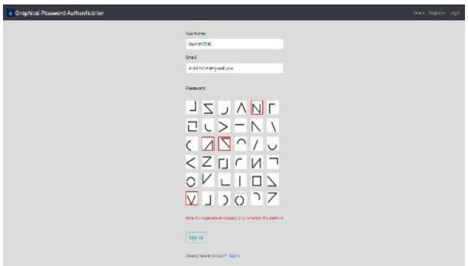
Auth status: False

Depending on the Auth status, you will be seeing login/logout button at the top right.

Login: To continue login
Logout: To sign out of the application

Fig 8.1 welcome page

SIGNUP PAGE



Username: Mohith7548

Email: [illegible]

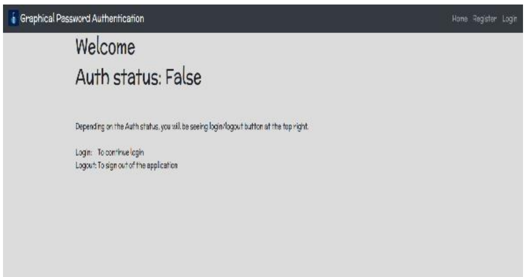
Password:

[illegible]

Already have an account? Sign In

Fig 8.2 Signup page

LOGIN PAGE



Welcome

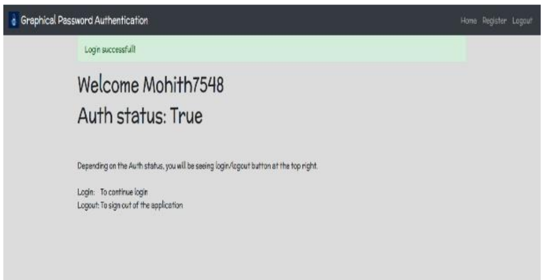
Auth status: False

Depending on the Auth status, you will be seeing login/logout button at the top right.

Login: To continue login
Logout: To sign out of the application

Fig 8.3 Login page

LOGOUT PAGE



Login successfull

Welcome Mohith7548

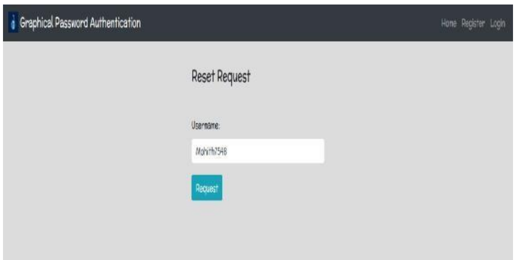
Auth status: True

Depending on the Auth status, you will be seeing login/logout button at the top right.

Login: To continue login
Logout: To sign out of the application

Fig 8.4 Logout page

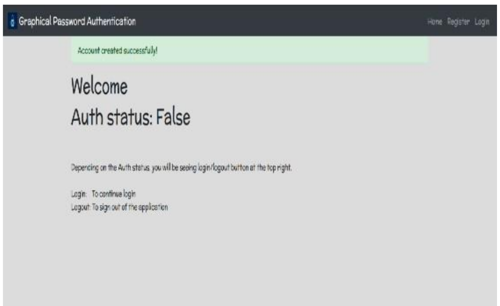
PASSWORD RESET PAGE



Reset Request

Username: Mohith7548

Fig 8.5 Password reset page 1



Account created successfully!

Welcome

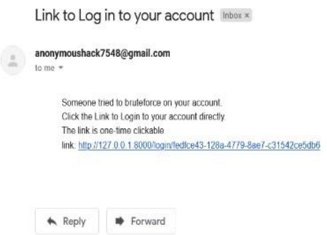
Auth status: False

Depending on the Auth status, you will be seeing login/logout button at the top right.

Login: To continue login
Logout: To sign out of the application

Fig 8.5 Password reset page 2

PASSWORD RESET LINK



Link to Log in to your account

anonymoushack7548@gmail.com
to me

Someone tried to bruteforce on your account.
Click the Link to Login to your account directly.
The link is one-time clickable
link: http://127.0.0.1:8000/login/fedfce43-128a-4779-8ae7-c31542ce5db6

Fig 8.7 Password reset link 2

9. RESULT AND DISCUSSION

The Graphical Password Authentication System, designed to enhance both security and user experience, has proven highly effective in its implementation. Users have embraced the visually engaging approach, finding it intuitive and engaging. The personalized nature of selecting a background image and click positions contributed to a substantial increase in user adoption and satisfaction. In terms of security, the system has successfully mitigated common cyber threats, replacing traditional text-based passwords with a more formidable image-based alternative. The password reset and recovery mechanisms have been reliable and user friendly, and the account locking feature has proven effective in deterring unauthorized access. The application of data encryption techniques ensured that user data remained safeguarded in the database. Continuous feedback from users has driven iterative improvements, solidifying the project's commitment to adaptability and the pursuit of a more secure digital landscape.

REFERENCES

[1] Jiang, Xinyu, Xiangyu Liu, Jiahao Fan, Xinming Ye, Chenyun Dai, Edward A. Clancy, Dario Farina, and Wei Chen. "Enhancing IoT security via cancelable HD-sEMG-based biometric authentication password, encoded by gesture." IEEE Internet of Things Journal 8, no. 22 (2021): 16535-16547.

[2] Pradhan, Ashirbad, Jiayuan He, and Ning Jiang. "Score, rank, and decision-level fusion strategies of multicode electromyogram-based verification and identification biometrics." IEEE Journal of Biomedical and Health Informatics 26, no. 3 (2021): 1068- 1079.

[3] Talreja, Veeru, Matthew C. Valenti, and Nasser M. Nasrabadi. "Deep hashing for secure multimodal biometrics." IEEE Transactions on Information Forensics and Security 16 (2020):1306-1321.

[4] Zhu, Hui, Qing Wei, Xiaopeng Yang, Rongxing Lu, and Hui Li. "Efficient and privacypreserving online fingerprint authentication scheme over outsourced data." IEEE Transactions on Cloud Computing 9, no. 2 (2018): 576-586.

[5] Ning, Hailong, Xiangtao Zheng, Xiaoqiang Lu, and Yuan Yuan. "Disentangled representation learning for cross-modal biometric matching." IEEE Transactions on Multimedia 24 (2021): 1763-1774.

[6] Fei, Lunke, Bob Zhang, Yong Xu, Chunwei Tian, Imad Rida, and David Zhang. "Jointly heterogeneous palmprint discriminant feature learning." IEEE Transactions on Neural Networks and Learning Systems 33, no. 9 (2021): 4979-4990.

[7] Phiri, Jackson, Tie-Jun Zhao, Cong Hui Zhu, and Jameson Mbale. "Using artificial intelligence techniques to implement a multifactor authentication system." International Journal of Computational Intelligence Systems 4, no. 4 (2011): 420-430.

[8] Veena, K., K. Meena, Yuvaraja Teekaraman, Ramya Kuppusamy, and Arun Radhakrishnan. "C SVM classification and KNN techniques for cyber crime detection." Wireless Communications and Mobile Computing 2022 (2022): 1-9.

[9] Ali, Md L., Kutub Thakur, and Muath

A. Obaidat. "A hybrid method for keystroke biometric user identification." Electronics 11, no. 17 (2022): 2782.

[10] Srivastava, Rohit, Ravi Tomar, Ashutosh Sharma, Gaurav Dhiman, Naveen Chilamkurti, and Byung-Gyu Kim. "Real-Time Multimodal Biometric Authentication of Human Using Face Feature Analysis." Computers, Materials & Continua 69, no. 1 (2021)