Journal of Carcinogenesis
Covering Genesis to Therapeutics
Journal of Carcinogenesis, ISSN: 1477-3163
2025; Vol 24: Issue 8s, https://carcinogenesis.com/

Hybrid Images with Biometric Authentication to Avoid Shoulder-Surfing Attacks

Rahaf Alzahrani[1], Enas Khairullah[2]

[1]Faculty of Computing and Information Technology, Computer Science Department, King Abdulaziz University, Jeddah, Saudi Arabia - KSA

Email ID: rattiahalzahrani@stu.kau.edu.sa

[2]Faculty of Computing and Information Technology, Information Technology Department, King Abdulaziz University, Jeddah, Saudi Arabia - KSA

Email ID: ekhairallah@kau.edu.sa

ABSTRACT

A shoulder-surfing attack aims to acquire personal data such as passwords and sensitive user credentials. It does not require special technical knowledge, just observation of the user's inputs. The rapid advancement of surveillance technology and covert tools, including closed-circuit cameras, is leading to an increase in shoulder surfing attacks. To resist them, an authentication approach is proposed that combines several defensive techniques, such as an Illusion Personal Identification Number (IPIN), entered via a virtual keypad. The approach employs a hybrid image displaying two keypads, or a hybrid keypad overlaying another designed for direct and indirect lines of sight, seeking the shortest distance at which an attacker is incapable of tracking the inputs. The approach uses an innovative algorithm to shuffle the keypads for each authentication session, as well as a novel keypad pattern exclusive to the IPIN. Even if an attacker remembers the spatial layout of the keypad, they will be unable to trace the IPIN in the next session. To provide more security, the IPIN approach has been added to biometric authentication (fingerprint) and one-time-password (OTP) verification to proposed a new approach to prevent this kind of attack. The proposed approach was tested in terms of usability, clarity, user awareness of an attack, and ease of use of these blended techniques. The suitability of the proposed approach was examined for vital departments within organizations. In addition, the proposed approach was compared with other authentication systems to gauge resilience against certain attacks. The results are promising, although as an authentication approach, continuous enhancements are required, including testing with a larger number of users.

Keywords: *Shoulder-surfing attack, Hybrid Image, Illusion-PIN (IPIN), OTP, Biometric Authentication.*

How to Cite: Rahaf Alzahrani, Enas Khairullah, (2025) Hybrid Images with Biometric Authentication to Avoid Shoulder-Surfing Attacks, *Journal of Carcinogenesis*, *Vol.24, No 8s*, 17-32

1. INTRODUCTION

Shoulder surfing is a prevalent type of attack that is more likely to occur in crowded environments and because of the ubiquity of surveillance cameras. This type of attack can reveal data that could lead to the leakage of sensitive information. It is not necessary to have any technical knowledge to carry out such attacks, and all that is required is a keen observation of the user's behavior [1]. As such, shoulder-surfing attacks draw the attention of many researchers in the technology security field. As an example, in a supermarket, a user has finished shopping then joins the queue at the cash desk and intends to pay via a credit card. When it's the user's turn, the cashier gives them a Point of Sale (POS) device, into which their card is inserted followed by their PIN. The user feels safe using this system because the person behind them is supposedly looking at their phone, watching a YouTube video or reading some news website (or so the user thinks). Instead, the person behind them is recording the user's finger movement tracking the numbers entered on the (POS) device, which has a keypad like the touch screen on a phone, to obtain the user's PIN [2]. As a result, a text-based password is not enough. A combination of many types of authentications in addition to (OTP) verification technique will help to prevent this kind of attack [3]. Graphic graphical authentication incorporates image-based authentication where proven to be effective in terms of the user and the time it takes to remember the password [4-6]. A hybrid image is a technique that created an optical deception using images, in which two different images with different spatial frequencies are superimposed. Thus, the hybrid images looked different at different distances. Accordingly, the perception of the image depended on the distance of the person viewing the image. It as an expression of a combination of two keypads with a different digital order. One is high frequency, and one is low frequency. This technique is mainly used in devices that support touch screens, such as an Automated Teller Machine (ATM), computers, and smart mobile devices [7].

Moreover, biometric authentication is a security process that relies on the unique biological characteristics of a user to verify their identity. Biometric authentication systems compare physical features, such as fingerprints, a palm print, hand geometry, eye (iris and retina), and face shape. Or behavioral patterns, such as voice recognition, keystroke dynamics, gestures, and signature dynamics (pen movement speed, acceleration, pressure exerted), with data stored in a database. Thus, if both samples of biometric data match, authentication is confirmed [8]. Biometric authentication, particularly fingerprint, represents the most powerful current solution that supports authentication for the following reasons [8-11]:

- Uniqueness: fingerprints differ even between identical twins. Thus, it makes it possible to distinguish between one person or another.
- Convenient: users are not required to remember various, long, complex and constantly changing passwords.
- Recordable (with or without consent): ensures that users cannot repudiate their presence at the time of recognition or later deny they had access to the system.
- Non-transferable: unlike passwords, PIN, or smart card, fingerprints cannot be shared, stolen, lost, copied, distributed, or forgotten.
- The possibility of proving forgery: this is especially the case for biometric authentication (face pattern or fingerprint).
- Proven: fingerprint recognition has a long history of success in identifying tasks, with the United States and other countries having substantial real-world experience with fingerprint recognition.

In this research, the goal is to reduce especially shoulder-surfing attacks against standard PCs, but also touch mobile devices. Thus, in the proposed approach, the secure login method requires a two or three-way procedure to complete the authentication process and entering a password via a virtual keyboard that uses hybrid image technology to produce an illusion-PIN (IPIN). The spatial arrangement of the keys is shuffled randomly for each authentication process to increase the level of security for inputting user credentials. Along with this, a fingerprint is captured by the fingerprint reader device to provide a unique identifier to the user, thus sending a one-time password (OTP) for the purpose of verifying the matching of user credentials though a random set of password elements with a specified expiration period to improve the security of the approach. As a result, the proposed approach provides high security against shoulder- surfing attacks, attacks that simulate such an attack, such as dictionary, spyware, keystroke/mouse logger, and brute-force attacks. Moreover, hybrid graphical authentication improves user awareness and usability. The proposed approach has high resilience in terms of the additional hardware needed where this approach can be adopted according to an organization's requirements.

2. RELATED WORK

In [7], an improved version of IPIN has been proposed. It aims to reach a higher authentication rate and reduce the process time. The proposed method improved the IPIN by shifting the drawing area of the high-frequency digit slightly from the area of the low-frequency digit, allowing both digits to be clearly seen. According to the results, the authentication success rate increased from 76 % with the original IPIN to 95 % in the improved method, increasing the usability of the authentication process within a shorter period and successful authentication. This enhanced version needs further investigation of the fonts and image processing parameters before implementation in real applications, as well as experiments detailing video recording attacks.

In [1], some additional authentication schemes have been introduced. The first is an IPIN on a digital screen. It applied hybrid images with two intermingled keypads, designed for human eyesight. It determined the minimum distance at which an attacker will be incapable of understanding the keys. Second, an innovative shuffling algorithm randomly programmed the keys for each PIN entry. Third, an OTP generation technique increased security along with the algorithm, offering promising results against shoulder-surfing attacks. However, for the convenience of older users, the screen displayed the digit being entered is not clear. This means that this IPIN technique is not suitable for all users, which reduces the efficiency of the system.

In [14], a new algorithm is proposed for an authentication system using IPIN with hybrid images to prevent shoulder-surfing attacks. It blended two plates with numbers in a different order using hybrid images and the user's keypads are shuffled on each authentication attempt. The Meaning a Structural Similarity Index (MSSIM) 10 index value is used to calculate the visibility index. based on image-based authentication using IPIN (IBAUIP). The algorithm calculates the visibility index and compares it to the value, due to the algorithm's reliance on MSSIM. Since the threshold value will vary for different observers, the global setting corresponds to people with the best vision. This setting, though, can lead to confusion and mislead a user with worse vision when entering the log-in password, thus taking a long time during the authentication process and resulting in less usability. Furthermore, if the PIN is entered incorrectly, the user starts over, and the PIN is vulnerable to a brute force attack.

In [15], a three-layer validation strategy is proposed to improve ATM machine authentication. The first layer supports authentication based on biometrics using facial recognition and a fingerprint. The second layer provides SMS verification via OTP with reverse processing. The third layer is the hybrid keypad application. This proposal enhanced security on the client side, but on the server side it is vulnerable to attack in the event of a login failure as the login is attempted again without sending an alert to the client, making it subject to a brute force attack. Moreover, the reverse OTP token verification mechanism may be vulnerable to man-in-the-middle attacks.

In [16], three defensive techniques have been presented based on camouflaged characters for mobile devices using the Android platform. The proposed techniques employed two main keys (enable/disable). The user enters any number of camouflage characters randomly followed by correct password characters in the enable key. The user then enters the disable key, followed by any number of random camouflage characters. The implementation of this mechanism in the three defensive techniques varies according to the length of the camouflaged letters (user-specified enable/disable keys are same length/variable length/one character each) According to experiments and tests, the third technique demonstrated the highest efficiency. It allows for a complex set of characters that mask the actual password and thus resist a shoulder- surfing attack. On the client side, however, the technique consists of complex usage mechanisms that may confuse the user and require more time while entering the password, thus weakening usability. On the server side, the use of these techniques makes the password long and requires a large amount of storage space

In [17], an authentication process is proposed that combines biometrics with hybrid security technology based on facial recognition and graphical password authentication. The proposed system first employed facial recognition, then the user's password is recorded as a set of images (four of the nine images presented to them). In addition, for each login, the images are displayed in a different order and with random symbols. The proposed authentication process may be limited by the different lighting conditions that may affect the facial recognition rate, possibly requiring a longer time and reducing efficiency. Moreover, despite random distribution of numbers and symbols, some are repeated on more than one image, which can be extracted to crack the password.

In [7], hybrid graphical password technologies (graphic password) have been proposed and comprised an alternative technology based on the pass-image scheme (recall-based techniques). Users choose their favorite images to compose a password. Because this stage is considered easy to predict and therefore vulnerable to attack, this research proposed to improve it by presenting an image in the form of a 6x5 array, meaning it is displayed in 30 cells, and then the user enters their username and text password in addition to the preferred image. The "graphic password" is stored in the database as a text password, thus saving storage space. While this scheme is implemented a fix-based method only on the client side, on the server side, the password contents are stored as text, which is vulnerable to attack.

In [6], an image-based authentication system with a graphical password and validation by interpreting images via pass object, skip object, and flag object has been implemented. The objects have been classified for the purpose of transmitting hidden messages during the authentication process, which comprises several stages to provide the password, which thus affects usability. Moreover, the number of images included in each password application screen during authentication affects storage space and ease of use. And because information security is sequential, this will affect the security aspect of the proposed solution.

In [18], investigation strategies have been presented that contribute to preventing shoulder-surfing attacks on users to establish and develop effective methods to overcome shoulder-surfing activities while using mobile device-based interactions. The strategies have been categorized based on the effort expended and the user's awareness of their needs. Furthermore, strategies include distracting observers, changing the way they interact, and masking the device in various ways. This proposal requires more investigation on different groups and environments to sharpen results.

In [19], a mobile application called DSSytem has been introduced to detect over-the-shoulder surfers. It communicated the concept of shoulder-surfing attacks to the user to create awareness in the user. The DSSytem application employed the user-facing camera to detect shoulder surfers and their position in blind spots behind or to the user's side. The user is notified via vibro-tactile feedback, iconic screen overlay, live video streaming, or front LED blinking. According to the testing statistics, for many people, vibration proved to be the best warning, because it notifies the user only, not the shoulder surfer. This proposal requires an accurate camera set up in order to detect whether a potential attacker is nearby.

In [20], it is proposed to investigate and estimate the gaze of potential attackers and thus check whether potential attackers are looking at the user's screen (e.g., mobile phone). An algorithm that used gaze estimation techniques using the front camera of the phone and Google Vision API face detection methods can identify shoulder surfers and distinguish them from passing spectators by estimating the gaze period. The system then notifies the user of any incident. There are some limitations regarding the devices that can be used, such as smartphone cameras, which are not effective compared to dedicated eye trackers. Moreover, the proposed mechanism may lead to increased battery consumption and the relatively limited processing power of smartphones.

In [21], a methodology is presented of 360-degree videos in virtual reality (VR) with eye tracking to investigate surveillance attacks. It recorded 360-degree videos, and then displayed them on a head-mounted screen. The evaluation of gaze behavior

is carried out by eye-tracking in the direction of the phone. The results showed that all participants peeked at the phone at least once, with an average duration of 3.5 seconds. Short glances may be sufficient to reveal the content and thus violate an individual's privacy. In this methodology, the resolution of the camera limits the readability of the textual content of the phone. Moreover, VR cannot represent all aspects of the real environment.

In [22], the authors introduced a study of how relationships affect shoulder surfing through an analysis of 11 modern strategies aimed at mitigating an attack. According to the results, users prefer to hard-to-observe and unclear mechanisms that do not affect personal relationships with the observer, and screen distortion filters for siblings, family, and friends. This analysis demonstrated that appropriate action is taken based on the user's relationship with the observer. The analysis, though, was based on a pool too small and should be expanded.

In [23], it is proposed to combine script and graphical password schemes to develop an authentication method that is less vulnerable to attacks. The scheme contained two authentication steps. The user must learn their graphical password, then set up the text password. After the user chooses a password image, it is distorted and becomes the user's "password". Distortion of password images may cause confusion for some users and requires increasing the space for passwords in the image library.

In [24], a password system is offered that combines both graphical and textual password authentication methods called PassTag. The mechanism consisted of a secret image provided by the user, hence a text description of an image (meaning a text password). The system generated decoy images while the user completes the authentication by completing the password. User-supplied images improve the memorization of text passwords. This system was performed on a small sample size, however, and was predominantly a young age group in a controlled environment. The participants were unwilling to use specific secret passwords for studies of real-world applications. Thus, there is a research gap in terms of the suitability of this system for all users.

In [29], investigates the vulnerabilities of Personal Identification Numbers (PINs) in Unstructured Supplementary Service Data (USSD) transactions, particularly within the context of financial services in developing countries like Nigeria. Given that USSD transmits data in plain text, users' PINs are susceptible to shoulder surfing attacks. The study underscores the necessity for a secure authentication model compatible with USSD's textual constraints. It proposes a challenge-response mechanism with randomization obfuscation to protect PIN entry, supplemented by features such as Bag of Soft Biometrics (BoSB) and One-Time Passwords (OTP) to enhance security. This contribution aims to advance mobile security measures in financial transactions where USSD is widely utilized.

In [30], examines the vulnerabilities of recognition-based graphical password (RBGP) methods, particularly their susceptibility to shoulder-surfing attacks (SSAs). While graphical passwords are favored for their user-friendly design and enhanced security, many existing techniques remain exposed to unauthorized observation, allowing attackers to capture user interactions in public settings. A systematic review identified 28 RBGP schemes, highlighting significant variations in their effectiveness against different SSA types. The findings indicate that while some methods can prevent direct observation, they may still be vulnerable to video capture and pattern analysis. This study addresses a critical gap in the literature by providing a comprehensive assessment of RBGP techniques, emphasizing the need for improved defenses against SSAs and guiding future research toward more secure authentication solutions.

In [31], examines the security vulnerabilities of graphical password (GP) systems, particularly their susceptibility to attacks such as shoulder surfing, SQL injections, and spyware. A comprehensive review of 16 key studies identified 19 distinct attack types, with shoulder surfing and brute force attacks being the most prevalent. The literature categorizes countermeasures into three main strategies: randomization, obfuscation, and password space complexity. While these measures have demonstrated some effectiveness, none provide complete protection, highlighting the need for ongoing research to enhance security. This study emphasizes the importance of a multidisciplinary approach that integrates insights from security, psychology, and design to develop more robust graphical password solutions capable of addressing evolving threats, especially those leveraging advanced technologies like deep learning.

In the Table below Table 1, we categorize the studies based on technique, objectives, strengths, and weaknesses

Ref.	Year	Technique (s)	Objective (s)	Strength (s)	Weakness (es)
[16]	2021	Camouflaged characters with enable/disable key techniques.	Hide the password within a set of randomly selected entries.	Ensured that the password remained hidden by the large number of keystrokes.	Very simple passwords but a complex mechanism for the user.
[17]	2018	Hybrid-security technology based on facial recognition and graphical passwords.	Ensure that the password remains hidden between a large number of keystrokes.	Scores high in security, ease of use, and reliability from surveys.	Various factors may influence the quality of the facial recognition part.
[2]	2021	360° Video Technique in Virtual Reality (VR).	Contributes to the body of knowledge about surfing through new methodologies.	Created a realistic experience through gaze data analysis.	Virtual reality cannot represent all aspects of the real environment.
[4]	2021	Hybrid graphical password technologies based on recall-type techniques.	Overcomes security and usability problems that face graphical password schemes.	Does not require any additional or expensive hardware.	Allows the use of images for authentication, similar to previous proposals.
[6]	2018	Graphical password techniques.	Transmission of hidden messages during the authentication process.	Provides secure and usable systems compared to textual passwords.	The stages of multiple authentication mechanisms affect usability.
[18]	2019	Investigation of strategies to prevent shoulder surfing from the users' perspective.	Develop effective ways to design useful interactions that overcome shoulder-surfing attack issues.	Measures users' awareness and effort as they experiment with authentication processes.	Need for further studies with diverse user groups.
[19]	2018	DSSytem application mechanism for front camera and notifications.	Protecting the user against shoulder-surfing attacks throughout interaction.	Vibro-tactile feedback resulted in the lowest reaction time by participants to potential attacks.	Camera resolution may be a key factor.
[20]	2020	Front camera of the phone and Google Vision API face detection.	Eliminate the possibility that an attacker is standing nearby and not looking at the user' s device.	Reduced the number of false notifications disturbing the user.	Some limitations regarding the devices.
[29]	2024	Challenge-response mechanism, randomization, OTP	Investigate PIN vulnerabilities in USSD transactions and propose a security model.	Enhances security for financial transactions.	Susceptible to shoulder surfing due to plain text.
[30]	2023	Systematic review of 28 RBGP schemes	Examine vulnerabilities of graphical passwords against shoulder-surfing attacks.	Identifies varied effectiveness against SSAs.	Vulnerable to video capture and pattern analysis.
[31]	2024	Review of 16 studies, categorization of countermeasures	Review vulnerabilities of graphical password systems against multiple attacks.	Highlights need for multidisciplinary approaches.	None of the countermeasures provide complete protection; ongoing research is needed.

3. THE PROPOSED AUTHENTICATION APPROACH

The proposal offers an enhancement of the authentication process by using innovative and flexible authentication techniques that complement each other to meet the needs of organizations and their environments. It also bridges a gap left by most previous research, which revealed weaknesses in various biometric authentication technologies in terms of cost and requirements for adding hardware, which could be problematic for some organizations.

The proposal aims to develop authentication techniques using a shuffling Illusion-PIN (IPIN) keypad for entering a password or performing any authentication process, as well as utilizing fingerprint biometrics to achieve more accurate authentication. The one-time password (OTP) is used to validate the correctness of the data submitted by the user.

3.1 Graphical Authentication Phase

The process of graphical authentication using the hybrid image technique to create a virtual keypad for IPIN consists of two keypads overlayed into a seemingly single image with digits in different arrangements: a low-frequency keypad presents the digits in the original, or normal, order, while a high-frequency keypad behind it presents randomly arranged digits. Hence, a client close to the device can see both keypads, while an attacker, who is viewing the device from afar, can see only the front keypad of low frequency and original arrangement.

As an improvement on this technique, we edited an existing algorithm that shuffles the high-frequency keypad for each exclusive PIN entry. Namely when the PIN is entered as a password on the keypad, the spatial arrangement of the keys is shuffled to enter the next PIN. The shuffle algorithm allows for digits 0 to 9 as inputs into the array. Then, a function is called to generate a random digit each time and store it in the array to avoid repeating the digit in the same place twice. In addition, the elements are swapped in the process. Thus, the shuffling algorithm is used to change the positions of the digits in the keypads randomly. As a result, even if an attacker memorizes the squeezed digits' spatial manipulation, they are unable to track the PIN. The combination of the two keypads results in overlapping of the graphic regions of the two keypads, which may result in an increase in the authentication process time, affecting the usability and reducing the security of the system [7]. Accordingly, we upgraded our approach and shifted the keypad digits behind the low-frequency ones from the left margin by 0.5 pixel. The margin was determined after conducting many experiments in the code until the optimal clarity was reached. We noticed that when testing lower values, this margin unlike larger values allowed the graphic areas of both keyboards to mix. This reduced the possibility of user confusion when entering the password, and therefore authentication is carried out in a shorter time, boosting the level of security.

3.2 Biometric Authentication Phase

Fingerprint recognition in our research was set in two different modules: registration module and login module, which is linked to the verification process, as shown in the figure below Fig. 1.

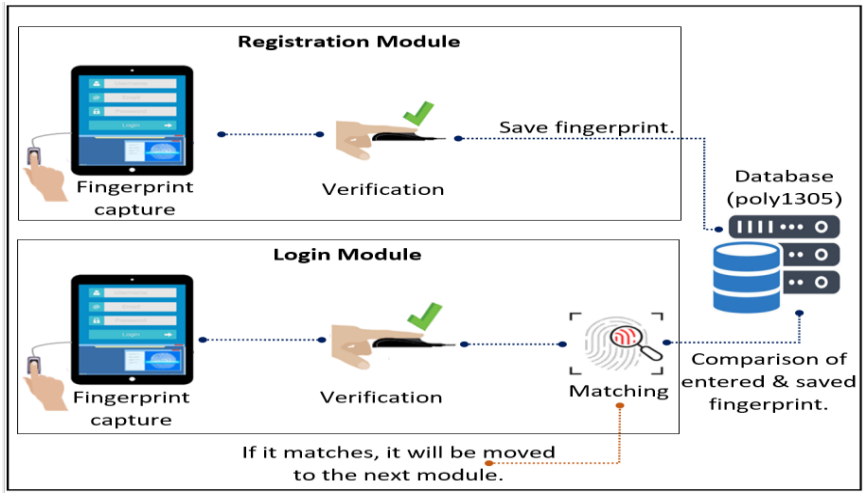


Fig. 1. Fingerprint Recognition Mechanism

The registration module is used to register credentials for users. and requires the following: the first name, last name, e-mail, and the username, in addition to the password. Then comes the hardware (fingerprint reader), which captures fingerprints. To ensure a high-quality scan, the reader checks the quality of the image entered by the user. In the database, the fingerprints are saved in an encrypted form encryption algorithm poly1305 based on the Advanced Encryption Standard (AES) but with Message Authentication Code (MAC) for verify the data integrity and the authenticity of a message.

The login module through which verification is carried out and verification of the user's credentials is applied requires the following:

- Filling in the username and password fields.
- Fingerprints are captured by the fingerprint reader.
- The fingerprint is compared with the one registered in the database to check whether the two biometric samples are identical.

If they match, the process will move to the next authentication phase, which is OTP verification.

3.3 One-Time Password (OTP) Phase

OTP authentication ensures that the IPIN password and fingerprint match data stored by the user in the registration process. In this research, we chose to send the verification code via e-mail. When the code is entered in the field assigned to it, authentication is performed using a keypad with IPIN technology to further raise the level of security. This phase of authentication has flexibility in the sense that it is optional. The architecture of the proposed approach is shown in Fig. 2.

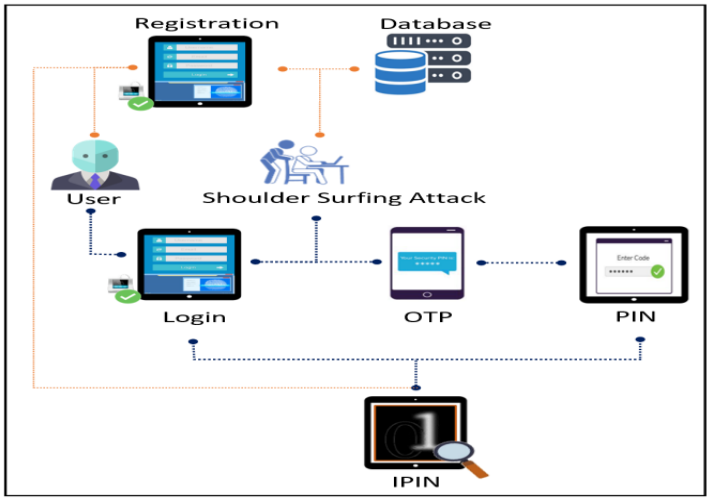


Fig. 2. Architecture of Proposed Approach.

4. IMPLIMANATION

The prototype of the proposed approach was built by designing, programming, and developing the three primary modules, namely registration, login module, and OTP verification, as well as the two secondary modules which make up the process flow, namely the profile and logout modules.

4.1. Implementation Environment

The Visual Studio Code editor was used to build and develop the web applications. We used the HTML language to create and design the front pages of the modules, including the registration page, login page, OTP verification page, profile page, and logout page, and the CSS language for the pages and buttons on the virtual keypad. Using the PHP language, we created the scripts for user access control and connection with the database and local host, in addition to calling the PHPMailer library. JavaScript was used to invoke the JQuery library to program virtual keypad functions. We installed the SDK package for the DigitalPersona 4500 fingerprint reader. To encrypt the fingerprint format in the database, we use the Sodium cryptography library. And XAMPP as a development environment for a virtual local web server, as well as MySQL to create a database for the purpose of storing the customer data which each new user was required to register.

4.2. Modules in the Proposed Approach

The techniques for the interface screens provided by the proposed approach are as follows:

Registration Module: We created a registration page using HTML, as shown in Fig. 3. This page requires the user to enter personal information including first and last name, email, username, and password, in addition to a fingerprint capture scan. When the user has ensured all the fields on the page have been filled and the fingerprint capture has been scanned, they click on the "Submit" button.

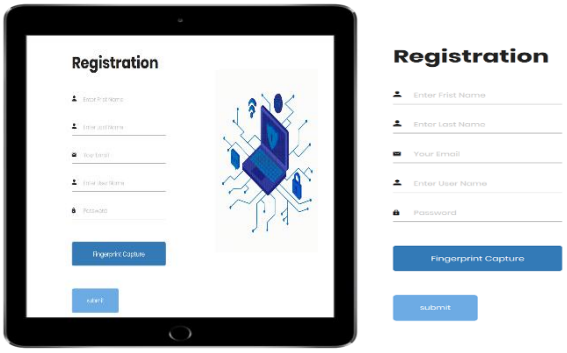


Fig. 3. Registration Module

Fingerprint Capture in the Registration Module: When you click on the "Capture Fingerprint" button in the registration module, a pop-up window will appear called "Create Enrollment," as shown in Fig. 4. The fingerprint is captured in the registration Module four times, according to the recommendation of [25], which stated that at least two fingerprint capture processes should be provided to ensure that a clear sample is taken from all sides and angles of the finger. In addition, the choice of the index finger was based on [25], who stated that it is often recommended to use the index or middle finger, because they are less worn.

After the process of capturing the index finger four times is complete, the user presses the "Complete Fingerprint" button to store the fingerprint value in Fingerprint Minutiae Data (FMD) format. This is stored in a hidden HTML element; the rationale for placing it in a hidden element is that the fingerprint value is very long, and, as it is an unreadable digital representation, there is no point in showing it to the user.

Fig. 4. Capture the Fingerprint in the Registration Module

Login Module: In the login module of the application in the proposed approach, the user must enter their credentials, which were created in the registration step, as shown in Fig. 5, which include username, password, and fingerprint capture scan, if any.

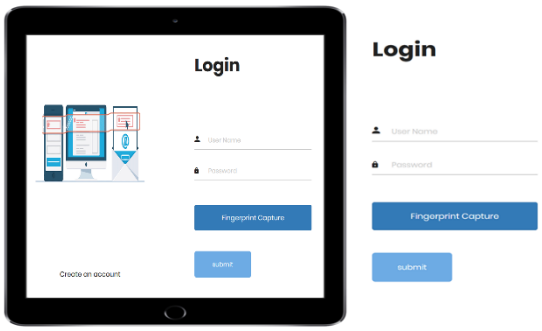


Fig. 5. Login Module

Capturing the Fingerprint in the Login Module: Clicking on the "Capture Fingerprint" button in the login module causes a pop-up window to appear with the name "Identity Verification," as shown in Fig. 6. The "Capture Fingerprint" pop-up window in the login contains all the characteristics of the registration window; the difference between the two lies

in the most important function, which is verification. Accordingly, one icon has been placed to capture the index finger, and therefore requires one capture process for the purpose of verification.

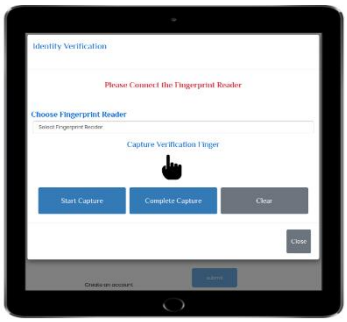


Fig. 6. Capture the Fingerprint in the Login Module

Verification Module: The OTP verification module comes after the user credentials entered at the login stage are matched with the data saved in the database at the registration stage. If the data is verified and valid, a verification code is sent to the user's email consisting of four random digits, utilizing the PHPMailer library and tuned with the local server settings, and then programming it with an algorithm to generate random numbers to produce one-time passwords during the authentication procedure, as shown in Fig. 7. This code is valid for a specific time, as programmed.

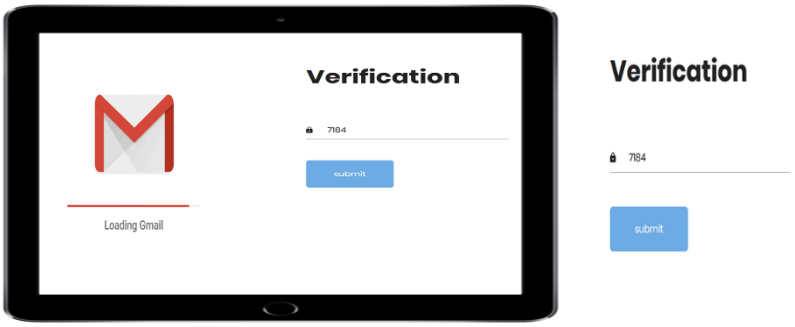


Fig. 7. Verification Module

Virtual Keypad: In the Registration, Login, and OTP Verification modules, clicking on the Password and OTP Verification fields causes a popup window to appear for the illusion-PIN IPIN virtual keypad so the personal identification number can be entered. The interface looks like a digital keypad, consisting of nine numbers and two icons. The icon on the right is a backspace icon, which is used for deleting, while the square icon above is used to hide the window, as shown in Fig. 8. This keypad follows the same mechanism as the hybrid image, in which the user can select the shaded digit that appears behind each digit in the foreground keypad. Thus, if we press on the digit shown on the front keypad, the other digit, behind the pressed number, will appear, meaning there is another keypad behind the main keypad, which can consequently be called a hybrid or blend keypad. If the user wants to perform another actual transaction and log into the application again, they do not get a keypad with the same spatial arrangement of background numbers. Hence, when any authentication process is performed, the spatial arrangement of the digits on the keypad shuffles automatically.

Fig. 8. virtual keypad

5. RESULTS AND DISCUSSION

5.1 Determining the Suitability of Approach to the Organization

Fingerprint biometric authentication is prohibitively expensive and may require the addition of devices for a specific organization. The proposed defensive approach, with its three techniques, may satisfy the security requirements of certain sections in the organization and thus provide security against shoulder-surfing attacks. Therefore, we conducted a comparison to demonstrate the efficacy of the proposed defensive techniques in the most critical departments of the organization. By default, important departments of the organization are classified according to the importance of the information assets they contain, based on certain local and international regulatory frameworks and standards, including National Cybersecurity Authority (NCA) controls [26], International Organization for Standardization (ISO) 27001 standards [27] and the National Institute of Standards and Technology (NIST) cybersecurity framework [28], as shown in Table 3.

Table 2. Organizational Departments are Classified Based on their Information Assets

Organization Departments	Assets	Classification
Cyber Security Department.	Networks, information technology systems, operational technology systems, their hardware and software components, the services they provide, and the data they contain, in addition to backup copies, portable devices, monitoring of event records and physical security.	Restricted Information.
Human Resources Department.	Sensitive data for employees from contracts and agreements and their procedures from security surveys and awareness of cyber security requirements and review of cyber security requirements related to workers from access privileges.	Restricted Information.
Information Technology Department.	Networks, servers, storage, applications, and services.	Restricted Information.
Finance and Accounting Department.	Network devices, operating systems, applications, and files.	Restricted Information.

We can see from table 3 that the more importance assets a department contains that require high security, the higher the rate of application and adoption of defensive techniques proposed for this department should be. The Cybersecurity Department is top-ranked, as it includes the concept of information security, electronic security, and digital security, based on what [26] states is the highest evaluation, and assets that require high protection.

5.2 Comparison with Other Authentication Architectures.

We compared the proposed approach with the other authentication system techniques. Security attacks were utilized as a comparison parameter, as shown in Table 4. We use a three-point rating system (Strong, Moderate, Weak) to measure the security of the system techniques against a specific attack, with this rating indicating the effort necessary to crack the

password using a particular attack. A "Strong" score implies that breaking the password demands a significant amount of effort, and hence the system has a high level of resilience against a specific element of attack. A "Moderate" score indicates that the system is resilient to a specific attack on a medium level, while a "Weak" score shows that the system is vulnerable to a specific attack on a low level.

Table 3. Comparison of Different Authentication Approach Against Various Security Attacks

Approach/System	Shoulder-Surfing	Brute Force	Dictionary	Multiple Recording	Keystroke Mouse Logger
PassTag:Graphical-Textual Authentication System. [23]	Strong	Moderate	Strong	Moderate.	Strong.
Hybrid User Authentication Schemes. [24]	Strong	Strong.	Strong.	Moderate.	Strong.
Face Recognition and Graphical Password. [17]	Strong	Strong.	Strong.	Moderate.	Strong.
Proposed Approach	Strong	Strong	Strong	Strong	Strong

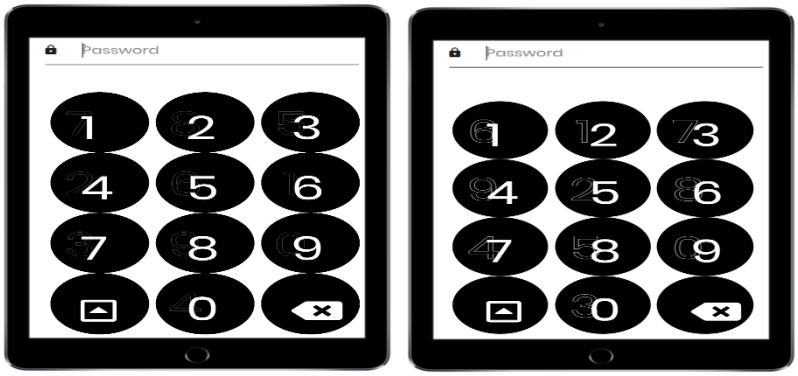
The intensity or level of effort required to crack a password under attack on a given system is found by comparing the search results for each approach with those of our proposed approach. If use of a particular attack requires a level of effort similar to the graphical password scheme to crack a password, we consider the approach to be "Weak" because all the systems compared are rated as strong to moderate against a particular attack. For shoulder-surfing attacks, all systems are rated which has been compared to being strong on his part. However, we note that the systems in which the two types of authentications are combined are strong against many attacks, such as the system proposed by (Face Recognition and Graphical Password) [17] and the proposed approach, in contrast to the system developed by (Hybrid User Authentication Schemes) [24], (PassTag:Graphical-Textual Authentication System) [23], which uses different techniques but is derived from a graphical authentication type, that is, a single type of authentication. On the other hand, our proposed approach to other types of attacks can be classified as "moderate" to "weak". In our comparison, we focused only on the kinds of security attacks that can be resisted based on the defensive techniques used in our approach and the techniques of other systems that have similar protection goals to ours that contribute to protecting against a shoulder-surfing attack in particular.

5.3 Experimental Study of the Proposed Approach.

We evaluated the efficacy of the proposed approach in terms of visibility, usability, user-friendliness, and user awareness. We tested the proposed approach on 10 participants and then conducted a survey.

5.3.1. Visibility Analysis

First, when programming and designing the virtual keypad for the IPIN, it became evident to us that, when trying the defensive techniques of the proposed approach on different types of browsers, the contrast sharpness of the high-frequency or background-digits varies. Therefore, we tested the use of the virtual IPIN keypad technique on two different browsers: Firefox and Chrome to measure the ideal contrast of the virtual keypad and reach a good level of security against shoulder-surfing attacks, as shown in Fig. 9.



(a) The First Browser, Chrome **(b) The Second Browser, Firefox**

Fig. 9. Virtual Keypad in Two Browsers

To determine the level of IPIN visibility, we tested the proposed approach on 10 participants who employed the defensive techniques, then we sent each participant a questionnaire with the questions shown in Table 5.

Table 4. Question of Survey about Visibility

Survey Question	
Q1	Contrast level for the (user) in the First Browser.
Q2	Contrast level for (shoulder-surfing attack) in the First Browser.
Q3	Contrast level for the (user) in the Second Browser.
Q4	Contrast level for (shoulder-surfing attack) in the Second Browser.

The first browser, Chrome Fig. 9a, showed a balance between the visibility results of the user experience and resistance to shoulder-surfing attacks. It thus raised the level of security, because it achieved ease of use for the user, so the authentication process occurred in record time. In addition, at a distance of (150 cm) or more, a shoulder-surfing attacker could not guess the password. This is a fairly short distance, so this browser's default keypad contrast metrics are ideal, meaning the technique was successful.

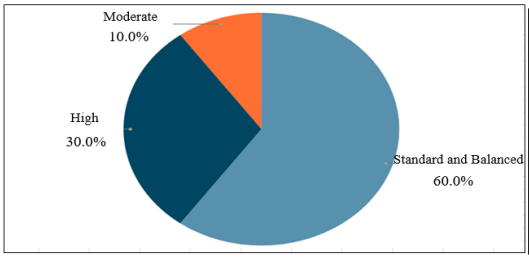


Fig. 9**. Q1-Contrast level for the (user) in the First Browser.**

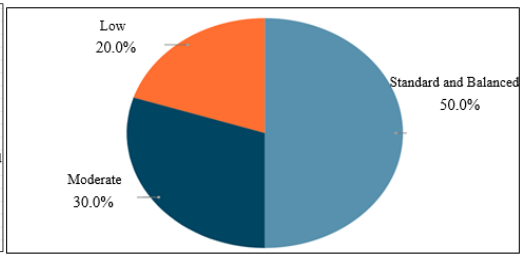


Fig. 10. **Q2-Contrast level for (shoulder-surfing attack) in the First Browser.**

The second browser, Firefox Fig. 9b**,** showed that the apparent contrast represents a high resistance against shoulder-surfing attacks, as the distance (90 cm) is considered very small, so the attacker cannot guess the password. In terms of usability, however, it may require people with a good level of vision and may not be suitable for people with low vision. Moreover, if this defensive technique means the user takes time to complete the authentication process, thus reducing the level of usability, it may end up compromising the security approach.

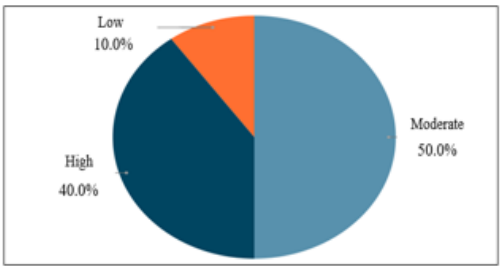


Fig. 11. Q3-Contrast level for the (user) in the Second Browser

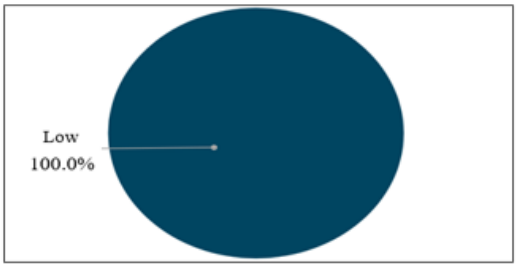


Fig. 12. Q4-Contrast level for (shoulder-surfing attack) in the Second Browser.

Two questions were included in the survey of the 10 participants about the extent to which the proposed defensive tactics affected their awareness of shoulder-surfing attacks and their evaluation of the ease of use of the graphical interfaces of the approach, as shown in Table 7.

Table 5. Question of Survey about Awareness and User Friendly

Survey Question	
Q1	1. Have the techniques piqued your interest and thus increased awareness against shoulder-surfing attack?
Q2	2. Is the user interface easy to use?

5.3.2. Awareness Analysis

During the experimental study of the proposed technique, the users' awareness of shoulder-surfing attacks was measured. As a result, the contribution of the proposed techniques became clear to us, particularly the virtual keypad for the (IPIN) technique, which prompts user inquiries about this technique and its benefit because it piques users' interest. This suggests that the defensive techniques of the proposed approach boost user awareness of shoulder-surfing attacks, in particular.

5.3.3. User Friendly Analysis

Users were asked about their satisfaction with the interfaces, and their impressions were very good. They mentioned that everything is sequential, and they did not find it difficult to understand the authentication mechanism in terms of capturing the fingerprint. Some asked about the strangeness of the IPIN keypad, its benefits, and how it works, which is very valuable because it increases user awareness of this type of attack.

5.3.4. Usability Analysis

To evaluate the effectiveness of the proposed approach, we conducted a usability experiment through the web-based application as mentioned before. This application was developed using the programming language PHP, the server in XAMPP, and the database in MySQL. Operations have been implemented in the application to calculate the login time, which includes entering the user-name an, password and fingerprint capture. The user must enter these credentials correctly to match the data entered in the registration module-and then they press the submit button.

Experiment Procedure for Testing: To evaluate login time, we asked ten different participants to use our authentication techniques. The test was divided into two sessions. The first session included participants registering and logging in on the first day, and after a week, only users logged in. For each successful login, the user login time was noted for both sessions. The participants were introduced to the techniques of the proposed approach before the first session. After this introduction, all test activities (registration and login) were explained and then presented to the participants. When all participants fully understood how to conduct the testing activities, each participant was asked to conduct the tests.

Experimental Results: By analyzing the results obtained from Table 7, we can conclude that users took a longer time to log in during the first session compared to the second session because they were new to the approach and therefore the authentication process required more time. In the second session, we noted that they were quicker because they were familiar with the approach and therefore the authentication process required considerably less time on average. Moreover, this user study also indicated that the participants were faster in finding the Illusion digits (which are behind the more visible digits) of their password. This approach also prompted them to memorize their password because of the spatial changes of the high frequency Illusion digits.

Table 6. Authentication Time

Users	**Authentication time in seconds (First day).**	**Authentication time in seconds (After 5 days).**
Users 1	**32.56**	**24.84**
Users 2	**23.6**	**23.88**
Users 3	**28.58**	**14.7**
Users 4	**20.3**	**23.54**
Users 5	**17.61**	**16.32**
Users 6	**26.95**	**22**
Users 7	**22.76**	**17.24**
Users 8	**21.28**	**21**

Users 9	**14.7**	**19.81**
Users 10	**29.59**	**14.33**
Average login time	**23 .793 s**	**19 .766 s**

6. CONCLUSIONS

We proposed an approach that consists of integrating several highly flexible defense techniques for user authentication that combine the advantages of both biometric and graphical password schemes, Thus, this scheme is less susceptible to a shoulder-surfing attack especially and to some other kinds of attacks. The main idea behind the use of this combined technique to enter a password is the increasing occurrence of shoulder-surfing attacks on users, which happen without their knowledge. If a user notices the attack, they react quickly to defend against such physical attacks, e.g., changing their physical position to cover their device or placing the device under a table for the purpose of concealment [18]. Moreover, this approach puts less cognitive load on the user compared to other authentication schemes because the user only must remember and find their password. At the time of the user experience study, the participants reported that they enjoyed the experience and collaborated with us on this approach based on a hybrid method with biometric authentication for greater protection and awareness, as it made them curious and eager for knowledge about the technique.

7. FUTURE WORK

Improving the proposed approach is necessary to keep abreast of technological developments and changes in security attacks. Some of the enhancements that can be made:

- The proposed approach can be used with biometric authentication of the user's face or on devices that support fingerprint authentication, in order to avoid the requirements of adding devices and increasing the cost.
- Further experimentation and analysis of the proposed approach can be carried out with a larger number of users to verify the strength and accuracy of the authentication approach.
- Verifying fingerprint reader devices and, when using them, unify them be type to avoid programming problems, as each type has a various SDK identification package and, as a result, the programming is different.

8. LIMITATIONS

In addition to costs related to fingerprint devices, their effectiveness can be diminished by certain user characteristics, e.g. sweaty hands.

REFERENCES

[1] Kavitha, M. & Haran, D. & Meenan, P. & Priya, J.. (2019). Shuffled Illusion PIN Framework to Prevent Shoulder – Surfing. International Journal of Recent Technology and Engineering (IJRTE). 8. 11555-11559. 10.35940/ijrte.D4580.118419.

[2] DeFino, S., Kaufman, B., Valenteen, N., & Greenblatt, L. (2010). Official certified ethical hacker review guide. Course Technology, Cengage Learning.

[3] Gopali, S., Sharma, P., Khethavath, P. K., & Pal, D. (2021). HyPA: A Hybrid Password-Based Authentication Mechanism. In Advances in Information and Communication: Proceedings of the 2021 Future of Information and Communication Conference (FICC), Volume 1 (pp. 651-665). Springer International Publishing.

[4] J. AL-Ojeli, A., A. Bozed, K., & I. Eltarhoni, W. (2021, October). Develop Graphical Passwords Authentication System Resistant To Shoulder Surfing Attacks. In The 7th International Conference on Engineering & MIS 2021 (pp. 1-6).

[5] Arun Kumar, S., Ramya, R., Rashika, R., & Renu, R. (2021). A survey on graphical authentication system resisting shoulder surfing attack. In Advances in Artificial Intelligence and Data Engineering: Select Proceedings of AIDE 2019 (pp. 761-770). Springer Singapore.

[6] Bin, G. W., Safdar, S., Akbar, R., & Subramanian, S. (2018, June). Graphical authentication based on anti-shoulder surfing mechanism. In Proceedings of the 2nd International Conference on Future Networks and Distributed Systems (pp. 1-6).

[7] Hirakawa, Y., & Motojima, K. (2019). Improvement of Shoulder-Surfing Resistant Authentication Method Using Hybrid Images. International Journal of Technology & Engineering Studies, 5(4).

[8] Bawarith, R., Basuhail, A., Fattouh, A., & Gamalel-Din, S. (2017). E-exam cheating detection system.

International Journal of Advanced Computer Science and Applications, 8(4).

[9] Thales Group. (2022). Biometrics (facts, use cases, biometric security). Retrieved March 27, 2022, from https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/inspired/biometrics

[10] Yang, W., Wang, S., Hu, J., Zheng, G., & Valli, C. (2019). Security and accuracy of fingerprint-based biometrics: A review. Symmetry, 11(2), 141.

[11] Maltoni, D., Maio, D., Jain, A. K., & Prabhakar, S. (2009). Handbook of fingerprint recognition (Vol. 2). London: springer.

[12] HID Global. (2022). Eat digitalpersona 4500 reader datasheet. Retrieved March 26, 2022, from https://www.hidglobal.com/sites/default/files/resource_files/eat-digitalpersona-4500-reader-ds-en.pdf

[13] Nizamani, S. Z., Hassan, S. R., Shaikh, R. A., Abozinadah, E. A., & Mehmood, R. (2021). A novel hybrid textual-graphical authentication scheme with better security, memorability, and usability. IEEE Access, 9, 51294-51312.

[14] Prabhu, K. D. D. P. (2018). Image based authentication using illusion pin for shoulder surfing attack. Int. J. Pure Appl. Math, 119(7), 835-840.

[15] S. R., D. T., M. S., & U. K. (2021). Multilevel password authentication using biometric verification for smart ATM. Turkish Journal of Physiotherapy Rehabilitation, 32(2), 2208–2212. Retrieved from https://search.ebscohost.com/login.aspx?direct=true&db=edb&AN=151006221&site=eds-live

[16] Alsuhibany, S. A. (2021). A Camouflage Text-Based Password Approach for Mobile Devices against Shoulder-Surfing Attack. Security and Communication Networks, 2021(1), 6653076.

[17] Wajid, A. (2018). A Face Recognition and Graphical Password Based Hybrid Technique of Information Security. Pakistan Journal of Science, 70(4).

[18] Kühn, R., Korzetz, M., & Schlegel, T. (2019, November). User strategies for mobile device-based interactions to prevent shoulder surfing. In Proceedings of the 18th International Conference on Mobile and Ubiquitous Multimedia (pp. 1-5).

[19] Saad, A., Chukwu, M., & Schneegass, S. (2018, November). Communicating shoulder surfing attacks to users. In Proceedings of the 17th International Conference on Mobile and Ubiquitous Multimedia (pp. 147-152).

[20] Saad, A., Elkafrawy, D. H., Abdennadher, S., & Schneegass, S. (2020, June). Are they actually looking? identifying smartphones shoulder surfing through gaze estimation. In ACM symposium on eye tracking research and applications (pp. 1-3).

[21] Saad, A., Liebers, J., Gruenefeld, U., Alt, F., & Schneegass, S. (2021, September). Understanding bystanders' tendency to shoulder surf smartphones using 360-degree videos in virtual reality. In Proceedings of the 23rd International Conference on Mobile Human-Computer Interaction (pp. 1-8).

[22] Farzand, H., Bhardwaj, K., Marky, K., & Khamis, M. (2021). The interplay between personal relationships & shoulder surfing mitigation. In Proceedings of Mensch und Computer 2021 (pp. 338-343).

[23] Dabeer, S., Ahmad, M., Sarosh Umar, M., & Hasan Khan, M. (2019). A novel hybrid user authentication scheme using cognitive ambiguous illusion images. In Data Communication and Networks: Proceedings of GUCON 2019 (pp. 107-118). Singapore: Springer Singapore.

[24] Han, J. K., Bi, X., Kim, H., & Woo, S. S. (2020, October). PassTag: a graphical-textual hybrid fallback authentication system. In Proceedings of the 15th ACM Asia Conference on Computer and Communications Security (pp. 60-72).

[25] Crossmatch. (2022). U.are.U SDK - developer guide. Retrieved August 10, 2022, from https://devportal.digitalpersona.com/U.are.U%20SDK%20Developer%20Guide.pdf

[26] ITIG Iraq. (2022). Essential cybersecurity controls 2018. Retrieved May 8, 2022, from https://itig-iraq.iq/wp-content/uploads/2019/08/Essential-Cybersecurity-Controls-2018.pdf

[27] Documentation, T. P. S., & LOGICAL, C. (2005). Information technology–Security techniques–Information security management systems–Requirements.

[28] Leclercq, L. (2004). Apport du stockage inertiel associé à des éoliennes dans un réseau électrique en vue d'assurer des services systèmes (PhD thesis). Lille University. Retrieved from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800

[29] Binitie, A. P., & Babatunde, J. (2024). ADAPTING USER INTERFACE DESIGN TO MITIGATE SHOULDER SURFING ATTACKS IN USSD CHANNEL.

[30] Adebimpe, L. A., Ng, I. O., Idris, M. Y. I., Okmi, M., Ku, C. S., Ang, T. F., & Por, L. Y. (2023). Systemic Literature Review of Recognition-Based Authentication Method Resistivity to Shoulder-Surfing Attacks.

Applied Sciences, 13(18), 10040.

[31] Saadi, Z. M., Sadiq, A. T., Akif, O. Z., & Farhan, A. K. (2024). A Survey: Security Vulnerabilities and Protective Strategies for Graphical Passwords. Electronics, 13(15), 3042.