Computer Systems
Science and Engineering

Tech Science Press

DOI: 10.32604/csse.2024.057439

ARTICLE

A Secure Authentication Indexed Choice-Based Graphical Password Scheme for Web Applications and ATMs

Sameh Zarif[1,2,*], Hadier Moawad[2], Khalid Amin[2], Abdullah Alharbi[3], Wail S. Elkilani[4], Shouze Tang[5] and Marian Wagdy[6]

[1]Artificial Intelligence Department, Faculty of Artificial Intelligence, Egyptian Russian University, Menoufia, 32511, Egypt

[2]Information Technology Department, Faculty of Computers and Information, Menoufia University, Menoufia, 32511, Egypt

[3]Computer Science Department, Community College, King Saud University, Riyadh, 11362, Saudi Arabia

[4]College of Applied Computer Science, King Saud University, Riyadh, 19676, Saudi Arabia

[5]School of Communication and Information Engineering, Chongqing University of Posts and Telecommunications, Chongqing, 400065, China

[6]Department of Information Technology, Faculty of Computers and Information, Tanta University, Tanta, 31527, Egypt

*Corresponding Author: Sameh Zarif. Email: sameh.shenoda@ci.menofia.edu.eg; sameh-zarief@eru.edu.eg

Received: 17 August 2024 Accepted: 31 October 2024 Published: 03 January 2025

ABSTRACT

Authentication is the most crucial aspect of security and a predominant measure employed in cybersecurity. Cloud computing provides a shared electronic device resource for users via the internet, and the authentication techniques used must protect data from attacks. Previous approaches failed to resolve the challenge of making passwords secure, memorable, usable, and time-saving. Graphical Password (GP) is still not widely utilized in reality because consumers suffer from multiple login stages. This paper proposes an Indexed Choice-Based Graphical Password (ICGP) scheme for improving the authentication part. ICGP consists of two stages: registration and authentication. At the registration stage, the user registers his/her data user name a number called Index Number (IN), and chooses an image from a grid of images. After completing the registration, ICGP gives the user a random unique number (UNo) to be a user ID. At the authentication stage, the user chooses a different image from the grid based on the random appearance of the registered image dimensions on the grid plus the registered Index Number. ICGP password is a combination of three factors; user's name, UNo, and any image. According to the experiments, the proposed ICGP has achieved great improvements when compared to prior methods. The ICGP has increased the possible password numbers from 9.77e + 6 to 3.74e + 30, the password space from 1.20e + 34 to 1.37e + 84, and decreased the password entropy from 7.16e − 7 to 8.26e − 30.

KEYWORDS

Authentication; graphical password; indexed choice-based graphical password; user image; system user number; index number; password space; password entropy

1 Introduction

Information security significantly depends on authentication since it is the initial step in the login stage. Authentication is the most predominant measure employed in cybersecurity which verifies that is the authorized user and provides the basis for access control. The most popular mechanism of authentication and identification is the password. The password is a secret used to identify users in computer and communication networks. The authentication techniques are classified into Knowledge-based Authentication (text-based password, Image-based password), Biometric-based Authentication (fingerprint, eye scan, Iris scan, etc.), and Token-based authentication (Bank Card, Key Card, Smart Card) [1–4].

A graphical password (GP) is an image-based password that accesses the system using images rather than text, instead of a textual password that uses text. Textual passwords (TP) are the most common and traditional password techniques for user authentication that use the alphabet, symbols, and numbers as passwords to provide user identity and access resources. Because of the vulnerabilities of textual passwords against attacks and short password space, graphical and textual graphical passwords were proposed.

Graphical password schemes have been proposed because pictures are easier to remember than text and psychology studies found that the human brain is better at remembering and recognizing images than text [3,4]. When a text password is simple and short, it becomes easily guessable, prioritizing usability over security. Conversely, if the password is complex and long to enhance security, users may struggle to memorize it. Therefore, a graphical password aims to achieve a balance between security, reliability, usability, memorability, and login time.

The majority of research on security and usability support the notion that systems often face a trade-off between security and usability. Achieving a balance between these factors poses a significant challenge. When a technique prioritizes security, it typically becomes less user-friendly, less memorable, and more time-consuming. This is often due to the need for multiple images to choose from and numerous operations required for logging in, consequently slowing down the system and causing user confusion and fatigue from having to remember various images and login operations. As a result, users may revert to using textual passwords [2,4]. The number of pictures needed is reduced from four to only one under the proposed Indexed Choice-Based Graphical Password (ICGP) method. Furthermore, by giving users the option to choose their preferred level of protection, the ICGP method enhances user security. The number of images that are available and the index number used to choose an authorized image password for system login determine this security level. The index number allows the user to select an image dimension on the grid that equals the registered image dimension plus the index number, making the password dynamic rather than fixed as in earlier methods.

The future scope for most researchers involves developing a method that maintains both security and usability while using fewer images. However, despite this aim, all studies have only managed to reduce the number of image selections from six to four [3–5]. Researchers have linked security with the number of images, believing that increasing the number of images enhances security [6].

This approach's thought has led to graphical passwords being less favorable and desirable, while our indexed GP reduced this number to one and improved security.

Cybersecurity is a significant concern for individuals and organizations alike, aiming to increase user awareness regarding the selection of secure passwords and determining the most effective type of password for safeguarding data against cyber threats [7,8]. The increase in internet usage has led to an increase in cyber threats. To combat the growing number of cyber threats, organizations need to have strong cybersecurity policies in place [9,10].

Ensuring the safe and secure preservation of data, user authentication stands as a vital tool within information security. It serves to protect systems from potential threats posed by hackers and spies [7,11–13]. Authentication is a process employed to verify the identity of users and their associated actions [14].

Cloud computing is a shared electronic device that has computing resources configured to serve people and organizations by storing and accessing data and using apps via the internet, rather than via computer devices at any time and from any location [15,16].

Despite the cloud's effectiveness and strength, based on National Institute of Standards and Technology (NIST), which refers to the internet as a cloud, while the internet is vulnerable to attacks all the time, there's no way to protect all the data [17]. In addition, in the view of the cloud users, it is an insecure platform, therefore, it is vulnerable to hacking, so an authentication technique must be present and researchers must invent secure passwords when login and security systems to protect data from attackers [18–21].

The GP approaches used for web applications can be used for cloud environments to successfully authenticate users to secure data from attackers. An authentication technique must be present in cloud computing and services. Different methods can access these services; the best was a GP because of other methods' drawbacks [22,23].

Graphical password techniques typically require less memory space compared to textual passwords. However, optimal authentication is achieved by employing multi-authentication techniques to enhance data security [22–26]. A survey conducted on users authenticated through five levels of authentication (simple password, graphical password, biometric password, third-party authentication, and 3D password object) revealed their perspectives. It was observed that while multi-level passwords increase security and entropy, they also elevate user frustration [27–30].

In response, this paper has innovated the ICGP scheme, which operates as a two-level and multifactor authentication system to improve security. Therefore, the proposed scheme suggested using only one image to be memorable and usable for the user, and at the same time increasing the security by using an index number for choosing a different image every logging session than the registered image when the prior methods users select the same registered image when authenticating and it's easy for attackers to guess it when monitoring. In addition, use random shuffling to show the authenticated grid images randomly every logging session to make it difficult for the attackers to guess the password image, and increase the search area by making a dynamic grid. One of the drawbacks is the proposed method may still require some level of user familiarity with technology, but we can overcome this drawback by users training.

The rest of the paper is structured as follows: Section 2 provides a review of relevant works on graphical passwords. Section 3 introduces the ICGP scheme proposed in this paper. Section 4 outlines the design specifics of the proposed approach. Section 5 presents the experimental results obtained from the proposed method. Section 6 presents the possible attacks on the ICGP scheme. Proposed method limitations are presented in Section 7. Finally, Section 8 concludes the paper and discusses avenues for future research.

2 Related Work

A lot of studies have been carried out on graphical passwords. Blonder originally introduced it in 1996 [31]. There are three different categories of GP approaches: recognition-based technique, recall technique (pure recall and cued recall), and hybrid procedures. The recognition-based technique used images as a password for accessing systems. Registration and authentication are the first two steps in GP. The user selects a number of images displayed in a grid of images or in a graphical user interface (GUI) during the registration procedure. The GP is sometimes called graphical user authentication (GUA), and then during authentication, the user chooses the same registered images [1–3].

Numerous recognition studies on GP approaches have been conducted. The user chooses at least five categories during the registration process, and as a result, chooses one image for each category as his or her password, the user should select the same images later during the authentication stage [18,32–35].

Recognition-based methods offer a narrower password space in comparison to text-based passwords, leading to vulnerabilities such as susceptibility to social engineering, shoulder-surfing, spyware, educated guesses, sniffing, phishing, and dictionary attacks.

The pure recall used images and performed an operation to draw a pattern or clicks, and the cued recall performed the same actions as the pure recall but provided hints by writing text [36–38]. The hybrid is a combination of the two techniques, the recognition and recall [19,33].

In the recall-based approaches, participants underwent a registration process where they were required to memorize two system-assigned images before selecting four categories and four images as their passwords. Each participant could only choose one image from each category. After submitting the information to the database, the user created secret clicks for the selected images and then confirmed the clicks on the same area [36–39]. The GP has been used in deep learning, IoT, the internet of medical things, and car security for driving seats [40–42].

The recall-based methods faced susceptibility to attacks similar to recognition-based techniques. Furthermore, they offered a larger password space. However, despite this advantage, they lacked usability, with users frequently forgetting the necessary operations [32,43–45].

Al-Shqeerat et al. [19] introduced a multi-factor authentication method based on questions within a cloud system. In this approach, when a new user registered, they were prompted to create a unique username, while the system simultaneously generated a random number. This number was utilized later in the hashing process to generate an h-code specific to each user's hotspot. The h-code facilitated the identification of region area coordinates that the user would need to select when authenticating to answer their chosen question, which was associated with their registered image. The system comprises three categories containing a total of 45 images, with each category containing 15 images. Additionally, each image is associated with three questions. During the authentication process, users select one image and one question from a grid of 5 × 3 images, which does not involve random scrambling. The system displays images to users with dimensions of either 280 × 480, while storing images in the database with dimensions of 480 × 480. The designated pixel point for user interaction is set at 30 × 30. Authentication involves three steps aligned with hybrid stages: entering a username, selecting a registered question, and providing the correct answer at the designated point. Users have the flexibility to engage in any number of authentication rounds.

The Choice-Based Graphical Password (CGP) approach outlined in [21] involved combining the user's name with a random number generated by the CGP system, along with an image or images selected by users from either their own devices or the CGP dataset. This approach deviated from previous methods that compelled users to choose images exclusively from their dataset, which often led to frustration and forgetfulness, thereby weakening the password. However, when users utilized their own pictures, recall became easier. The CGP password comprised five components: the user's name, the system-generated user number, and the registered image matched in name, size, and resolution. This combination significantly enhanced the complexity of the CGP password, making it challenging for attackers to guess and resistant to various forms of attack.

Carrillo-Torres et al. [29] introduced a multi-factor authentication mechanism called 'MFA', which required users to create a more configurable process. This approach encompassed a multi-recognition technique involving both the system and the user, coupled with the establishment of user relations. Initially, users were prompted to create a username and password for their account. Subsequently, they were required to upload a minimum of 9 and a maximum of 20 non-redundant images from a dataset of 500 images, as well as associate at least five relation names and ten MFA relations. During authentication, the process involved two-factor authentication. In the first factor, users entered their authorized account credentials. In the second factor, MFA presented a grid containing twelve randomly selected images, four of which were chosen from the images uploaded by the user. From these four images, the user had to select two non-redundant ones and then select the relation previously registered from a dropdown menu. If the user fails at any stage of the authentication process, the authentication will fail and restart.

The Pass Face method is the most widely adopted in GP due to the inherent ease of remembering faces compared to other image types. In this approach, users select four images from a grid layout of 3 by 3 images. Towhidi et al. [32] suggested increasing the number of chosen images to five and expanding the image grid to 25 images to bolster security. However, this adjustment resulted in prolonged authentication times and rendered it easier for hackers to observe user passwords by monitoring mouse movements.

In Vaddeti et al. [35], upon the user's profile registration, the system employed visual cryptography to convert the user ID into two images. One of these images, known as the user share, was dispatched to the user's email, while the other, referred to as the server share, was retained on the server. Subsequently, the user selected four images from a 5 × 5 grid. During authentication, the system combined the user share and server share, prompting the user to choose one of the previously selected images from the registration step. While this method was considered one of the earliest recognition approaches, it advocated restricting the number of images to four and challenged the notion that increasing the number of images compromised security. However, it suffered from prolonged processing times and susceptibility to hacking, failing to effectively address the threefold challenge of enhancing security, memorability, and usability simultaneously.

In Gokhale et al. [36], during the registration phase, the user was presented with a set of 25 photos, which were shared among all users. From these images, the user selected one to serve as their password, with the option to choose any image more than once. Subsequently, the user was presented with a list of questions and the same set of photographs. From this list, the user had to select three questions. To answer a question, the user clicked on a point within the chosen image, resulting in three distinct points corresponding to three different questions. Each individual point was denoted as the ROA (Region of Answer), resulting in three separate ROAs. During authentication, the user inputted their username along with two images.

Dias et al. [25] introduced a graphical password authentication model, named Deep Residual Network-based Graphical Password, the two-step registration process uses the secret pass image selection and challenge set generating processes. The creation of the challenge sets is mostly dependent on creating pass and bogus images through the use of edge detection. Additionally, the Deep Residual Network classifier is used for edge detection. With an information retention rate of 0.1716 and a password diversity score of 0.1643, the new Deep Residual Network-based Graphical Password algorithm outperforms other graphical password authentication methods.

In Rasheed et al. [46], instead of selecting images, the system draws them and classifies them using deep learning models. To increase network performance in terms of storage and data required to broadcast, a novel method dubbed "selected pixels (SP)" has been developed. This method delivers simply the color pixels from the drawing images, rather than the entire image. It is specifically built to take Arabic digits, however, it is not limited to this format of the input. The system can be modified to take other sorts of digits, characters, and even objects. The proposed system was evaluated based on login time, total data required for sending and storing, and password entropy. That proposed system was a highly flexible platform that can be easily integrated into any e-commerce ecosystem.

In Singh et al. [47], authentication is done using both textual and graphical passwords. They chose this approach because humans are naturally visual beings, and we believe that adopting a cued-recall and recognition-based method can increase a system's defenses. A password with an entropy of at least 60 is considered strong. This password technique, once rigorously tested, can prove to be a very good alternative to multi-factor authentication, which would force the user to wait for an One Time Password (OTP) or some other annoyance. Our method seeks to alleviate all of the difficulties faced during the process by proposing a simple gateway for user identification. This strategy assists in producing passwords with a password entropy close.

In RAY, Palash et al. [48] introduced a brand-new graphical authentication system that guarantees both usability and security. This approach incorporates random graphical objects blended with a background image, resulting in the generation of a distinct graphical challenge. The selected objects need to be verified using the YOLOv3 object detection technique. User data is encrypted and then saved on the server to improve the security of GPOD (Graphical Password with Object Detection). This reduces the possibility of database attacks. Furthermore, the user data is encrypted before being sent to the server to reduce the possibility of man-in-the-middle attacks. Simple, practical, robust, shoulder-surf-resistant, and secure graphical authentication is what the suggested GPOD approach offers.

Several research approaches relied on image selection for verification or subsequent operations, making the GP susceptible to rendering attacks [37,38,44,45]. Moreover, users became disenchanted with the multitude of categories and methods associated with GP registration and authentication, prompting them to switch to traditional passwords [40]. Hence, this paper proposes an innovative ICGP scheme—a textual GP comprising a blend of text and images—to enhance GP's user-friendliness and usability. With ICGP, users need only select one image for memorability, thus reducing login time while maintaining the integrity of the system. Additionally, ICGP enhances security by employing the index number (IN). Users seek heightened security can increase the index above one or choose two or three images.

3 Proposed ICGP Method

The proposed indexed choice-based graphical password ICGP method is a textual graphical password that follows the category of recognition-based Techniques.

The system architecture of the proposed indexed choice-based graphical password scheme is shown in Fig. 1.

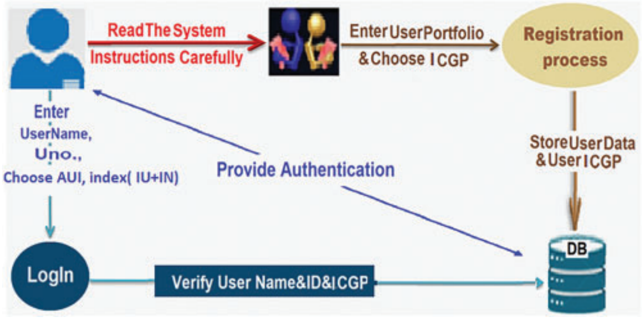

Figure 1: The system architecture of the indexed choice-based graphical password scheme

In the proposed ICGP scheme, users are cautioned by the ICGP system to pay close attention to its instructions and thoroughly review them prior to the registration stage. This precaution is taken because the ICGP system refrains from sending instructions via email or short message service (SMS) to prevent hacking attempts.

The ICGP registration process entails two stages. Initially, users provide their personal information, followed by selecting at least one image referred to as a user image (UI), which becomes a component of their ICGP password. Additionally, users input an IN, which determines the selection of the authenticated password (AUI). Subsequently, the ICGP system assigns users a random and unique number. For enhanced security, users have the option to input an index number greater than one. The AUI serves as the image users need to input to authenticate the system; its position on the grid is calculated based on the appearance of the UI on the grid combined with the IN. Furthermore, the UI's position on the grid changes randomly with each login.

Upon confirmation of their username, UI, and IN, the ICGP system provided the user with a unique number briefly displayed on the screen, following the instructions outlined in the ICGP guidelines. This number formed an integral part of the ICGP system, marking the successful completion of the registration process, as illustrated in Fig. 2. Unlike previous methods where users were required to memorize at least four or five images, ICGP simplified authentication by prompting users to remember only one image. The intricate ICGP password comprised a composite record stored in the database, including the User's Name, User Index Number 'IN', User Image 'UI', and the system user number 'UNo'. The format of the ICGP's user record was structured as a list, represented as [User Name, UI, UNo, IN].

During the ICGP authentication process, the user initially inputted their name and UNo. into the ICGP system. Upon successful authorization, the user proceeded to select their "AUI" from a grid of 5 × 5 images suggested by the ICGP System. The selection of the "AUI" was determined based on the position of the user's registered UI on the grid, along with their IN. If the authentication was successful, the user was granted access to log in to the ICGP system.

The registration and authentication processes are shown in Fig. 2 and explained in detail in the following subsections.

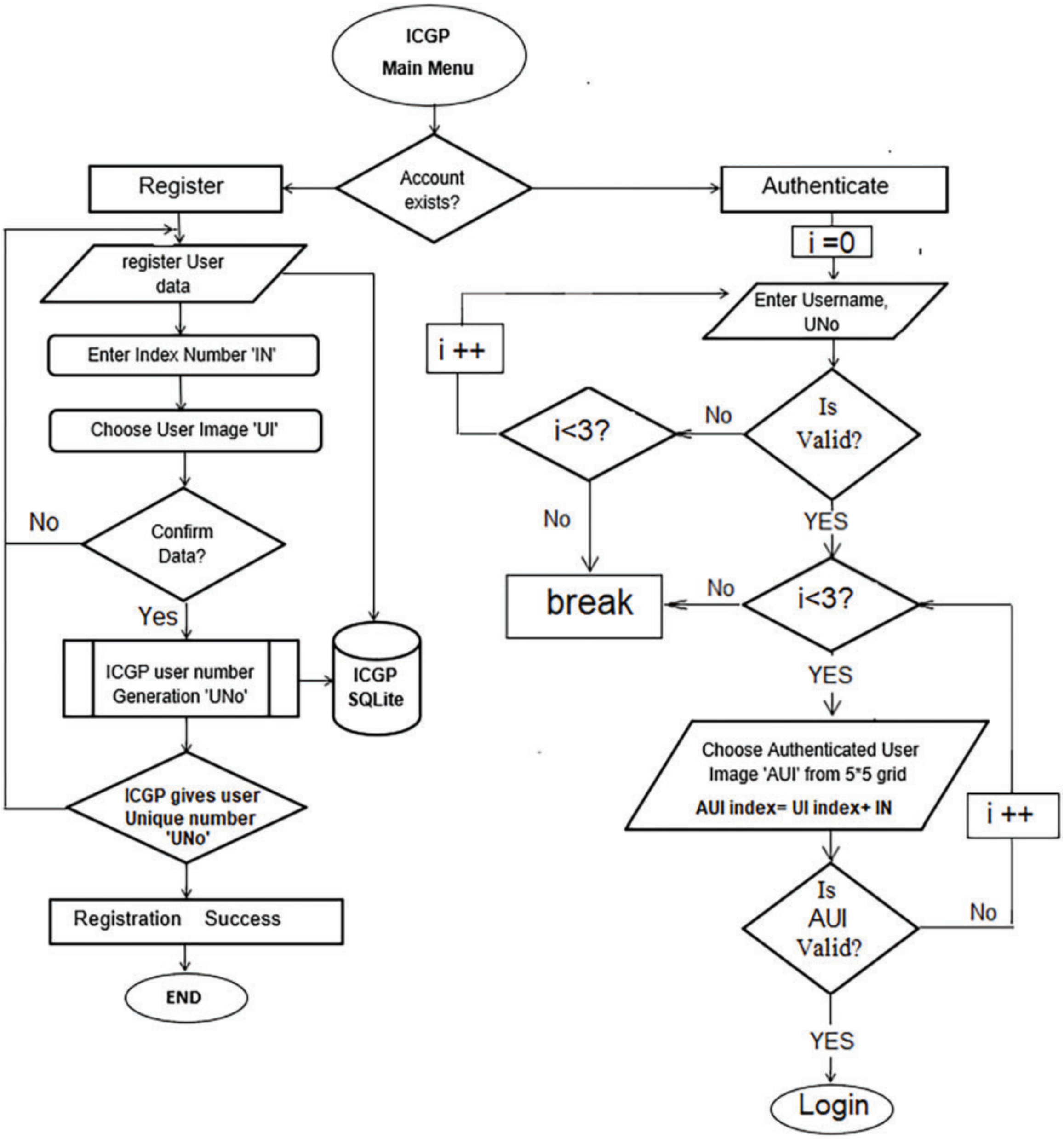

Figure 2: Registration and authentication block diagram of the proposed ICGP

3.1 Registration Process

The registration process comprises the following steps:

1. Users are required to carefully review the instructions provided by ICGP.
2. Users proceed to create their profiles, entering personal details including username, gender, email, mobile number, and age.
3. Users select an image from the ICGP image grid, which serves as their chosen ‘UI’ (User Image). This selected image is stored in the ICGP database, and the system records its name.

4. Before storing the UI, ICGP performs various operations to enhance its complexity and security, thereby safeguarding against potential threats from hackers or spies.

Most of the previously introduced methods involved resizing images from 200 × 200 to 100 × 100. However, our ICGP proposed a different approach, resizing them to 5 × 5, applying a blurring effect, and then encrypting them, the resized image was first blurred using Gaussian Blur, and then the blurred image was encrypted using the A-Es encryption technique. The output image was referred to as 'NUI' and stored in the ICGP's database for each user record.

Once the user confirms their profile data, the ICGP system generates a unique number called "UNo". This number is briefly displayed on the user's screen before being promptly removed. The system refrains from sending the generated number to the user to mitigate the risk of social engineering attacks or interception by internet media tools, thereby enhancing the cybersecurity measures of the ICGP.

The final record of the ICGP User stored in the ICGP's database comprises the user's name, the unique system-generated user number 'UNo', the original user image 'UI', the newly processed image 'NUI' (resulting from resizing, blurring, and encryption), as well as the user's identification number (IN). Additionally, the ICGP scheme ensures heightened security by implementing keyboard locks to prevent various hacking attempts.

3.2 Authentication and Login Process

The Authentication and Login process includes the following steps:

1. The user inputs their unique name and the suggested unique number "UNo" provided during the ICGP registration process, and selects the AUI index from the ICGP's grid as their login identifier. The user is required to choose the 'AUI' from a grid of 25 images, based on their registered UI index combined with their IN.
   For instance, if the UI is located at coordinates (3, 3) and the IN is set to one, the resulting AUI index on the grid would be (3, 3) + (0, 1), yielding (3, 4). Similarly, if the UI is positioned at Index (5, 5) and the IN is equal to one, the correct AUI index on the grid would be (0, 1).
2. The ICGP scheme incorporated user data, including the unique user name, the user's system number (UNo), the UI, the UI's name, and the IN, to ascertain the correct user's AUI.
3. The ICGP system conducted a comparison between the user's login record and the corresponding entry retrieved from the ICGP database. If they matched, the user was granted access to the system, signifying successful authorization.

If login attempts fail and the user exceeds three attempts, the ICGP system will be disabled for one hour.

4 Experimental Study

In earlier approaches, users were required to select the same set of five or more images they had chosen during the registration phase. Consequently, these methods were more susceptible to spying. In contrast, the proposed concept of ICGP relies on the index placement of the user's chosen image from the ICGP grid rather than a predetermined image. Furthermore, the intricate composition of its components enhances password complexity, making it more challenging to guess, as indicated by experimental findings.

The ICGP technique operates on any desktop or online application on websites or in the cloud. The user needs to submit an authorized password to visit a web page; otherwise, the website will block them. We suggest using the ICGP on automated teller machines (ATMs), the user name is the card name, and the system user number can be the card number or a number the user should enter to have permission to log into the ICGP grid view for choosing the authenticated image, then the ICGP grid must be displayed on the ATM screen by the system for the user to choose the correct password and proceed with making withdrawals, deposits, and other transactions if the user is unable to choose the correct password, the machine will eject the card. If the registered image is a cat, the index number equals one, and the cat appears in row one, column one; the user should choose the image in row one column two. Every login session, the system displays images with a random shuffling, and he or she will choose a different image each time signing in, making it difficult for the attacker to guess which user's image to monitor because the image is not determined as in prior techniques.

4.1 Dataset Description

The effectiveness of any recognition-based graphical authentication system is heavily reliant on the quality and diversity of its image dataset. Since the password comprises images, the dataset's significance in the GP system cannot be overstated.

Users are advised to carefully select their image for the ICGP password to ensure easy memorization during login.

The ICGP dataset encompasses 1000 images across a wide array of categories, including but not limited to sports, football, countries, age, gender, jobs, robots, flowers, trees, plants, car brands, universities, food, hobbies, famous people, traffic signals, alphabets, clothes, dressing styles, colors, and many more. Each category is further detailed with internal descriptions.

4.2 Description Table of ICGP Components

The proposed ICGP scheme has 11 parameters as shown below in Table 1.

Table 1: The notation description of the proposed ICGP

No.	Item	Description	Value
1	R	The number of rounds	From 1:3
2	UI	User image	From 1:3
3	UNo	ICGP system user number	Using six digits out of 0–9
4	N	Total number of images	25
5	Nik	Number of attempts per login session from i = 1 to i = 3	I = 1:3
6	W, H	W number of rows, H number of columns	5, 5
7	X, Y	X ∗ Y is the dimension of 'UI'	200 × 200
8	ROA	Z ∗ Z is the dimension of the resized UI	5 × 5
9	NUI	UI after resizing, Blurring then Encryption	
10	AUI	Authenticated user image to login	
11	IN	Index number used to choose the AUI	

5 ICGP Performance Evaluation

Systems rely on the pass-face and biometric techniques. Thus, research is currently being conducted on GP to make it reliable and provide the user confidence in choosing the GP instead [17,21].

The strength, efficiency, and success rate of any GP system depend on several key factors: security, usability, processing and login time, reliability, memorability, password space, and password entropy. Almost all research endeavors concentrate on the intricate task of striking a balance among these factors, which remains a significant challenge for future researchers to address [17,18,21]. The proposed ICGP scheme aims to tackle this challenge and achieve equilibrium among these factors, as demonstrated by the calculated results.

5.1 Security and Reliability Analysis of Proposed ICGP

The reliability of a methodology stems from its security. When a system is secure, users feel confident and trust in its functionality. Security serves as a shield against various threats, including attacks and spies, and acts as a metric to gauge the robustness of the methodology employed. In evaluating the security of the ICGP, three key factors were considered: Password Space, Password Entropy, and its resilience against attacks.

5.1.1 Password Space (PS)

The PS represents the complexity of a password and acts as a composite key size utilized for system authentication. It offers users a wide range of options during the password selection phase, thereby expanding the search space for potential passwords and making it challenging for attackers to guess or crack them. In essence, PS serves as a composite key, amalgamating specified records within a database table to establish a unique identifier for each record, ensuring data integrity and precision. This proves particularly beneficial in situations where a single column alone fails to uniquely identify a record. PS quantifies the total number of potential passwords achievable by combining various password elements, resulting in an exceptionally large number beyond comprehension, thereby enhancing security. To make these numbers more manageable, entropy is introduced as the binary logarithm of these values, indicating the number of bits necessary to represent the magnitude of potential passwords.

The PS is generated by combining k randomly chosen images from a set of available images N in the database. It is a combination number of the possible password images. Whenever the system has a combination of many passwords, attackers have millions of possibilities, thus making the password space higher and the methodology strength was increased against many attacks like brute force attacks, guessing attacks, and many others.

The password space formula depends on the types of passwords used and the random scrambling of images or not so, it is calculated by variant equations either by the techniques used or by using all image sizes or working on a region area or a determined point of an image.

If the approach used has many types of passwords, the PS would equal the multiplication of PS of each password type as discussed in Eqs. (1)–(6), and it mainly depends on a row size [18,22,41].

Nearly, many previous algorithms used 25 images and a user chooses some images out of these images. Our ICGP process can maximize these numbers of grid images to increase the search area and make it difficult for the attacker to guess the password, but we used 5 × 5 grid images in equations to make a fair comparison between all algorithms used, as shown in Fig. 3.

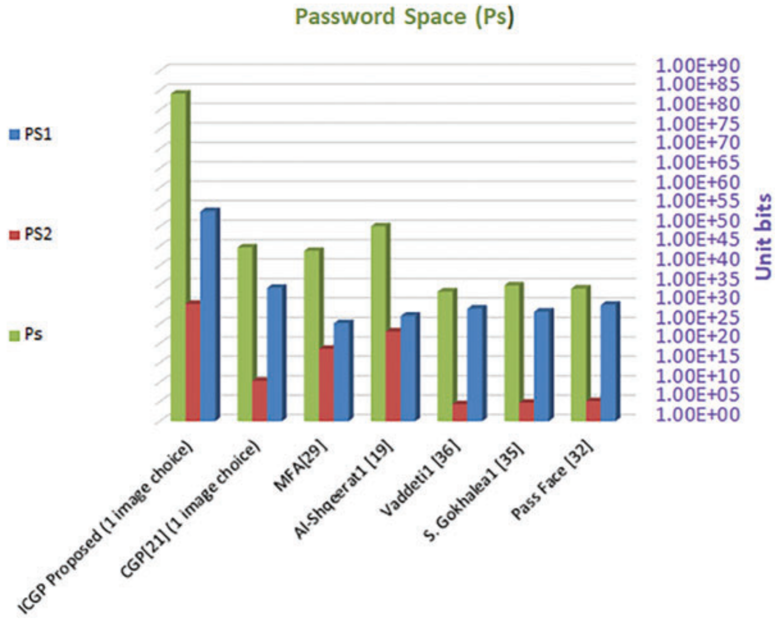

Figure 3: The password space of the compared methods as shown in Tables 2 and 3

There were many methodologies of the recall or recognition techniques and each needed different requirements thus, there were many formulas for calculating the PS at the authentication stage [32,36,41,42].

The authentication stage has two steps. The first calculates the password space based on the techniques used, and the second is based on using all image sizes or working on a region area of its "ROA".

The first-step equation Ps_1, when the methodology used is a recognition-based technique only, is calculating the number of possible passwords Ps_1 to choose k images from a set of N images on a grid without any randomization where N is $(X \times Y)$, X is the row number and Y is the column number, as in Eq. (1) Case 1, and if there is a random scrambling, the Ps is calculated as shown in Eq. (1) Case 2 [16].

In the recall technique, users do any operation or a pattern C on the chosen images either a click or drawing on an area of the image, i.e., hotspot or use colors for example. If the methodology used is a hybrid, i.e., a combination of recognition and recall techniques then the Ps_1 is calculated as in Eq. (1) Case 3.

In a textual password, the Ps depends on N symbols and password symbols k, and the total number of possible symbols available is calculated as shown in Eq. (1) Case 4.

If it is a combination of recognition and textual techniques, the Ps_1 is calculated as shown in Eq. (1) Case 5 when R equals one otherwise if there were a relation between the password components, it would equal the number of these components.

In the textual password, there were 95 symbols with the space, and the password length (PL) is some symbols, the PS of the textual password would equal T^P.

If we use numbers (0:9) only from T symbols, the probability of Ps_1 depends on numbers used only (ten numbers only) and password length PL (if PL equals nine numbers), the total number of possible symbols available = $T^P = 10^9$ as shown in Eq. (1) Case 4. The ICGP depends on the relation 'R' of four factors together and R = 4, the ICGP's Ps_1 is as in Eq. (1) Case 5.

The ICGP scheme assigned a unique ideassigned a unique identified number,ntified number, UNo, to each user, registered using six digits, and UNo. is equal to 10^6 where the username password length is fifteen, and the TP is 95^{15}.

$$Ps_1 = \begin{cases} \binom{N}{k}\ Case\ 1 \\ N! \times \binom{N}{k}\ Case\ 2 \\ C \times \binom{N}{k}\ Case\ 3 \\ N^k\ Case\ 4 \\ N^k \times \binom{N}{k} \times R\ Case\ 5 \end{cases} \tag{1}$$

The second-step authentication Stage depends on the image size; either the methodology used worked on the whole image selected, and the Ps_2 is as Eq. (2) Case 1, or it worked on a region or a point of the image chosen so, the Ps_2 is as Eq. (2) Case 2.

If y was the total number of images, Z was the password size, and x was the maximum number of chosen images, the Ps_2 is calculated as shown in Eq. (2) Case 1.

If the methodology used depended on a region area of an image to work (ROA) and X, Y was the image size, Z is the ROA, and q is the number of questions, clicks, or maximum chosen image numbers, then the Ps_2 is calculated as shown in Eq. (2) Case 2 [16,21,29].

$$Ps_2 = \begin{cases} \sum_{z=1}^{x} \binom{y+z-1}{y-1}\ \text{Case 1} \\ \sum_{i=1}^{q} i! \times \left(\frac{x \times y}{z^2}\right)^i\ \text{Case 2} \end{cases} \tag{2}$$

The PS = $Ps_1 \times Ps_2$; The more rounds, images, or relations were available for users, the larger the password space would be, and While the PS is high, the more secure the mechanism used would be. Our proposed ICGP is the most secure approach, as shown in Table 2 and Fig. 3.

Table 2: The comparison methodologies used

Methodology	GP Technique used
Pass face [32]	Recognition only
S. Gokhalea1 [35]	Recognition + Recall 'Click'
Vaddeti1 [36]	'Image' + Recognition
Al-Shqeerat1 [19]	Recognition + Recall 'Select Relation'
MFA [29]	'Textual' + Recognition + Recall 'Click'
CGP [21]	'Random No.'+Recognition
ICGP proposed	'Textual' + Recognition

The PS of method MFA [29] were calculated by the equation, Ps = $(20c_4 \times 500c_8) \times (4c_2 \times 15) = 3.99e + 22$. MFA has a larger password space than other approaches compared to six-digit Ps used but still has a lower Ps than our proposed ICGP's Ps, which equals 9.29e + 53 as presented in Table 3.

Table 3: The password space based on Eqs. (1) and (2)

Methodology	Ps_1	Ps_2	PS
Pass face [32]	8.24e + 29	1.42505e + 5	1.195e + 34
S. Gokhalea1 [35]	1.39e + 28	6.051e + 4	8.43e + 34
Vaddeti1 [36]	8.9e + 28	2.3746e + 4	2.11e + 33
Al-Shqeerat1 [19]	1.16e + 27	1.09e + 23	1.26e + 50
MFA [29]	1.55e + 25	4.06e + 18	6.49e + 43
CGP [21] (1 image choice)	1.94e + 34	2.458e + 10	4.769e + 44
ICGP proposed (1 image choice)	9.29e + 53	1.47e + 30	1.37e + 84

5.1.2 Usability and Memorability Analysis of Proposed ICGP

When dealing with a considerable quantity of passwords, the likelihood of guessing the correct one diminishes, thereby thwarting potential attackers. At the time, there was no established formula for quantifying the password space or estimating the probability of guessing accurately. Instead, we derived our calculation method, as detailed in Eq. (1) Case 5 and elaborated on in [4,21,23,24].

When fewer images were utilized in the methodology, users tended to prefer it, yet they remained uncertain about its security. The methodology needed to enhance both usability and security, despite their inherent opposition.

The ICGP boasted a large password space, resulting in a low probability of guessing the correct password, thereby enhancing system security. Even as the number of chosen images decreased, usability improved, while the system remained more secure compared to previous mechanisms, as illustrated in Table 4 and Figs. 4 and 5.

- Probability of Guessing the Correct User Password

Table 4: The password entropy and security based on Eqs. (3) and (4)

Methodology	Possible password number	P	PE
Pass face [32]	9.77e + 06	1.024e − 7	7.158e − 7
S. Gokhalea1 [35]	1.88e + 03	5.33e − 4	1.745e − 3
Vaddeti1 [36]	3.91e + 05	2.56e − 6	1.432e − 5
Al-Shqeerat1 [19]	1.62e + 22	6.17e − 23	1.370e − 21
MFA [29]	1.35e + 21	7.41e − 22	1.566e − 20
CGP [21]	1.56e + 10	6.4e − 11	6.524e − 10
ICGP proposed	3.74e + 30	2.7e − 31	8.255e − 30

The number of possible passwords = $(N)^k$, and the Probability of Guessing the correct user's password P = 1/number of possible passwords as shown in Fig. 4.

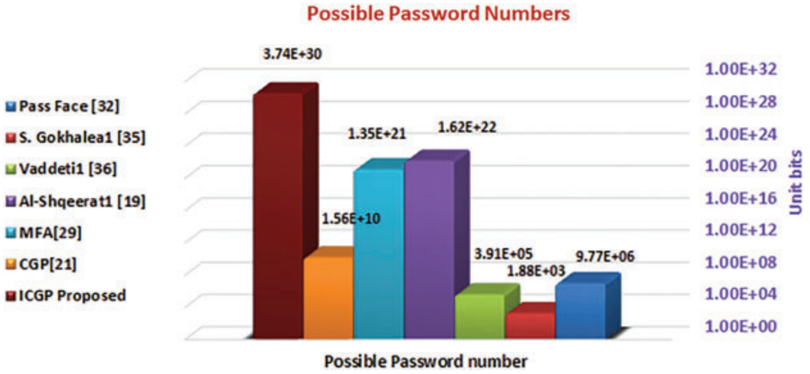

Figure 4: The password numbers of the compared methods as shown in Table 4. Pass face [32]; S. Gokhalea1 [35]; Vaddeti1 [36]; Al-Shqeerat1 [19]; MFA [29]; CGP [21]; ICGP proposed

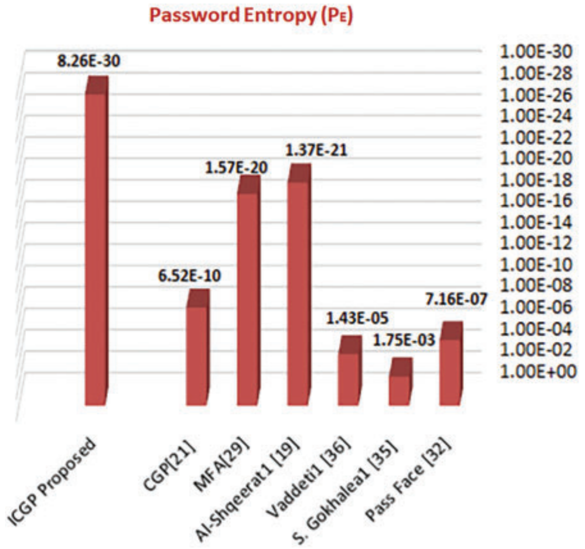

Figure 5: The password entropy of the compared methods as shown in Table 4. ICGP proposed; CGP [21]; MFA [29]; Al-Shqeerat1 [19];Vaddeti1 [36]; S. Gokhalea1 [35]; Pass face [32]

The password entropy PE is the amount of information in the available data and is the password's strength and difficulty not to be predicted as shown in Eq. (3) and Fig. 5 [21].

$$\text{PE} \ = plog\frac{1}{\text{p}} \tag{3}$$

The higher the possible password numbers are, the less the password entropy is and the greater the defense against attack as shown in Eq. (4) [42].

$$\text{PE} \ = log_2(Ps) \tag{4}$$

5.1.3 Processing Speed and Time Analysis of the ICGP Scheme

The number of ICGP rounds, the processing time, and the login time decreased. Nearly most previous approaches introduced, users suffer from the more rounds and the long-time of the login process, thus they were recommended to innovate methodologies that have fewer rounds and fewer images to be as user-friendly as possible and at the same time preserve the security and enhance login time and be as user-friendly as possible.

6 Possible Attacks on the ICGP Scheme

The Common Attack Pattern Enumeration and Classification (CAPEC) has identified and categorized various attacks on recognition-based graphical password techniques into six types: dictionary, brute force, spyware, guessing, social engineering, and shoulder-surfing [19]. Additionally, phishing and sniffing attacks are also included in this classification. There was a study covering the security threats between 2009 and 2023, with precisely defined exclusion criteria [44] and specifically the recognition-based passwords' vulnerabilities [45]. This study identified security risks along with solutions for graphical password schemes. The investigation begins with discovering relevant information using databases and search engines. The inclusion and analysis prioritize attacks and countermeasures for graphical password systems. They found a total of 13 security attacks like Shoulder surfing, video recording, Smudge, Spyware, brute force, computer vision (AI), dictionary, Eavesdropping, a man-in-the-middle, The frequency of occurrence analysis (FOA), database attack, social engineering, Image gallery attacks and a sonar attack for mobile phones [44].

6.1 Shoulder Surfing

In these attacks, attackers compile a list of potential user passwords and then attempt to hack systems using this list. This method relies more on keyboard input than mouse clicks, making textual passwords more susceptible to such attacks compared to graphical passwords. If the number of possible passwords is reduced, the system becomes easier to hack. Among graphical password techniques, only the pass-face technique was notably vulnerable to dictionary attacks [17,18]. The ICGP scheme could potentially be compromised in the first step of logging in when the user inputs their username and a random number. However, since it utilizes multi-factor authentication, it is not vulnerable to dictionary attacks.

6.2 Brute Force Attack

It works like the dictionary attack we explained in Section 6.1. It also depends on reducing the password space and the probability of guessing the correct ICGP password. Because graphical passwords depend on mouse clicks, it would be difficult for attackers to monitor passwords [17,18]. So, our ICGP-proposed scheme prevents brute-force attacks.

6.3 Spyware Attack

It is a software or tool installed for recording the user's screen input. Any movement of the user's mouse or key is recorded by this malware. Spyware attackers use spy cameras to record user data. Past research proves that screen monitoring and keylogging spyware are not enough to crack the GP as they require additional data such as time, window size, and position [20,21,44,45]. Because our proposed ICGP depends on the user index and every login chooses another image and implicitly depends on all user record parameters, it was difficult for spyware attacks to hack our ICGP proposed scheme.

6.4 Guessing Attack

Since users often select passwords based on personal information, attackers can guess these passwords using probabilistic methods. Previous research [18] found that GP could be easily guessed by attackers, leading to a recommendation for users to avoid using personal images. Unlike these methods, our ICGP does not rely on the user selecting a specific image at each login. Instead, it combines the image name, user number, user image, and user index, and displays a blurred image grid. This approach prevents educated attacks and is not vulnerable to guessing attacks.

6.5 Social Engineering Attack

Social engineering is a type of crime where individuals are manipulated into revealing confidential information, often through phone messages or calls to obtain passwords or bank details [17]. Our proposed ICGP scheme mitigates this risk by instructing users, before registration, not to disclose their ICGP system number or share their registered images with anyone. Additionally, since sending images via SMS is impractical, our ICGP system is less susceptible to social engineering attacks.

6.6 Shoulder-Surfing or Hidden Camera Attack

This type of attack involves capturing the user's authorized information by watching over their shoulder or recording their login session as they select or generate their graphical passwords. GP is particularly vulnerable to shoulder surfing attacks [6,13,17,18]. However, our ICGP system mitigates this risk. Even if an attacker uses external recording devices like hidden cameras or high-resolution video cameras to capture the user-input ICGP image during registration or authentication, it would be difficult to exploit. This is because the proposed ICGP system hides mouse clicks, displays the grid images blurred, and doesn't rely on selecting a specific image for each login. Instead, it changes the image frequently, requiring users to choose their passwords based on a combination of image appearance and index number.

6.7 Phishing, Sniffing, or Wiretapping Attack

Phishing websites are designed to deceive users into revealing personal or financial information by mimicking legitimate websites. These fake sites aim to divert traffic from genuine websites to fraudulent ones. Sniffing attacks involve capturing sensitive user data as it is transmitted through media channels, public networks, or when it is unencrypted. The proposed ICGP system prevents sniffing attacks by not sending the system user number to users via SMS or email and by encrypting only the cropped part of the UI, rather than the entire interface.

6.8 Video Recording Attack

In this attack, attackers record a video for users when authenticating. Hackers can steal cryptographic keys by video-recording power LEDs 60 feet away. The proposed ICGP scheme prevents video-recording attacks as the user chooses a different password image every time he/she logs in and our system uses a random shuffling to show images on the grid and uses the index number to make the user choose another image than the image he/she registered.

7 The Limitation of the Proposed Method

- Users should have the option to select personal images, not limited to those in the ICGP dataset.
- Must provide greater flexibility and personalization and apply it in other domains.
- The proposed method needs an educated user, but if the user trained successfully, there wouldn't be any problems with it.
- The system's performance with a significantly larger user base or grid size remains to be explored
- The proposed system has not yet been tested in real environment such as universities or ATMs.

- The proposed method primarily focuses on traditional threat models. Testing the system's vulnerability to more sophisticated, emerging cyber threats, such as AI-driven attacks does not sufficiently addressed yet.

8 Conclusions and Future Work

This paper presents a multifactor authentication ICGP scheme designed for web applications, cloud computing, and ATMs. By integrating both textual and recognition-based techniques, the proposed ICGP system addresses the limitations inherent in using these methods individually. It utilizes multiple factors—username, user number, and image selection based on an index number—to ensure robust authentication. This multifactor approach makes the ICGP scheme highly resistant to various attacks. The effectiveness of the ICGP scheme was evaluated using metrics such as password guessing probability, password space, and entropy. The results demonstrated the scheme's superiority in terms of security and accuracy compared to traditional recognition and recall techniques. In the future, we envision extending the ICGP scheme's feasibility to a broader audience by allowing the use of two or three images to further enhance security. Additionally, users will have the option to select personal images, not limited to those in our dataset, thereby providing greater flexibility and personalization. Future research also will address the explored cyber threats against GP. Also, future work will involve deployment and user testing in real environments such as universities or ATMs to validate the system's usability and effectiveness.

Acknowledgement: None.

Funding Statement: The authors would like to thank Research Supporting Project number (RSP2024R444), King Saud University, Riyadh, Saudi Arabia.

Author Contributions: All authors contributed to the study conception and design. Material preparation, data collection and analysis were performed by all authors. The first draft of the manuscript was written by Hadier Moawad and all authors commented on previous versions of the manuscript. All authors reviewed the results and approved the final version of the manuscript.

Availability of Data and Materials: The general created dataset is available upon request.

Ethics Approval: Not applicable.

Conflicts of Interest: The authors declare no conflicts of interest to report regarding the present study.

References

[1] C. Singh and D. Singh, "A 3-level multifactor authentication scheme for cloud computing," *Int. J. Comput. Eng. Technol.*, vol. 10, no. 1, pp. 184–195, 2019. doi: 10.34218/IJCET.10.1.2019.020.

[2] X. Suo, Y. Zhu, and G. S. Owen, "Graphical passwords: A survey," in *21st Annu. Comput. Secur. Appl. Conf. (ACSAC'05)*, IEEE, 2005.

[3] R. Biddle, S. Chiasson, and P. C. Van Oorschot, "Graphical passwords: Learning from the first twelve years," *ACM Comput. Surv.*, vol. 44, no. 4, pp. 1–41, 2012. doi: 10.1145/2333112.2333114.

[4] V. Rodda, G. R. Kancherla, and B. R. Bobba, "Shouldersurfing resistant graphical password system for cloud," *Int. J. Appl. Eng. Res.*, vol. 12, no. 16, pp. 6091–6096, 2017.

[5] A. R. I. Pratama, M. Alshaikh, and T. Alharbi, "Increasing cybersecurity awareness through situated e-learning: A survey experiment," in *The 2nd Global Trends in E-Learning Forum*, 2023.

[6] W. Shafik, "A comprehensive cybersecurity framework for present and future global information technology organizations," in *Effective Cybersecurity Operations for Enterprise-Wide Systems*, 2023, pp. 56–79.

[7] A. Mishra, Y. I. Alzoubi, M. J. Anwar, and A. Q. Gill, "Attributes impacting cybersecurity policy development: An evidence from seven nations," *Comput. Secur.*, vol. 120, 2022, Art. no. 102820. doi: 10.1016/j.cose.2022.102820.

[8] A. A. Darem, A. A. Alhashmi, T. M. Alkhaldi, A. M. Alashjaee, S. M. Alanazi and S. A. Ebad, "Cyber threats classifications and countermeasures in banking and financial sector," *IEEE Access*, vol. 11, pp. 125138–125158, 2023. doi: 10.1109/ACCESS.2023.3327016.

[9] M. Bay, "What is cybersecurity," *French J. Med. Res.*, vol. 6, pp. 1–28, 2016.

[10] O. Devrukhkar and S. Chouhan, "Artificial Intelligence in cyber security," *Int. J. Softw. Comput. Testing*, vol. 5, no. 1, pp. 9–14, 2019.

[11] B. S. Sagar, S. Niranjan, N. Kashyap, and D. N. Sachin, "Providing cyber security using artificial intelligence—A survey," in *2019 3rd Int. Conf. Comput. Methodol. Commun. (ICCMC)*, IEEE, 2019, pp. 717–720.

[12] I. A. Mohammed, "Artificial intelligence for cybersecurity: A systematic mapping of literature," *Artif. Intell.*, vol. 7, no. 9, pp. 1–5, 2020.

[13] N. R. Mosteanu, "Artificial intelligence and cyber security-face to face with cyber attack—Maltese case of risk management approach," *Ecoforum J.*, vol. 9, no. 2. 2020.

[14] H. Sedjelmaci, F. Guenab, S. M. Senouci, H. Moustafa, J. Liu and S. Han, "Cyber security based on artificial intelligence for cyber-physical systems," *IEEE Netw.*, vol. 34, no. 3, pp. 6–7, 2020. doi: 10.1109/MNET.2020.9105926.

[15] A. Rashid and A. Chaturvedi, "Cloud computing characteristics and services: A brief review," *Int. J. Comput. Sci. Eng.*, vol. 7, no. 2, pp. 421–426, 2019. doi: 10.26438/ijcse/v7i2.421426.

[16] A. Khang and A. K. Sivaraman, "Big data, cloud computing and IoT: Tools and applications/edited," *J. Future Revol. Comput. Sci. Commun. Eng.*, vol. 4, no. 4, pp. 599–602, 2023.

[17] D. Patil and N. Mahajan, "An analytical survey for improving authentication levels in cloud computing," in *2021 Int. Conf. Adv. Comput. Innov. Technol. Eng. (ICACITE)*, IEEE, 2021, pp. 6–8.

[18] L. Y. Por, L. A. Adebimpe, M. Y. I. Idris, C. S. Khaw, and C. S. Ku, "LocPass: A graphical password method to prevent shoulder-surfing," *Symmetry*, vol. 11, no. 10, 2019, Art. no. 1252. doi: 10.3390/sym11101252.

[19] K. H. Al-Shqeerat and K. I. Abuzanouneh, "A hybrid graphical user authentication scheme in mobile cloud computing environments," *Int. J. Commun. Netw. Inform. Secur.*, vol. 13, no. 1, pp. 68–75, 2021.

[20] J. A. Herrera-Macías, C. M. Legón-Pérez, L. Suárez-Plasencia, L. R. Piñeiro-Díaz, O. Rojas and G. Sosa-Gómez, "Test for detection of weak graphic passwords in passpoint based on the mean distance between points," *Symmetry*, vol. 13, no. 5, 2021, Art. no. 777. doi: 10.3390/sym13050777.

[21] H. M. Seksak, K. M. Amin, and S. Zarif, "Choice-based Graphical Password (CGP) scheme for web applications," *IJCI. Int. J. Comput. Inform.*, vol. 10, no. 3, pp. 104–112, 2023. doi: 10.21608/ijci.2023.236026.1127.

[22] P. Andriotis, M. Kirby, and A. Takasu, "Bu-dash: A universal and dynamic graphical password scheme," in *HCI for Cybersecurity, Privacy and Trust*, Cham: Springer International Publishing, 2022, pp. 209–227.

[23] S. Abhijith, S. Sam, K. U. Sreelekshmi, T. T. Samjeevan, and S. Mathew, "Web based graphical password authentication system," *Int. J. Eng. Res. Technol.*, vol. 9, no. 7, pp. 29–32, 2021.

[24] A. Constantinides *et al.*, "Security and usability of a personalized user authentication paradigm: Insights from a longitudinal study with three healthcare organizations," *ACM Trans. Comput. Healthcare*, vol. 4, no. 1, pp. 1–40, 2023. doi: 10.1145/3564610.

[25] N. I. Dias, M. S. Kumaresan, and R. S. Rajakumari, "Deep learning based graphical password authentication approach against shoulder-surfing attacks," *Multiagent Grid Syst.*, vol. 19, no. 1, pp. 99–115, 2023. doi: 10.3233/MGS-230024.

[26] M. Bartłomiejczyk and M. Kurkowski, "Multifactor authentication protocol in a mobile environment," *IEEE Access*, vol. 7, pp. 157185–157199, 2019. doi: 10.1109/ACCESS.2019.2948922.

[27] A. Wells and A. B. Usman, "Privacy and biometrics for smart healthcare systems: Attacks, and techniques," *Inform. Secur. J.: A Glob. Perspect.*, pp. 1–25, 2023.

[28] S. A. Lone and A. H. Mir, "A novel OTP based tripartite authentication scheme," *Int. J. Pervasive Comput. Commun.*, vol. 18, no. 4, pp. 437–459, 2022. doi: 10.1108/IJPCC-04-2021-0097.

[29] D. Carrillo-Torres, J. A. Pérez-Díaz, J. A. Cantoral-Ceballos, and C. Vargas-Rosales, "A novel multi-factor authentication algorithm based on image recognition and user established relations," *Appl. Sci.*, vol. 13, no. 3, 2023, Art. no. 1374. doi: 10.3390/app13031374.

[30] M. A. Khan, I. U. Din, and A. Almogren, "Securing access to internet of medical things using a graphical-password-based user authentication scheme," *Sustainability*, vol. 15, no. 6, 2023, Art. no. 5207. doi: 10.3390/su15065207.

[31] G. Blonder, "Graphical passwords," United States Paten 5559961. Murray Hill: Lucent Technologies. Inc., 1996.

[32] F. Towhidi, M. Masrom, and A. A. Manaf, "An enhancement on Passface graphical password authentication," Doctoral dissertation, Universiti Teknologi Malaysia, Malaysia, 2010.

[33] M. Z. Osman and N. Ithnin, "Category-based Graphical User Authentication (CGUA) scheme for web application," in *Pattern Analysis, Intelligent Security and the Internet of Things*. Springer International Publishing, 2015, pp. 315–326.

[34] J. Goldberg, J. Hagman, and V. Sazawal, "Doodling our way to better authentication," in *CHI'02 Extended Abstracts on Human Factors in Computing Systems*, 2002, pp. 868–869.

[35] A. Vaddeti, D. Vidiyala, V. Puritipati, R. B. Ponnuru, J. S. Shin and G. R. Alavalapati, "Graphical passwords: Behind the attainment of goals," *Secur. Priv.*, vol. 3, no. 6, 2020, Art. no. e125. doi: 10.1002/spy2.125.

[36] M. A. S. Gokhale and V. S. Waghmare, "The shoulder surfing resistant graphical password authentication technique," *Procedia Comput. Sci.*, vol. 79, pp. 490–498, 2016. doi: 10.1016/j.procs.2016.03.063.

[37] A. L. C. Yeung, B. L. W. Wai, C. H. Fung, F. Mughal, and V. Iranmanesh, "Graphical password: Shoulder-surfing resistant using falsification," in *2015 9th Malaysian Softw. Eng. Conf. (MySEC)*, IEEE, 2015, pp. 145–148.

[38] M. Z. Jali, "A study of graphical alternatives for user authentication," Doctoral dissertation, Univ. of Plymouth, UK, 2011.

[39] Y. Meng, "Designing click-draw based graphical password scheme for better authentication," in *2012 IEEE Seventh Int. Conf. Netw., Archit., Storage*, IEEE, 2012, pp. 39–48.

[40] D. L. Nelson, V. S. Reed, and J. R. Walling, "Pictorial superiority effect," *J. Exp. Psychol.: Human Learn. Memory*, vol. 2, no. 5, pp. 523–528, 1976.

[41] E. Alesand and H. Sterneling, "A shoulder-surfing resistant graphical password system," 2017. Accessed: Sep. 20, 2024. [Online]. Available: https://api.semanticscholar.org/CorpusID:39022151.

[42] Y. Li, X. Yun, L. Fang, and C. Ge, "An efficient login authentication system against multiple attacks in mobile devices," *Symmetry*, vol. 13, no. 1, 2021, Art. no. 125. doi: 10.3390/sym13010125.

[43] L. V. Bonfati, J. J. A. Mendes Junior, H. V. Siqueira, and S. L. Stevan Jr., "Correlation analysis of in-vehicle sensors data and driver signals in identifying driving and driver behaviors," *Sensors*, vol. 23, no. 1, 2022, Art. no. 263. doi: 10.3390/s23010263.

[44] L. Y. Por *et al.*, "A systematic literature review on the security attacks and countermeasures used in graphical passwords," *IEEE Access*, vol. 12, pp. 53408–53423, 2024. doi: 10.1109/ACCESS.2024.3373662.

[45] L. A. Adebimpe *et al.*, "Systemic literature review of recognition-based authentication method resistivity to shoulder-surfing attacks," *Appl. Sci.*, vol. 13, no. 18, 2023, Art. no. 10040. doi: 10.3390/app131810040.

[46] A. F. Rasheed, M. Zarkoosh, and F. R. Elia, "Enhancing graphical password authentication system with deep learning-based arabic digit recognition," *Int. J. Inform. Technol.*, vol. 16, no. 3, pp. 1419–1427, 2024. doi: 10.1007/s41870-023-01561-8.

[47] M. Singh, V. Nedungadi, and R. Radhika, "A hybrid textual-graphical password authentication system with enhanced security," in *2023 Int. Conf. Netw. Commun. (ICNWC)*, IEEE, 2023, pp. 1–7.

[48] R. A. Y. Palash *et al.*, "GPOD: An efficient and secure graphical password authentication system by fast object detection," *Multimed. Tools Appl.*, vol. 83, no. 19, pp. 56569–56618, 2024.