IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 28 October 2024, accepted 17 November 2024, date of publication 21 November 2024, date of current version 3 December 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3503637

RESEARCH ARTICLE

A Dynamic and Incremental Graphical Grid Authentication Technique for Mobile and Web Applications

JIAMING GONG[1], OLUWATOBI NOAH AKANDE[2], (Member, IEEE), CHIA-CHEN LIN[3], (Member, IEEE), AND SAURABH AGARWAL[4]

[1]School of Economics and Management, Beijing Forestry University, Beijing 100083, China
[2]Department of Computer Science, Baze University, Abuja 251101, Nigeria
[3]Department of Computer Science and Information Engineering, National Chin-Yi University of Technology, Taichung 411, Taiwan
[4]Department of Information and Communication Engineering, Yeungnam University, Gyeongsan 38541, Republic of Korea

Corresponding authors: Chia-Chen Lin (ally.cclin@ncut.edu.tw) and Saurabh Agarwal (saurabh@yu.ac.kr)

This work was supported in part by the National Science and Technology Council under Grant NSC113-2410-H-167-012-MY3 and NSC113-2634-F-005-001-MBK.

ABSTRACT Knowledge-based authentication techniques remain one of the proven ways of maintaining confidentiality, ensuring integrity, and guaranteeing the availability of an information system. They employ what a user knows (Passwords or PINs) to authorize or grant access to an information system. While passwords employ a fixed combination of characters, Personal Identification Numbers (PINs) are majorly numbers. Existing implementations of these authentication techniques involve the repetitive use of static passwords and PINs at every login instance. These have been exposed to various attacks, such as keyloggers, shoulder surfing, brute force, and dictionary attacks. To overcome these attacks, this study presents an authentication technique where users' PINs are incremented during successive login attempts. Users are expected to choose a preferred incremental factor, which can be any number they can remember, that will be added to the default 6-digit PIN to produce a dynamic PIN that can be used in subsequent login sessions. Furthermore, an additional layer of security that involves the use of a dynamic 4 by 4 graphical grid was integrated into the proposed incremented PIN technique. At every login session, users are presented with a set of 16 possible PINs to choose from. The security analysis of the proposed authentication technique revealed that the proposed technique could resist existing password attacks, thereby enhancing security. A performance testing and usability analysis was also carried out among 1145 individuals who interacted with the web application that uses the incremental authentication technique. The questionnaire items were structured based on the constructs of the Unified Theory of Acceptance and Use of Technology (UTAUT) Model. Statistical analysis of the responses received showed an appreciable level of acceptance in terms of performance expectancy, effort expectancy, social influence, and facilitating conditions. The positive user acceptance results provide reassurance about the practicality and effectiveness of the proposed technique. It is believed that the proposed incremental graphical grid authentication technique will further enhance the security of our growing mobile and web applications.

INDEX TERMS Authentication techniques, information security, personal identification number, UTAUT model.

I. INTRODUCTION

The continuous advancements in Information and Communication Technologies (ICT) have made it possible for individuals, businesses, and organizations to conduct their

The associate editor coordinating the review of this manuscript and approving it for publication was Tyson Brooks.

daily activities over the Internet. These ICT advancements can be attributed to the widespread adoption of 4G & 5G networks, the rise of Artificial Intelligence and machine learning applications, the proliferation of the Internet of Things (IoT), and the rapid development of cloud computing technologies. According to Forbes, the total number of web applications available on the internet as of June 2024 was 1.1 billion, while 252,000 new websites are created daily [1]. Most of these websites are e-commerce websites used to conduct financial transactions. Also, according to Statista, between the years 2023 and 2030, it is anticipated that the number of IoT devices around the globe will almost double, going from 15.9 billion in 2023 to more than 32.1 billion in 2030 [2]. Most of these are industrial, consumer, enterprise, and medical IOT devices, which, if hacked, can result in substantial financial loss or eventual death of their users. Therefore, the continuous acceptance and growth of online applications always generate security concerns among cybersecurity experts. The truth of it all is that the World Wide Web's pervasive nature means that once information is put online, it leaves an electronic trail that can be exploited by cybercriminals, as seen in cases like the iCloud leak of Hollywood actresses' nude pictures [3]. So, the online realm is indeed exposed to various cyber threats, ranging from cyberbullying [4], [5] to malicious software attacks [6], financial fraud in online transactions [7], and sophisticated malware like ransomware targeting critical infrastructure and businesses [8], [9]. Therefore, the ubiquitous presence of the internet in daily life makes individuals vulnerable to cyber threats, necessitating increased awareness and efficient countermeasures to protect against hackers, data breaches, and other malicious activities [10]. Hackers continuously develop new methods to exploit vulnerabilities in online systems, making cyber-attacks a growing concern in today's technology-driven world [11]. From personal information security to safeguarding financial transactions and critical systems, the digital landscape requires continuous vigilance and proactive measures to mitigate the risks posed by cyber threats across various online activities and platforms. Therefore, implementing security measures is crucial to mitigating the risks of cyber-attacks in the online environment [12].

All security measures are aimed at guaranteeing confidentiality, maintaining integrity, and ensuring the availability of information systems. Authentication and authorization techniques are significant ways of achieving these [13]. Authentication refers to the act of confirming the identity of a user, device, or system. It is an essential element of security as it serves as the foundation for determining whether access to resources should be allowed or denied. Authentication measures use what a user knows (passwords, PINs, or answers to security questions), what a user has (tangible objects like smart cards, security tokens, or mobile phones), what a user is (unique biological and behavioral features like fingerprints, face, iris, typing patterns, voice, etc.) and where a user is (this uses the geographical location of the user as an authentication factor). Authentication measures based on what a user knows are widely referred to as knowledge-based authentication systems [14]. Authorization in security systems comes into play after a successful authentication. Authorization is the procedure of ascertaining and implementing the specific actions that an authenticated person or system is permitted to undertake within a given network or system. Therefore, while authentication confirms the user's identity, authorization regulates their access to resources and actions according to their identification and permissions.

Passwords and Personal Identification Numbers (PINs) are the most widely implemented and criticized knowledge-based authentication measures [15], [16], [17]. Passwords that are typically longer permit the use of alphabets (uppercase and lowercase), numbers, and special characters in any specified order. However, PINs, which are generally shorter, only allow the use of numbers and could be 4 to 6 digits long. Although password and PIN security are vulnerable to the growing number of cyber breaches and various cyber threats [18], they continue to be the most widely utilized security approach by companies globally in 2023 [14], [19] attributed to the vast usage of passwords to its simplicity, practicality, ease of use, low cost and lack of specialized hardware requirements. Remembering multiple passwords and PINs used across different web and mobile applications also remains an issue of concern among its users [20]. However, research has revealed that password management applications have been widely adopted to overcome this limitation, and their market is expected to grow to seven billion U.S. dollars by 2030 [19]. Nevertheless, the issue of password security has escalated significantly as a result of recent advancements in password attacks that exploit publicly exposed credentials, personal data, and sophisticated password prediction methods. These attacks raise doubts about the effectiveness of current password schemes and highlight the necessity for new methods to enhance their security.

Most importantly, knowledge-based authentication systems need to be resistant to two primary forms of attacks: capturing and guessing assaults [21]. Capturing refers to the act of obtaining the exact password or an extract of it. This could be achieved by utilizing keyloggers or witnessing the password being entered by shoulder-surfing. A guessing attack refers to the act of an attacker attempting to deduce the password through repeated trial and error. Depending on the situation, an attacker may have the ability to thoroughly explore the entire range of possible passwords (the complete set of passwords allowed by an authentication system), ensuring success, or they may be restricted in the number of attempts they can make. An attacker can leverage their understanding of password distributions to prioritize passwords with higher probabilities of being used by users. In order to withstand guessing attacks, authentication systems must possess a sufficiently vast theoretical password space and prohibit the usage of predictable patterns in user-selected passwords.

Efforts to enhance password security have led to the development of hybrid systems combining textual, recognition-based, and recall-based passwords, which have shown improved resistance against eavesdropping and guessing attacks. Furthermore, the ongoing evolution in user authentication techniques is highlighted by advancements like the FIDO2 authentication standard, which aims to replace passwords with biometric and possession-based authentication methods. Despite their vulnerabilities, passwords continue to be a popular choice for user authentication due to their balance between security and usability. A survey revealed that a combination of emails and passwords, software tokens, and Hardware Tokens are the most commonly used authentication methods by organizations, while biometric authentication, tokenless authentication, and social security credentials are the least used.

This study presents an innovative, robust password authentication technique that improves security and user experience through an innovative approach. The first step in the process involves the user selecting an initial four-digit password, such as "8700," and a personalized incremental factor, such as "4." The initial password is used for the first login, and the predetermined incremental factor increments the password for each subsequent login. The initial password is used for the first login. As an illustration, the sequence of consecutive passwords would be structured in the following manner: 8700, 8704, 8708, 8712, 8716, and so forth. The concept of incrementality in cryptography was first introduced in [23]. At any point in time, when an underlying message is modified, the digital signature of the message is expected to be updated. The proposed technique builds on this principle, where, for every successful login attempt by a user, the password is incremented instead of remaining static. If the user has logged in nine times, the password is expected to be incremented nine times. However, the user will choose the incremental factor. The incremental factor is likely to be between 01 and 99; however, to increase that password space, a two-digit incremental factor is advisable. An additional layer of security was also provided by using a dynamic GRID graphical approach to implement the proposed incremental authentication technique. For every login attempt, the user is expected to select the PIN from a 4 by 4 graphical GRID that changes the position of the current PIN from the possible option of sixteen (16) PINs.

The remaining sections of this article are structured as follows: Section II presents extensive related works, while Section III presents the methodology behind the proposed technique. Section IV discusses the study's results, while Section V provides a conclusion and future recommendations.

II. RELATED WORK

The literature has proposed and implemented several knowledge-based authentication techniques. Regarding the techniques employed in generating and storing passwords or PINs, existing knowledge-based authentication techniques can be categorized into challenge-response authentication techniques, graphical pattern-based techniques, and One-Time Passwords (OTPs).

A. ONE-TIME PASSWORD

OTPs are the most common dynamic improvements to static passwords. For every login attempt, a new password is generated and sent to the user's email or displayed on the user's hardware or software tokens. This has been widely employed in several financial mobile and web applications. For instance, authors in [24] introduced a multi-factor authentication technique. The proposed technique uses components such as communication routes, a Trusted Execution Environment (TEE), a password vault, and OTPs for data authentication and security. The password vault protects sensitive user IDs and access codes, and many communication channels lessen the likelihood of secrets falling into the wrong hands. In addition, the password vault can be securely updated at regular intervals. To ensure that web apps and an interactive remote shell are adequately protected from attacker-conducted penetration tests, the expiration period of the code in the Vault remains unchanged. For anonymous client authentication, authors in [25] also presented DGTOTP, a novel lightweight cryptographic method. The method enables the efficient generation of group-specific, time-based one-time passwords while concealing the identity of the real client; all that is revealed is their membership in the group. In a static group management situation, where all group members are required to be established during the group beginning phase, the security features of GTOTP with regard to traceability and anonymity have been described. A Merkle tree architecture and a family of chameleon hash functions were used to implement the proposed method. In the context of dynamic group management, the proposed approach offered improved security guarantees without resorting to random oracles. On top of that, authors in [26] suggested a solution that uses two-factor OTP. The suggested method of two-factor authentication makes use of both fixed and changing passwords. Users choose the static password, while a technique generates the dynamic password, and the latter is only suitable for a given amount of time. At the outset, users are required to provide authentication information, which consists of their username and password. The second step involves authenticating users by providing them with one-time passwords. The suggested method was determined to be effective in user authentication. In a similar vein, authors in [27] introduced a two-factor authentication method tailored to the safety of home equipment. The home appliance's electrically erasable programmable read-only memory stores the default password at startup. A randomization-based verification mechanism will be activated once the right password is entered. For two-factor authentication, a user's device—like a smartphone—transmits an OTP over a Bluetooth connection with another device. If the provided key or OTP is a match, the system will be unlocked, and the necessary task can be

initiated. Suppose either the key or the OTP is inputted incorrectly; access will be refused, and the user will be allowed a limited number of attempts. OTPs frequently necessitate users to possess an extra gadget or utilize an application to produce the password, which can be burdensome. In addition, OTPs transmitted by SMS can be intercepted if the communication route is compromised. Their limited duration can be a drawback in cases of user delay or time synchronization issues. In contrast to conventional passwords, OTPs require additional infrastructure for their generation, transmission, and validation.

B. GRAPHICAL PASSWORDS

In recent times, Graphical passwords, also known as the Graphical User Authentication (GUA) technique, have also been widely implemented in literature. Their friendly and attractive user interfaces have made them an acceptable option across several mobile and web applications. Kawamura, 2024 categorized them into recall, cued-recall, or recognition-based graphical authentication categories. In recall graphical authentication type, users are expected to remember and provide a sequence of passwords they have selected during registration. In this approach, no clue or hint will be provided to the users that will aid them in remembering their chosen passwords. However, in cued-recall alternatives, hints or clues can be provided to help users remember their chosen passwords if they have forgotten them. However, in recognition-based graphical authentication implementations, users are expected to identify and choose an image or text they have selected during the registration phase. Several instances of these categories of graphical authentication techniques have been proposed and implemented in the literature. This includes a graphical password authentication method, as presented in [28]. The authentication method employs a blend of encrypted one-time passwords and image authentication to secure and grant access to applications/apps on the Android platform. The server will provide a randomly generated encrypted one-time password for integration, which will only be usable for a single login session. Once the session is complete, it will be terminated. The AES technique is used to encrypt all passwords and critical data, even in the system's database. This alternative method is designed to strengthen the current authentication system by protecting it from data theft, shoulder surfing, and man-in-the-middle attacks. Furthermore, a graphical and pattern-based authentication technique was proposed in [29]. The technique expects the user to choose a set of images during registration; then, a unique pattern will be drawn with the images. During authentication, the users are expected to select the same set of images and draw the same pattern before access is granted. However, the position of the images will be rotated during every authentication period. With this arrangement, the technique was able to prevent shoulder surfing. Authors in [30] also integrated a 3D graphical authentication technique with Hyper Ledger Fabric blockchain technology. The proposed technique uses blockchain technology to reduce the risk of compromised credentials during the authentication process. Evaluation results revealed that the proposed technique was effective. Similarly, authors in [31] presented a method for creating graphical passwords to be drawn instead of selecting images. The technique utilized deep learning models to categorize the drawn images. The technique selectively transmits only the color pixels of the drawn images and not the entire image. The proposed technique achieved a good result based on login time, the overall data transmission rate, and password entropy. Camera recording attacks remain one of the limitations of some graphical password techniques; authors in [32] proposed a graphical authentication technique that is resistant to these camera recording attacks. Users are expected to provide five images to be used for authentication during registration. However, during authentication, a sufficiently distorted version of the images is presented to the user. It will be difficult for an attacker to recognize the original image because of the loss of feature points in the image as a result of cropping and distortion.

From the graphical password implementations explored so far, it can be deduced that graphical passwords require users to memorize and properly replicate a series of grid positions, which can be psychologically demanding. Occasionally, users may establish discernible patterns on the grid, thereby compromising the passwords' security. Furthermore, graphical passwords are vulnerable to social engineering attacks, in which users can be deceived into disclosing their grid patterns. Additionally, the number of possible combinations in graphical passwords can be restricted, mainly if the grid size is small.

C. CHALLENGE-RESPONSE PASSWORDS

Challenge-response passwords are authentication techniques where the authentication system prompts the user with a challenge, such as a question or a CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart), and requires the user to supply the accurate solution. Several implementations of this password technique have been proposed and implemented in the literature. Authors in [33] proposed a challenge-response authentication technique for the Programmable Logic Controller (PLC) system utilized in securing the Advanced Power Reactor (APR) of a Nuclear Power Plant (NPP). One side poses a question (''challenge''), and the other side gives the right answer (''response'') to authenticate using the given technique. To further strengthen security and reduce the likelihood of password reuse issues, the OTP authentication technique was also included in the challenge-response system. The system generates unique one-time passwords for each login session by integrating OTP technology, which significantly hinders the ability of attackers to intercept or undermine the authentication process. A challenge-response authentication technique that uses users' emotions for authentication

was presented in [34]. Users are expected to choose images of varying emotions, which will be subsequently used for authentication. The technique was verified to be an effective authentication technique. Authors in [35] also presented a two-layer authentication technique that could be used to verify the identity of users of financial mobile and web applications. The first layer uses the user's username and password, while the second layer employs a challenge-response technique. Performance evaluation based on security and usability revealed that the challenge-response technique, where users were asked personal questions, added a layer of security. This authentication technique is widely applied in Nigerian financial applications. However, some challenges presented to users could be complex to tackle and could waste much time, which could end up frustrating them. Yet, if common challenges that could be quickly resolved are presented to users, this could be easily explored by hackers as well. Therefore, the challenges must be well-randomized and balanced. In addition, implementing the technique may require more time and computational resources. Thus, careful planning must go into its implementation.

D. CAPTCHA PASSWORD TECHNIQUE

An example of challenge-based authentication is a CAPTCHA password, which uses a combination of text-based passwords and visual challenges to strengthen security further. The primary aim of the technique is to provide a variant of the graphical authentication technique with distorted texts and images that will make them resistant to dictionary attacks. Several variants of the CAPTCHA graphical authentication technique have been reported in the literature. Authors in [36] introduced a challenge-response authentication technique that uses CAPTCHA and AI complex problems. The technique throws a challenge at the user, and the user is expected to embed the response to the challenge in an image that will be uploaded to the server. The server is then expected to extract the password from the uploaded image. Once the extracted text is the expected response to the challenge, the user is authenticated and granted access. Authors in [37] also introduced a CAPTCHA-based graphical authentication technique called Devanagari CAPTCHA. Devanagari is a script that is based on Sanskrit and Hindi characters. Therefore, users are asked to reproduce a text in this script that has been blended with artificial noise and distortions so as to make it difficult for the computer bot to comprehend. The performance of the proposed technique was evaluated to be effective for user authentication. Similarly, a dynamic image CAPTCHA-based authentication technique that employed the concept of multi-secret sharing was proposed in [38]. The technique employed an image CAPTCHA that is divided into two pieces called shares. One share is the user share, while the second is the server's share. The user's share is imprinted on physical transparency while the server's share is in digital mode. For authentication purposes, the users are presented with multiple secret pictures with overlapping sets of shares at different angles. The technique was proposed to be effective in authenticating users of mobile and web applications. Similarly, a CAPTCHA authentication technique for mobile applications that was built on the concept of recall and cued recall was proposed in [39]. Users are presented with alphanumeric symbols, visual (V) symbols, and click symbols that can be used to draw a preferred shape or pattern on n×n grid points. The three categories of symbols from which users can draw their patterns result in huge password space (2.4 × 104 bits of entropy) combinations. The proposed technique proved to be effective in authenticating users who participated in the usability test, and it also proved to be resistant to shoulder surfing. Authors in [40] carried out a comparative study between two CAPTCHA schemes. The first scheme is an interactive hand-written CAPTCHA image, while the second is a text-based handwritten Arabic CAPTCHA scheme. In the text-based scheme, users are expected to type the Arabic text shown in the CAPTCHA image while they are expected to select broken joints that complete the displayed Arabic CAPTCHA image. The comparative results showed that the interactive scheme is more secure and effective than the text-based scheme. Authors in [41] introduced a technique that made CAPTCHA systems resistant to automated bots. The technique incorporated a deep learning approach to distinguishing between a human user and automated bots. The literature reviewed has shown that CAPTCHA-based authentication techniques are effective in preventing automated attacks. However, they suffer from usability, accessibility, security, and operational efficiency [42]. Yet, solving CAPTCHA can often be difficult for users if they are complex and challenging to understand. In terms of conversion rates, legitimate users may end up abandoning CAPTCHAs that they cannot solve, thereby denying them access to their applications. In addition, they are best suited for web applications and may not be appropriate for mobile applications due to their smaller screens. Most importantly, CAPTCHAs are resource-intensive as they require additional infrastructures for implementation and management, especially on high-traffic websites.

E. GRID-BASED PASSWORDS

GRID-based authentication techniques are special implementations of graphical user authentication techniques. Here, the images presented to users are combinations of grids whose positions may change during subsequent use. Therefore, users are expected to remember the sequence of grid positions used during the registration stage. A typical implementation of grid authentication was presented in [43]. When creating a password, users must click on particular cells in a grid to choose them as their password and memorize their position and associated static text. Upon subsequent login, users are required to remember the selected cells and input the variable text from each cell into a password field. The technology conceals the entered text in order to ensure its security, similar to a conventional text password. Developers of GridMap

set out to make it harder for brute-force attackers to guess passwords by expanding the key space of possible passwords. User research with 50 people confirmed GridMap's effectiveness. According to the study, GridMap is excellent for users who have to login a lot and who may discover personal significance in the map they choose, which makes it more memorable and enhances their experience. Another implementation called Passnumbers was proposed in [44]. Here, users are expected to select their passwords from the coordinates of graphical grid cells. Afterward, the passwords are encrypted based on the pixels of the image. The technique proved to be resistant to eavesdropping and shoulder surfing. Similarly, authors in [45] presented a grid graphical authentication technique that combines a verification grid with a map-slipping strategy. During registration, users are required to select a password route sequentially on a map. In addition to the password route, they are also expected to choose pre-generated grids as a specific verification grid for subsequent authentication. Therefore, the complete password is a combination of the selected route and the pre-generated grids. During the authentication, the users are expected to slip the map so that each point on the password route sequentially fits inside the verification grid. The map-slipping strategy and the specific verification grid introduced proved to be resistant to shoulder-surfing attacks. Remembering the chosen patterns on a grid is a significant requirement of graphical grid authentication techniques. In contrast, the number of possible combinations in a smaller grid could be a considerable challenge.

In addition to the categories of knowledge-based authentication techniques reviewed so far, there have been instances where biometric features have been employed for authentication or where biometric features are combined with traditional passwords to form multifactor authentication techniques. Such was introduced in [46]. In their implementation, users' facial image, an image generated from the password provided, and another special image chosen by the user were employed as a multifactor authentication technique. Another unique knowledge-based authentication technique was BrightPass, which was proposed in [47]. The proposed technique uses the brightness of the smartphone screen in combination with the PIN selected by the user. During authentication, if the brightness of the circle containing the PIN is high, the user is required to input the correct PIN digit. Whenever the user encounters a situation that appears unfavorable, they must input a deliberately wrong. However, authors in [48] showed that the original BrightPass approach is susceptible to recording attacks. Hence, an improved version of BrightPass that incorporates three distinct methods was proposed. Each of the three authentication techniques employs a distinct secret key that is separate from the original PIN. The first method involves extracting the secret key from a 2×5 matrix and utilizing it alongside the original PIN for authentication purposes. The 4-digit secret key is obtained by using the original PIN. The second approach involves acquiring the secret key through a graphical interface that relies on password-based authentication. The initial 10 cells are populated with random orientations, and the subsequent twenty-five cells are filled with random digits ranging from 0 to 9. The third option eliminates the requirement for a second authentication step by conducting the authentication process only within the graphical password-based interface. Although the authentication techniques reviewed so far provide certain advantages and can improve security in specific situations, they also have specific constraints that must be carefully addressed to maintain the overall security and usability of information systems. However, the proposed incremental graphical grid authentication technique significantly differs from existing authentication techniques, majorly due to its dynamic and incremental approach to password creation and use. Existing graphical and grid authentication techniques employ a static approach to PIN generation and use. The generated PINs remain the same for every login. However, the proposed technique presents a dynamic PIN that changes at every login session. In addition, the position of the PIN on the grid is also dynamic; this adds an additional layer of security against shoulder surfing or pattern recognition.

III. METHODOLOGY

The flow of processes in the proposed technique is presented in Figure 1. During the registration phase, the user is expected to provide an email address, a 6-digit PIN, and an incremental factor between 01 and 99. To provide an additional layer of security against brute force attacks, the provided PIN is hashed using SHA-256. Therefore, should the database used to store the PIN be compromised by an attacker, the original PIN cannot be retrieved except with the hash values of the PIN. During the login phase, a registered user is expected to login with the incremented PIN and not the original PIN (even during the first login after registration). In case users forget their PIN, they are allowed to attempt to login thrice before being hindered from login in further. However, users are allowed to reset their PIN and choose a new PIN and an incremental factor at any point. The authentication phase is activated when a user attempts to login. The incremental factor is subtracted from the provided PIN, while the result is compared with the stored hashed value of the original PIN. Once it has been confirmed that a correct PIN is provided, the users will be granted access to their applications, and a notification will be sent to their email addresses.

A. INCREMENTAL PIN GENERATION

The process of generating the incremental PIN is the following:

1) HASHING THE PROVIDED PIN

To ensure the security of the provided PIN against brute-force attacks, the 6-digit PIN is transformed into a fixed-length cryptographic hash using the SHA-256 algorithm. Hashing provides a non-reversible one-way transformation of the original PIN. It involves the following steps:

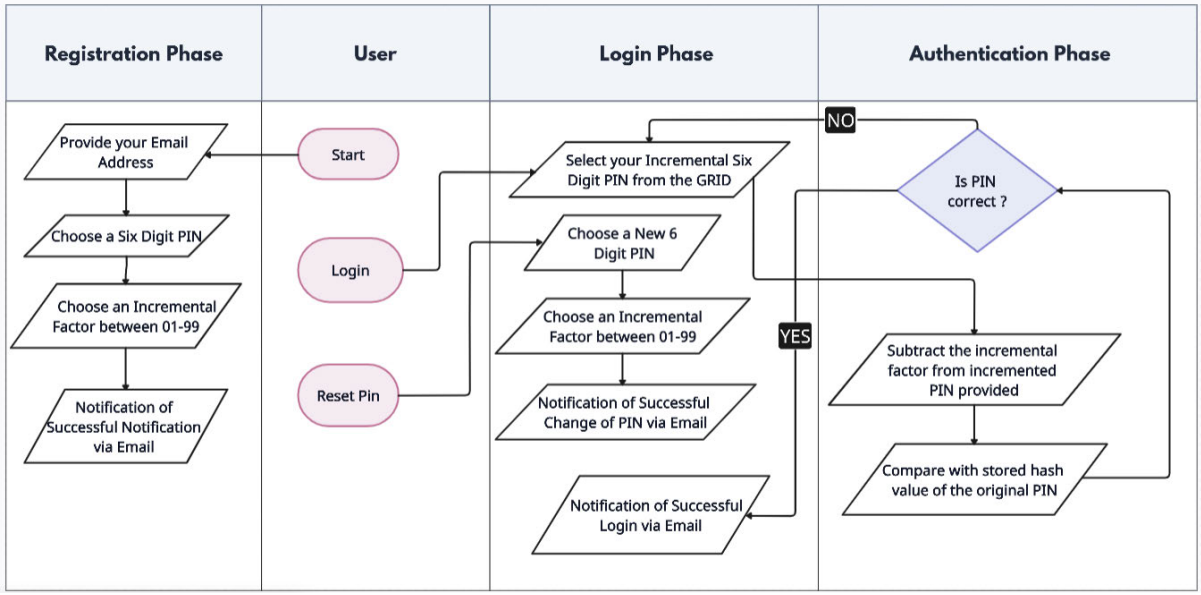

FIGURE 1. Flow of processes in the proposed technique.

- Using the provided 6-digit PIN as an input
- Padding the input PIN so that its length is congruent to 448 modulo 512
- Appending the length of the input PIN to the padded input as a 64-bit big-endian integer.
- Breaking the padded input into 512-bit blocks in chunks
- Compressing the padded input in chunks into a 256-bit output

Haslib module in Python was used to implement the SHA-256. For instance, the SHA-256 hash value for a PIN: 123456 is: e1d1993a11f16e0ccf406bdf5e01058e3b6765db4 4e42957b524738957c8988c

2) GENERATING RANDOM NUMBERS USING LINEAR CONGRUENTIAL GENERATOR (LCG) ALGORITHM

Linear Congruential Generator (LCG) algorithm is one of the most common pseudo-random number generators. It generates a sequence of numbers using equation (1) such that:

$$Y_{n+1} = a_n^{*Y} + k \; mod \; p \tag{1}$$

where Y_n is the sequence of random numbers and Y_0 is the seed (here, the 6-digit PIN), a is the multiplier used to generate the pseudorandom sequence, and c is the increment. At the same time, p is the modulus, and mod is the modulus operation. Its pseudocode is:

Algorithm LCG(seed, a, k, p, n):
  Inputs:
    Seed: initial value (Y_0)
    a: multiplier
    k: increment
    p: modulus
    n: number of random values to generate
  Output:
    Sequence of n pseudorandom numbers
  Step 1: Initialize
    Y_0 = seed
    i = 0
    Output_list = []
  Step 2: Generate n random numbers
    while i < n:
     $Y_1 = a*Y_0 + k \; mod \; p$
    Append Y_1 to Output_list
    $Y_0 = Y_1$
    i = i + 1
  Step 3: Return the Output_list

3) GENERATING A 4 × 4 GRID USING THE RANDOM NUMBERS GENERATED BY THE LCG ALGORITHM AND THE INCREMENTED PIN

The pseudocode goes thus:

a. Start
b. Input:
- Fifteen (15) random_numbers generated using the LCG algorithm
- The calculated incremental PIN

c. Randomize the position of the incremental PIN:
- Generate a random index between 0 and 15 (inclusive).
- If the correct PIN is not already at this index, swap the number at the random index with the correct PIN.

d. Initialize an empty 4 × 4 grid.
e. Assign the numbers from the random_numbers list to the grid:
- For i = 0 to 15:

Assign random_numbers[i] to grid position:
  row = i // 4
  column = i % 4

f. Display the grid:

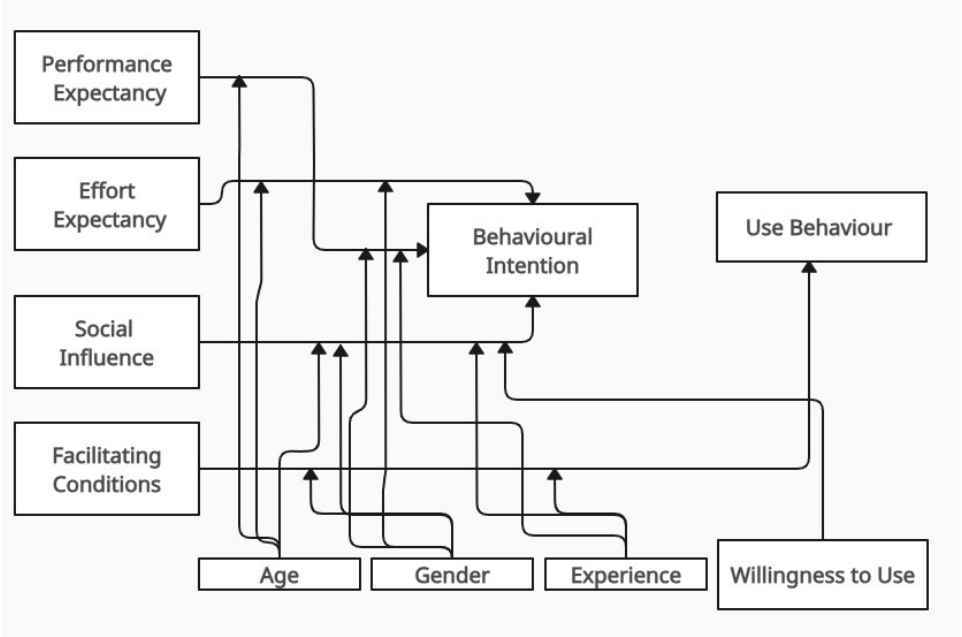

FIGURE 2. UTAUT model [49].

For each row in the grid:
Print the row with numbers separated by spaces.
g. End
4) Presenting a dynamic 4 × 4 grid to the user.

B. PERFORMANCE EVALUATION OF THE PROPOSED INCREMENTAL AUTHENTICATION TECHNIQUE

A web application was developed to evaluate the proposed technique's performance. HTML, CSS, JavaScript, and the React framework were used for the front-end development, while MySQL was used as the database. Python and Node.js were used to implement the authentication service. The web application was hosted on a local host, and users were allowed to create an account and interact with it via the University's intranet service.

The proposed technique was analyzed for security and Usability via the UTAUT Model. Its security analysis was carried out against known password attacks, such as brute force, dictionary, phishing, social engineering, and malware or virus intrusions.

1) USER ACCEPTANCE AND USABILITY ANALYSIS

The user acceptance and usability analysis of the proposed model was conducted using the Unified Theory of Acceptance and Use of Technology (UTAUT) Model presented in Figure 2. The UTAUT theory was introduced in [49] to examine people's willingness to accept and use a new technology. The model opines that people's intention to accept technology is dependent on their behavioral intention, while constructs such as facilitating conditions, effort expectancy, performance expectancy, and social influence determine if they will actually adopt and use the new technology. Performance Expectancy (PE) evaluates the degree to which users believe that using a technology will help them improve their job performance. At the same time, Effort Expectancy (EE) measures how easily the users can use the new technology. Social Influence evaluates the extent to which users believe that other users' opinions could persuade them to either use or ignore the new technology. At the same time, Facilitating Conditions (FC) measures the extent to which users perceive that their organizations have the needed technical infrastructure that could help them while using the new technology. How strong a predictor is on purpose is based on how age, gender, experience, and willingness to use affect it. The effect of all four indicators is tempered by age. The connections between effort expectancy, achievement expectancy, and social influence are different for men and women. The strength of the links between effort expectation, social impact, and facilitating conditions can be changed by experience. The only thing that changes the link between social influence and behavioral intention is how voluntary the use is [49].

Five questions each were prepared to evaluate users' opinions about each of the four UTAUT constructs. The questions were structured as presented in Table 1. The respondents were allowed to decide if they Strongly Agreed (SA), Agreed (A), Disagreed (D), or Strongly Disagreed (SD) with the questions asked. There was no provision for the respondents to be neutral so as to have an all-inclusive response to the questions asked.

2) POPULATION SAMPLE

One thousand One hundred and forty-five (1145) respondents participated in the evaluation process. These are participants

TABLE 1. Questions used to evaluate the UTAUT model constructs.

UTAUT Constructs	Questions
PE1	Using the proposed incremental graphical GRID authentication technique will enhance the security of my application.
PE2	This technique will help me manage my password more efficiently than traditional password methods.
PE3	The technique will improve my login experience in terms of speed and reliability.
PE4	This new authentication method will help me achieve my security goals more effectively when accessing the application.
PE5	This new authentication method will make my other security tasks easier to accomplish
EE1	The process of setting up my initial password and incremental factor is straightforward.
EE2	I will not have difficulties remembering and using successive passwords generated by the incremental factor.
EE3	The process of using this incremental password technique is intuitive.
EE4	Transitioning from my current password system to this new one will require little effort.
EE5	This new authentication technique is user-friendly.
SI1	It is important to me that my peers and colleagues think positively about this new password system.
SI2	My supervisors or managers will support the use of this incremental password system.
SI3	The opinions of my friends and family influence my decision to use this new authentication method.
SI4	Influential people in my organization would endorse this new system.
SI5	Based on my perception of its acceptance among my peers, I am likely to recommend this incremental password system to others.
FC1	There is adequate technical support available to help me use this new authentication technique.
FC2	My organization has the necessary resources to implement and maintain this technique effectively.
FC3	There are sufficient training materials and resources available to help me understand and use this technique.
FC4	The existing IT infrastructure in my organization can support this new authentication technique well.
FC5	I am confident that the technical support team will quickly address any potential issues with the new password technique.

of an ongoing Digital Skills Acquisition program and undergraduate students of Baze University, Abuja.

IV. RESULTS AND DISCUSSION

A. THE WEB VERSION OF THE DEVELOPED AUTHENTICATION TECHNIQUE

Figure 3 shows the simple registration page used to capture users' email addresses, default PINs, and incremental factors, while Figures 4 and 5 show the two consecutive login pages of the same user. The users are expected to select the incremental PIN needed to log in to their mobile or web applications in these two instances. Based on the chosen default PIN (123456) and incremental factor (14), the correct incremented PIN ought to be 123470 for the first login attempt and 123484 for the second login attempt. It should be observed that the first incremented PIN is in row 1, column 3 of the grid shown in Figure 4, while the second incremented PIN is in row 4, column 3 of the grid shown in Figure 5. Users who cannot remember their PIN can attempt to log in thrice before they are advised to reset their PIN using the interface shown in Figure 6.

B. SECURITY ANALYSIS OF THE PROPOSED TECHNIQUE

The security of the proposed technique was analyzed against known attacks.

1) BRUTE FORCE ATTACK

A brute force attack occurs when hackers systematically try to guess the password by generating all possible combinations of the passwords until the correct one is found. This attack is computationally intensive and can be very time-consuming, especially if the password is long and complex. Brute force attacks leverage the power of modern computers to try as many combinations as possible in a short amount of time. The incremental password technique offers superior protection as the password changes with each login, requiring hackers to start the brute force process anew each time. Even if the hacker sees the PIN initially used, once the hacker is not aware of the incremental authentication type or the incremental factor, the chances of becoming prey to brute-force attacks are low. The PINs are only valid for a particular session, as they are incremented during the next login session. This is why the incremental factor should be a two-digit number that increases the search space. Therefore, the dynamic nature of incremented PIN increases the complexity exponentially, making it impractical for attackers to brute force the entire sequence within a reasonable time frame.

2) DICTIONARY ATTACK

A dictionary attack uses a pre-defined list of possible passwords, known as a "dictionary," to guess the authentic password. This list typically contains common passwords, phrases, or words that people are likely to use. The attacker systematically tries each word in the dictionary until the correct password is found. This method is faster than brute force since it narrows down the possibilities to common choices. However, the proposed technique enhances security by requiring both an initial password and an incremental factor, making it more resilient against dictionary attacks as it adds a layer of protection. Efforts of the hackers have been doubled as they now have to crack two pieces of information, thereby reducing the effectiveness of dictionary attacks over time.

3) SHOULDER SURFING

Shoulder surfing involves a hacker physically observing the target as they enter their password. This can happen in public places, such as cafes or on public transportation, where someone can easily watch the keyboard or screen. Shoulder surfers might also use cameras or binoculars to gain a better view. However, the one-time validity nature of the incremented PIN makes it resilient to shoulder surfing. If a hacker records your PIN while entering it, it will not be helpful for subsequent login sessions. Also, the graphical grid interface provides

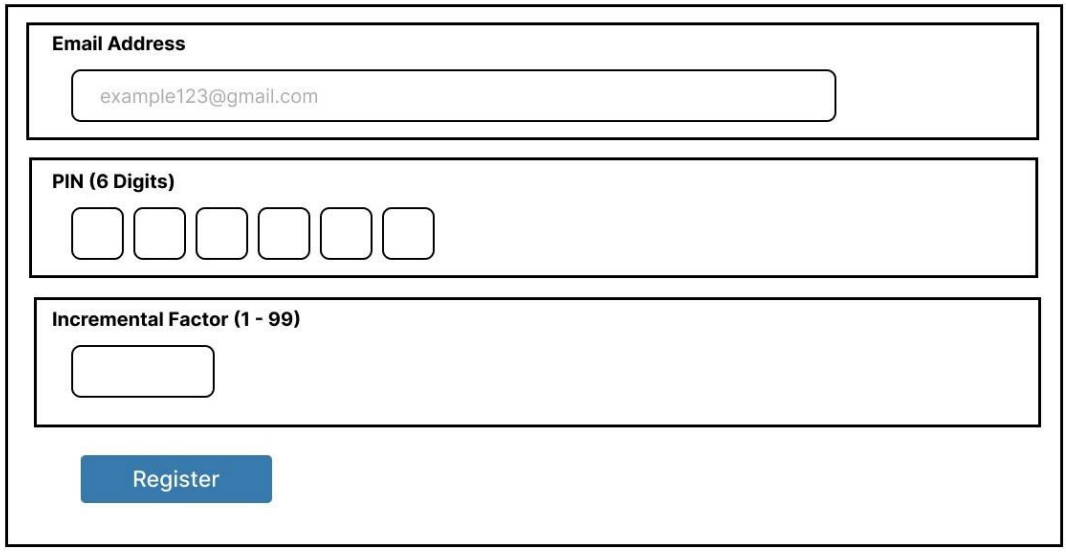

FIGURE 3. Registration page.

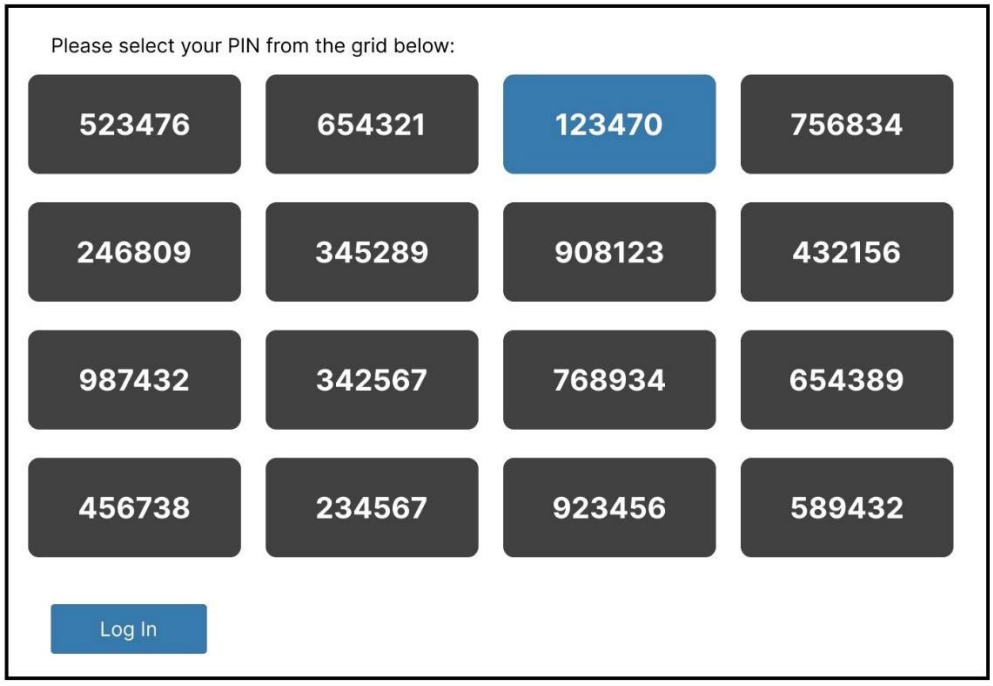

FIGURE 4. First login attempt for user one.

better protection against shoulder surfing, as the dynamic presentation and the need to select the correct option from a grid complicates observation efforts. So, if the hacker sees the PIN being selected, once the hacker is not aware that the password is an incremental one and does not know the incremental factor, the user is secured. Also, the grid's dynamic nature means the displayed options can vary, making it difficult for an observer to determine the correct password from a single observation.

4) ADVANCED PHISHING

Phishing is a technique where a hacker tricks the victim into revealing their password or other sensitive information by pretending to be a legitimate entity. This often involves fraudulent emails, websites, or messages that look like they come from a trusted source, such as a bank or an online service. Once the victim enters their credentials on the fake site, the attacker captures the information. However, the technique significantly reduces the utility of captured

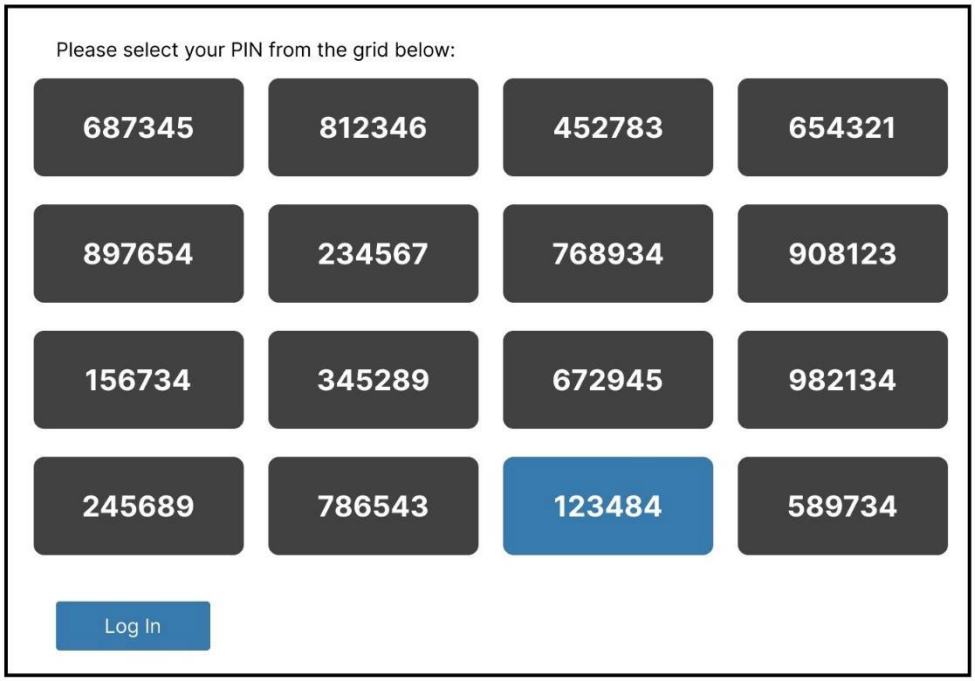

FIGURE 5. Second login attempt for user one.

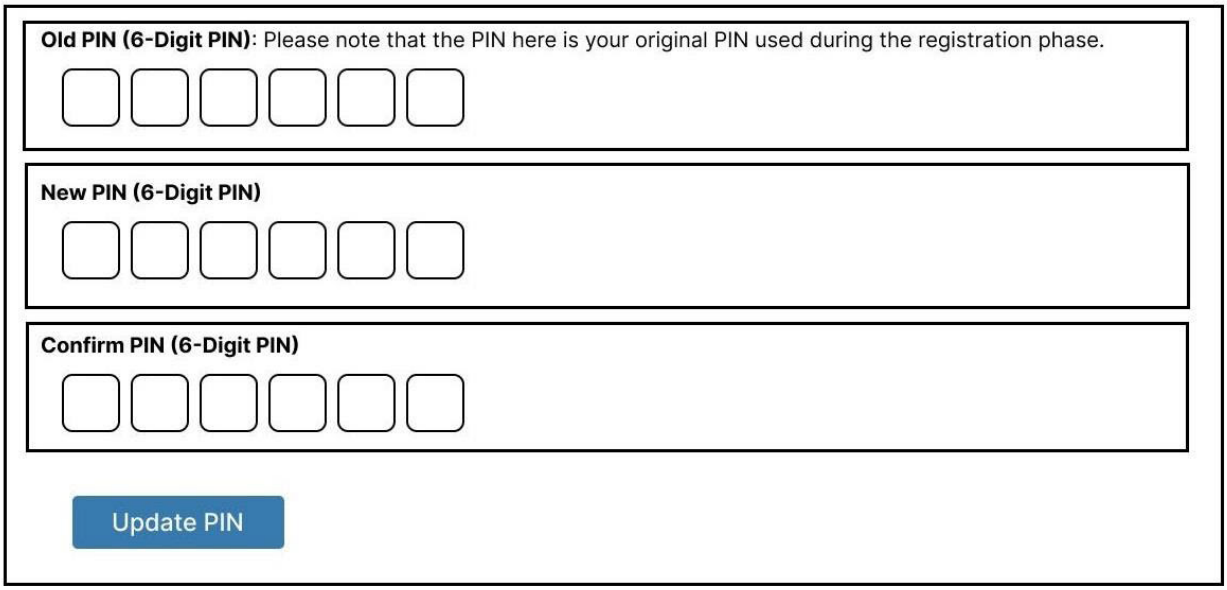

FIGURE 6. Interface to change PIN.

passwords since each password is only valid once. Even if the initial password is phished, the incremental nature means the attacker would need to continue phishing for each subsequent login. However, if the initial password and the incremental factor are captured during the registration stage and the hacker is aware of what the incremental factor is, then the user could be a victim of phishing attacks.

5) SOCIAL ENGINEERING

Social engineering attacks manipulate individuals into divulging confidential information. This can involve psychological manipulation, where the attacker exploits human behavior and trust. Examples include pretexting (creating a fabricated scenario to trick someone), baiting (offering something enticing to get the victim to reveal information), and tailgating (following someone into a secure area). If the

users could still be tricked into revealing their initial password and incremental factor, then subsequent passwords could be predicted. Therefore, education about the importance of not disclosing the default password and the incremental factor, as well as the need for vigilance even with dynamic passwords, is essential.

6) MALWARE OR VIRUS INTRUSIONS

Malware or virus intrusions involve malicious software that is installed on a victim's computer or device. This software can capture passwords through keyloggers (which record every keystroke made on a device), screen scrapers (which capture images of the screen), or by exploiting vulnerabilities in the system to gain access to stored passwords. Malware can be delivered through various means, such as email attachments, malicious websites, or infected software downloads. However, the proposed technique limits the usefulness and longevity of captured incremented PINs since they change with each login. However, if the initial password and incremental factor were captured during the registration stage, then the user could be a victim of malware or virus intrusions. Yet, this is possible if and only if the hacker is aware that an incremental password is being used. Nevertheless, continuous protection against malware is essential for all applications.

7) REVERSE ENGINEERING

This is an attack where the attackers acquire successive PINs that have been used and try to examine the PINs and their generation process so as to unveil the logic behind the password generation. Existing authentication techniques are more vulnerable to reverse engineering than the proposed dynamic authentication techniques. Successive PINs in existing authentication techniques are the same in every login session. Therefore, they can be easily revealed through reverse engineering. However, the one-time use nature of the proposed PIN authentication technique, incremental factor obscurity, and the dynamic nature of its presentation on a graphical grid present multiple barriers a hacker must overcome before breaking the proposed technique. Nevertheless, no matter how secure an authentication technique is, it is the responsibility of the users to ensure they protect their PINs and not reveal them to anyone so as to make them resistant to social engineering.

8) AI-BASED PATTERN RECOGNITION ATTACKS

AI-based pattern recognition attacks employ machine and deep learning techniques to unveil password patterns. With increasing attempts, AI can predict correct user patterns and passwords. Therefore, the attack is evolving in cybersecurity, especially against authentication techniques that do not employ enough randomness or dynamic elements. The proposed techniques exhibit some strengths and weaknesses against AI-based pattern recognition attacks. Its one-time PIN usage, dynamic grid PIN display, and incremental PIN generation nature are the strengths of the proposed technique. However, an advanced AI attack could correctly predict the incremented passwords after a number of simulations.

Nevertheless, the proposed incremental graphical GRID authentication technique enhances security against various forms of attacks. The incremental nature of the password, the dynamic display of the password on the grid, the uniqueness of the technique, and the hackers' ignorance of the type of authentication technique being used are added advantages that the technique has come to offer.

C. ACCEPTANCE AND USABILITY ANALYSIS OF THE PROPOSED TECHNIQUE USING THE UTAUT MODEL

Five questions were used to evaluate each of the UTAUT variables (PE, SI, EE, and FC). This section analyzes the responses received.

1) PERFORMANCE EXPECTANCY

Five questions were used to evaluate the performance expectancy of the proposed technique. The first variable was used to examine whether using the proposed incremental graphical GRID authentication technique would help respondents advance their job performance. As presented in Figure 7, nine hundred and nineteen (919) respondents agree, while one hundred and eighty-one (181) respondents disagree. This shows that 84% of the respondents believed that the proposed technique would enhance the security of their applications. The second variable was used to examine if the technique would help respondents manage their PIN more efficiently compared to traditional password methods. Nine hundred and ninety-two (992) respondents agreed with this, while two hundred and eight (208) respondents disagreed. When the respondents were asked if the proposed technique would improve their login experience in terms of speed and reliability, 76% of the respondents agreed to this. Eighty-one (81) percent of the respondents agree that adopting the proposed technique will help them achieve their security goals more effectively. At the same time, eight hundred and twenty-five (825) decided that the new authentication method would make their other security tasks easier to accomplish. Therefore, an average of 81% of respondents agreed that the proposed authentication technique will enhance the security of their applications.

2) EFFORT EXPECTANCY

This variable was used to examine how easily the respondents could use the proposed technique. As presented in Figure 8, when the respondents were asked if the process of setting up their initial password and incremental factor was easy, 88% (969) of respondents agreed. Similarly, the respondents were asked if they would need help remembering and using successive passwords generated by the incremental factor. 33% of the respondents envisaged they could have some challenges when trying to remember the incremental passwords needed to login to their applications. Also, 82% (900) of the respondents agree that the proposed technique is intuitive, while 74% (819) respondents agree that transitioning from

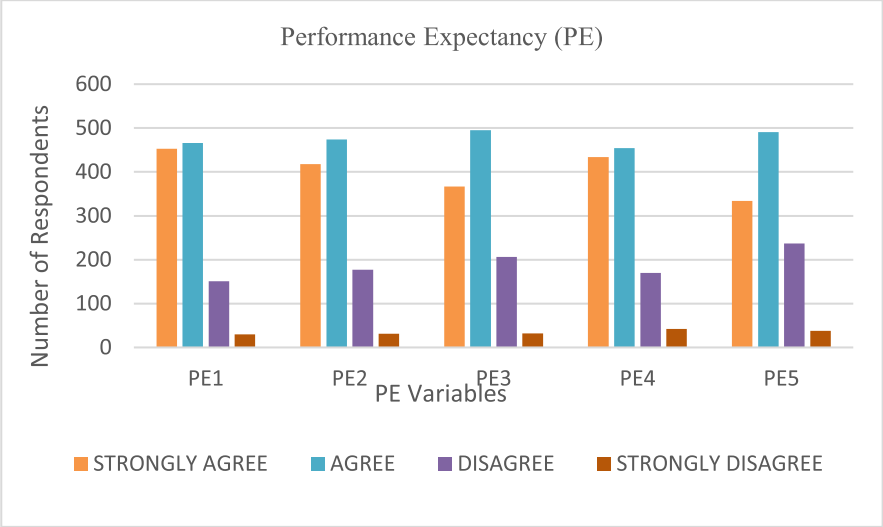

FIGURE 7. Analysis of the performance expectancy.

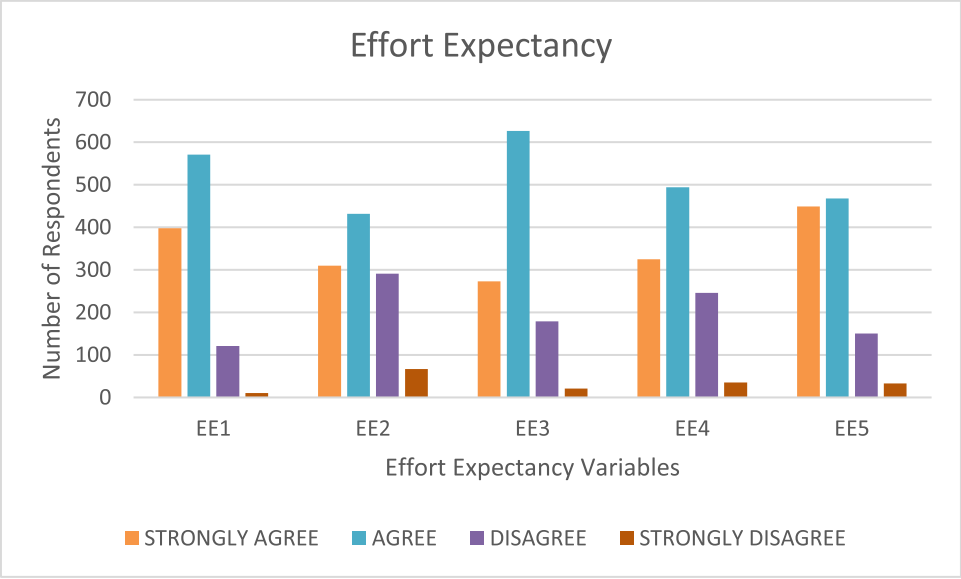

FIGURE 8. Analysis of the effort expectancy.

their current password system to the proposed method will require little effort. Finally, 83% (917) of the respondents agreed that the new authentication technique is user-friendly.

3) SOCIAL INFLUENCE

As a social being, the opinions of people around us could either motivate us to accept or refuse to use a new technology. The social influence variable was used to examine this. As presented in Figure 9, 82% (904) of respondents agree that it is essential that their peers and colleagues think positively about this new authentication technique. On the contrary, 46% (509) of respondents disagree that the opinions of their friends and family could influence their decision to use the new authentication technique. This connotes that the opinion of their colleagues at work matters regarding the choice of the authentication technique, but the opinion of their family members does not matter. Furthermore, if the views of their colleagues in their place of work are not positive, then they may not accept the usage of the proposed authentication technique. However, 78% (854) of the respondents are of the opinion that their supervisors or managers will support the use of the incremental authentication technique. Also, 74% (810) of respondents agree that Influential people in their organization would endorse the proposed technique. This may be senior members of staff in their organization. However, 26% (290) of respondents disagree with this. It is pleasing to know that 81% (893) of respondents are willing to recommend the proposed technique to others based on

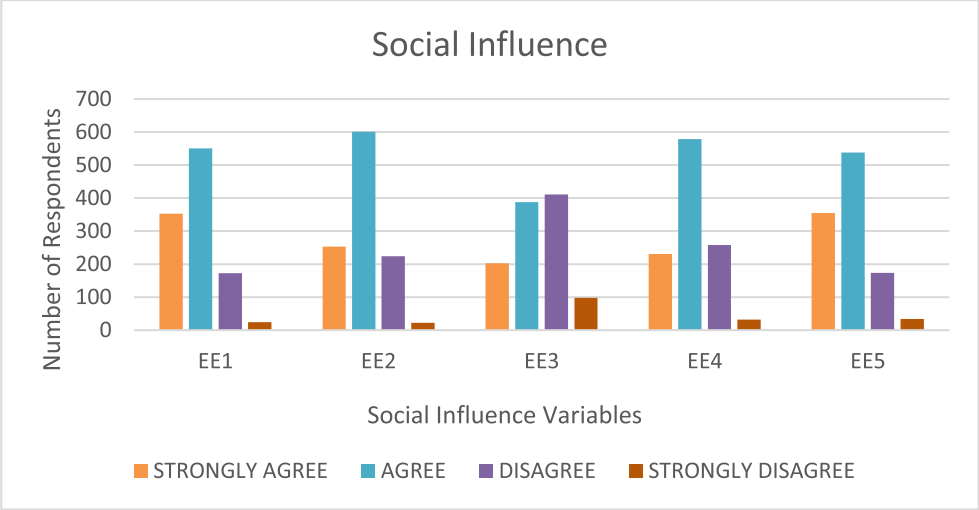

FIGURE 9. Social influence variables.

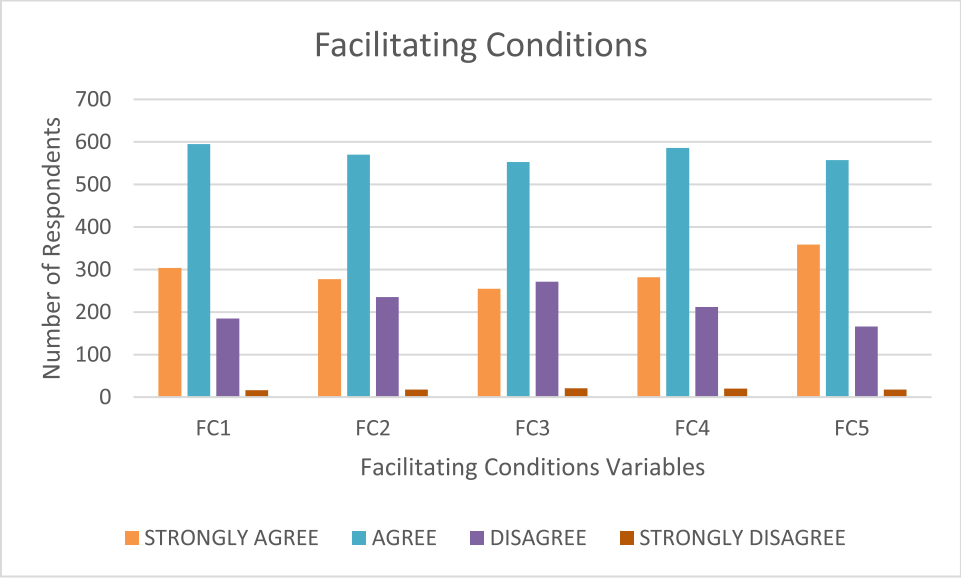

FIGURE 10. Facilitating conditions variables.

their perception of its acceptance among their peers; 19% (207) respondents are not willing to recommend the proposed technique.

4) FACILITATING CONDITIONS

Certain technologies may require some infrastructures (software, hardware, or peopleware) for the effective implementation of a new technology. This factor was used to measure the extent to which the respondents believed that their organizations have put in place such infrastructures. From the results presented in Figure 10, when the respondents were asked if their organizations have adequate technical support that can help them use the new authentication technique (FC1), 82% (899) of the respondents agreed. In comparison, 18% (201) disagreed. However, 77% (847) of the respondents agreed that should their organizations be interested in implementing the new technique, their organizations have the necessary resources to implement and maintain the technique effectively (FC2). Similarly, 79% (868) of the respondents agreed that the existing IT infrastructure in their organization can support this new authentication technique (FC4). Moreover, 83% (916) of the respondents are confident that any potential issues with the latest authentication technique would be quickly addressed by the technical support team of their organization. Additionally, 73% (808) of the respondents (FC3) agreed that there are sufficient training materials and resources available to

help them understand and use the proposed authentication technique.

D. STATISTICAL ANALYSIS OF THE SURVEY RESPONSES BASED ON UTAUT MODEL CONSTRUCTS

1) PERFORMANCE EXPECTANCY

Table 2 presents a detailed statistical analysis of the responses received based on the performance expectancy items. A count value of 4 indicates the total number of options that each respondent responded to, while the mean value shows that the average number of responses across all questions is 286.25 for each category. The variability of the responses was determined by computing their Standard Deviation. For instance, PE1 (Using this incremental password system will enhance the security of my application) has a standard deviation of 226.94, suggesting higher variability compared to PE5(This new authentication method will make my job tasks easier to accomplish), which has a standard deviation of 198.38. This connotes that most of the respondents are positively inclined to PE1 than PE5. The minimum and maximum metrics are the lowest and highest counts of responses. For example, the minimum number of ''Strongly Disagree'' responses is 31 for PE1, while the maximum number of ''Agree'' responses is 518 for PE3. This connotes that PE1 received the least ''Strongly Disagree'' responses while PE3 received the highest number of ''Agree'' responses. PE1 received the highest number of ''Strongly Agree'' responses. The percentiles computed the distribution of the responses. For instance, 25% of the responses for PE1 are below 127, and 75% are below 476.25. The negative skewness values indicate a slight left skew for each variable. This means that there are relatively fewer lower values (e.g., ''Strongly Disagree'' responses) and more higher values (e.g., ''Strongly Agree'' responses). This connotes that a significant number of respondents have a favorable opinion towards the proposed technique (more ''Agree'' and ''Strongly Agree'' responses). Therefore, the respondents have a positive perception of the proposed technique. Furthermore, all the kurtosis values are negative, indicating that the distributions are flatter than a normal distribution (platykurtic). A platykurtic distribution suggests that the responses have lighter tails and a flatter peak when compared to a normal distribution. This means there are fewer extreme values (outliers) than in a normal distribution. The presence of negative kurtosis suggests that the responses to the performance expectancy are generally consistent, without many outliers. This connotes that there is a more uniform perception among the respondents, and this is a wide range of acceptance levels.

TABLE 2. Statistical analysis of the responses to performance expectancy construct.

Statistics	PE 1	PE2	PE3	PE4	PE5
Count	4	4	4	4	4
Mean	286.25	286.25	286.25	286.25	286.25
Std. Deviation	226.94	217.10	210.45	210.64	198.38
Minimum	31.00	32.00	33.00	44.00	39.00
25th Percentile	127.00	144.50	166.50	143.00	193.50
Median (50th)	317.00	309.50	297.00	315.00	296.50
75th Percentile	476.25	451.25	416.75	458.25	389.25
Maximum	480.00	494.00	518.00	471.00	513.00
Skewness	-0.155	-0.195	-0.137	-0.187	-0.162
Kurtosis	-1.796	-1.664	-1.387	-1.747	-1.164

2) EFFORT EXPECTANCY

Table 3 presents the statistical analysis of the responses received from the effort expectancy constructs. EE1 has the highest standard deviation value of 258.45, suggesting higher variability compared to EE2, which has a standard deviation of 177.89. This connotes that most of the respondents are positively inclined to EE1 than EE5. Also, the minimum number of ''Strongly Disagree'' responses is 10 for EE1, while the maximum number of ''Agree'' responses is 651 for EE3. This connotes that EE1 received the least ''Strongly Disagree'' responses while eE3 received the highest number of ''Agree'' responses. EE1 received the highest number of ''Strongly Agree'' responses. The distribution of the responses was captured with the percentile values. For instance, 25% of the responses for EE1 are below 110.25, and 75% are below 421.50. The skewness values are generally close to zero, indicating that the distribution of responses is approximately symmetrical for most items. For instance, EE3 has a slight positive skew (0.022), while the other items have slight negative skew values, indicating a tendency towards lower values in those responses. Also, all kurtosis values are negative, indicating that the distributions are flatter than a normal distribution (platykurtic). This suggests fewer extreme values and a more uniform distribution of responses.

TABLE 3. Statistical analysis of the responses to effort expectancy construct.

Statistics	EE 1	EE2	EE3	EE4	EE5
Count	4	4	4	4	4
Mean	286.25	286.25	286.25	286.25	286.25
Std. Deviation	258.45	177.89	267.11	199.71	221.73
Minimum	10.00	67.00	21.00	35.00	36.00
25th Percentile	110.25	192.25	130.75	189.50	139.50
Median (50th)	370.50	263.50	236.50	296.00	288.50
75th Percentile	421.50	357.50	391.00	392.75	435.25
Maximum	595.00	451.00	651.00	518.00	532.00
Skewness	-0.324	-0.114	0.022	-0.285	-0.221
Kurtosis	-1.925	-1.675	-1.840	-1.828	-1.717

3) SOCIAL INFLUENCE

The statistical analysis of the responses to the social influence construct is documented in Table 4. A higher standard

deviation suggests that responses are more spread out across the different categories. For instance, SI2 has the highest standard deviation of 252.18, indicating greater variability in how respondents feel about this item. In terms of minimum and maximum responses, SI2 has a minimum value of 22, which indicates that the least number of respondents selected "Strongly Disagree" for this item. Similarly, SI2 (My supervisors or managers will support the use of this incremental password system) has the highest maximum value of 629, which means that the highest number of respondents selected "Agree" for this item. Also, SI3 having a 50% percentile of 308 means half of the respondents rated it 308 or lower, while 75% of the respondents rated SI2 353 or lower. In terms of skewness, SI3 (The opinions of my friends and family influenced my decision to use this new authentication method) having a value of −0.701 means more respondents leaned towards "Disagree" and "Strongly Disagree." However, a positive skewness means responses received tend towards "Agree" and "Strongly Agree." SI has the highest skewness value. A near-zero skewness indicates a fairly symmetric distribution. For instance, SI1 and SI5 have skewness values close to zero, meaning responses are balanced around the mean. Furthermore, all items having a negative kurtosis means the responses are more evenly spread out across the categories rather than clustered around the mean. This is a normal distribution. For example, SI1 and SI5 have kurtosis values around −1.85, indicating a very flat distribution.

TABLE 4. Statistical analysis of the responses to social influence construct.

Statistics	SI 1	SI 2	SI 3	SI 4	SI 5
Count	4	4	4	4	4
Mean	286.25	286.25	286.25	286.25	286.25
Std. Deviation	236.49	252.18	157.82	234.29	227.97
Minimum	24	22	99	32	34
25th Percentile	141.75	180.25	184.5	188.75	145
Median (50th)	275	247	308	257	276
75th Percentile	419.5	353	409.75	354.5	417.25
Maximum	571	629	430	599	559
Skewness	-0.042	0.347	-0.701	0.326	-0.052
Kurtosis	-1.840	-1.267	-0.888	-1.165	-1.856

4) FACILITATING CONDITIONS

Table 5 presents the statistical analysis of the responses received from the facilitating condition constructs. These high mean values recorded for all the responses indicate that a positive reaction was obtained toward the conditions supporting the new technique. Similarly, the values of the standard deviation depict moderate variability in responses, which suggests that while many respondents strongly agree, there is some diversity in their opinions across the questions asked about the facilitating condition. Also, the minimum of 268 and maximum of 373 responses indicates the range of respondents who strongly agreed with the FC constructs. The wide range suggests varying levels of strong agreement. Using FC1 (There is adequate technical support available to help me use this new authentication technique) as a case study, percentile values of 288, 296, and 315 for 25%, 50%, and 75% percentiles indicate that 25% of respondents had a score of 288 or lower, 50% had a score of 296 or lower, and 75% had a score of 315 or lower. This distribution shows that most responses are clustered around the lower end of the range, but a notable proportion shows higher strong agreement. Examining the results of the skewness, it was observed that all the FC constructs have positive skewness values, indicating that the distribution of responses is slightly skewed to the right. This implies that some respondents had particularly strong positive reactions to the facilitating conditions. Similarly, all the FC constructs have negative kurtosis values, indicating that the distribution of responses is platykurtic. This means the distribution is flatter than the normal distribution, with fewer extreme values (outliers).

TABLE 5. Statistical analysis of the responses to facilitating condition construct.

Statistics	FC 1	FC 2	FC 3	FC 4	FC 5
Count	4	4	4	4	4
Mean	315.75	286.25	286.25	286.25	286.25
Std. Deviation	35.82	18.33	39.13	1.74	18.33
Minimum	268	288	173	17	373
25th Percentile	288	580	193	19	580
Median (50th)	296	592	217	19	592
75th Percentile	315	611	246	21	611
Maximum	373	620	284	22	620
Skewness	0.397	0.278	0.157	0.397	0.145
Kurtosis	-1.103	-1.003	-0.998	-1.028	-1.389

E. ADVANTAGES OF THE PROPOSED TECHNIQUE OVER EXISTING KNOWLEDGE-BASED AUTHENTICATION SYSTEMS

The proposed authentication mechanism provides numerous benefits and advantages compared to conventional password authentication methods. Such include:

1) ENHANCED SECURITY THROUGH INCREMENTAL CHANGES

In contrast to static passwords that remain unchanged until modified by the user, this approach produces a fresh password for every login attempt by incrementing the previous password. The proposed authentication technique's dynamic nature makes it difficult for hackers to predict or recycle the

PIN. Also, the PIN's incremental nature ensures that should hackers acquire a PIN during any login session, it cannot be used in subsequent login sessions. These layers of security are not present in traditional static passwords.

2) GRAPHICAL GIRD APPROACH FOR PIN SELECTION

For every login session, users are presented with a grid of 16 PINs and are expected to choose the incremented PIN from the grids. The position of the PIN is rotated for every login session, which adds an added layer of security. Should a hacker see a PIN being selected at any login session, the PIN would have been incremented during the next login session, and the position of the PIN would have changed. This makes it difficult for the hacker to brute force.

3) RESISTANCE TO KNOWN PASSWORD ATTACKS

The proposed technique's incremental and dynamic nature makes it resistant to common password attacks such as dictionary attacks, keylogging, shoulder surfing, and phishing. However, if a user willingly reveals his PIN and explains its incremental nature, then its security features have been defeated.

4) EASY APPROACH TO PASSWORD MANAGEMENT

The proposed technique requires users to remember only their original PIN and the incremental factor. Since the PIN is 6 digits, remembering the first three digits could give a clue to the correct PIN among the numerous PINs presented. In addition, the system automatically updates user PINs at every login attempt. This saves the user from the mental strength needed to remember numerous fixed passwords.

5) EASY INTEGRATION WITH EXISTING SYSTEMS

The proposed technique does not require additional infrastructure for its implementation; therefore, it can be easily integrated with existing systems.

F. POSSIBLE RESPONSE TIME, MEMORY USAGE, AND CPU OVERHEAD OF THE PROPOSED TECHNIQUE

A favorable response time, memory usage, and CPU overhead of the proposed technique are expected. Response time denotes the time taken by the users to identify their PIN on the grid. This could be relatively slower when the users are not yet familiar with the incremented and dynamic approach of the authentication technique. However, this is expected to be faster when users are familiar with the new authentication technique. In addition, the memory usage is expected to be manageable and moderate. However, this majorly depends on how the technique is implemented on mobile and web applications. Since the system is only expected to store the initial password, incremental factors, and incremented PIN, the memory usage should not be huge. Therefore, the proposed technique is not likely to have a significant memory overhead when compared to traditional authentication techniques. Moreover, the proposed technique is expected to exhibit a moderate CPU overhead. The subsequent PIN generation does not involve complex computations, and the graphical grid generation is not a highly intensive operation. Therefore, the computational load on the CPU is expected to be low.

V. CONCLUSION

This study presents an innovative way of improving security in mobile and web applications via an incremental graphical grid authentication technique. The proposed technique expects a user to choose a six-digit PIN and an incremental factor between 01 and 99 during registration. During every login attempt, users are required to use the incremented version of the original PIN to gain access to their application. To introduce another layer of security in a more mentally engaging manner, a 4 by 4 graphical grid approach was used to present sixteen PINS to the users. These sixteen PINs are a mixture of fifteen wrong PINs and one correct PIN. The position of the correct PIN changes at every login session, which introduces an additional layer of security. Therefore, the technique uses a blend of numerical progression and dynamic grid graphical interfaces to achieve a balance between security and usability. Users are also notified of login activities via email; therefore, they are always on high alert every time. The proposed technique is simple to implement as it does not require additional infrastructure. Most importantly, the technique has been shown to provide a level of mitigation against known password attacks such as shoulder surfing, dictionary attacks, brute force, reverse engineering, and phishing. Nevertheless, no matter how secure an authentication technique is, it is the responsibility of the users to ensure they protect their PINs and not reveal them to anyone so as to make them resistant to social engineering. Future research can explore how the proposed incremental authentication technique can be used with other authentication factors, such as biometric and hardware tokens. Studies can also be conducted to understand user behavior and preferences. To improve the robustness of the technique against emerging threats, the proposed technique can be continuously simulated under different attack scenarios. Also, users can customize different aspects of the grid or interface to suit their preferences better and improve ease of use.

REFERENCES

[1] *Global Website Statistics*. Accessed: Jun. 16, 2024. [Online]. Available: https://www.forbes.com/uk/advisor/business/software/website-statistics/

[2] *Number of IoT Connections Worldwide 2022-2033*. Accessed: Jun. 16, 2024. [Online]. Available: https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/

[3] D. Odunze, "Cyber victimization by hackers: A criminological analysis," *Public Policy Admin. Res.*, vol. 8, no. 1, pp. 8–15, 2018.

[4] A. Arora, H. Garg, and S. Shivani, "Anti-phishing technique based on dynamic image captcha using multi secret sharing scheme," *J. Vis. Commun. Image Represent.*, vol. 88, Oct. 2022, Art. no. 103624, doi: 10.1016/j.jvcir.2022.103624.

[5] 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.

[6] M. W. Nadeem, H. G. Goh, Y. Aun, and V. Ponnusamy, "Detecting and mitigating botnet attacks in software-defined networks using deep learning techniques," *IEEE Access*, vol. 11, pp. 49153–49171, 2023, doi: 10.1109/ACCESS.2023.3277397.

[7] A. A. Almazroi and N. Ayub, "Online payment fraud detection model using machine learning techniques," *IEEE Access*, vol. 11, pp. 137188–137203, 2023, doi: 10.1109/ACCESS.2023.3339226.

[8] M. Kokila and S. Reddy K, "Authentication, access control and scalability models in Internet of Things security—A review," *Cyber Secur. Appl.*, vol. 3, Dec. 2025, Art. no. 100057, doi: 10.1016/j.csa.2024.100057.

[9] T. Chen, H. Zeng, M. Lv, and T. Zhu, "CTIMD: Cyber threat intelligence enhanced malware detection using API call sequences with parameters," *Comput. Secur.*, vol. 136, Jan. 2024, Art. no. 103518, doi: 10.1016/j.cose.2023.103518.

[10] T. Nandy, M. Y. I. B. Idris, R. Md Noor, L. M. Kiah, L. S. Lun, N. B. A. Juma'at, I. Ahmedy, N. Abdul Ghani, and S. Bhattacharyya, "Review on security of Internet of Things authentication mechanism," *IEEE Access*, vol. 7, pp. 151054–151089, 2019, doi: 10.1109/ACCESS.2019.2947723.

[11] A. Yeboah-Ofori, S. Islam, S. W. Lee, Z. U. Shamszaman, K. Muhammad, M. Altaf, and M. S. Al-Rakhami, "Cyber threat predictive analytics for improving cyber supply chain security," *IEEE Access*, vol. 9, pp. 94318–94337, 2021, doi: 10.1109/ACCESS.2021.3087109.

[12] A. W. Burange, V. M. Deshmukh, Y. A. Thakare, and N. A. Shelke, "Safeguarding the Internet of Things: Elevating IoT routing security through trust management excellence," *Comput. Standards Interfaces*, vol. 91, Jan. 2025, Art. no. 103873, doi: 10.1016/j.csi.2024.103873.

[13] A. A. S. AlQahtani, T. Alshayeb, M. Nabil, and A. Patooghy, "Leveraging machine learning for Wi-Fi-based environmental continuous two-factor authentication," *IEEE Access*, vol. 12, pp. 13277–13289, 2024, doi: 10.1109/ACCESS.2024.3356351.

[14] M. Aldayel, N. Alsedairy, A. Al-Nafjan, and S. Alsenan, "Systematic review of brain-computer interface-based user authentication system: Trends, challenges, and directions," *IEEE Access*, vol. 12, pp. 96848–96861, 2024, doi: 10.1109/ACCESS.2024.3421264.

[15] J. Jiang, W. Susilo, and J. Baek, "Security analysis of 'SMAKA: Secure many-to-many authentication and key agreement scheme for vehicular networks,'" *IEEE Trans. Inf. Forensics Security*, vol. 17, pp. 3006–3007, 2022, doi: 10.1109/TIFS.2022.3198858.

[16] X. Jiang, X. Liu, J. Fan, X. Ye, C. Dai, E. A. Clancy, and W. Chen, "Measuring neuromuscular electrophysiological activities to decode HD-sEMG biometrics for cross-application discrepant personal identification with unknown identities," *IEEE Trans. Instrum. Meas.*, vol. 71, pp. 1–15, 2022, doi: 10.1109/TIM.2022.3180434.

[17] Y. Gu, Y. Wang, M. Wang, Z. Pan, Z. Hu, Z. Liu, F. Shi, and M. Dong, "Secure user authentication leveraging keystroke dynamics via Wi-Fi sensing," *IEEE Trans. Ind. Informat.*, vol. 18, no. 4, pp. 2784–2795, Apr. 2022, doi: 10.1109/TII.2021.3108850.

[18] I. Alkhwaja, M. Albugami, A. Alkhwaja, M. Alghamdi, H. Abahussain, F. Alfawaz, A. Almurayh, and N. Min-Allah, "Password cracking with brute force algorithm and dictionary attack using parallel programming," *Appl. Sci.*, vol. 13, no. 10, p. 5979, May 2023.

[19] *Password Security—Statistics & Facts*. Accessed: Jun. 18, 2024. [Online]. Available: https://www.statista.com/topics/9360/password-security/#topicOverview

[20] A. Ezugwu, E. Ukwandu, C. Ugwu, M. Ezema, C. Olebara, J. Ndunagu, L. Ofusori, and U. Ome, "Password-based authentication and the experiences of end users," *Sci. Afr.*, vol. 21, Sep. 2023, Art. no. e01743, doi: 10.1016/j.sciaf.2023.e01743.

[21] M. Bala Krishna and P. Lorenz, "Location, context, and social objectives using knowledge-based rules and conflict resolution for security in Internet of Things," *IEEE Internet Things J.*, vol. 8, no. 1, pp. 407–417, Jan. 2021, doi: 10.1109/JIOT.2020.3008771.

[22] *Companies' Authentication Methods Deployment Status Worldwide 2023*. Accessed: Jun. 18, 2024. [Online]. Available: https://www.statista.com/statistics/1441144/companies-authentication-methods-deployment-status-worldwide/

[23] B. Mihir, O. Goldreich, and S. Goldwasser, "Incremental cryptography: The case of hashing and signing," in *Proc. Annu. Int. Cryptol. Conf.*, 1994, pp. 216–233.

[24] J. Oliveira, A. Santin, E. Viegas, and P. Horchulhack, "A non-interactive one-time password-based method to enhance the vault security," in *Proc. Int. Conf. Adv. Inf. Netw. Appl.*, in Lecture Notes on Data Engineering and Communications Technologies, vol. 202, 2024, pp. 201–213, doi: 10.1007/978-3-031-57916-5_18.

[25] X. Cao, Z. Yang, J. Ning, C. Jin, R. Lu, Z. Liu, and J. Zhou, "Dynamic group time-based one-time passwords," *IEEE Trans. Inf. Forensics Security*, vol. 19, pp. 4897–4913, 2024, doi: 10.1109/TIFS.2024.3386350.

[26] I. A. Turapbayevich, G. S. Karimovich, and S. Usmanov, "Algorithm of generating one-time passwords for two-factor authentication of users," in *Proc. World Conf. Intell. Syst. Ind. Autom.*, in Lecture Notes in Networks and Systems, vol. 912, 2024, pp. 132–139, doi: 10.1007/978-3-031-53488-1_16.

[27] M. Premalatha and N. Srinivas, "A 2-way verification process using one time password key for home authentication system," *Int. J. Innov. Sci. Res. Technol.*, vol. 9, pp. 972–977, Mar. 2024.

[28] N. Y. Abdullah, I. S. Anizam, H. R. M. H. Hamid, and W. H. W. Ismail, "Pass matrix based graphical password authentication on the Android platform," in *Applied Problems Solved By Information Technology and Software* (SpringerBriefs in Applied Sciences and Technology). Cham, Switzerland: Springer, 2024, doi: 10.1007/978-3-031-47727-0_15.

[29] M. A. Khan, I. U. Din, S. U. Jadoon, M. K. Khan, M. Guizani, and K. A. Awan, "G-RAT| A novel graphical randomized authentication technique for consumer smart devices," *IEEE Trans. Consum. Electron.*, vol. 65, no. 2, pp. 215–223, May 2019, doi: 10.1109/TCE.2019.2895715.

[30] S. Shiaeles, "GRABLOK: A novel graphical password authentication utilising blockchain technology," in *Proc. IEEE Int. Conf. Comput. (ICOCO)*, Kota Kinabalu, Malaysia, Nov. 2022, pp. 179–184, doi: 10.1109/ICOCO56118.2022.10031783.

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

[32] T. Kawamura, T. Ebihara, N. Wakatsuki, and K. Zempo, "EYEDi: Graphical authentication scheme of estimating your encodable distorted images to prevent screenshot attacks," *IEEE Access*, vol. 10, pp. 2256–2268, 2022, doi: 10.1109/ACCESS.2021.3138093.

[33] J. Son, S. Noh, J. Choi, and H. Yoon, "A practical challenge-response authentication mechanism for a programmable logic controller control system with one-time password in nuclear power plants," *Nucl. Eng. Technol.*, vol. 51, no. 7, pp. 1791–1798, Oct. 2019, doi: 10.1016/j.net.2019.05.012.

[34] M. Ezz, A. M. Mostafa, and A. Elshenawy, "Challenge-response emotion authentication algorithm using modified horizontal deep learning," *Intell. Autom. Soft Comput.*, vol. 35, no. 3, pp. 3659–3675, 2023, doi: 10.32604/iasc.2023.031561.

[35] T. G. Tersue, O. Emmanuel, and G. Terlumun, "An improved second level challenge response authentication for online banking security systems in Nigeria," *East Afr. Scholars J. Eng. Comput. Sci.*, vol. 2, pp. 89–97, Jan. 2024.

[36] M. Alajmi, I. Elashry, H. S. El-Sayed, and O. S. Faragallah, "A password-based authentication system based on the CAPTCHA AI problem," *IEEE Access*, vol. 8, pp. 153914–153928, 2020, doi: 10.1109/ACCESS.2020.3018659.

[37] S. K. M. Kumar, "Devanagari CAPTCHA: For the security in web," *Tuijin Jishu/Journal Propuls. Technol.*, vol. 44, no. 4, pp. 292–310, Oct. 2023, doi: 10.52783/tjjpt.v44.i4.837.

[38] A. Mishra, S. Sinha, and C. P. George, "Shielding against online harm: A survey on text analysis to prevent cyberbullying," *Eng. Appl. Artif. Intell.*, vol. 133, Jul. 2024, Art. no. 108241, doi: 10.1016/j.engappai.2024.108241.

[39] M. Sapkal, N. Sarulkar, K. Shaikh, P. Sarode, and P. A. A. Shirode, "A captcha-based graphical password with strong password space and usability study," *Int. J. Res. Appl. Sci. Eng. Technol.*, vol. 11, no. 3, pp. 274–281, Mar. 2023, doi: 10.22214/ijraset.2023.49072.

[40] S. A. Alsuhibany and A. A. Alnoshan, "Interactive handwritten and text-based handwritten Arabic CAPTCHA schemes for mobile devices: A comparative study," *IEEE Access*, vol. 9, pp. 140991–141001, 2021, doi: 10.1109/ACCESS.2021.3119571.

[41] N. Dinh, K. Tran-Trung, and V. T. Hoang, "Augment CAPTCHA security using adversarial examples with neural style transfer," *IEEE Access*, vol. 11, pp. 83553–83561, 2023, doi: 10.1109/ACCESS.2023.3298442.

[42] P. Wang, H. Gao, C. Xiao, X. Guo, Y. Gao, and Y. Zi, "Extended research on the security of visual reasoning CAPTCHA," *IEEE Trans. Depend. Sec. Comput.*, vol. 20, no. 6, pp. 4976–4992, Dec. 2023, doi: 10.1109/TDSC.2023.3238408.

[43] V. N. Balen and H. Wang, "GridMap: Enhanced security in cued-recall graphical passwords," in *Proc. Int. Conf. Secur. Privacy Commun. Netw.*, in Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol. 15. Cham, Switzerland: Springer, 2015, pp. 75–94, doi: 10.1007/978-3-319-23829-6_6.

[44] S. W. Jirjees, A. M. Mahmood, and A. R. Nasser, "Passnumbers: An approach of graphical password authentication based on grid selection," *Int. J. Saf. Secur. Eng.*, vol. 12, no. 1, pp. 21–29, Feb. 2022, doi: 10.18280/ijsse.120103.

[45] Z. Wang, L. Liao, R. Meng, C.-N. Yang, Z. Zhou, and H. Yang, "Verification grid and map slipping based graphical password against shoulder-surfing attacks," *Secur. Commun. Netw.*, vol. 2022, pp. 1–9, Apr. 2022, doi: 10.1155/2022/6778755.

[46] J. Han, "CNN-based multi-factor authentication system for mobile devices using faces and passwords," *Appl. Sci.*, vol. 14, no. 12, p. 5019, Jun. 2024, doi: 10.3390/app14125019.

[47] M. Guerar, M. Migliardi, A. Merlo, M. Benmohammed, F. Palmieri, and A. Castiglione, "Using screen brightness to improve security in mobile social network access," *IEEE Trans. Depend. Sec. Comput.*, vol. 15, no. 4, pp. 621–632, Jul. 2018, doi: 10.1109/TDSC.2016.2601603.

[48] C. Thotadi, M. Debbala, S. Rao, A. Eeralla, B. Palaniswamy, S. Mookherji, V. Odelu, and A. G. Reddy, "E-brightpass: A secure way to access social networks on smartphones," *Cyber Secur. Appl.*, vol. 2, Jan. 2024, Art. no. 100021, doi: 10.1016/j.csa.2023.100021.

[49] V. Venkatesh, M. G. Morris, G. B. Davis, and F. D. Davis, "User acceptance of information technology: Toward a unified view," *MIS Quart.*, vol. 27, no. 3, pp. 425–478, 2003, doi: 10.2307/30036540.

JIAMING GONG was born in Datong, Shanxi. He received the degree in information management and information systems from the School of Economics and Management, Beijing Forestry University, in 2024. His research interests includes information system security.

OLUWATOBI NOAH AKANDE (Member, IEEE) received the B.Tech. and M.Tech. degrees in computer science from the Department of Computer Science and Engineering, Ladoke Akintola University of Technology, Ogbomoso, Nigeria, in 2012 and 2015, respectively, and the D.Phil. degree in computer science from the Department of Computer Science, University of Ilorin, Nigeria, in 2021. He is currently a Senior Lecturer with the Department of Computer Science, Baze University, Abuja. He has a passion for problem-oriented research, which employs the knowledge of computing he has acquired over the years to solve his immediate societal problems. His research interests include biometrics, data and information security, medical image analysis, and machine learning. The output of his research has been published in more than 60 journals and international conferences. He is an active member of professional bodies, such as IAENG Computer Science, Nigeria Computer Society (NCS), Academics in IT Professions (AITP), and Computer Professionals Registration Council of Nigeria (CPN).

CHIA-CHEN LIN (Member, IEEE) received the Ph.D. degree in information management from National Chiao Tung University, in 1998. Since 2018, she has been a School Counselor with Providence University. She is currently a Professor of computer science and information engineering with the National Chin-Yi University of Technology. Her research interests include image and signal processing, information hiding, mobile agents, and electronic commerce. Since 2018, she has been a fellow of IET. From 2009 to 2012, she served as the Vice Chair for Tainan Chapter of the IEEE Signal Processing Society. She also serves as an associate editor and an editor for several representative EI and SCIE journals.

SAURABH AGARWAL received the Ph.D. degree in computer engineering from the University of Delhi, India, in 2017. From 2019 to 2023, he was a Korean Research Fellow in South Korea. Since 2024, he has been a Research Professor at Yeungnam University, Gyeongsan, South Korea. His research interests include image forensics, computer vision, and machine learning.