A Comparison of a Touch-Gesture- and a Keystroke-Based Password Method: Toward Shoulder-Surfing Resistant Mobile User Authentication

Lina Zhou, *Senior Member, IEEE*, Kanlun Wang, Jianwei Lai, and Dongsong Zhang

***Abstract*—The pervasive use of mobile devices exposes users to an elevated risk of shoulder-surfing attacks. Despite the prior work on shoulder-surfing resistance of mobile user authentication methods, there is a lack of empirical studies on textual password authentication methods, particularly the hybrid passwords that integrate textual passwords with biometrics. To fill the literature gap, this research compares two hybrid password methods, touch-gesture- and keystroke-based passwords, with respect to their shoulder-surfing resistance performance. We select a touch-gesture-based password method that deploys multiple shoulder-surfing resistance strategies and a keystroke-based password method that leverages keystroke dynamics. To gain a holistic understanding of these password methods, we examine them under a variety of shoulder-surfing settings by varying interaction mode, observation angle, entry error, and observation effort. Going beyond effectiveness metrics, we also introduce efficiency metrics to assess shoulder-surfing resistance performance more comprehensively. We hypothesize and test the effects of shoulder-surfing settings by conducting both a longitudinal lab experiment and an online experiment with diversified participants. The results of both studies demonstrate the superior performance of the touch-gesture-based password method to the keystroke-based counterpart. The results also provide evidence for the effects of interaction mode, observation angle, and observation effort on shoulder-surfing resistance of hybrid passwords. Our findings offer suggestions for the design and strategies for strengthening the security of password authentication methods.**

***Index Terms*—Keystroke behavior, mobile user authentication, password, shoulder-surfing resistance, touch gesture.**

Manuscript received 22 November 2021; revised 27 March 2022, 28 June 2022, 9 August 2022, and 29 September 2022; accepted 6 January 2023. Date of publication 15 February 2023; date of current version 15 March 2023. This work was supported by the National Science Foundation under Grant CNS 1917537. This article was recommended by Associate Editor B. Guo. *(Corresponding author: Lina Zhou.)*

This work involved human subjects or animals in its research. Approval of all ethical and experimental procedures and protocols was granted by UNC Charlotte Institutional Review Board under Application No. IRBIS-18-0470, and performed in line with the Code of Federal Regulations.

Lina Zhou, Kanlun Wang, and Dongsong Zhang are with the University of North Carolina at Charlotte, Charlotte, NC 28223 USA (e-mail: lzhou8@uncc.edu; kwang17@uncc.edu; dzhang15@uncc.edu).

Jianwei Lai is with the School of Information Technology, Illinois State University, Normal, IL 61790 USA (e-mail: jlai12@ilstu.edu).

Color versions of one or more figures in this article are available at https://doi.org/10.1109/THMS.2023.3236328.

Digital Object Identifier 10.1109/THMS.2023.3236328

I. Introduction

MOBILE users increasingly store personal, work-related, and sensitive information on their smartphones and access them in public venues. Nearly 70.7% of users store confidential information, and 68.1% enter personal and sensitive information, on their mobile devices [1]. Thus, it is critical to keep mobile devices secure. Mobile user authentication is one way to minimize security and privacy threats [2] by verifying a user's identity when attempting to access a mobile device. Nevertheless, password authentication, the most commonly used method on mobile devices, is vulnerable to security threats, such as shoulder-surfing attacks.

Shoulder-surfing is an attempt to spy on a victim in order to obtain his/her credentials or personal information via direct observation or video recording without the victim's knowledge [3]. This definition excludes opportunistic shoulder-surfing [4] due to its lack of malicious intention. To minimize the risk of shoulder-surfing attacks, an emerging stream of studies focuses on the design of mobile user authentication methods to improve their shoulder-surfing resistance [5], [6], [7]. However, some of the existing methods lack usability assessment [8], [9], [10] while some other methods may introduce accessibility issues due to their requirement for special hardware (e.g., [11]). A few empirical shoulder-surfing studies in the context of mobile user authentication have compared a PIN and an augmented PIN [12], PINs and pattern lock variations [13], PINs and graphical passwords [14], textual and graphical passwords [15], and different textual password variations [7], [16]. The process of password entry makes it vulnerable to shoulder-surfing attacks [17]. Yet, the levels of shoulder-surfing resistance of different types of textual password authentication methods remain unclear.

Mobile user authentication methods can be grouped into two broad categories: password-based and biometrics-based [18]. *Password-based methods* match a user-entered password against a predefined secret password that typically consists of a string of letters, numbers, graphics, and/or symbols, with textual passwords being the most common [19]. *Biometrics-based methods* leverage unique physiological and behavioral characteristics of individuals [18]. Physiological biometrics (e.g., face and fingerprint recognition) are difficult to be stolen and forged but are vulnerable to replay attacks (e.g., fingerprint residue [20])

2168-2291 © 2023 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission.
See https://www.ieee.org/publications/rights/index.html for more information.

Authorized licensed use limited to: University of North Carolina at Charlotte. Downloaded on June 02,2023 at 02:37:13 UTC from IEEE Xplore. Restrictions apply.

and spoofing attacks (e.g., a latex face mask [21]). Behavioral biometrics rely on invariant features of human behaviors [22]. Compared with physiological biometrics, behavioral biometrics that is based on features of behaviors, such as gestures and keystrokes, can better mitigate the risks of replay and spoofing attacks. Gesture biometrics authenticates users based on their movements of certain body parts [23], and touch gesture (e.g., swiping or stroking) is one of the most commonly used types of gestures (e.g., [18], [24], [25]). Keystroke biometrics is extracted from user interaction with a keyboard while entering a password [26]. In light of their complementary strengths, it is promising to integrate behavioral biometrics with password methods to create *hybrid passwords* (e.g., [18]). In this study, we consider two types of hybrid passwords for mobile user authentication: 1) *touch-gesture-based hybrid password*; and 2) *keystroke-based hybrid password*, which refer to password authentication augmented by touch gestures and keystroke dynamics, respectively. None of the previous studies has compared whether and to what extent these two hybrid password methods are resistant to shoulder-surfing attacks.

Shoulder-surfing take place in a variety of settings, such as different observation angles and observation attempts. However, the impact of those factors on the shoulder-surfing resistance of hybrid password methods remains significantly underexplored. In addition, password entry is not always error-free [27], which may increase the difficulty of password identification [28], yet it has been overlooked in prior shoulder-surfing studies. Furthermore, the measurement of shoulder-surfing resistance performance has primarily focused on success rate (e.g., [13], [31], [32]) and not efficiency. The latter is important for direct observation attacks because the opportunities are transient, lasting as long as the duration of an authentication session. Given adversaries' limited cognitive capacity [13], their ability to memorize and recall the credential information is restricted.

This research aims to fill the above-mentioned research gaps by systematically investigating the shoulder-surfing resistance of two hybrid password methods, including one touch-gesture-based and one keystroke-based, under different settings. It answers the following research questions: 1) How does a touch-gesture-based hybrid password method compare with a keystroke-based hybrid password method with respect to shoulder-surfing resistance? 2) Do shoulder-surfing settings affect the resistance of the hybrid password methods? If so, how? 3) How to measure shoulder-surfing resistance performance more comprehensively? We answer these questions by conducting both a lab and an online user experiment with two hybrid password methods.

II. Background and Related Work

A. Shoulder-Surfing Resistance Strategies

Shoulder-surfing attacks can take the form of either direct observation or recording attacks [3]. A direct observation attack refers to looking over a victim's shoulder to steal his/her password [31] while a recording attack refers to stealing a victim's password indirectly by video recording a password entry first, then viewing the recorded video later to identify the password [13], [29]. Shoulder-surfing resistance is defined as the capability of protecting users from shoulder-surfing attacks.

Based on an extensive literature review, we identify four common strategies for resisting shoulder-surfing attacks: 1) visibility reduction; 2) action segmentation; 3) knowledge transformation; and 4) characteristics verification.

Visibility reduction reduces the saliency of viewable areas on the touch screen of a mobile device where sensitive information is displayed. It can be achieved by using a cupped hand to physically block an attacker's observation [12] or by visualization techniques, such as using hybrid images to blend keypads with numbers in different orders [32]. Alternatively, keypress-free interaction mitigates the dependence on the keyboard during human-device interaction (e.g., [10], [25], [26], [27], [35], [36]), which reduces the risk of shoulder-surfing attacks based on the observation of fixed arrangement of key locations. This strategy imposes a minimal cognitive load on a mobile user possibly at the cost of reduced usability of authentication schemes.

Action segmentation divides an input action temporally or spatially into subactions that will be performed sequentially or concurrently. For example, region-on-answer [36] requires a user to click on the correctly registered points in preselected images sequentially; a multi-touch-based method requires selecting a number of images from an image pool to form a story order and then touching multigrid points on a specific image [37]; and a QWERTY-keyboard-based method asks a user to select correct characters in the first place and then move emoticons to associated positions that tie to the characters [38]. By requiring more than one action to complete an authentication key, this strategy makes it difficult for adversaries to interpret a user's actions. However, it may increase the user's learning curve and the time needed to enter user credentials for authentication.

Knowledge transformation transforms users' credentials (e.g., a password) into a different form by applying specific knowledge or a pattern. Sample strategies include symbolic coding (e.g., selecting a symbol with the designated color, number, and icon from a randomized set of system-generated symbols [39]), matrix indexing (e.g., reconstructing a password by selecting characters from certain indexes of rows and columns in a table [10]), vectorization (e.g., requiring a user to calculate and enter a vector combination of direction and distance between challenge characters based on the character arrangement in a cellular layout [31]), and image reforming (e.g., selecting randomized user-selected images that are evolved into sketches with further reduced information [40]). The transformation can be carried out easily without requiring an excessive amount of calculation or memory from the user.

Characteristics verification aims to verify physiological or behavioral characteristics of a user's body or behavior, which offers advantages, such as uniqueness, transparency, and continuity. For example, incorporating password entry time, finger pressure, x- and y-coordinates of pattern locks [41], and a user's unique gaze patterns [23], [42] into an authentication model can be effective against shoulder-surfing attacks. However, users may raise privacy concerns about using such characteristics for verification, drawing on the protection motivation theory [43].

Authorized licensed use limited to: University of North Carolina at Charlotte. Downloaded on June 02,2023 at 02:37:13 UTC from IEEE Xplore. Restrictions apply.

B. Touch-Gesture- and Keystroke-Based Passwords

The touch-gesture-based password method requires a user to enter a password for authentication via touch gestures on the screen of a mobile device [24]. The touch gestures are captured from a user's finger interactions with a mobile touch screen, such as swipes [24], finger taps, flicks, scrolls, zooms [44], handwritings [34], [35], or drawings [6], [9], [45]. Accordingly, a rich set of features can be extracted from touch gestures as authentication inputs, including spatial (e.g., [9], [35], [44], [45]), temporal (e.g., [10], [35], [36], [45], [46], [47]), geometrical (e.g., [10], [25], [35], [45], [46]), and statistical (e.g., [46], [34]), and finger pressure-based features (e.g., [10], [25], [36], [47]). Given that these features are inferred instead of directly observed, they can be used to enhance the robustness of touch-gesture-based password methods against shoulder-surfing attacks. In addition, keypress-free interaction [47] is another way for a touch-gesture-based password method to achieve shoulder-surfing resistance. Keypress-free interaction can be enabled by designs, such as drawing PINs [9], swiping with Morse code vibration feedback of PINs [33], handwriting textual passwords [34], [35], and drawing shapes sequentially [47], on the touch screen of a mobile device. Furthermore, a touch-gesture-based password method can support the entry of consecutive touch gestures on the same/adjacent area(s) of a mobile touch screen (e.g., [10], [26], [27], [35], [36]), increasing the complexity of decoding an authentic password by an adversary. Broadly speaking, different types of passwords include textual passwords, PINs, and graphical passwords (including pattern lock). Among them, textual passwords are the most prevalent authentication method used in practice [19]. However, our review of the existing touch-gesture-based password methods shows that textual passwords have not received much attention, and previous methods (e.g., [35], [36]) are vulnerable to forgery attacks and error-prone [48].

The keystroke-based password authentication allows a user to enter a password via tapping corresponding keys on a soft keyboard, commonly a QWERTY-based keyboard of a mobile device (e.g., [7], [39], [50], [51]). Accordingly, textual passwords and PINs are the most common types of keystroke-based passwords. These methods extract features from the user's keystroke-based behaviors, such as the time of typing events, the locations of keys, sizes of fingertips, and motion data captured by built-in motion sensors [26], [49], [51]. On a separate note, studies have explored shoulder-surfing resistance strategies, such as manipulating the password focus-area display (e.g., skipping a few characters [7] and inserting camouflage digits [16]), rearranging the keypad display (e.g., randomizing the order of PIN display using Mersenne twister [51]), and adding an additional layer of knowledge (e.g., assigning an emoticon to an associated key [38]) to confuse the attacker's effort in identifying a real password. However, these strategies do not involve keystroke-based features and are thus not considered in this study.

Empirical studies on shoulder-surfing resistance performance of mobile user authentication methods remain scarce. Most password methods (e.g., [8], [30], [33]) have not been empirically evaluated with respect to their shoulder-surfing resistance. The majority of empirical studies are focused on the performance of user authentication (e.g., equal error rate [9] and success rate [6], [16], [41]) instead. Among the extant shoulder-surfing studies, only a few have compared password methods, but they focused on the comparisons between different types of password methods, such as pattern lock variations versus PINs [13], graphical passwords versus PINs [14], and textual versus graphical passwords [15]. Another two studies compared different password methods of the same type, such as two textual passwords [7] and a PIN versus an augmented PIN [12], yet both studies collected data about user perception rather than actual user performance. To the best of our knowledge, existing studies have not compared shoulder-surfing resistance of touch-gesture- and keystroke-based hybrid textual password methods.

(a) (b)

Fig. 1. Keyboards used in the hybrid password methods. (a) Touch-gesture-based. (b) Keystroke-based.

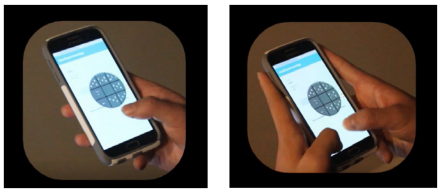
III. Hybrid Password Methods and Shoulder-Surfing Settings

This research aims to investigate shoulder-surfing resistance of touch-gesture- and keystroke-based textual password methods under various shoulder-surfing settings. Based on the shoulder-surfing resistance strategies and the review of related work, we selected one touch-gesture- and one keystroke-based hybrid textual password method for comparison. As briefly discussed earlier, both methods integrate behavioral biometrics and password methods. In addition, they both extract behavioral patterns by drawing on common behaviors of user interaction with the mobile device screen without requiring any additional hardware. On the other hand, the two methods also have important differences in their design of password entry and shoulder-surfing resistance strategies. We introduce the selected methods and shoulder-surfing settings in detail in this section.

A. Hybrid Textual Password Methods

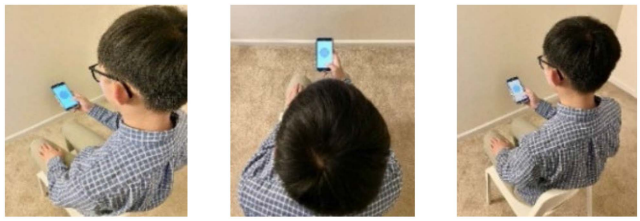
1) Touch-Gesture-Based Password Method: The touch-gesture-based password method supports textual password entry with the ThumbStroke keypad [54], a circular keypad where characters are distributed across eight different grids (see Fig. 1(a)). The grids are located in eight different directions from the center of the keyboard, including up, down, left, right, up-left, down-left, up-right, and down-right. The center is the default starting reference point for touch gestures. Each grid contains five or fewer characters, which are located in one of the four directions from the grid center as well as the grid center itself. Accordingly, entering a character requires one or two consecutive touch gestures. For example, to enter the letter "e," the user needs to perform one upstroke on the touch screen and then lift the finger up from the screen. To enter the letter "b", the user needs to first make an upper-left stroke to select the corresponding grid, followed by an upper-right stroke to select

Authorized licensed use limited to: University of North Carolina at Charlotte. Downloaded on June 02,2023 at 02:37:13 UTC from IEEE Xplore. Restrictions apply.



(a) (b)

Fig. 2. Interaction mode of a target user. (a) One-handed. (b) Two-handed.



(a) (b) (c)

Fig. 3. Shoulder-surfing observation angles. (a) Near-shoulder. (b) Overhead. (c) Far-shoulder.

the character before lifting the finger up. To delete a character, the user makes one lower-left touch stroke on the touch screen. The user's touch gestures and entered characters are recorded in a system log file. The system first compares a password entry with the actual password. If a match is found, the system proceeds with analyzing extracted features from the logged data. Sample touch gesture features include the coordinates of the start and end points of a touch gesture (spatial feature), gesture velocity and acceleration (temporal feature), the length of a thumb stroke trajectory and the average direction of all segments of a trajectory (geometric feature), and the distribution of the number of segments of a thumb stroke trajectory (statistical feature) [18]. These features serve as the inputs to a classification model that finally determines whether the user should be authenticated or not.

2) Keystroke-Based Password Method: The process of keystroke-based password authentication starts with a user entering a password using a standard QWERTY keyboard (see Fig. 1(b)), followed by the system trying to match the password entry to the actual password. A user's keystroke-based behaviors and entered characters are also captured in a system log file. Upon a successful match, the method proceeds with analyzing keystroke features from the system log, such as key down and up, and their associated spatial (e.g., tap position on the touchscreen), temporal (e.g., tap duration and latency), and operational features, which are used to determine the final authentication outcome.

Each of the entered password characters is masked as "$*$" in the screen display by default. Given the focal problem of this study and the transparency of the authentication models to both a mobile user and an adversary, we did not consider the classification models of the two authentication methods in this study. In other words, the authentication outcomes are determined solely based on password entries.

B. Shoulder-Surfing Settings

Interaction mode: A target user (i.e., who is under a shoulder-surfing attack) may interact with a mobile device in a one-handed or two-handed mode. In one-handed interaction (see Fig. 2(a)), a user holds and interacts with a mobile phone using the same hand [54], [55]. In contrast, two-handed interaction refers to using both hands when performing mobile user authentication (see Fig. 2(b)).

Observation angle: An adversary may observe an authentication session from different angles and distances. Based on the literature [13], [29], we selected three observation angles (see Fig. 3), namely near-shoulder, where an adversary is 60 cm away from the target user's mobile screen, far shoulder, where an adversary is 80 cm away, and overhead with an observation distance of 95 cm.

Entry error: Nearly 3% of users fail to enter a password correctly [27], and the number of failures is even doubled when employing more complex passwords [56]. To increase the ecological validity of this research, we considered password entries involving errors (one or two errors) with immediate follow-up corrections in addition to error-free entries. An entry error could occur at any position of a password.

Observation effort: A shoulder-surfing adversary may deploy an attack on the same target user more than once. This issue has been largely overlooked by previous studies except for Aviv et al. [13], which used two attempts. While the participants in [57] tried to identify passwords three times, they were allowed to make one observation attempt only. None of the previous studies has empirically examined shoulder-surfing with more than two observation attempts. We consider three attempts in a shoulder-surfing attack to understand the effect of increased observation effort (i.e., attempts).

C. Hypotheses Development

Our analysis of the selected touch-gesture-based password method via the lens of the four shoulder-surfing resistance strategies (see Section II-A) shows that the method embraces them all. First, the touch-gesture-based password method offers high visibility reduction via the support of keypress-free interactions that solely rely on the directions of touch gestures in entering characters without the need of looking at the screen. Second, the method supports action segmentation by requiring two touch gestures to enter most of the characters. Such split-source information imposes a cognitive burden on an adversary. Moreover, the overlapping touch gestures (i.e., directions) among different characters further increase the perplexity of password identification. Third, it exemplifies knowledge transformation by translating consecutive touch gestures into corresponding characters, which requires extra cognitive processing effort. Fourth, the method manifests characteristics verification by drawing on both behavioral biometrics from touch gestures and the physiological characteristics of the thumb of a target user.

Our analysis of the keystroke-based password method reveals that it operationalizes characteristics verification by extracting and analyzing keystroke biometrics. However, the method does not employ any other shoulder-surfing resistance strategies. Given that a keystroke-based password method inevitably relies on a keyboard, an adversary could guess the key entries based on

Authorized licensed use limited to: University of North Carolina at Charlotte. Downloaded on June 02,2023 at 02:37:13 UTC from IEEE Xplore. Restrictions apply.

their observations of the keyboard-dependent patterns by leveraging landmarks, and/or the direction and distance relative to the previous keystroke as behavioral patterns for password identification. In contrast, a touch-gesture-based password method, as discussed earlier, is able to avoid the exploitation of landmarks by eliminating the reliance on keypads. Thus, we propose the first hypothesis as follows:

H1. The touch-gesture-based password method is more resistant to shoulder-surfing attacks than the keystroke-based password method.

Typos are not uncommon during password entry [27]. Based on a cognitive model of password recall and typing [58], entry errors can be attributed to memory and motor errors. The errors, along with subsequent error-correction operations, such as deletions and insertions, increase the "length" and accordingly complexity of a password, elevating the cognitive load and challenges for shoulder-surfing attackers. Therefore, we propose:

H2. Entry errors have a positive effect on the shoulder-surfing resistance of hybrid password methods.

While the interaction mode does not show an effect on the performance of shoulder-surfing in PIN and pattern lock [13], hand movement may introduce visual obstruction to an adversary [59], which in turn negatively influences shoulder-surfing resistance performance. Compared with two-handed interaction, one-handed interaction causes less visual occlusion to the adversary's observation. Thus, we hypothesize the effect of the interaction mode as follows:

H3. Two-handed authentication with a hybrid password is more resistant to shoulder-surfing attacks than one-handed authentication.

Aviv et al. [13] found that the near-shoulder observation from the left was more effective for shoulder-surfing attacks than the far-shoulder counterpart. However, their study focused on PINs and Android pattern locks, which are different authentication methods from ours. A comparison of PIN and ForcePIN (pressure-sensitive PIN) [29] did not find any significant difference in shoulder-surfing success between the left-shoulder and overhead observations. Nevertheless, that study did not consider the impact of observation distance (e.g., near-versus far-shoulder) and textual passwords. It is reasonable to predict that observations from a shorter distance and from a less unobstructed angle would be easier for shoulder-surfing attacks. Thus, we hypothesize the effect of the observation angle as follows:

H4. Far-shoulder observation is more resistant to shoulder-surfing attacks than overhead observation, and the latter is more resistant than near-shoulder observation.

We operationalize observation effort as the number of attempts for a shoulder-surfing attack. Khan et al. [60] found that 27% of shoulder-surfing attacks took more than one attempt. In addition, autolock (i.e., automatically locking a mobile device after a specific length of inactivity) is a vital time-based safeguarding mechanism of modern mobile devices [61]. On the other hand, autolock also forces a mobile user to reauthenticate whenever he/she tries to access the device, which creates an opportunity for an adversary to decode a target user's password more than once during a recorded attack. We extend the trial and error approach [62] to explain an attacker's behavior in shoulder-surfing—an attacker can make a conscious "correction" of the previous incorrect trial. Thus, the chance of success for shoulder-surfing attacks is expected to increase as the number of observation attempts increases. We propose the last hypothesis as follows:

H5. Observation effort has a negative effect on shoulder-surfing resistance of hybrid password methods.

IV. Study 1

We conducted two empirical studies to test the hypotheses, which were approved by the Institutional Review Board of the first author's home institute. In both studies, participants were cast into the role of adversaries to identify passwords through the observation of video-recorded authentication sessions. We chose to use the recorded shoulder-surfing attack because of its support for the examination of observation effort. Recorded shoulder-surfing attacks have also been commonly used in related studies (e.g., [13], [26]). The prototypes of the two hybrid password methods were used in both user studies.

Study 1 was a longitudinal controlled lab experiment for investigating the effects of the hybrid password method, interaction mode, observation angle, entry error, and observation effort on the performance of shoulder-surfing resistance. The study followed a within-subjects design with the order of shoulder-surfing settings counterbalanced across participants to avoid potential learning effects, except for observation effort (i.e., always starting with the first attempt).

A. Tasks and Procedure

The experimental procedure began with the study introduction, consent for participation, and pre-experiment survey. The pre-experiment survey was about the participants' demographics and experience with mobile devices and mobile user authentication. The survey results show that all the participants had prior experience with the keystroke-based password method, but none had any experience with the touch-gesture-based password method. We designed a series of training and practice sessions using our prototype systems to familiarize the participants with both password methods.

The participants were asked to complete daily practices for one week. The daily practice involved entering a set of 5 different textual passwords with both touch-gesture- and keystroke-based password methods in both interaction modes, a total of 20 password entries. The researchers checked the system logs of participants' practice every day and sent an email or short text message reminder to the participants as needed. After completing the weeklong practices, the participants took a password entry familiarity test with both password methods and two interaction modes in the lab. Next, the participants were asked to repeat the daily practice for a second week and the qualification test after that. Only those participants who were able to keep up with the daily practice and achieve a sufficient level of password entry accuracy (75% or higher) with both password methods were eligible for the shoulder-surfing study. The accuracy was defined as the percentage of password characters entered correctly.

The formal shoulder-surfing session started with a different training session where the participants were asked to watch sample video recordings of password entry sessions first, similar

Authorized licensed use limited to: University of North Carolina at Charlotte. Downloaded on June 02,2023 at 02:37:13 UTC from IEEE Xplore. Restrictions apply.

to those later used in the formal study, and then practice password identification. Upon completion of the training, the participants proceeded with watching 24 videos of prerecorded password entry sessions under different settings and identifying the entered password one by one. The video sequence was randomized for the participants. Each participant was asked to watch the video recording of each password entry session three times in a row and enter/modify the identified password after each observation. We developed an experimental system that streamlined the entire experiment procedure. The system recorded the participants' interaction behaviors, such as the start and end time of playing a video recording and password submissions, in log files.

B. Participants

It is common to use student participants in mobile authentication studies. Previous shoulder-surfing studies [42], [63] showed that it would be extremely challenging to recruit a large number of participants for a longitudinal study. We recruited 17 participants who were undergraduate and graduate students from a university on the east coast of the U.S. All the participants owned a touch-screen smartphone and had experience with interacting with mobile devices in the past three months. 13 participants successfully completed all the tasks and each received a $45 gift card. Among them, five were male and eight were female; nine were aged from 19 to 24 years old; and four were from 25 to 36 years old.

C. Apparatus and Materials

Previous studies showed that 87% of passwords would have 6 to 10 letters in length [64] and users tend to create simple and memorable passwords [65]. One possible solution to overcoming user-generated simple and user-friendly passwords is by implementing system-generated random passwords to minimize the risk of password attacks. The information processing theory [66] posits that most people keep 7 ± 2 elements in their short-term memory, regardless of the format of the elements (e.g., digits, words). Therefore, a quality password should consist of 8 or more random characters to prevent easy recall by an adversary, which is also a common practice nowadays. Therefore, in this study, we created 8-character nondictionary word as passwords by following the recommendation from the National Institute of Standards and Technology [67]. We prepared 24 passwords (e.g., "aelpwsxf" and "nxafuwoj") and assigned one to each unique setting, except that the same passwords were repeated across three observation attempts. The orders of hybrid password methods and shoulder-surfing settings were randomized across different participants. We used a Samsung Galaxy S6 smartphone with a 5.1" touch screen, which was reported to have high grip comfort during texting and high user satisfaction [68].

The password entry sessions were recorded in advance by an expert user who was familiar with both password methods and prototypes for two main reasons: 1) supporting data collection from the large number of shoulder-surfing settings and entry error manipulations; and 2) eliminating confounding factors introduced by individual variations in password entry behaviors. To make the password authentication sessions more representative of the average user, we asked an expert user to follow the average text entry speed of the participants based on the data collected from the qualification test in the first training session in recording the videos.

D. Variables and Measures

The dependent variables measure both the effectiveness and efficiency of shoulder-surfing resistance. We selected two effectiveness metrics: 1) accuracy; and 2) distance. Accuracy was defined as the percentage of correctly identified characters in a password (e.g., [13], [26], [27]), and distance as the difference between an identified password and the actual one in terms of the minimum number of single-character edits, which was operationalized with the Levenshtein Distance [15].

We introduced two efficiency metrics, namely identification time and recall time. Identification time was defined as the time elapsed between the time an adversary started watching a password entry session and the time he/she submitted an identified password. Recall time was defined as the time elapsed between the time a participant finished watching a video and the time he/she submitted an identified password. Both were measured in seconds.

There were five independent variables, including hybrid password method (touch-gesture-based versus keystroke-based), interaction mode (one-handed versus two-handed), observation angle (near-shoulder, overhead, versus far-shoulder), entry error (with one entry error versus with no error), and observation effort (first, second, versus third attempt).

E. Results

The descriptive statistics of shoulder-surfing performances are reported in Table I. We first performed Shapiro–Wilk tests on the data residuals to check for data normality. The results show that the residuals for accuracy and distance were largely normally distributed with very few exceptions. In those cases, the violation of normality was minor ($p < 0.05$). The literature suggests that parametric tests work well even for moderately skewed distributions of the outcome variable [69] and do not result in loss of information [70]. Compared with nonparametric tests, parametric tests are more discriminant by revealing the size and direction of the observed effect across multiple experiment settings [69]. Thus, we performed repeated-measures ANOVA and reported the test results in Table II. In addition, we conducted post-hoc multiple comparisons for observation angle and observation effort with Bonferroni adjustments to test the related hypotheses. The results are reported in Tables III and IV.

The analyses of accuracy yield significant main effects of password method ($p < 0.01$), interaction mode ($p < 0.001$), observation angle ($p < 0.001$), and observation effort ($p < 0.001$), yet an insignificant effect of entry error ($p > 0.05$). Specifically, the accuracy of password identification was higher for the keystroke-based password (mean = 0.536) than that for the touch-gesture-based counterpart (mean = 0.462); and the accuracy was higher for the one-handed interaction (mean = 0.562) than the two-handed counterpart (mean = 0.435). The results of multiple comparisons of observational angles show that the accuracy for the far-shoulder observation was lower than those for the near-shoulder ($p < 0.001$) and overhead ($p < 0.01$) observations, and

Authorized licensed use limited to: University of North Carolina at Charlotte. Downloaded on June 02,2023 at 02:37:13 UTC from IEEE Xplore. Restrictions apply.

TABLE I
DESCRIPTIVE STATISTICS [MEAN (STD)] OF SHOULDER-SURFING RESISTANCE PERFORMANCE IN STUDY 1

(a) Touch-gesture-based password

Shoulder-surfing settings		Accuracy	Distance	Identification time	Recall time
Interaction mode	One-handed	0.47 (0.202)	5.18 (1.874)	24.63 (4.009)	10.30 (3.380)
	Two-handed	0.45 (0.132)	5.56 (1.060)	24.16 (2.096)	10.16 (1.929)
Observation angle	Near	0.67 (0.067)	3.54 (0.895)	23.72 (3.445)	9.72 (3.387)
	Overhead	0.35 (0.063)	6.30 (0.568)	25.89 (4.113)	11.39 (3.108)
	Far	0.36 (0.028)	6.28 (0.206)	23.58 (1.039)	9.58 (1.199)
Entry error	w/o error	0.47 (0.154)	5.28 (1.427)	23.39 (2.257)	10.06 (2.385)
	with one error	0.45 (0.185)	5.46 (1.633)	25.40 (3.616)	10.40 (3.066)
Observation effort	First attempt	0.35 (0.142)	5.97 (1.194)	25.30 (4.948)	11.14 (4.833)
	Second attempt	0.48 (0.173)	5.27 (1.559)	23.48 (3.698)	9.31 (3.440)
	Third attempt	0.56 (0.181)	4.87 (1.689)	24.41 (5.217)	10.25 (4.773)

(b) Keystroke-based password

Shoulder-surfing settings		Accuracy	Distance	Identification time	Recall time
Interaction mode	One-handed	0.65 (0.089)	3.77 (1.129)	20.99 (1.212)	9.33 (2.065)
	Two-handed	0.42 (0.064)	5.75 (0.739)	17.86 (1.372)	7.03 (0.684)
Observation angle	Near	0.56 (0.181)	4.44 (1.652)	19.67 (2.507)	8.92 (2.131)
	Overhead	0.59 (0.135)	4.03 (1.109)	19.95 (2.240)	7.45 (2.216)
	Far	0.46 (0.096)	5.80 (0.838)	18.67 (1.694)	8.17 (1.511)
Entry error	w/o error	0.54 (0.135)	4.90 (1.505)	19.44 (2.415)	8.60 (2.068)
	with one error	0.53 (0.160)	4.62 (1.362)	19.42 (1.843)	7.75 (1.785)
Observation effort	First attempt	0.40 (0.104)	5.67 (1.003)	18.26 (1.759)	7.01 (1.507)
	Second attempt	0.57 (0.159)	4.55 (1.464)	17.80 (2.010)	6.55 (2.090)
	Third attempt	0.64 (0.169)	4.06 (1.706)	22.22 (5.336)	10.97 (5.210)

TABLE II
RESULTS OF REPEATED ANOVA OF SHOULDER-SURFING RESISTANCE PERFORMANCE IN STUDY 1

Settings	Accuracy		Distance		Identification time		Recall time	
	F-value	Sig.	F-value	Sig.	F-value	Sig.	F-value	Sig.
Password method	F(1,12)= 2.36	0.004**	F(1,12)= 11.75	0.005**	F(1,12)= 1.02	0.001**	F(1,12)= 3.47	0.087†
Interaction mode	F(1,12)= 17.10	<0.001***	F(1,12)= 91.88	<0.001***	F(1,12)= 2.69	0.127	F(1,12)= 1.25	0.286
Observation angle	F(2,24)= 0.60	<0.001***	F(2,24)= 70.66	<0.001***	F(2,24)= 1.16	0.325	F(2,24)= 0.14	0.826
Entry error	F(1,12)= 1.50	0.244	F(1,12)= 0.62	0.732	F(1,12)= 0.44	0.519	F(1,12)= 0.06	0.806
Observation effort	F(2,24)= 4.86	<0.001***	F(2,24)= 44.84	<0.001***	F(2,24)= 4.55	0.026*	F(2,24)= 4.55	0.026*

[a]:mean difference; ***: $p<0.001$; **: $p<0.01$; *: $p<0.05$; †: $p<0.1$.

TABLE III
MULTIPLE-COMPARISON RESULTS OF OBSERVATION ANGLE IN STUDY 1

Angles		Accuracy			Distance			Identification time			Recall time		
(I)	(J)	(I-J)[a]	Std. Error	Sig.	(I-J)[a]	Std. Error	Sig.	(I-J)[a]	Std. Error	Sig.	(I-J)[a]	Std. Error	Sig.
near	**far**	0.206	0.016	<0.001***	-2.050	0.169	<0.001***	612.1	915.1	1.00	487.1	915.1	1.00
	overhead	0.146	0.016	<0.001***	-1.180	0.172	<0.001***	-1289.6	1436.6	1.00	-164.6	1436.6	1.00
far	**overhead**	-0.060	0.013	0.001**	0.869	0.178	0.001**	-1901.7	1409.4	0.606	-651.7	1409.4	1.00

[a]:mean difference; ***: $p<0.001$; **: $p<0.01$; *: $p<0.05$.

TABLE IV
MULTIPLE-COMPARISON RESULTS OF OBSERVATION EFFORT IN STUDY 1

Attempts		Accuracy			Distance			Identification time			Recall time		
(I)	(J)	(I-J)[a]	Std. Error	Sig.	(I-J)[a]	Std. Error	Sig.	(I-J)[a]	Std. Error	Sig.	(I-J)[a]	Std. Error	Sig.
1st	**2nd**	-0.151	0.019	<0.001***	0.913	0.132	<0.001***	1240.4	878.3	0.550	1240.4	878.3	0.550
	3rd	-0.226	0.025	<0.001***	1.356	0.196	<0.001***	-1676.4	1128.9	0.490	-1676.4	1128.9	0.490
2nd	**3rd**	-0.075	0.008	<0.001***	0.442	0.090	0.001**	-2916.8	881.9	0.019*	-2916.8	881.9	0.019*

[a]:mean difference; ***: $p<0.001$; **: $p<0.01$; *: $p<0.05$.

the accuracy for the overhead was lower than that for the near-shoulder observation ($p < 0.001$). In addition, the accuracy showed an increasing linear trend as the observation attempt increased ($p < 0.001$). The results of multiple comparisons of observation attempts show that the accuracy of the second observation attempt was higher than that of the first attempt ($p < 0.001$) and yet lower than that of the third attempt ($p < 0.001$).

The analyses of the distance of shoulder-surfing attacks yield significant main effects of password method ($p < 0.01$), interaction mode ($p < 0.001$), observation angle ($p < 0.001$), and observation effort ($p < 0.001$), but no effect of entry error ($p > 0.05$). Specifically, the distance was smaller for the keystroke-based password (mean = 4.759) than that for the touch-gesture-based password (mean = 5.370); and the distance was smaller for the one-handed interaction (mean = 4.474) than

Authorized licensed use limited to: University of North Carolina at Charlotte. Downloaded on June 02,2023 at 02:37:13 UTC from IEEE Xplore. Restrictions apply.

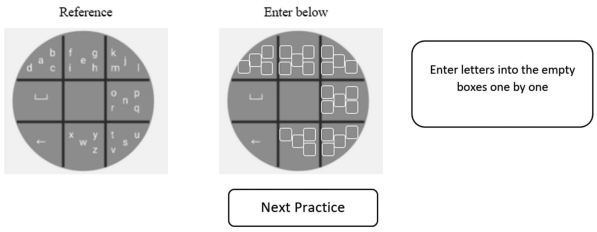


Fig. 4. Keyboard interface for the touch-gesture-based password training.

that for the two-handed counterpart (mean = 5.654). The results of multiple comparisons of observation angles reveal that the distance for the far-shoulder observation was greater than that for the near-shoulder ($p < 0.001$) and overhead observations ($p < 0.01$), and the distance for the near-shoulder was greater than that for the overhead observation ($p < 0.001$). In addition, the distance exhibited a linearly decreasing trend as the number of observation attempts increased ($p < 0.001$). The results of multiple comparisons of observation attempts show that the distance of the second observation attempt was smaller than that of the first attempt ($p < 0.001$), and the distance of the third attempt was lower than that of the second attempt ($p < 0.01$).

The analyses of identification time yield significant main effects of password method ($p < 0.01$) and observation effort ($p < 0.05$), yet no significant main effect of interaction mode ($p > 0.05$), observation angle ($p > 0.05$), and entry error ($p > 0.05$). Specifically, the identification time was longer for the touch-gesture-based password (mean = 24.232) than that for the keystroke-based password (mean = 19.318). The multiple-comparison results of the observation effort show that there was an increase in identification time from the second to the third observation attempt ($p < 0.05$), but no change in the identification time between the first two attempts ($p > 0.05$). Similarly, the analysis of the recall time of shoulder-surfing attacks yielded significant main effects for the password method ($p < 0.05$) and observation effort ($p < 0.05$) but no significant main effect of interaction mode, observation angle, and entry error ($p > 0.05$). Specifically, the recall time was longer for the touch-gesture-based password (mean = 10.065) than that for the keystroke-based password (mean = 8.069). The multiple-comparison results of observation attempts show that there was an increase in recall time from the second to the third observation attempt ($p < 0.05$), yet no difference in the recall time between the first two attempts was detected ($p > 0.05$).

V. Study 2

The sample size of Study 1 was relatively small, and the participants were homogeneous. Additionally, the task of shoulder-surfing might induce stress in the participant adversaries, which may further influence task performance but was not accounted for in Study 1. Technically, an adversary should be able to launch a shoulder-surfing attack as long as he/she is familiar, even though not necessarily skillful, with an authentication method. To address the above-mentioned issues, we designed an online experiment in Study 2, which incorporated perceived stress and recruited participants from a larger and more diverse user population. Furthermore, based on the findings of Study 1, we excluded two-handed interaction and far-shoulder observation to manage task complexity and reduce participant fatigue in Study 2. We also replaced the one-error setting with a two-error setting to further examine the effect of entry error. For the sake of space, we will mainly introduce differences in the method design between the two studies.

A. Tasks and Procedure

The participants were prescreened based on the following eligibility criteria:

1) 18 years of age or older;
2) capable of watching a video and entering text using a keyboard on a device screen;
3) owning a touch-screen mobile device;
4) experienced with entering text and performing mobile user authentication in the past three months.

Like study 1, the formal experimental procedure consisted of a pre-experiment survey, password entry training and familiarity testing, and shoulder-surfing sessions. The pre-experiment survey included additional questions on perceived stress. The password method training involved watching a demonstration video of the keyboard used in the touch-gesture-based password, and practicing with an online prototype by entering 26 English letters into the designated text fields one by one in a blank keyboard for the touch-gesture-based password (see Fig. 4). The participants must enter all the letters accurately and repeat them for two rounds to familiarize themselves with the method. The familiarity tests included questions on the memorability of letters on the keyboards of touch-gesture-based and keystroke-based password methods separately. The responses show that 75% of the participants could enter 16 or more letters without looking at the keyboard used in the touch-gesture-based password, and the percentage was 68% for the keyboard used in the keystroke-based password. The shoulder-surfing sessions started with training and then proceeded to the formal shoulder-surfing tasks, which were identical to those of study 1.

B. Participants

We recruited participants from Amazon Mechanical Turk (MTurk) for this study. MTurk has been widely used to examine user attitudes and perceptions toward mobile user authentication [43] and to collect data for touch-based authentication [71]. Importantly, MTurk workers are much more diverse than participants recruited via other methods [72]. Despite concerns about the quality and validity of data collected from MTurk [73], there are countermeasures. To this end, we selected participants from interested MTurkers who had a 95% HIT approval rate and completed more than 500 approved HITs on MTurk, and incorporated attention questions into the surveys. Among the 912 MTurkers who signed up for the study, 477 passed the prescreening, and 181 were identified as eligible based on their responses to the pre-experiment survey. Finally, a total of 63 participants successfully completed the entire study and received $5 each. To motivate the participants, we offered an extra $3 as a bonus to each of the top 10 performers.

Among the 63 participants, 7 were aged between 19 and 24 years old; 33 between 25 and 34 years old; 16 between 35 and 44 years old; 5 between 45 and 54 years old; and 2 between 55 to 64 years old. Twenty-eight participants were female, and 35

Authorized licensed use limited to: University of North Carolina at Charlotte. Downloaded on June 02,2023 at 02:37:13 UTC from IEEE Xplore. Restrictions apply.

TABLE V
DESCRIPTIVE STATISTICS [MEAN (STD)] OF SHOULDER-SURFING RESISTANCE PERFORMANCE IN STUDY 2

(a) Touch-gesture-based password

Shoulder-surfing settings		Accuracy	Distance	Identification time	Recall time
Observation angle	Near	0.32 (0.161)	7.34 (1.781)	42.54 (61.195)	29.94 (61.108)
	Overhead	0.29 (0.173)	7.53 (1.707)	34.85 (52.440)	22.21 (52.303)
Entry error	w/o error	0.31 (0.165)	7.08 (1.672)	33.64 (42.973)	22.47 (42.978)
	with two errors	0.30 (0.170)	7.79 (1.749)	43.75 (68.019)	29.68 (68.018)
Observation effort	First attempt	0.27 (0.158)	7.45 (1.464)	56.88 (69.387)	44.25 (69.261)
	Second attempt	0.31 (0.163)	7.44 (1.794)	33.59 (59.912)	20.97 (59.831)
	Third attempt	0.33 (0.176)	7.41 (1.951)	25.62 (29.427)	12.99 (29.256)

(b) Keystroke-based password

Shoulder-surfing settings		Accuracy	Distance	Identification time	Recall time
Observation angle	Near	0.60 (0.266)	4.46 (2.962)	38.41 (56.659)	26.34 (56.491)
	Overhead	0.49 (0.260)	5.64 (2.742)	32.18 (37.100)	20.49 (37.062)
Entry error	w/o error	0.56 (0.279)	4.71 (2.897)	30.86 (35.734)	20.23 (35.762)
	with two errors	0.54 (0.258)	5.39 (2.893)	39.60 (57.089)	26.50 (57.025)
Observation effort	First attempt	0.45 (0.244)	5.74 (2.531)	51.83 (67.501)	39.96 (67.339)
	Second attempt	0.57 (0.260)	4.87 (2.924)	30.00 (35.122)	18.12 (35.005)
	Third attempt	0.62 (0.271)	4.55 (3.131)	22.70 (21.398)	10.82 (21.265)

TABLE VI
RESULTS OF REPEATED ANOVA ON SHOULDER-SURFING RESISTANCE PERFORMANCE IN STUDY 2

Settings	Accuracy		Distance		Identification time		Recall time	
	F-value	Sig.	F-value	Sig.	F-value	Sig.	F-value	Sig.
Password method	F(1,4)= 483.588	<0.001***	F(1,4)= 398.447	<0.001***	F(1,4)=2.132	0.144	F(1,4)=1.385	0.240
Observation angle	F(1,4)= 36.626	<0.001***	F(1,4)= 33.344	<0.001***	F(1,4)=6.531	0.011*	F(1,4)=6.203	0.013*
Entry error	F(1,4)= 2.068	0.151	F(1,4)=33.858	<0.001***	F(1,4)=12.660	<0.001***	F(1,4)=6.480	0.011*
Observation effort	F(2,8)= 39.590	<0.001***	F(2,8)= 9.356	<0.001***	F(2,8)= 47.016	<0.001***	F(2,8)=47.016	<0.001***

[a]:mean difference; ***: p<0.001; **: p<0.01; *: p<0.05; †: p<0.1.

were male. Six had a high school degree or equivalent; 5 had some college yet without a degree; 2 had an associate degree; 35 had a bachelor's degree; 12 had a master's degree; and 3 had a doctorate. The distributions of the participant demographics in this study are much more diverse than those of Study 1 participants.

C. Variables and Measures

Based on the findings of Study 1, we adopted all the variables except the interaction mode. In addition, we removed the far-shoulder angle and replaced the one-error with a two-error setting. We measured stress through perceived stress [74], a well-established scale commonly used by psychometric studies [75]. It consists of six items of negative statements rated on a 5-point scale, ranging from never to very often, and four items of positive statements rated reversely [74].

D. Results

The descriptive statistics of shoulder-surfing performances are presented in Table V. We performed repeated measures ANCOVA by using perceived stress as a covariate first. The analysis did not yield a significant interaction effect between perceived stress and any of the independent variables ($p > 0.05$) on any of the dependent variables except an interaction between perceived stress and observation effort on identification time and recall time ($p < 0.05$). Yet the significance level of the above interaction effects was much lower than that of the main effect of observation effort ($p < 0.001$). Thus, we dropped perceived stress from the model in subsequent analyses. The results of repeated-measures ANOVA are reported in Table VI.

The analyses of accuracy yield significant main effects of the password method ($p < 0.001$), observation angle ($p < 0.001$), and observation effort ($p < 0.001$), yet an insignificant effect for entry error ($p > 0.1$). Specifically, the accuracy of password identification from the keystroke-based password (mean = 0.547) was higher than that from the touch-gesture-based password (mean = 0.304); and the accuracy was higher for the near observation (mean = 0.459) than that for the overhead counterpart (mean = 0.392). The results of multiple comparisons of observation effort show that the accuracy of the third observation attempt was higher than that of the second attempt ($p < 0.05$), and the latter was higher than the accuracy of the first attempt ($p < 0.001$).

The analyses of distance yield significant main effects for the password method ($p < 0.001$), observation angle ($p < 0.001$), entry error ($p < 0.001$), and observation effort ($p < 0.001$). Specifically, the distance was smaller for the keystroke-based password (mean = 5.053) than that for the touch-gesture-based password (mean = 7.435); the distance was smaller for the near-shoulder observation (mean = 5.899) than that for the overhead observation (mean = 6.589); and the distance was smaller for password entries with no error (mean = 5.897) than that for the two-error entries (mean = 6.591). The of multiple-comparison results of observation effort show a smaller distance in the second observation attempt than that in the first attempt ($p < 0.01$) and the distance was smaller in the third attempt than that in the first attempt ($p < 0.001$), yet there was no difference between the second and the third attempts ($p > 0.1$).

The analyses of identification time yield significant main effects of observation angle ($p < 0.05$), entry error ($p < 0.001$), and observation effort ($p < 0.001$) but no effect of password

Authorized licensed use limited to: University of North Carolina at Charlotte. Downloaded on June 02,2023 at 02:37:13 UTC from IEEE Xplore. Restrictions apply.

method ($p > 0.1$). Specifically, the identification time was longer for the near-shoulder (mean = 40.149) than for the overhead observation (mean = 33.366); and the identification time was longer for a password entry with two errors (mean = 41.479) than for the no-error counterpart (mean = 32.035). The results of multiple comparisons of observation effort show that there was a decrease in identification time from the first observation attempt to the second attempt ($p < 0.001$) and from the first to the third attempt ($p < 0.001$), and a decrease from the second to the third attempt was marginal ($p < 0.1$). The analysis results of recall time were identical to those of identification time.

In summary, Study 1 results provide support for hypothesis H1, partial support for hypotheses H3, H4, and H5 in terms of effectiveness, but no support for hypothesis H2. Study 2 confirms the findings of Study 1 for all of its tested hypotheses except for the effects on efficiency.

VI. Discussion

In this study, we examined two hybrid password methods under different shoulder-surfing settings. The findings of the two studies consistently demonstrate that the touch-gesture-based password method was more effective in shoulder-surfing resistance than its keystroke-based counterpart. In addition, the overhead observation was more resistant to shoulder-surfing than the near-shoulder observation, and increased effort weakened the shoulder-surfing resistance of password methods. Study 1 also found that the far-shoulder observation was more effective than the one-handed mode, in shoulder-surfing resistance.

This study makes multifold research contributions to the field of mobile user authentication, particularly hybrid password methods. First, this is the first study that compares a touch-gesture-based password with a keystroke-based password in shoulder-surfing resistance and offers empirical evidence for the superior performance of the former. Thus, exploiting rich information in touch gestures holds great promise for enhancing password security. Second, this study provides a holistic understanding of hybrid password methods with respect to their shoulder-surfing resistance in multiple aspects, including behavioral biometrics, interaction mode, observation angle, observation effort, and entry error. These various aspects can serve as the essential components of a framework to guide future comparative shoulder-surfing studies. Third, to the best of our knowledge, this is the first shoulder-surfing study that examines the effects of entry errors and multiple attempts. The reduced shoulder-surfing resistance of hybrid passwords from the second to the third attempt underscores the importance of understanding the dynamics of shoulder-surfing resistance of hybrid passwords over multiple attempts. Researchers should revisit the number of allowed attempts per authentication session because repeated attempts may impair the shoulder-surfing resistance of a password method. This suggestion can be extended to the design of auto screen lock [61], which may force a user to re-log in repetitively, which is more likely to invite shoulder-surfing attacks. Fourth, we introduce new efficiency metrics (e.g., recall time) to address real-world scenarios where shoulder-surfing attacks are carried out under time pressure. Combining efficiency with effectiveness measures offers a more comprehensive evaluation of shoulder-surfing resistance of password methods.

From a methodological perspective, we deployed a multimethod approach that consisted of a longitudinal controlled lab experiment and an online experiment to deepen and validate our understanding of the hybrid password methods in guarding users against shoulder-surfing attacks.

The findings on the impact of entry errors were unexpected, suggesting that deliberately injecting one or even two errors into a password entry would not make passwords more shoulder-surfing resistant. One possible explanation is that the effect of entry error might be overshadowed by that of the hybrid password methods. Another is that two or fewer errors may still be insufficient to derail an adversary's password identification effort. A third alternative explanation is that the process of error correction gives adversaries extra observation time, negating the effect of error(s). On the other hand, the findings of Study 2 show that injecting entry errors hampered the efficiency of password identification. Thus, an erroneous password entry has the potential to help mobile users deter password identification via shoulder-surfing by increasing the effort or the cost of attacks.

Although observation effort showed an effect on shoulder-surfing efficiency across both studies, the between-attempts comparison results of the two studies reveal some differences. For instance, the third observation attempt was found to be less efficient than the second attempt in Study 1, yet the two attempts were not found to be significantly different in Study 2. In contrast, the first observation attempt was found to be less efficient than the other two attempts in Study 2, yet no difference was detected between the first and either of the last two attempts in Study 1. While the touch-gesture-based password method showed a lower shoulder-surfing efficiency compared with the keystroke-based counterpart in Study 1 only, observation angle and entry error were found to impact shoulder-surfing efficiency in Study 2 only. One possible explanation for these differences is that it is easier for researchers to monitor the task completion process in a lab than in an online environment. Another explanation is that the participants in the lab may have perceived task effectiveness as more important and efficiency as less important than those in the online environment. As a result, Study 1 participants took the most time for the best outcomes in their last attempts.

The research findings have practical implications for mobile users. Our findings can help increase their awareness of the threat of shoulder-surfing attacks to keystroke-based passwords and suggest touch-gesture-based passwords as a safer alternative. In addition, a mobile user should pay attention to his/her close surroundings to minimize the risks of shoulder-surfing attacks from the near-shoulder and overhead angles. For instance, while accessing a mobile device in a sitting position, a user may consider tilting the device away from an observer [29] or using a free hand or fingers to cover part of the screen. In a public space, a mobile user should enter a password with two hands rather than one hand whenever possible. The user may also occasionally switch his/her position to avoid repeated attacks.

This research has several limitations that offer future research opportunities. First, we fixed the password length in the experiments. Whether our findings are generalizable to passwords with varying lengths or degrees of complexity is worthy of future investigation. Second, future studies may extend the current study's evaluation framework for shoulder-surfing resistance

Authorized licensed use limited to: University of North Carolina at Charlotte. Downloaded on June 02,2023 at 02:37:13 UTC from IEEE Xplore. Restrictions apply.

methods by exploring alternative efficiency metrics such as the number of attempts necessary for identifying a password. Third, correct identification of a password does not necessarily lead to successful access to a mobile device, particularly when using hybrid password methods such as a touch-gesture-based password. Thus, it would be interesting to explore the shoulder-surfing resistance of the above methods as a whole. Last but not least, stress did not show a significant interaction effect with most of the independent variables. The participants were allowed to take as much time as needed for each observation attempt in our studies. Limiting the time per attempt and using direct observations in a future study may induce stress, which could further affect the shoulder-surfing resistance performance.

ACKNOWLEDGMENT

The authors would like to thank Zhe Fu for his assistance with setting up the online experiment for Study 2.

REFERENCES

[1] A. M. Gubernatorov, I. B. Teslenko, N. V. Muravyova, D. V. Vinogradov, and N. O. Subbotina, "Information security of mobile systems," in *Growth Poles of the Global Economy: Emergence, Changes and Future Perspectives*, E. G. Popkova, Ed. Cham, Switzerland: Springer, 2020, pp. 677–686, doi: 10.1007/978-3-030-15160-7_68.

[2] D. Kunda and M. Chishimba, "A survey of android mobile phone authentication schemes," *Mobile Netw. Appl.*, vol. 26, pp. 2558–2566, 2021, doi: 10.1007/s11036-018-1099-7.

[3] C. G. Krishna and R. B. Dinakar, "The shoulder surfing resistant graphical authentication technique," *Int. J. Trend Res. Develop.*, Apr. 2017, pp. 11–12.

[4] M. Eiband, M. Khamis, E. von Zezschwitz, H. Hussmann, and F. Alt, "Understanding shoulder surfing in the wild: Stories from users and observers," in *Proc. CHI Conf. Hum. Factors Comput. Syst.*, 2017, pp. 4254–4265, doi: 10.1145/3025453.3025636.

[5] Y. Abdrabou, M. Khamis, R. M. Eisa, S. Ismail, and A. Elmougy, "Just gaze and wave: Exploring the use of gaze and gestures for shoulder-surfing resilient authentication," in *Proc. 11th ACM Symp. Eye Tracking Res. Appl.*, Jun. 2019, pp. 1–10, doi: 10.1145/3314111.3319837.

[6] S. A. Alsuhibany, "Usability and shoulder surfing vulnerability of pattern passwords on mobile devices using camouflage patterns," *J. Ambient Intell. Humanized Comput.*, vol. 11, no. 4, pp. 1645–1655, Apr. 2020, doi: 10.1007/s12652-019-01269-3.

[7] J. Lai and E. Arko, "A shoulder-surfing resistant scheme embedded in traditional passwords," in *Proc. 54th Hawaii Int. Conf. Syst. Sci.*, 2021, pp. 7144–7152, doi: 10.24251/HICSS.2021.860.

[8] N. Chakraborty, G. S. Randhawa, K. Das, and S. Mondal, "Mobsecure: A shoulder surfing safe login approach implemented on mobile device," *Procedia Comput. Sci.*, vol. 93, pp. 854–861, 2016, doi: 10.1016/j.procs.2016.07.256.

[9] T. V. Nguyen, N. Sae-Bae, and N. Memon, "DRAW-A-PIN: Authentication using finger-drawn PIN on touch devices," *Comput. Secur.*, vol. 66, pp. 115–128, May 2017, doi: 10.1016/j.cose.2017.01.008.

[10] S. Prabhu and V. Shah, "Authentication using session based passwords," *Procedia Comput. Sci.*, vol. 45, pp. 460–464, Jan. 2015, doi: 10.1016/j.procs.2015.03.079.

[11] D. Schneider et al., "ReconViguRation: Reconfiguring physical keyboards in virtual reality," *IEEE Trans. Visual. Comput. Graph.*, vol. 25, no. 11, pp. 3190–3201, Nov. 2019, doi: 10.1109/TVCG.2019.2932239.

[12] T. Kwon and S. Na, "SteganoPIN: Two-faced human–machine interface for practical enforcement of PIN entry security," *IEEE Trans. Human-Mach. Syst.*, vol. 46, no. 1, pp. 143–150, Feb. 2016, doi: 10.1109/THMS.2015.2454498.

[13] A. J. Aviv, J. T. Davin, F. Wolf, and R. Kuber, "Towards baselines for shoulder surfing on mobile authentication," in *Proc. 33rd Annu. Comput. Secur. Appl. Conf.*, 2017, pp. 486–498, doi: 10.1145/3134600.3134609.

[14] F. Tari, A. A. Ozok, and S. H. Holden, "A comparison of perceived and real shoulder-surfing risks between alphanumeric and graphical passwords," in *Proc. 2nd Symp. Usable Privacy Secur.*, 2006, pp. 56–66, doi: 10.1145/1143120.1143128.

[15] L. Bošnjak and B. Brumen, "Shoulder surfing: From an experimental study to a comparative framework," *Int. J. Human-Comput. Stud.*, vol. 130, pp. 1–20, 2019, doi: 10.1016/j.ijhcs.2019.04.003.

[16] S. A. Alsuhibany, "A camouflage text-based password approach for mobile devices against shoulder-surfing attack," *Secur. Commun. Netw.*, vol. 2021, 2021, Art. no. 6653076, doi: 10.1155/2021/6653076.

[17] G. Cho et al., "On the security and usability implications of providing multiple authentication choices on smartphones: The more, the better?," *ACM Trans. Privacy Secur.*, vol. 23, no. 4, pp. 22:1–22:32, Aug. 2020, doi: 10.1145/3410155.

[18] L. Zhou, Y. Kang, D. Zhang, and J. Lai, "Harmonized authentication based on ThumbStroke dynamics on touch screen mobile phones," *Decis. Support Syst.*, vol. 92, pp. 14–24, 2016, doi: 10.1016/j.dss.2016.09.007.

[19] I. Velásquez, A. Caro, and A. Rodríguez, "Authentication schemes and methods: A systematic literature review," *Inf. Softw. Technol.*, vol. 94, pp. 30–37, 2018, doi: 10.1016/j.infsof.2017.09.012.

[20] Y. Zhang, W. Zhou, Y. Xue, J. Yang, and D. Liu, "Multiplexed imaging of trace residues in a single latent fingerprint," *Anal. Chem.*, vol. 88, no. 24, pp. 12502–12507, 2016, doi: 10.1021/acs.analchem.6b04077.

[21] S. Kumar, S. Singh, and J. Kumar, "A comparative study on face spoofing attacks," in *Proc. Int. Conf. Comput., Commun. Automat.*, 2017, pp. 1104–1108, doi: 10.1109/CCAA.2017.8229961.

[22] K. Sundararajan and D. L. Woodard, "Deep learning for biometrics: A survey," *ACM Comput. Surv.*, vol. 51, no. 3, pp. 65:1–65:34, May 2018, doi: 10.1145/3190618.

[23] S. Eberz, K. B. Rasmussen, V. Lenders, and I. Martinovic, "Looks like eve: Exposing insider threats using eye movement biometrics," *ACM Trans. Privacy Secur.*, vol. 19, no. 1, pp. 1:1–1:31, Jun. 2016, doi: 10.1145/2904018.

[24] D. Zhang, L. Zhou, and S. Pisupati, "Tracing one's touches: Continuous mobile user authentication based on touch dynamics," in *Proc. 25th Americas Conf. Inf. Syst.*, 2019, pp. 1–8. [Online]. Available: https://aisel.aisnet.org/amcis2019/human_computer_interact/human_computer_interact/3

[25] W. Meng, Y. Wang, D. S. Wong, S. Wen, and Y. Xiang, "TouchWB: Touch behavioral user authentication based on web browsing on smartphones," *J. Netw. Comput. Appl.*, vol. 117, pp. 1–9, 2018, doi: 10.1016/j.jnca.2018.05.010.

[26] H. Lee, J. Y. Hwang, D. I. Kim, S. Lee, S.-H. Lee, and J. S. Shin, "Understanding keystroke dynamics for smartphone users authentication and keystroke dynamics on smartphones built-in motion sensors," *Secur. Commun. Netw.*, vol. 2018, 2018, Art. no. 2567463, doi: 10.1155/2018/2567463.

[27] R. Chatterjee, A. Athayle, D. Akhawe, A. Juels, and T. Ristenpart, "pASSWORD tYPOS and how to correct them securely," in *Proc. IEEE Symp. Secur. Privacy*, 2016, pp. 799–818, doi: 10.1109/SP.2016.53.

[28] K. K. Kumbhare and K. V. Warkar, "A review on noisy password, voiceprint biometric and one-time-password," *Procedia Comput. Sci.*, vol. 78, pp. 382–386, 2016, doi: 10.1016/j.procs.2016.02.078.

[29] H. Khan, U. Hengartner, and D. Vogel, "Evaluating attack and defense strategies for smartphone PIN shoulder surfing," in *Proc. CHI Conf. Hum. Factors Comput. Syst.*, 2018, pp. 1–10, doi: 10.1145/3173574.3173738.

[30] D. Kim et al., "Multi-touch authentication on tabletops," in *Proc. 28th Int. Conf. Hum. Factors Comput. Syst.*, 2010, Art. no. 1093, doi: 10.1145/1753326.1753489.

[31] J.-N. Luo and M.-H. Yang, "A mobile authentication system resists to shoulder-surfing attacks," *Multimedia Tools Appl.*, vol. 75, no. 22, pp. 14075–14087, Nov. 2016, doi: 10.1007/s11042-015-3129-9.

[32] K. Divyapriya and P. Prabhu, "Image based authentication using illusion pin for shoulder surfing attack," *Int. J. Pure Appl. Math.*, vol. 119, no. 7, pp. 835–840, 2018, doi: 10.20894/IJCOA.101.007.001.009.

[33] G. Dhandapani, J. Ferguson, and E. Freeman, "HapticLock: Eyes-free authentication for mobile devices," in *Proc. Int. Conf. Multimodal Interact.*, 2021, pp. 195–202, doi: 10.1145/3462244.3481001.

[34] T. Kutzner, C. F. Pazmiño-Zapatier, M. Gebhard, I. Bönninger, W.-D. Plath, and C. M. Travieso, "Writer identification using handwritten cursive texts and single character words," *Electron.*, vol. 8, no. 4, Apr. 2019, Art. no. 391, doi: 10.3390/electronics8040391.

[35] L. Fang et al., "HandiText: Handwriting recognition based on dynamic characteristics with incremental LSTM," *ACM Trans. Data Sci.*, vol. 1, no. 4, pp. 25:1–25:18, Nov. 2020, doi: 10.1145/3385189.

Authorized licensed use limited to: University of North Carolina at Charlotte. Downloaded on June 02,2023 at 02:37:13 UTC from IEEE Xplore. Restrictions apply.

[36] 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] W. Meng, W. Li, L.-F. Kwok, and K.-K. R. Choo, "Towards enhancing click-draw based graphical passwords using multi-touch behaviours on smartphones," *Comput. Secur.*, vol. 65, pp. 213–229, 2017, doi: 10.1016/j.cose.2016.11.010.

[38] W. I. Khedr, "Improved keylogging and shoulder-surfing resistant visual two-factor authentication protocol," *J. Inf. Secur. Appl.*, vol. 39, pp. 41–57, 2018, doi: 10.1016/j.jisa.2018.02.003.

[39] T. joo Fong, A. Abdullah, N. Z. Jhanjhi, and M. Supramaniam, "The coin passcode: A shoulder-surfing proof graphical password authentication model for mobile devices," *Int. J. Adv. Comput. Sci. Appl.*, vol. 10, no. 1, pp. 302–308, 2019, doi: 10.14569/IJACSA.2019.0100140.

[40] X. Yu, Z. Wang, Y. Li, L. Li, W. T. Zhu, and L. Song, "EvoPass: Evolvable graphical password against shoulder-surfing attacks," *Comput. Secur.*, vol. 70, pp. 179–198, Sep. 2017, doi: 10.1016/j.cose.2017.05.006.

[41] J.-N. Luo, M.-H. Yang, and C.-L. Tsai, "An anti-shoulder-surfing authentication scheme of mobile device," *J. Internet Technol.*, vol. 19, no. 4, pp. 1263–1272, 2018, doi: 10.3966/160792642018081904028.

[42] V. Rajanna, S. Polsley, P. Taele, and T. Hammond, "A gaze gesture-based user authentication system to counter shoulder-surfing attacks," in *Proc. CHI Conf. Extended Abstr. Hum. Factors Comput. Syst.*, 2017, pp. 1978–1986, doi: 10.1145/3027063.3053070.

[43] A. Skalkos, I. Stylios, M. Karyda, and S. Kokolakis, "Users' privacy attitudes towards the use of behavioral biometrics continuous authentication (BBCA) technologies: A protection motivation theory approach," *J. Cybersecurity Privacy*, vol. 1, no. 4, pp. 743–766, Dec. 2021, doi: 10.3390/jcp1040036.

[44] A. Ramadan, H. Hemeda, and A. Sarhan, "Touch-input based continuous authentication using gesture-level and session-level features," in *Proc. IEEE 8th Annu. Inf. Technol., Electron. Mobile Commun. Conf.*, Oct. 2017, pp. 222–229, doi: 10.1109/IEMCON.2017.8117198.

[45] X. Zhang, Y. Yin, L. Xie, H. Zhang, Z. Ge, and S. Lu, "TouchID: User authentication on mobile devices via inertial-touch gesture analysis," *Proc. ACM Interactive, Mobile, Wearable Ubiquitous Technol.*, vol. 4, no. 4, pp. 162:1–162:29, Dec. 2020, doi: 10.1145/3432192.

[46] W. Li, W. Meng, and S. Furnell, "Exploring touch-based behavioral authentication on smartphone email applications in IoT-enabled smart cities," *Pattern Recognit. Lett.*, vol. 144, pp. 35–41, Apr. 2021, doi: 10.1016/j.patrec.2021.01.019.

[47] W. Li, Y. Wang, J. Li, and Y. Xiang, "Toward supervised shape-based behavioral authentication on smartphones," *J. Inf. Secur. Appl.*, vol. 55, 2020, Art. no. 102591, doi: 10.1016/j.jisa.2020.102591.

[48] R. Tolosana, R. Vera-Rodriguez, J. Fierrez, and J. Ortega-Garcia, "Presentation attacks in signature biometrics: Types and introduction to attack detection," in *Handbook of Biometric Anti-Spoofing: Presentation Attack Detection*, S. Marcel, M. S. Nixon, J. Fierrez, and N. Evans, Eds. Cham, Switzerland: Springer, 2019, pp. 439–453, doi: 10.1007/978-3-319-92627-8_19.

[49] J. Kim and P. Kang, "Freely typed keystroke dynamics-based user authentication for mobile devices based on heterogeneous features," *Pattern Recognit.*, vol. 108, 2020, Art. no. 107556, doi: 10.1016/j.patcog.2020.107556.

[50] L. Zhou, K. Wang, J. Lai, and D. Zhang, "Behaviors of unwarranted password identification via shoulder-surfing during mobile authentication," in *Proc. IEEE Int. Conf. Intell. Secur. Inform.*, 2021, pp. 1–3, doi: 10.1109/ISI53945.2021.9624730.

[51] M. Choi, S. Lee, M. Jo, and J. S. Shin, "Keystroke dynamics-based authentication using unique keypad," *Sensors*, vol. 21, no. 6, Jan. 2021, Art. no. 2242, doi: 10.3390/s21062242.

[52] V. Gunjkar, S. Belure, S. Prasad, S. Jaiswal, and R. Goudar, "Shoulder surfing resistant graphical password authentication system," *Int. J. Sci. Res. Rev.*, vol. 7, no. 3, pp. 19–23, 2019.

[53] N. Jitendra, N. S. Vinay, P. S. Ram, P. N. Sidhardha, and D. Deepthi, "Text-based shoulder surfing and key logger resistant graphical password," *J. Eng. Sci.*, vol. 11, no. 3, pp. 214–223, Mar. 2020.

[54] J. Lai, D. Zhang, S. Wang, I. D. Y. Kilic, and L. Zhou, "ThumbStroke: A virtual keyboard in support of sight-free and one-handed text entry on touchscreen mobile devices," *ACM Trans. Manage. Inf. Syst.*, vol. 10, no. 3, pp. 11:1–11:19, Sep. 2019, doi: 10.1145/3343858.

[55] K. Wang, L. Zhou, and D. Zhang, "User preferences and situational needs of mobile user authentication methods," in *Proc. IEEE Int. Conf. Intell. Secur. Inform.*, 2019, pp. 18–23, doi: 10.1109/ISI.2019.8823274.

[56] M. Keith, B. Shao, and P. Steinbart, "A behavioral analysis of passphrase design and effectiveness," *J. Assoc. Inf. Syst.*, vol. 10, no. 2, pp. 63–89, Feb. 2009, doi: 10.17705/1jais.00184.

[57] F. Schaub, R. Deyhle, and M. Weber, "Password entry usability and shoulder surfing susceptibility on different smartphone platforms," in *Proc. 11th Int. Conf. Mobile Ubiquitous Multimedia*, 2012, pp. 13:1–13:10, doi: 10.1145/2406367.2406384.

[58] F. P. Tamborello and K. K. Green, "Memory and motor processes of password entry error," presented at the *Proc. Hum. Factors Ergonom. Soc. 59th Annu. Meeting*, 2015, pp. 672–676, doi: 10.1177/1541931215591146.

[59] S. Maqsood, S. Chiasson, and A. Girouard, "Bend passwords: Using gestures to authenticate on flexible devices," *Pers. Ubiquitous Comput.*, vol. 20, no. 4, pp. 573–600, Aug. 2016, doi: 10.1007/s00779-016-0928-6.

[60] H. Khan, U. Hengartner, and D. Vogel, "Mimicry attacks on smartphone keystroke authentication," *ACM Trans. Privacy Secur.*, vol. 23, no. 1, pp. 2:1–2:34, Feb. 2020, doi: 10.1145/3372420.

[61] D. Brumby and V. Seyedi, "An empirical investigation into how users adapt to mobile phone auto-locks in a multitask setting," in *Proc. 14th Int. Conf. Human-Comput. Interaction Mobile Devices Serv.*, Sep. 2012, pp. 281–290, doi: 10.1145/2371574.2371616.

[62] D. T. Campbell, "Blind variation and selective retentions in creative thought as in other knowledge processes," *Psychol. Rev.*, vol. 67, no. 6, pp. 380–400, 1960, doi: 10.1037/h0040373.

[63] C. Holz, S. Buthpitiya, and M. Knaust, "Bodyprint: Biometric user identification on mobile devices using the capacitive touchscreen to scan body parts," in *Proc. 33rd Annu. ACM Conf. Hum. Factors Comput. Syst.*, 2015, pp. 3011–3014, doi: 10.1145/2702123.2702518.

[64] J. Ma, W. Yang, M. Luo, and N. Li, "A study of probabilistic password models," in *Proc. IEEE Symp. Secur. Privacy*, 2014, pp. 689–704, doi: 10.1109/SP.2014.50.

[65] C. Shen, T. Yu, H. Xu, G. Yang, and X. Guan, "User practice in password security: An empirical study of real-life passwords in the wild," *Comput. Secur.*, vol. 61, pp. 130–141, Aug. 2016, doi: 10.1016/j.cose.2016.05.007.

[66] G. A. Miller, "The magical number seven plus or minus two: Some limits on our capacity for processing information," *Psychol. Rev.*, vol. 63, no. 2, pp. 81–97, 1956, doi: 10.1037/h0043158.

[67] W. Burr et al., "Electronic authentication guideline," National Institute of Standards and Technology, NIST Special Publication (SP) 800-63-2 (Withdrawn), Aug. 2013, doi: 10.6028/NIST.SP.800-63-2.

[68] J. Yi, S. Park, J. Im, S. Jeon, and G. Kyung, "Effects of display curvature and hand length on smartphone usability," in *Proc. Proc. Hum. Factors Ergonom. Soc. Annu. Meeting*, vol. 61, no. 1, pp. 1054–1057, Sep. 2017, doi: 10.1177/1541931213601868.

[69] S. le Cessie, J. J. Goeman, and O. M. Dekkers, "Who is afraid of non-normal data? Choosing between parametric and non-parametric tests," *Eur. J. Endocrinol.*, vol. 182, no. 2, pp. E1–E3, Feb. 2020, doi: 10.1530/EJE-19-0922.

[70] C. Mircioiu and J. Atkinson, "A comparison of parametric and non-parametric methods applied to a Likert scale," *Pharmacy*, vol. 5, no. 2, Jun. 2017, Art. no. 26, doi: 10.3390/pharmacy5020026.

[71] M. Georgiev, S. Eberz, H. Turner, G. Lovisotto, and I. Martinovic, "Common evaluation pitfalls in touch-based authentication systems," in *Proc. ACM Asia Conf. Comput. Commun. Secur.*, New York, NY, USA, May 2022, pp. 1049–1063, doi: 10.1145/3488932.3517388.

[72] Y. Majima, K. Nishiyama, A. Nishihara, and R. Hata, "Conducting online behavioral research using crowdsourcing services in Japan," *Front. Psychol.*, vol. 8, pp. 1–13, 2017. Accessed: Mar. 10, 2022. [Online]. Available: https://www.frontiersin.org/article/10.3389/fpsyg.2017.00378

[73] M. Chmielewski and S. C. Kucker, "An MTurk crisis? Shifts in data quality and the impact on study results," *Social Psychol. Pers. Sci.*, vol. 11, no. 4, pp. 464–473, May 2020, doi: 10.1177/1948550619875149.

[74] S. Cohen, T. Kamarck, and R. Mermelstein, "Perceived stress scale," *Measuring Stress: Guide Health Social Scientists*, vol. 10, no. 2, pp. 1–2, 1994.

[75] F. Huang et al., "Psychometric properties of the perceived stress scale in a community sample of Chinese," *BMC Psychiatry*, vol. 20, no. 1, Mar. 2020, Art. no. 130, doi: 10.1186/s12888-020-02520-4.

Authorized licensed use limited to: University of North Carolina at Charlotte. Downloaded on June 02,2023 at 02:37:13 UTC from IEEE Xplore. Restrictions apply.