A New Shoulder Surfing and Mobile Key-Logging Resistant Graphical Password Scheme for Smart-Held Devices

Sundas Hanif[1], Fahad Sohail[2], Shehrbano[3], Aneeqa Tariq[4], Muhammad Imran Babar[5]
Department of Computer Science and Software Engineering
Army Public College of Management and Sciences (UET, Taxila), Pakistan

***Abstract*—In globalization of information, internet has played a vital role by providing an easy and fast access of information and systems to remote users. However, with ease for authentic users, it has made information resources accessible to unauthorized users too. To authorize legitimate user for the access of information and systems, authentication mechanisms are applied. Many users use their credentials or private information at public places to access their accounts that are protected by passwords. These passwords are usually text-based passwords and their security and effectiveness can be compromised. An attacker can steal text-based passwords using different techniques like shoulder surfing and various key logger software, that are freely available over internet. To improve the security, numerous sophisticated and secure authentication systems have been proposed that employ various biometric authentication systems, token-based authentication system etc. But these solutions providing such high-level security, require special modification in the design and hence, imply additional cost. Textual passwords that are easy to use but vulnerable to attacks like shoulder surfing, various image based, and textual graphical password schemes are proposed. However, none of the existing textual graphical passwords are resistant to shoulder surfing and more importantly to mobile key-logging. In this paper, an improved and robust textual graphical password scheme is proposed that uses sectors and colors and introducing randomization as the primary function for the character display and selection. This property makes the proposed scheme resistant to shoulder surfing and more importantly to mobile key-logging. It can be useful for authentication process of any smart held device application.**

***Keywords*—Authentication; graphical password; shoulder surfing; mobile key-logging; security**

I. INTRODUCTION

Access control mechanisms are widely used to protect user resources especially information asset. The legitimate user is required to authorize himself by passing the authentication technique employed on the system [1]. The conventional and widely used authentication method is login system protected with a textual password [2]. It is a variable length combination of alphabets, digits and special characters. Though it provides considerable security level, this approach has its shortcomings. To make a textual password robust against various password-based attacks, user has to select random characters, and some authentication systems require the user to change the password frequently. Users for their ease in remembering the passwords, tend to use either minimum length allowed for passwords or use common words, names or simply write them down in a notebook or a system file or use same password for multiple personal accounts, which makes the attacks like, dictionary attack, brute-force attack, hybrid attacks, social engineering attack, dumpster diving attack, shoulder surfing and key logging attacks possible [17, 19].

To overcome the limitations of Textual passwords, Graphical passwords are developed and used as an alternative method for authentication purpose [3]. As the name implies, this authentication method makes use of sequence of images or shapes instead of text, as the password.

Graphical password overcomes the drawbacks of textual password. Studies have shown that human brain can retain images more easily as compared to text [4, 5], and this property entitles graphical passwords as a more easily memorable method [6]. It is comparatively secure than textual password against dictionary, brute-force, social engineering and key-logging attacks [2] but vulnerable to shoulder-surfing attack [6, 20] where authentic user is observed while entering the password [7].

Graphical password systems can be classified as either recognition-based or recall-based approach; the latter of which is further divided into cued recall-based and pure recall-based approach [2, 7, 18]. In the recognition-based approach, the user selects a set of images from the available images in the registration phase which are recognized and reselected in the same sequence in the login phase. In the second approach, i.e., recall-based, the user recalls something that was selected in the registration phase. For this process there might be a clue given to the user–cued recall-based or no clue given at all during login phase–pure recall-based approach; the former of which is easy to use.

The existing graphical password schemes are divided into two types; image-based graphical passwords [2, 7, 8] and textual graphical passwords [1, 7]. In image-based, as name implies, images / symbols are used for the password. Whereas, the textual graphical password consists of a pie shape containing colors and sectors, which further contains different characters for selection as password. However, image-based graphical passwords are susceptible to shoulder-surfing attack as images can be retained easily in mind [4]. Many textual graphical password schemes are developed but they lack

efficiency in terms of login time and robustness against shoulder-surfing and mobile key-logging attacks.

In this paper, we have proposed a textual graphical password scheme for smart held devices that is resistant to shoulder surfing and mobile-key logging attacks. This scheme is a combination of recognition-based and pure-recall based approach and incorporates randomization on every text character with a click. The rest of the paper is organized as follows. Section II reviews the related work, Section III explains the working of existing system. Section IV presents our proposed system and scheme. Section V gives an analysis of the proposed scheme and lastly, Section VI concludes the paper.

II. Related Work

S. Wiedenbeck et al. [9] proposed '*The Convex Hull Click (CHC)'* scheme which is a game like graphical authentication method where user without clicking on the images can select the graphical password in an unsecure environment. However, this scheme entails a longer authentication process. The login time consumption is reduced in a scheme presented by H. Gao et al. [10] where the author has proposed a graphical password scheme based on ColorLogin. In this scheme a group of chosen-color icons are displayed for the user to set as his pass-icons. The drawback of this scheme is a comparatively smaller password space and most importantly impracticality for colour blind users.

Prof Raut et al. [7] have presented another graphical password scheme that is also based on colours. This proposed scheme combines colours with textual characters in a pie chart. The user selects a colour and a sector as his password, however, only the characters fixed in a sector can be selected limiting the choice of characters for the user. A similar scheme is presented by Sumit H. et al. [1] which does not make use of colour in the pie chart. This scheme has the same limitation of fixed set of characters in any sector for a user to select. An image-based graphical password scheme is proposed by Pooja K. S. et al [8], for ATM systems where user has to select a sequence of images out of 16 images. The scheme provides shuffling of these images on every login but is prone to Hidden-camera attack.

Another image-based scheme is proposed by E. Darbanian et al. [11] in which a set of images are selected which are interpreted as characters at the back end. Each displayed image holds a value of a character that is translated by a pre-defined table. This scheme, however, is complex as user has to memorize the characters as well as the associated images. Mrs. Aakansha S. et al. [2] have presented an image-based graphical password scheme which is a combination of recognition and recall-based approach. In this scheme user is presented with a set of images and questions. The user has to select a number of images and three questions that are answered by clicking a specific point on the given images. This scheme provides a large password space but is inefficient in terms of time required for the login process. Another graphical password scheme is proposed by A. Ahmad et al. in [12] that comprises of textual characters shown in a grid. This scheme is tested to be robust against shoulder surfing attack but has high complexity and is not user-friendly.

L. Y. Por et al [13] presents a password scheme that is based on 'digraph substitution rules' that hides the activity performed to drive the password images. This scheme is resistant against shoulder surfing attacks as user clicks only on one of the pass images instead of both pass-images. However, this scheme requires the user to know the digraph substitution rules hence not very user friendly. Another graphical password scheme is presented in [14] by GC. Yang in 2017, and its improvement in 2018. This scheme is based on pass-position scheme which is similar to pass-point approach however in pass-position a relative value of the clicked location is also accepted rather than an exact value. This feature makes this approach user friendly but on the other hand prone to accidental logins, hence less secure.

A. Mishra et al. [6] have presented an image-based graphical password scheme which is based on falsification method. This scheme is resistant to graphical password attack but has poor security against key-logging attacks as user has to enter the credentials using a keyboard. Another image-based graphical password scheme is presented by K. Irfan et al. [15] which use both image-based and test-based approaches. The user selects few images on registration which are reselected on login. If these images match with the images stored in database, the user is asked to change his password by selecting new images. This approach makes this scheme less practical for changing the password on every login.

III. Existing System

The existing system [1] is a type of textual graphical password scheme that consists of pie that is divided into 6 sectors each having 12 randomly distributed characters in them. The divided sectors contain 72 characters in all; having 26 alphabets (26 upper case and 26 lowercase), 10 special characters and 10 decimal digits (0-9). The login page of the existing scheme is shown in Fig. 1. The user verification is done in two stages.

A. Registration Phase

The registration phase consists of the following steps;

1) The user selects one of the six sectors from the given pie shape, that is used as the pass-sector for further logins.

2) The selected sector has 12 of the 72 randomly placed characters that constitutes the textual password of the user.

3) The sector number and the textual password is encrypted and stored in the password table in the system.

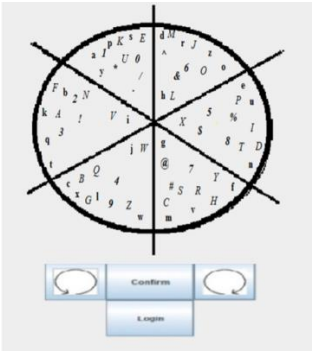


Fig. 1. Login Screen of the Existing Scheme [1].

B. Login Phase

The login phase consists of the following steps:

1) Upon login the system displays the pie shape having 6 sectors.

2) The system places the 72 characters equally divided among all the sectors.

3) The user has two buttons "Clockwise" and "Anti-clockwise" available.

4) The user by using these buttons in desired direction rotates the sectors in order to match the selected sector number and the characters of the set password.

5) When the desired sector coincides with the sector number, the user clicks the "Confirm" button and is allowed to successfully login into the system.

The existing system offers a fixed set of characters in each sector of pie for the registration or login phase. Thus, making the characters predictable, selected as password, as user has to select whole sector as the pass-sector. Secondly, a fixed sector containing the complete set of characters of password makes this approach vulnerable to mobile key-logging attack.

IV. Proposed Scheme

The proposed scheme is an improvement over the existing scheme and overcomes its shortcomings. It is a combination of recognition-based and recall-based graphical password scheme. Similar to the existing scheme, the proposed scheme is also based on text and sectors contained in a pie. The architecture of the proposed scheme is shown in the Fig. 2. It has been developed for Android based smart-held devices using Android studio, languages used are Java and Android.

The user selects the password from a range of 72 characters randomly distributed over 8 sectors during registration and login phase. The character set contains 26 upper-case and 26 lower-case alphabets, 0-9 digits and 10 special characters (@, !, #, $, %, *, &, ?, <, >). For securing the user credentials, the selected password along with other user-entered information, are hashed using hashing algorithm SHA-1 [16] and stored in the database, during both registration and login phase. Moreover, characters are always shuffled at the run time which will ensure security against shoulder surfing and mobile-key logging.

The proposed scheme comprises of a user registration and login phase that are described as follows:

A. Registration Phase

In Registration phase, user has to fill the registration form which includes First name, Last name and Email. Then user has to set the graphical password by first selecting the desired colour from the 8 available colours of the sectors. After that, the user will select different characters from the pie chart. When this data is submitted, the password is hashed using the hashing technique i-e SHA-1 (Secure Hash Algorithm). Fig. 3 shows the user registration process. SHA-1 is the cryptographic hash function which takes an input and produces a 160-bit (20 Bytes). Then this hashed password and all user details are stored into the database. The minimum requirement for the password is 8 characters that must contain 1 numeric, 1 uppercase letter, 1 lowercase letter and 1 special character.

The registration phase consists of the following steps:

1) On the registration page (Fig. 4(a)), user is asked to enter first name, last name and a valid email address. The user email will be used as username.

2) After filling these fields, the user selects the *'Generate password'* button and a new screen appears containing the pie chart with 8 sectors each having a different colour that are selected separately (Fig. 4(b)).

3) There are four buttons below the pie chart for the character selection:

a) First button is of upper-case letters (A... Z), by touching this button, upper case letters will randomly display in the sectors of the pie chart.

b) Second button is of numbers (0… 9), by touching this button, numbers will randomly display in the sectors of the pie chart.

c) Third button is of special characters (#*$%), by touching this button, special characters will randomly display in the sectors of the pie chart.

d) Forth button is of lower-case letters (a… z), by touching this button, lower case letters will randomly display in the sectors of the pie chart.

4) User selects the desired color and then selects characters for his password meeting the minimum requirement set for the password. The colour and characters are selected by simply touching the screen on the desired point.

5) Upon submitting the selected graphical password, the user Email and password are hashed using SHA-1 and stored in database.

6) After the complete registration process, login page appears.

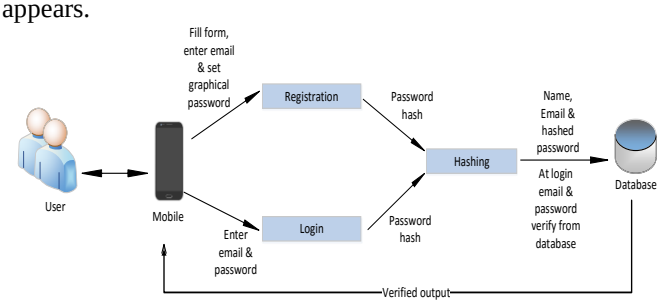


Fig. 2. Proposed Scheme Architecture.

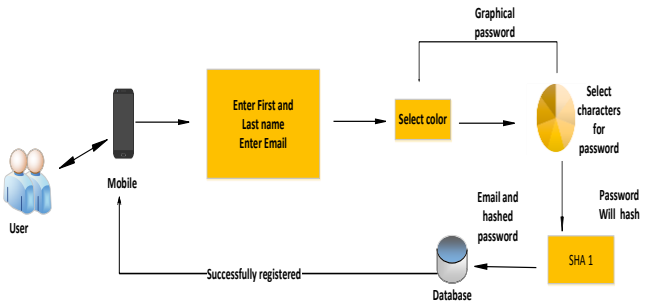
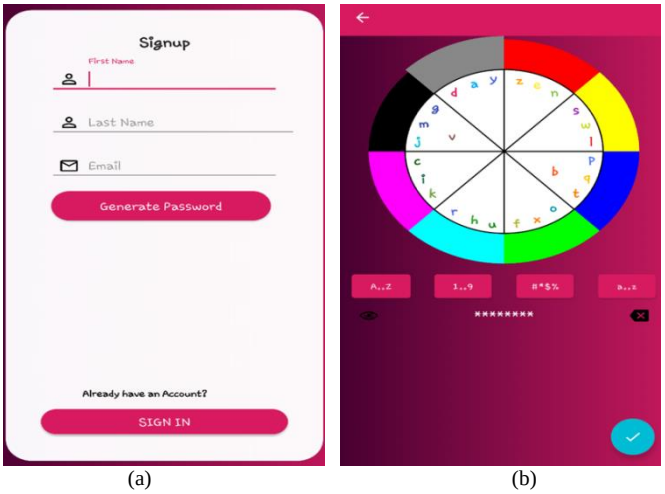


Fig. 3. User Registration.



(a) (b)

Fig. 4. (a). Example of a Signup Page. (b). Example of Password Generate Page.

B. Login Phase

Fig. 5 shows the user login process. When user submits the email and the graphical password, the entered password is hashed through the same hashing algorithm and compared with the already stored hashed credentials of the user in database. When both the hash values match, the user is verified and allowed to login to his account. If user forgets his password, it is sent to the user's linked email address.

The login phase consists of the following steps:

1) Step 1 is based on recognition-based approach in which user has to enter the username i.e., user email address. The application generates a message of incorrect email if user enters wrong username (email).

2) After entering the correct username, the user has to enter the graphical password by selecting the button shown on the login screen (Fig. 6(a)). It is based on pure recalled-based approach. The user enters the password that was set during registration repeating the same procedure as of password generation (Fig. 6(b)).

3) Let L = length of the set password (exclusive of selected colour) and I be the i^{th} character of the password. Whichever of the four buttons of characters are selected, the characters in the sectors will randomly be permuted if I < L.

4) Once the password is entered, the user submits the password which is hashed and verified from the database. Forget password button takes user on the recover password page in case user forget his password.

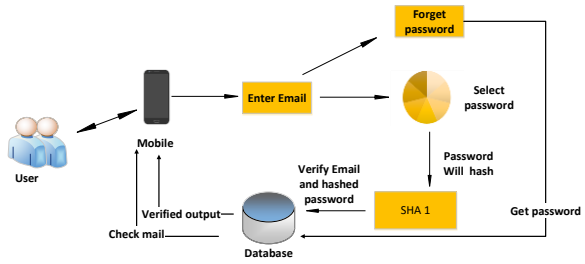
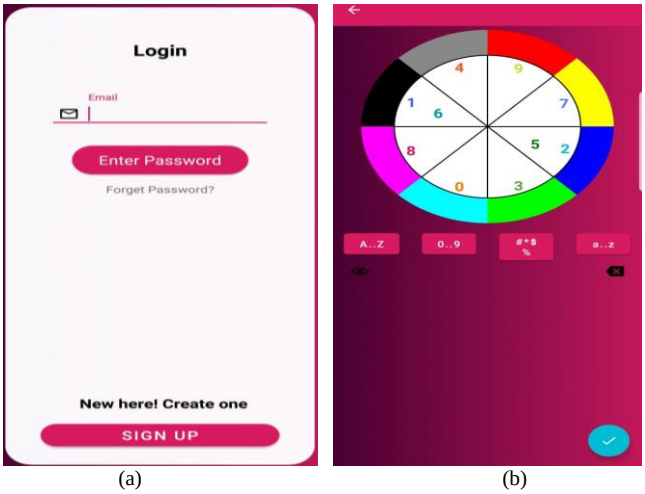


Fig. 5. User Login Process.



(a) (b)

Fig. 6. (a). Example of a Login Page. (b). Example of Enter Password Page.

V. Analysis of Proposed Scheme

In this section, the security analysis of the proposed scheme is made against shoulder surfing and mobile-key logging attacks and a comparison is done with the existing scheme.

A. Large Password Space

The proposed scheme is resilient against Brute force and Password guessing attacks. The total number of possible passwords that can be made with this scheme, make these attacks difficult. With the 72 characters, 8 sectors and considering the password length as '*L*', our scheme has a very large password space as compared with the existing scheme [1] which can be calculated as shown in (1):

$$Total\ no.\ of\ possible\ passwords = \sum_{L=8}^{15} 8 * 72^{L} = 5.88 * 10^{28} \quad (1)$$

B. Resistant against Accidental Login

The probability of correctly entering any character of the password is 1/72. The success probability of accidental login (P_{al}), with a password of length L, is calculated in (2)

$$P_{al(L)} = \left(\frac{1}{72}\right)^{L} \quad (2)$$

The comparison of password space and P_{al} of proposed scheme with existing scheme [1] is shown in Table I.

TABLE. I. Comparison of Proposed Scheme with Existing Scheme

Feature	Existing Scheme [1]	Proposed Scheme
Password Space	$4.346 * 10^{28}$	$5.88 * 10^{28}$
P_{al}(L)	$\left(\frac{1}{12}\right)^{L}$	$\left(\frac{1}{72}\right)^{L}$

C. Robust against Shoulder Surfing and Mobile-Key logging Attack

The proposed scheme is robust against shoulder surfing and mobile-key logging attacks. The existing schemes have a fixed set of characters displayed in each sector after the first

display which shows them randomly but after that, they are fixed for the whole session of registration or login whereas in our proposed scheme, the randomization works on every single click till the length of the password to be selected during registration or login.

This randomization works independently on each character and places them in a different sector upon every click thus decreasing the probability of a sector being selected in the same sector with the same characters. This increases the security level of our scheme as character position is totally unpredictable.

Let probability of a character to be placed in any sector to be denoted by P(c) which can be calculated as shown in (3) and (4).

$$P(c) = \frac{1}{Total\ No.of\ characters} \quad (3)$$

$$P(c) = \frac{1}{72} = 0.014 \quad (4)$$

This factor plays an important role against Shoulder Surfing attack and mobile-key logging attack as the probability for the attacker to correctly guess any character on a given location is substantially low even if he tried to memorize the password characters and tries to login into the system.

Another important factor that makes our scheme strong against shoulder surfing attack is the ***rotation feature*** of the pie chart. The user can rotate colour rim and the sectors independently in clockwise or anti-clockwise direction. The selected colour and the sectors don't have to be aligned to enter the password.

This feature enhances the security of our scheme against shoulder surfing attack. An attacker cannot guess the associated colour with the characters as they need not be aligned with any particular sector for the password to work.

The proposed scheme provides strong authentication process in case of password recovery scenario. If a user forgets his password, the system sends the password to the linked email account of the user. This is very beneficial for the authentic user but any imposter trying to login into the system cannot access the system in any way.

Thus, our proposed graphical password scheme is highly secure and easy to use.

VI. Conclusion

User authentication plays a vital role in securing user accounts and confidential information. In this paper, a new graphical password user authentication scheme for smart-held devices is presented which is a combination of recognition and pure recall-based graphical password approach. With a combination of colour and alphanumeric characters, this scheme is viable for users comfortable with textual passwords.

The proposed scheme provides high security against Brute-force attack as it offers a very large password space as compared to the existing scheme. The randomization feature, incorporated with every click, adds robustness against shoulder surfing and mobile-key logging attacks. In case an authentic user forgets his password, the password is email to the user hence adding another layer of security and making an attacker unable to get hold of the password. The proposed authentication graphical password scheme is designed for smart held application and can be easily used as a secure gateway for any application.

The work can further be extended by increasing the number of characters and sectors in the pie, and by also increasing the number of colours of the sectors. To further enhance the robustness of this scheme, two factor authentications can also be incorporated.

References

[1] S. H. Wagh, A. G. Ambekar, "Shoulder Surfing Resistant Text-based Graphical Password Scheme", ICCT 2015, International Journal of Computer Applications (0975 – 8887).

[2] Mrs. A. S. Gokhalea, Prof. V. S. Waghmare, "The Shoulder Surfing Resistant Graphical Password Authentication Technique" 7th International Conference on Communication, Computing and Virtualization 2016, Procedia Computer Science 79 (2016) 490 – 498.

[3] X. Suo, Y. Zhu, G. Scott. Owen, "Graphical Passwords: A Survey", Department of Computer Science Georgia State University. 21st Annual Computer Security Applications Conference (ACSAC'05), IEEE

[4] Kirkpatrick. "An experimental study of memory", Psychological Review, 1:602-609, 1894.

[5] R. Shepard. "Recognition memory for words, sentences and pictures", Journal of Verbal Learning and Verbal Behavior, 6:156-163, 1967.

[6] A. Mishra, R. Jadhav, S. Patil, "A Shoulder-Surfing Resistant Graphical Password System", International Research Journal of Engineering and Technology (IRJET), Volume 5, March 2018.

[7] Prof Raut S.Y., J. B. Baviskar, K. Rahul S, S. Aditya N, S. Yogesh S, "Shoulder Surfing and Keylogger Resistant using Graphical Password Scheme", International Journal of Advanced Research in Computer Science, Volume 5, No. 8, Nov-Dec 2014.

[8] Pooja K S, P. V. Dhooli, Prathvi, Prof. Ashwini N, "Shoulder Surfing Resistance Using Graphical Password Authentication in Atm Systems", International Journal of Information Technology & Management Information System (IJITMIS), Volume 6, Issue 1, January - June (2015), pp.01-10.

[9] S. Wiedenbeck and J. Waters, L. Sobrado, J. C. Birget, "Design and Evaluation of a Shoulder-Surfing Resistant Graphical Password Scheme", AVI '06, May 23-26, 2006.

[10] H. Gao, X. Liu, R. Dai, S. Wang and H. Liu, "Design and Analysis of a Graphical Password Scheme", Fourth International Conference on Innovative Computing, Information and Control, 2009.

[11] E. Darbanian, Gh. D. Fard, "A Graphical Password Against Spyware and Shoulder-surfing Attacks", International Symposium on Computer Science and Software Engineering, IEEE, 18-19 Aug. 2015.

[12] A. Ahmad, M. Asif, M. Hanif, R. Talib, "Secure Graphical Password Techniques against Shoulder Surfing and Camera based Attacks", International Journal of Computer Network and Information Security · November 2016.

[13] L. Y. Por, C. S. Ku, A. Islam, T. F. Ang, "Graphical password: prevent shoulder-surfing attack using digraph substitution rules", Higher Education Press and Springer-Verlag Berlin Heidelberg, 2017.

[14] GC Yang, "PassPositions: A secure and user-friendly graphical password scheme", 4th International Conference on Computer Applications and Information Processing Technology (CAIPT), 8-10 Aug. 2017, IEEE.

[15] K. Irfan, A. Anas, S. Malik, S. Amir "Text based graphical password system to obscure shoulder surfing", 15th International Conference on Applied Sciences and Technology (IBCAST), 2018, IEEE.

[16] D. Eastlake, P. Jones, "US Secure Hash Algorithm 1 (SHA1)", RFC Editor, ACM, 2001.

[17] M. Raza, M. Iqbal, M. Sharif, W. Haider, "A Survey of Password Attacks and Comparative Analysis on Methods for Secure Authentication", World Applied Sciences Journal 19 (4): 439-444, 2012

[18] GC Yang, H. Oh, "Implementation of a Graphical Password Authentication System 'PassPositions', Journal of Image and Graphics, Vol. 6, No. 2, December 2018.

[19] A. H. Lashkari, A. A. Manaf, M. Masrom, "A Secure Recognition Based Graphical Password by Watermarking" 11th International Conference on Computer and Information Technology, IEEE, 2011.

[20] Y. Higashiyama, N. Yanai, S. Okamura, T. Fujiwara, "Revisiting Authentication with Shoulder-Surfing Resistance for Smartphones", Third International Symposium on Computing and Networking (CANDAR), IEEE, 2015.