International Journal of Advanced Development in Science and Technology
IJADST Volume : 3 Issue : 03 April 2021 www.ijadst.com e-ISSN: 2582-1059

EFFICIENT HANDWRITTEN PASSWORDS TO OVERCOME SPYWARE ATTACKS

[1] B.Suruthi, [2] G.Yuvasri, [3] R.Reena, [4] R.K.Kapilavani,
[1,2] UG student [3]Associate Professor [4]Assistant Professor,
[1,2,3,4] Department of Computer Science and Engineering,
[1,2,3,4]- Prince Shri Venkateshwara Padmavathy Engineering College, Ponmar.
[2].yuvasriyuva17@gmail.com

ABSTRACT

This work enhances traditional authentication systems supported personal identification numbers (PIN) and One-Time Passwords (OTP) through the incorporation of biometric information as a second level of user authentication. In our proposed approach, users draw each digit of the password on the touch screen of the device rather than typing them as was common. a complete analysis of our proposed biometric system is run regarding the discriminative power of every handwritten digit so the robustness when increasing the length of the password so the number of enrolment samples. The new e-Bio Digit database, which comprises on-line handwritten digits from 0 to 9, has been acquired using the finger as input on a mobile device. This database is used within the experiments reported during this work and it's available along with benchmark leads to GitHub 1. Finally we discuss specific details for the deployment of our proposed approach on current PIN and OTP systems, achieving results with Equal Error Rates(EERs) ca.4.0% when the attacker knows the password. These results encourage the deployment of our proposed approach as compared to traditional PIN and OTP systems where the attack would have 100% success rate under the identical imposter scenario.

Key Words: Passwords, PIN, Handwritten touch biometrics, mobile, android application.

1.INTORDUCTION

Mobile devices became an imperative tool for many people nowadays .The rapid and continuous deployment of mobile devices round the world has been motivated not only by the high technological evolution and new features incorporated but also to the new internet infrastructures like 5G that permits the communication and use of social media in real time, among many other factors. during this way, both public and personal sectors are conscious of the importance of mobile devices for the society and are attempting to deploy their services through user friendly mobile

applications ensuring data protection and high security.

Traditionally, the 2 most prevalent user authentication approaches are Personal Identification Numbers (PIN) and One-Time Passwords (OTP). While PIN-based authentication systems require users to memorize their personal passwords, OTP-based systems avoid users to memorize them because the system is responsible of choosing and providing to the user a distinct password every time is required, e.g., sending messages to non-public mobile devices or special tokens. Despite the high popularity and deployment of PIN- and OTP-based authentication systems in real scenarios, many studies have highlighted the weaknesses of those approaches .First, it's common to use passwords supported sequential digits, personal information like birth dates, or just words like “password” or “qwerty” that are very easy to guess.

Second, passwords that are typed on mobile devices like tablets or smartphones are liable to “smudge attacks”, i.e., the deposition of finger grease traces on the touchscreen may be used for the impostors to guess the password .Finally, password-based authentication is additionally susceptible to “shoulder surfing”. this sort of attack is produced when the impostor can observe directly or use external recording devices to gather the user information. This attack has attracted the eye of the many researchers in recent years because of the increased deployment of handheld recording devices and public surveillance infrastructures .

Biometric recognition schemes are ready to address these challenges by combining both a high level of security and convenience. This study evaluates the benefits and potential of incorporating biometrics to password-based mobile authentication systems, asking the users to draw each digit of the password on the touchscreen rather than typing them as was common. This way, the standard authentication systems are enhanced by incorporating dynamic handwritten biometric information.

One example of use that motivates our proposed approach is on internet payments with credit cards. Banks usually send a numerical password (typically between 6 and eight digits) to the user’s mobile device. This numerical password must be inserted by the user within the security platform so as to complete the payment.

Our proposed approach enhances such scenario by including a second authentication factor supported the userbiometric information while drawing the digits. Fig. 1 shows a general architecture of our proposed password-based mobile authentication approach. The three following main modules are analyzed during this study: i) enrolment set, ii) password

generation, and iii) touch biometric system. betting on the ultimate application (i.e., PIN or OTP), the handwritten digits will be first recognized using as an example an Optical Character Recognition (OCR) system so as to verify the authenticity of the password.

After this first authentication stage, the biometric information of the handwritten digits is compared during a second authentication stage to the enrolment data of the claimed user, comparing each digit one by one. during this study we specialize in the second authentication stage supported the behavioral information of the user while performing the handwritten digits because the recognition of numerical digits has already shown to be an almost solved problem with errors near 0% [8], [9].

Therefore, during this study we make the belief that impostors pass the primary stage of the safety system (i.e., they know the password of the user to attack) and thus, the attack would have 100% success rate if our proposed approach wasn't present

2. EXISTING SYSTEM

In existing system handwritten signature is one amongst the foremost socially accepted biometrics because it has been employed in financial and legal agreements for several years and it also finds applications in mobile scenarios. These approaches are supported the mix of two authentication stages. the safety system checks that the claimed user introduces its unique password correctly, and its behavioral biometric information is employed for an enhanced final verification. The software for capturing handwritten numerical digits was developed so as to reduce the variability of the user during the acquisition process. the choice of a password that's robust enough for a selected application could be a key factor. the amount of digits that comprise the password depends on the scenario and level of security considered within the final application. This effect has proven to be vital for several behavioral biometric traits like the case of the handwritten signature.

LIMITATIONS OF EXISTING SYSTEM

A. The amount of knowledge requested to the user during the enrolment.
B. The security level provided by the biometric system. From the purpose of view of the safety system, it seems clear that the perfect case would be to possess the maximum amount information of the user as possible.

3. PROPOSED SYSTEM

Our proposed system target providing user-friendly mobile applications ensuring data protection and high security. User should draw each digit of the password on the touch screen

rather than typing them as was common. This way, the normal authentication systems are enhanced by incorporating dynamic handwritten biometric information. Our system involves two stages of authentication the drawn pin should be the same as pin entered during registration process.

Our second stage of authentication involves multiple options supported user preference where user can set multiple set of combinations. User can set second stage password as stroke, time, screen brightness or sensor based authentication system. The incorporation of biometric information on traditional password-based systems can improve the safety through a second level of user authentication.

ADVANTAGES OF PROPOSED SYSTEM

A. These approaches enable active or continuous authentication schemes, within which the user is transparently authenticated.
B. Handwritten signature is one amongst the foremost socially accepted biometrics.
C. The incorporation of biometric information on traditional password-based systems can improve the safety through a second level of user authentication.

4. PHASES OF SYSTEM

4.1. USER AUTHENTICATION AND ECOMMERCE VIEW PRODUCT

User has an initial level Registration Process. The users provide their own personal information for this process. The server successively stores the data in its database and user can view a listing of products in their page multiple list of products and their details.

4.2. CART AND PAYMENT USING BIOMETRIC HAND WRITTEN PASSWORD

User can select an inventory of product they want to get the chosen product are going to be listed in an exceedingly cart page and user can initiate general purchase information should be filled. Completing general detail user must draw their four digit pin one by one on screen. The drawn password then converted into a picture through optical character recognition numbers from each image fetched and verified with user password.

4.3. BIOMETRIC PASSWORD USING STROKES

User needs to register their four digit password with multiple strokes during their registration process once the method completed during confirm password .User must confirm their password with same password with stroke needs to be verified.

Strokes for every drawn digits should match with strokes given at time of registration.

4.4. BIOMETRIC PASSWORD USING SCREEN BRIGHTNESS AND TIME

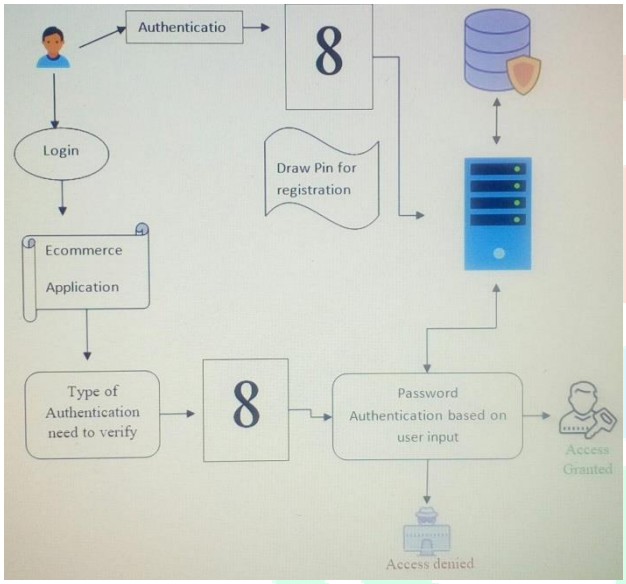
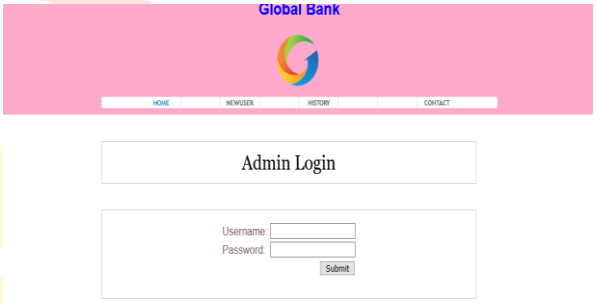
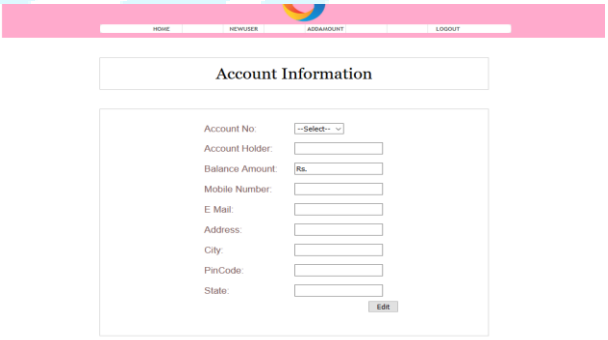
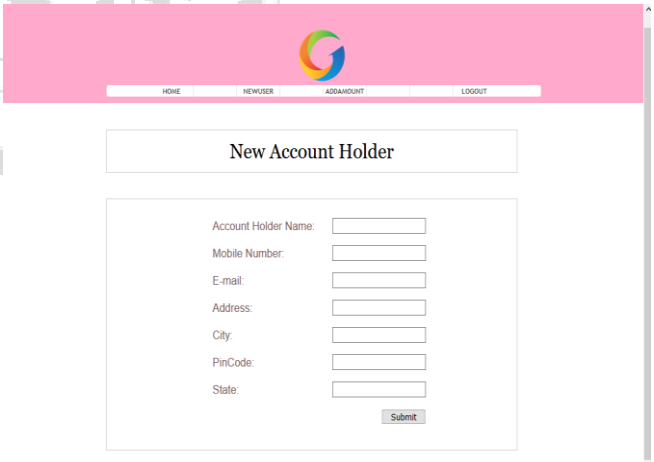


Fig 1: Flow chart

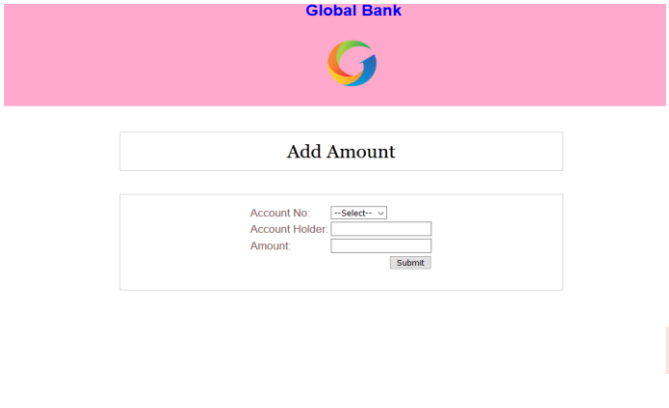
Spyware attack are going to be avoided by proposing the thought that uses the screen brightness as an authentication tool. The android secure environment generates the 6 digit binary value. supported the figure the brightness of the screen gets changed to high or low. If the screen brightness is high the user should input the proper PIN digit. Else the user should give the incorrect and random number. The system will remove the digits which inserted while the screen brightness is low and apply the HMac algorithm for the PIN given by user and generate the Signature for the user PIN which could be a digestible Value so as to avoid MAN-IN-MIDDLE attack. The server gets the signature of user generated PIN and generates the signature value for the first PIN and compare two signatures. If the 2 Signatures are equal the user can access the Profile of the user. If not user can't access the profit.

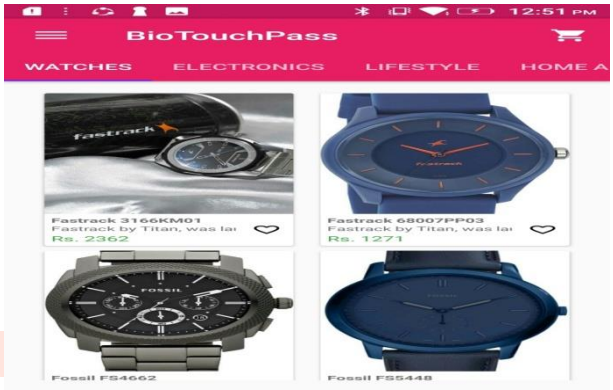


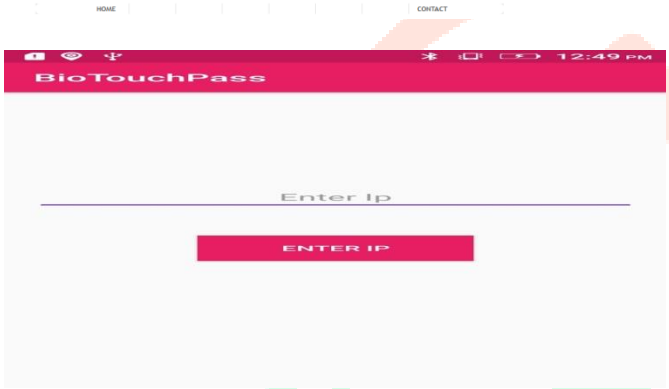


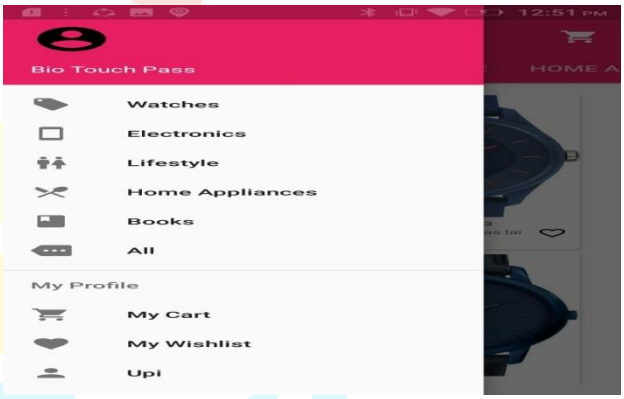


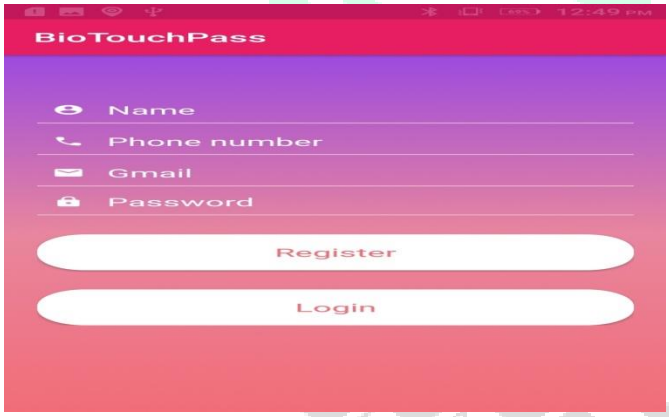
International Journal of Advanced Development in Science and Technology
Volume : 3 Issue : 03 April 2021 www.ijadst.com e-ISSN: 2582-1059

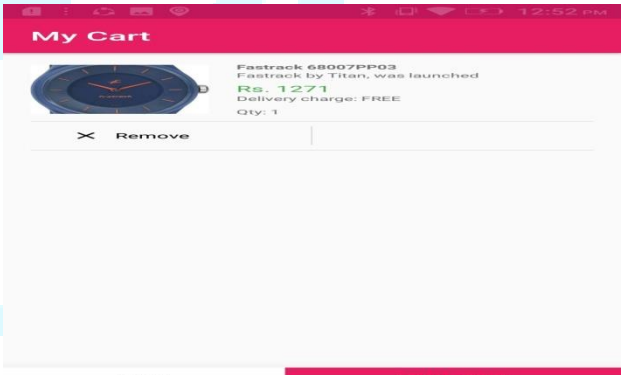


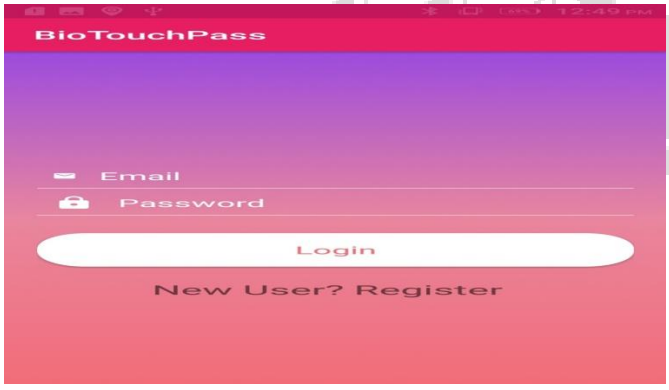












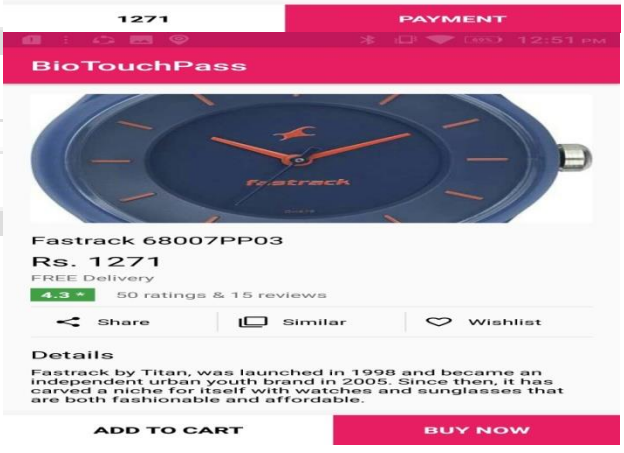


Fig 2: OUTPUT

5. CONCLUSION AND FUTURE ENHANCEMENT

5.1 CONCLUSION

This work evaluates the advantages and potential of incorporating handwritten touch biometrics to password-based mobile authentication systems. The new e-BioDigit database that comprises handwritten numerical digits from 0 to 9 is used in the experiments reported in this work and it is available together with benchmark results in GitHub.we propose a smart way to authenticate the social networking accounts belonging to them by using the screen brightness of android mobiles in order to avoid the spyware attack, shoulder surfing attack, and man in the middle attack.

5.2 FUTURE ENHANCE MENT

Future work will be oriented to incorporate the drawing of passwords by collecting the biometric information of the user uniquely i.e to collect the variations of ridges and valleys in fingerprints of the user.Therefore the passwords can be drawn on the screen display itself by using the in-display fingerprint sensor which are used in AMOLED displays. Also to enlarge the current e-BioDigit database in order to consider lower- and uppercase letters and also to train more complex deep learning architectures.

7. REFERENCES

[1] J. Galbally, I. Coisel, and I. Sanchez, “A New Multimodal Approach for Password Strength Estimation Part I: Theory and Algorithms,” IEEE Transactions on Information Forensics and Security, vol. 12, pp. 2829– 2844, 2017.

[2] A. Aviv, K. Gibson, E. Mossop, M. Blaze, and J. Smith, “Smudge Attacks on Smartphone Touch Screens,” in Proc. of the 4th USENIX

Conference on Offensive Technologies, 2010, pp. 1–7.

[3] D. Shukla, R. Kumar, A. Serwadda, and V. Phoha, "Beware, Your Hands Reveal Your Secrets!" in Proc. of the 2014 ACM SIGSAC Conference on Computer and Communications Security, 2014.

[4] Q. Yue, Z. Ling, X. Fu, B. Liu, W. Yu, and W. Zhao, "My Google Glass Sees Your Passwords!" in Black Hat USA, 2014.

[5] W. Meng, D. Wong, S. Furnell, and J. Zhou, "Surveying the Development of Biometric User Authentication on Mobile Phones," IEEE Communications Surveys Tutorials, vol. 17, no. 3, pp. 1268–1293, 2015.

[6] L. Wan, M. Zeiler, S. Zhang, Y. LeCun, and R. Fergus, "Regularization of Neural Networks using DropConnect," in Proc. of the 30th International Conference on Machine Learning, 2013, pp. 1058–1066.

[7] M. Liang and X. Hu, "Recurrent Convolutional Neural Network for Object Recognition," in Proc. of the IEEE Conference on Computer Vision and Pattern Recognition, 2015, pp. 3367–3375.

[8] J. Angulo and E. Wastlund, "Exploring Touch-Screen Biometrics for User Identification on Smart Phones," J. Camenisch, B. Crispo, S. Fischer-Hbner, R. Leenes, G. Russello (Eds.), Privacy and Identity Management for Life, Springer, pp. 130–143, 2011.

[9] P. Lacharme and C. Rosenberger, "Synchronous One Time Biometrics With Pattern Based Authentication," in Proc. 11th Int. Conf. on Availability, Reliability and Security, ARES, 2016.

[10] E. von Zezschwitz, M. Eiband, D. Buschek, S. Oberhuber, A. D. Luca, F. Alt, and H. Hussmann, "On Quantifying the Effective Password Space of Grid-based Unlock Gestures," in Proc. of the International Conference on Mobile and Ubiquitous Multimedia, 2016, pp. 201–212.

[11] D. Buschek, A. D. Luca, and F. Alt, "There is more to Typing than Speed: Expressive Mobile Touch Keyboards via Dynamic Font Personalisation," in Proc. of the International Conference on Human- Computer Interaction with Mobile Devices and Services, 2015, pp. 125– 130.

[12] ——, "Improving Accuracy, Applicability and Usability of Keystroke Biometrics on Mobile Touchscreen Devices," in Proc. of the CHI Conference on Human Factors in Computing Systems, 2015, pp. 1393–

[13] N. Sae-Bae, N. Memon, K. Isbister, and K. Ahmed, "Multitouch Gesture-Based Authentication," IEEE Transactions on Information Forensics and Security, vol. 9, no. 4, pp. 568–582, 2014.

[14] R. Tolosana, R. Vera-Rodriguez, J. Fierrez, A. Morales, and J. Ortega- Garcia, "Benchmarking Desktop and Mobile

Handwriting across COTS Devices: the e-BioSign Biometric Database," PLOS ONE, 2017.

[16] T. Kutzner, F. Ye, I. Bonninger, C. Travieso, M. Dutta, and A. Singh, "User Verification Using Safe Handwritten Passwords on Smartphones," in Proc. 8th International Conference on Contemporary Computing, IC3, 2015.

[17] T. Nguyen, N. Sae-Bae, and N. Memon, "DRAW-A-PIN: Authentication using finger-drawn PIN on touch devices," Computers and Security, vol. 66, pp. 115–128, 2017.

[18] R. Tolosana, R. Vera-Rodriguez, J. Fierrez, and J. Ortega-Garcia, "Incorporating Touch Biometrics to Mobile One-Time Passwords: Exploration of Digits," in Proc. IEEE Conference on Computer Vision and Pattern Recognition Workshops, 2018.