International Journal of Research in Engineering, Science and Management
Volume-2, Issue-3, March-2019
www.ijresm.com | ISSN (Online): 2581-5792

Graphical based Authentication System using Keystroke Parameters and Cued Click- Points: A Survey

Ruta Gore[1], Chaitrali Bokil[2], Chinmay Deshpande[3], Mrunalinee Patole[4]
[1,2,3]*Student, Department of Computer Engineering, RMDSSOE, Pune, India*
[4]*Professor, Department of Computer Engineering, RMDSSOE, Pune, India*

***Abstract*: User authentication is one of the important issues for illegal access, especially to computer systems. Alphanumeric passwords can easily be hijacked later by some malicious user. A possible remedy against such a scenario is to use Keystroke Dynamics for providing security in banking application. This paper gives the survey of different techniques used by the researcher for providing security.**

***Keywords*: authentication system, keystroke parameters**

1. Introduction

Now-a-days touch screen handheld mobile devices have become extensively used by people by using which people are able to access a variety of data and information everywhere and anytime. Most user authentication methods for these mobile devices use PIN-based (Personal Identification Number) authentication. PINs are short or simple which are easy to remember. Normally PIN and traditional alphanumeric pass-words are strings of letters and digits. Such passwords are easy to guess and vulnerable to attack i.e. attacker can easily break the password. For that reason, graphical passwords are most preferable authentication system where users click on images to authenticate themselves. The functionality of this biometric is to measure the dwell time and flight time for changing keyboard actions. Keystroke dynamics is biometric that aims to identify humans based on the analysis of typing of rhythms on a keyboard. Graphical passwords have been designed for more secure and that to make

passwords more memorable and easy to use by the people. Using this technique user click on the images rather than typing alphanumeric pass- words. User is shown with sequence of images with 4x4 blocks; user has to select N blocks from each image. If user enters an incorrect click-point during login, the next image displayed will also be incorrect. Unauthenticated users who see an unrecognized image know that they made an error with their previous click point. Conversely, this implicit feedback is not helpful to an attacker who does not know the expected sequence of images. Third, we measure KDA (Keystroke Dynamic-based Authentication) for a password. This project proposes a new graphical-based password and Keystroke Dynamic Authentication system for the secure authentication. The graphical password enlarges the password space size and promotes the KDA utility in touch screen handheld mobile devices.

2. Literature review

Cheng-Jung Tsai et al. [2] gives the system based on click data on the time instances during pressing and releasing the mouse button. The system proposes usefulness of a rhythm click- dynamics authentication system based on mouse clicks and a statistical-based classifier. Five features based on these time periods are calculated using clicking in rhythm that allow other people to easily observe and listen to a user's clicking rhythm and subsequently imitate the speed and tempo to impersonate the user. The experimental results showed that our authentication system can achieve a good accuracy. The paper showed that the rhythm clicked by a mouse can function as the second identifiable factor in general password authentication systems or as the standby identifiable factor in KDA systems.

Ahmed A et al.[3] provides a method with free text analysis of keystrokes that combines monograph and digraph analysis] and uses a neural network to predict missing digraphs based on the relation between the monitored keystrokes .These free text analysis systems, are based on limited or fixed text enrolment methods, the enrolment process of the proposed detection system is performed with a completely free text sample.

Ushir Kishori et al. [4] gives graphical passwords scheme in [4] to manage the difficulty level of guessing it along with the biometric authentication scheme by using a username with a graphical password using persuasive cued click points along with biometric authentication using fingernail plate. The scope of the scheme is limited to three fingers and it is used for high-security purpose where it is very important to keep tight security.

Soumik Mondal and Patrick Bours [5] propose three schemes for identifying a person when typing on a keyboard. Author uses different machine learning algorithms along with the pairwise user coupling technique and show the performance of each separate technique. The proposed multi-class pattern identification problem will be divided into several two-class

problems. These schemes could be useful for person identification when the biometric features are weak, or there are few samples present for learning. Extensive analysis was done with an online exam based keystroke datasets; this dataset was collected from 64 individuals with three different typing modes that gives 7% better identification accuracy when compared to the state of the art result on the same dataset.

Yan Sun et al .[6] focuses on normally ignored features like Shift and Comma and investigate their effectiveness in user verification/ authentication. Such features contain some valuable information that is characteristic of the individuals. Here support Vector Machine (SVM) is adopted for learning and classifying users. The identification of the potential and the extraction of the often ignored features provides good user discrimination in keystroke dynamics.

Joseph Roth et al .[7] gives a novel biometric modality named Typing Behavior (TB) for continuous user authentication. Author gives a novel approach, named bag of multi- dimensional phrases, to match the cross-feature and cross-temporal pattern between a gallery sequence and a probe sequence.

3. Proposed system

System aims to develop a Graphical-Based Password Keystroke Dynamic Authentication System. This system improves protection and confidentiality. User authentication can be performed using typing rhythm of the user. Clicking in rhythm will create noise

through the mouse, which could allow other people to easily observe and listen to a user's clicking rhythm and subsequently imitate the speed and tempo to impersonate the user.

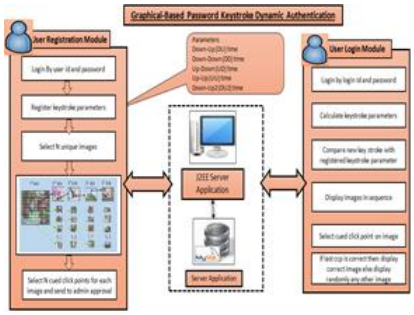

Fig. 1. Block diagram

At the time of registration user will keystroke dynamic authentication parameters in Database and select images (max 5) which he/she want as a credentials at the time of user login and user will also enter number of splits. Number of splits will indicate the size of matrix in which the image is going to divide. Then user will give check- point for each image i.e. for example for a particular image split is 3 then that image will get divided into a 3x3 matrix and then check point can be combination of row and column e.g. (1,2), (2,2) etc. Images and respective checkpoint is get stored in database. The KDA parameter can be measured by Down-Up (DU) time, Down-Down (DD) time, Up-Down (UD) time, Up-Up (UU) time, Down-Up2 (DU2) time. At the time of login, system will compare registered parameter of keystroke and login time keystroke parameter if it matches then open graphical password authentication window. User will enter click point (which is given at the time of registration) then system will check into the database using CCP, if checkpoint for each image matches with checkpoints stored in database then user login is successful.

4. Guidelines

User validation is one of the important issues for access restriction, especially to computer systems. Alphanumeric passwords can simply be break by the attacker. To deal with such illegal access there is need to provide higher security system for banking by using Keystroke Dynamics the security can be increased to great extent.

Here we discussed the various techniques for security in different application. By surveying the techniques given by the researcher we come to know that none of the system can guarantees with 100% accuracy. So there is need to develop a system that can give the high security to other application including banking application.

References

[1] Ting-YiChang,Cheng-JungTsai, Jyun-HaoLin,\A graphical-based password keystroke dynamic authentication system for touch screen handheld mobile devices", Journal of Systems and Software Volume 85, Issue 5, pp. 1157-1165, May 2012.

[2] Cheng-Jung Tsai, Ting-Yi Chang, Yu-Ju Yang, Meng-Sung Wu and Yu-Chiang Li, “An Approach for User Authentication On Non- Keyboard Devices Using Mouse Click Characteristics and Statistical-Based Classification" International Journal of Innovative Computing, Information and Control, Volume 8, Number 11, November 2012.

[3] Ahmed A. Ahmed and Issa Traore, “Biometric Recognition Based on Free-Text Keystroke Dynamics", IEEE transactions on cybernetics, Vol. 44, No. 4, April 2014.

[4] Ushir Kishori Narhar,Ram B. Joshi, “Highly Secure Authentication Scheme", 2015 International Conference on Computing Communication Control and Automation, 2015.

[5] S. Mondal and P. Bours, "Person Identification by Keystroke Dynamics Using Pairwise User Coupling," in *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 6, pp. 1319-1329, June 2017.

[6] Yan Sun, H. Ceker and S. Upadhyaya, "Anatomy of secondary features in keystroke dynamics - achieving more with less," *2017 IEEE International Conference on Identity, Security and Behavior Analysis (ISBA)*, New Delhi, 2017, pp. 1-6.

[7] J. Roth, X. Liu and D. Metaxas, "On Continuous User Authentication via Typing Behavior," in *IEEE Transactions on Image Processing*, vol. 23, no. 10, pp. 4611-4624, Oct. 2014.