iSafe - Authorization using Typing Rhythm: A Survey

Virendra Nagoriya[1], Saurav Yadave[2], Rohit Kumar[3],Prof. Laxmikant .M[4]

[123](Student, Dept. of Computer Engineering, D Y Patil School of Engineering Academy, Ambi, Maharashtra, India)
[5](Professor, Dept. of Computer Engineering, D Y Patil School of Engineering Academy, Ambi, Maharashtra, India)

Abstract – ***With the ever increasing demand for more secure access control in many of today's security applications, traditional methods such as PINs[1][7], tokens, or passwords fail to keep up with the challenges presented because they can be lost or stolen. On the other hand, biometrics based on "who" the person is or "how" the person behaves presents a significant security advancement to meet these new challenges. Among them, keystroke dynamics provide a natural choice for secure "password-free" computer access***

Keystroke dynamics refer to the habitual patterns or rhythms an individual exhibits while typing on a keyboard input device. These rhythms and patterns of tapping are distinctive in the same way as a person's handwriting or signature, due to their similar governing neurophysiological mechanism.
Here an attempt is made to develop a robust system to identify the users. The idea is to add three factors of authentication by entering the correct password, cued click point concept, and identifying the users typing pattern.

Keywords*: *Graphical Authentication, Dynamic Authorization, Keystroke Dynamic-Based Authentication, Level Securities.

I. INTRODUCTION

Authentication can be defined as verifying the validity of a user by using at least one form of the identification method. To grant access to the system, the user's identity should be verified. Dependence on computers to store and process sensitive information has made it necessary to secure them from intruders. Behavioral biometric such as keystroke dynamics which makes use of the typing rhythm of an individual can be used to strengthen existing security techniques effectively and cheaply.

Biometrics [2] refers to measurable human characteristics to define and identify a user. They are excellent and unique user characteristics to determine their identity. As the level of security decreases, the need for developing a highly secured identification and personal verification system increases. Physical biometrics is very useful to control access to secure buildings.

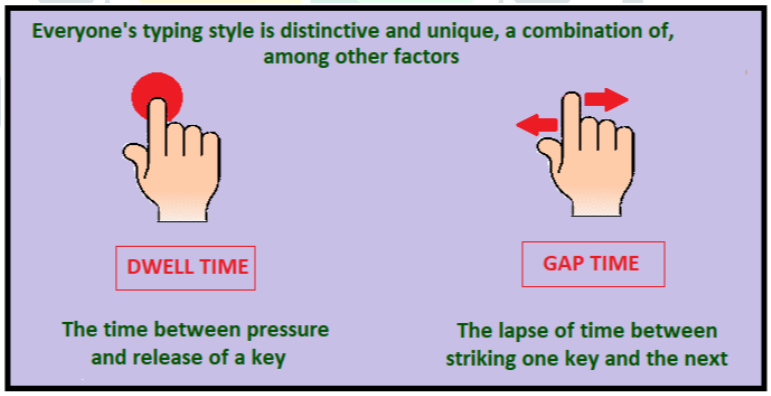

Figure 1: A Combination of Dwell Time and Flight Time

Keystroke dynamics [1][2], is behavioral biometry, refers to the unique patterns of rhythm and timing-based features that are created when a user types on a touchscreen in computing devices like keyboard. The biometric system uses a pattern recognition system to classify users based on their physical and behavioral characteristics. It is a method for identifying or verifying the users based on the way they type on a physical keyboard. This type of system uses artificial intelligence to differentiate legitimate users and illegitimate users. To protect a set of users from the illegitimate use of their accounts, the attributes of how they type and use the system are taken into account for authorizing the user. The typing dynamics gives the detailed timing information of when exactly each key was pressed and when it was released while a person is typing on a touch screen. Figure 1 shows the time in between pressure and release key.

II. LITERATURE REVIEW

Romain Giot et al.[3] presents biometric-based solutions to guarantee the security of the use of collaborative systems during the access control step. Sung-Shiou Shen et al.[4] extends dynamic keystroke concept and proposes pressure based dynamic keystroke methodology which is more secure and used as an alternative to the dynamic keystroke authentication.

G. Vinoth Kumar et al.[5] presents a novel approach for user authentication based on fingerprint and the keystroke dynamics of the password entry. The authentication process is done in three ways. Firstly user Login credentials based on Username and password; then Fingerprint, and finally Keystroke dynamics i.e patterns of rhythm and timing created when person types via keyboard are considered. The proposed approach provides a multimodal biometric authentication system.

Yu-Chiang Li et al.[6] Cheng-Jung Tsai et al. Gives the system based on click data on the time instances during pressing and releasing the mouse button. The system proposes the usefulness of a rhythm click- dynamics authentication system based on mouse clicks and a statistical-based classifier. Five features based on these periods are calculated using clicking in the rhythm that allows 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 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.

Ting-Yi Chang et al.[7] proposes a new graphical-based password KDA system for touch screen handheld mobile devices. The graphical password enlarges the password space size and promotes the KDA utility in touch screen handheld mobile devices. It also explores a pressure feature, which is easy to use in touch screen handheld mobile devices and applies it in the proposed system.

Lee et al.[8] done the feature evaluation including keystroke data such as time interval and motion data such as accelerometers and rotation values along with motion data and without motion, data is considered for keystroke dynamics that authenticate legitimate users. This paper demonstrates the opposite gender match between a legitimate user and impostors has to influence on authenticating by our experiment results.

Ushir Kishori et al. [9]gives a graphical passwords scheme in 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 the high-security purpose where it is very important to keep tight security.

Yan Sun et al. [10] 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 provide good user discrimination in keystroke dynamics.

Joseph Roth et al. [11]give a novel biometric modality named Typing Behavior (TB) for continuous user authentication. The author gives a novel approach, named bag of multidimensional phrases, to match the cross-feature and cross-temporal pattern between a gallery sequence and a probe sequence.

avaday narainsamy et al [12] evaluated the timing options for keystroke analysis. The user is authenticated depending on the keystrokes captured i.e. dwell time, flight time, etc which can be different depending on some factors like the operating system and the hardware used. Also, several factors affect the measurements captures like 1) Background processes running 2) Execution of tasks which intensively disk or memory operations.

N.L.Clarke and S.M. furnell[13] in 2007 worked on 30 users using FF MLP and proposed an Authentication Framework for Keystroke Analysis and identified the need to design a fully scalable multi-model system.

M. Alnabhan, et al.[14] presented an advanced keystroke authentication model improving users' validation strength. For each authorized user a keystroke structure had been defined that was used in the login attempts. The keystroke structure involved two components, firstly the deviation in typing time of user Secondly a unique user secret code. This system solved the problem of large deviations in keystroke dynamics and improved keystroke authentication level was provided. A strong authentication level had been achieved and participating users accepted this system model.

III. PROPOSED SYSTEM

The aim of this work is to provide 3 level securities for the transaction in banking applications. First, we are authenticating by login id and password. After user authentication, he will be shown with a graphical password screen. Graphical passwords have been designed for more secure and that to make passwords more memorable and easy to use by the people.

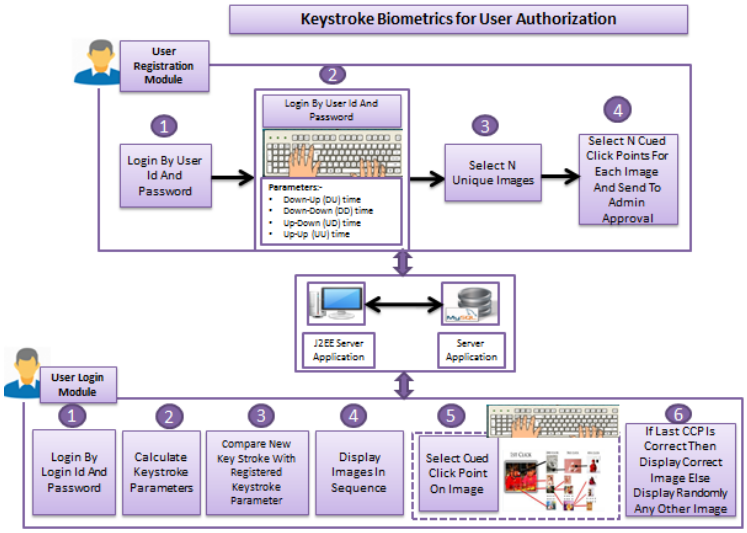

Figure 2: Proposed Architecture

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 match 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.

IV. CONCLUSION

Research on keystroke dynamics biometrics has been increasing, especially in the last decade. The main motivation behind this effort is due to the fact that keystroke dynamics biometrics is economical and can be easily integrated into the existing computer security systems with minimal alteration and user intervention. This paper gives an insight from the infancy stage to the current work done on this security domain which can be used by researchers working on this topic.

REFERENCES

[1] Faisal Alshanketi,Issa Traore,Ahmed Awad E. A,"Improving Performance and Usability in Mobile Keystroke Dynamic Biometric Authentication",2016 IEEE Security and Privacy Workshops.

[2] Fabian Monrosea;, Aviel D. Rubin"Keystroke dynamics as a biometric for authentication",2000 Elsevier Science B.V. All rights reserved.PII:S0167-739X(99)00059-X.

[3] Romain Giot, Mohamad El-Abed, Christophe Rosenberger ,"Keystroke Dynamics Authentication For Collaborative Systems",arxiv.org/ftp/arxiv/papers/0911/0911.3304.pdf.

[4] Sung-Shiou Shen ; Shen-Ho Lin ; Tsai-Hua Kang ; Wei Chien , "Enhanced keystroke dynamics authentication utilizing pressure detection", 2016 International Conference on Applied System Innovation (ICASI).

[5] G. Vinoth Kumar ; K. Prasanth ; S. Govinth Raj ; S. Sarathi ,"Fingerprint based authentication system with keystroke dynamics for realistic user", Second International Conference on Current Trends In Engineering and Technology - ICCTET 2014.

[6] Cheng-Jung Tsai1, Ting-Yi Chang, Yu-Ju Yang Meng-Sung Wuand Yu-Chiang Li ,"AN APPROACH FOR USER AUTHENTICATION ON NON-KEYBOARD DEVICES USING MOUSE CLICK CHARACTERISTICS AND STATISTICAL-BASED CLASSIFICATIO",International Journal of Innovative Computing, Information and Control ICIC International c 2012 ISSN 1349-4198Volume 8, Number 11, November 2012

[7] Ting-Yi Chang,Cheng-Jung Tsai,Jyun-Hao Lin,"A graphical-based password keystroke dynamic authentication system for touch screen handheld mobile devices",Journal of Systems and SoftwareDOI: 10.1016/j.jss.2011.12.044

[8] Hyungu Lee ,1 Jung Yeon Hwang ,2 Dong In Kim ,1 Shincheol Lee ,1 Sung-Hoon Lee ,3 and Ji Sun Shin ,"Understanding Keystroke Dynamics for Smartphone Users Authentication and Keystroke Dynamics on Smartphones Built-In Motion Sensors",Security and Communication Networks Volume 2018, Article ID 2567463,

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

[10] Yan Sun, Hayreddin Ceker and Shambhu Upadhyaya"Anatomy of Secondary Features in Keystroke Dynamics - Achieving More with Less".

[11] Yan Sun, Hayreddin Ceker and Shambhu Upadhyaya"Anatomy of Secondary Features in Keystroke Dynamics - Achieving More with Less".

[12] Pavaday narainsamy et al, "Investigating 7 Improving The Reliability and Repeatability of Keystroke Dynamics Timers," IJNSA, vol. 2, no. 3, 2010.

[13] N.L. Clarke and S.M. Furnell, "Authenicating mobile phone users using keystroke analysis," in International Journal of Information Security , pp 1 - 14 ,2007.

[14] A. K. Hussain and M. M. Alnabhan "Advanced Authentication Scheme Using a Predefined Keystroke Structure", Int. J. Comput. Sci. Inf. Technol., vol. 6, no. 2, pp. 163–169,2014.