International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-3 Issue-2, July 2013

Typing Speed Analysis of Human for Password Protection (Based on Keystrokes Dynamics)

Swarna Bajaj, Sumeet Kaur

Abstract--- Today is an important problem for describe as authentic, you mean that it is such a good imitation that it is almost the same as or good as the original in computer system. Specially those used in e-banking, e-commerce, virtual offices, e-learning, distributed, computing and other services over the internet. Using keystroke dynamics technology we can secure our password. This technology is based on human behavior to type their password. We analysis the human behavior with their typing pattern. Keystroke dynamics are hardware independent, no extra hardware is used. Only software based technology keyboard is required for password protection. The results provide emphasis with pleasure security that growing in demand in web-based application based on internet.

Index Terms—Keystroke dynamics, Net bean IDE, Pressing time, secure password.

I. INTRODUCTION

Biometric is the most secure and convenient authentication tool. It can't be borrowed, stolen, or forgotten, and forging one is practically impossible. Biometrics measure is individual's physical or behavioral characteristics to recognize or authenticate their identity.

The security field uses three different types of authentication:

- Something you know password, PIN, or piece of information.
- Something you have a card key, smart card, or token
- Something you are a biometric.

Common physical biometrics include fingerprints; hand or palm geometry; and retina, iris, or facial characteristics. Behavioral characters include signature, voice, keystroke pattern, and gait. Of this class of biometrics, technologies for signature and voice are most developed. Mouse dynamic [9] is also used for security purpose but tracking of keyboard activity is much more practical now a days. Keystroke dynamics is a behavioral biometric based on the assumption that different people type in a unique manner.

Neurophysiologic factors make written signatures unique per person. These factors are also expected to make typing characteristics unique per person. The idea behind keystroke dynamics appeared in the 20th century when telegraph operators could recognize each other based on their distinctive patterns when keying messages over telegraph lines. Keystroke dynamics is known with other names such as keyboard dynamics, keystroke analysis, typing biometrics and typing rhythms.

Manuscript published on 30 July 2013.
***Correspondence Author(s)**
Swarna Bajaj, Computer Science Deptt., YCOE Talwandi Sabo, Punjabi University , Patiala, India.
Sumeet Kaur, AP in Computer Science Deptt., YCOE Talwandi Sabo/Punjabi University, Patiala, India.

Keystroke dynamics have advantage as compare to another biometric methods that another biometric may evenly change due to slight accident and other environment factors but keystroke have based on behavior of typing keys. The important terms used in keystroke is that there we required software and keyboard is needed for input. Using keyboard input system we check the human behavior to type there password, what shortcuts typing methods, special keys, characters used by user. There all things are different in every human and this behavior used to achieve a particular result in authentication. Performance of keystroke dynamics is depend on what type of keyboard is used by user

(a) Desktop keyboard

(b) Laptop keyboard

Fig.1: Difference of shape of two classical keyboards [4],[5]

A. *KEYSTROKE DYNAMICS FEATURES*

There are several different features [8] which can be detected when the user presses keys on a Keyboard. Possible features include:

A. Pressing time (the time in which the key is held down)
B. Releasing time (the time in which the key is released).
C. Latency (the time between two consecutive keys 2).
D. Pressure used when hitting keys while typing (requires a special keyboard).
E. Finger placement (the place where the finger is placed on the key or even the angel of the finger when pressing the key). In this case a camera is required.
F. Finger choice (which finger is used on the key of the keyboard): In this, a camera is required.

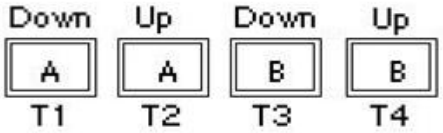

Fig. 2: Timing of key pressing & releasing[6]

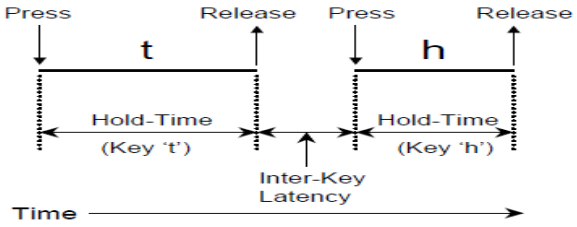

Fig. 3: Relationship between key hold-time and inter latency-time [7]

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

II. RELATED WORK

Mariusz Rybnik et al., (2009) [1] proposed an approach, aimed at better security with keystroke dynamics using short fixed text. In this paper they present experiment on one word phrase. This can stand for a simple user password and extracted the pressing time and duration between two keys. They calculate new term overlapping between two keys (one key is pressed and last key is not released). The best results are obtained and encourage further development in this area. They introduced three issues for any computer system with restricted access. Memory- based authentication, Token-based authentication and Biometric-based authentication.

Saurabh Singh et al., (2011) [2] proposed a novel technique for free text keystroke dynamics. In this study, keys are classified in to two halves (left-right) and four lie (total eight groups). They used timing vector to calculate the flight time. Timing vector technique used to define the difference between fraud and actual users. The best results are obtained and very supporting.

Mudhafar M.AL-Jarrah et al., (2012) [3] present a paper an anomaly detector for keystroke dynamics authentication, based on a statistical measure of proximity, evaluated through the empirical study of an independent benchmark of keystroke data. A password typing rhythm is used to detect the actual and unauthenticated user. They introduced two phases training phase and testing phase. They calculate key down/up time of every key and latency time between keys. The comparison in testing phase check the value in binary for analysis if value is near about then 1 else 0. The use of benchmark data in the study of the detection performance of authentication systems is a scientific approach.

III. PROPOSED WORK

The proposed method is based on to calculate the pressing time, dwell time and total time of password. We analyses this work on laptop keyboard. There statistical method is used to measure the mean time and average time. The NetBeans IDE is an open-source integrated development environment. NetBeans IDE supports development of all Java application types. The NetBeans IDE is written in Java and runs everywhere where a JVM is installed, including Windows, Mac OS, Linux, and Solaris.

A. LOGIN PROCESS

When a user starts the application, a login activity is launched where a registered user submits his 4 character password and an unregistered user can register him by clicking on New User button. (See Fig. 4)

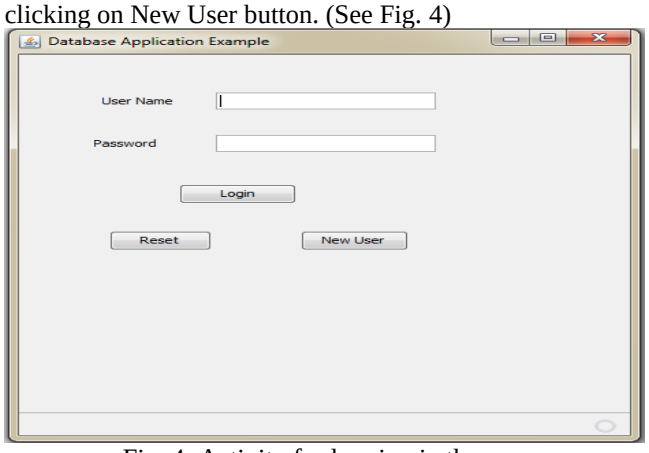

Fig. 4: Activity for logging in the user.

After entering the password and clicking on Login button, if the password is not found in the database an error message is displayed.

B. NEW USER REGISTRATION

New user clicks new user button, then registration activity is displayed where user is asked to enter user name, 4 character password and login for four times and then save data in data base. See Figure 5.While the user is typing on keyboard for submitting a sample, factors like dwell time (time interval between consecutive key press and key release), flight time (time interval between consecutive key release and key press), total time and pressing time of characters key is calculated and upon clicking the save button, the values are stored in the respective table. Every user is identified by his 4 unique characters but every sample entered by a single user is identified by the timestamp. Hence values calculate while typing the unique character is stored in database along with password, time interval calculated and timestamp.

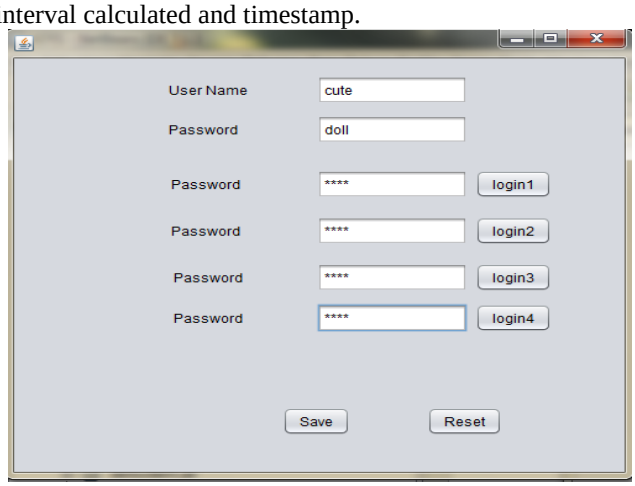

Fig. 5: New User registration

Table 1 is the image of the table login name which will be used as an example for description. As from the image it can be seen that ten samples of the user with User name and password are present. Total time taken in milliseconds by the user to enter his 4 unique characters is stored in database total time column.

C. STORAGE DATABASE

#	PRESS1	PRESS2	PRESS3	PRESS4	DULL1	DULL2	DULL3	TT	USERNAME	PASSWORD
1	82	62	66	66	327	89	686	1103	raam	raam
2	62	97	70	93	197	322	286	928	life	save
3	116	112	93	97	692	276	889	1813	jcdv	jcdn
4	105	90	89	70	520	654	431	1560	rats	star
5	84	91	100	88	386	406	804	1563	back	home
6	84	141	87	74	203	347	259	995	ctrl	page
7	70	113	74	70	234	285	431	1041	ycae	sabo
8	78	62	97	62	166	618	489	1255	caps	lock
9	148	116	105	105	629	385	473	1591	save	girl
10	140	144	121	93	676	722	441	1880	long	life

Table 1: Data values collected for total login time

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

D. MATCHING PROCESS

We find the difference between actual value stored in database and current value of login user. We assume the threshold value to compare with time. These thresh hold values are increases the efficiency of result. We compare this value to the current time of login user if the value will be match according to the threshold value the person accepted or called authenticated user. This value will be change according to analysis. Using this output we calculate FAR (False accept ratio) and FRR (false Reject Ratio) values.

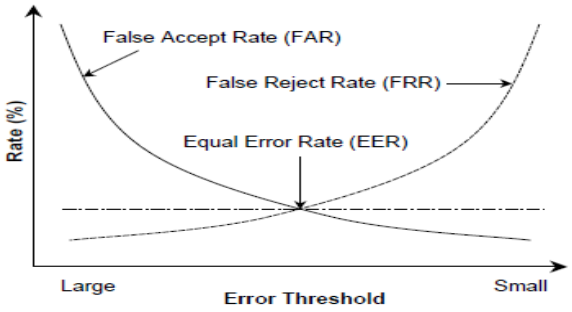

Fig. 6: Relationship between FAR, FRR and EER [7]

IV. ANALYSIS AND RESULTS

Data collected from 10 Users shown in table 1, each user was asked to register him/her & then each was invited to for login. Analysis for one value for 10 times by 10 Users shown in table 2. And this table 2 shows the differences between values stored in data-base and different Users login Time.

Table 2: Pressing & dwell time of password "save" & User Name "life" entered by 10 User

user	1	2	3	4	5	6	7	8	9	10	data base
p1	156	78	156	203	78	78	141	78	109	94	62
p2	140	109	141	203	125	109	140	94	141	93	97
p3	94	78	172	218	78	78	78	78	109	63	70
p4	78	93	172	219	63	78	78	78	109	62	93
d1	468	94	234	593	93	110	78	47	78	156	197
d2	1061	390	483	1092	1903	249	1092	281	343	125	322
d3	1060	156	390	655	203	297	406	265	125	296	286
TT	3057	998	1748	3183	2543	999	2013	921	1014	889	928

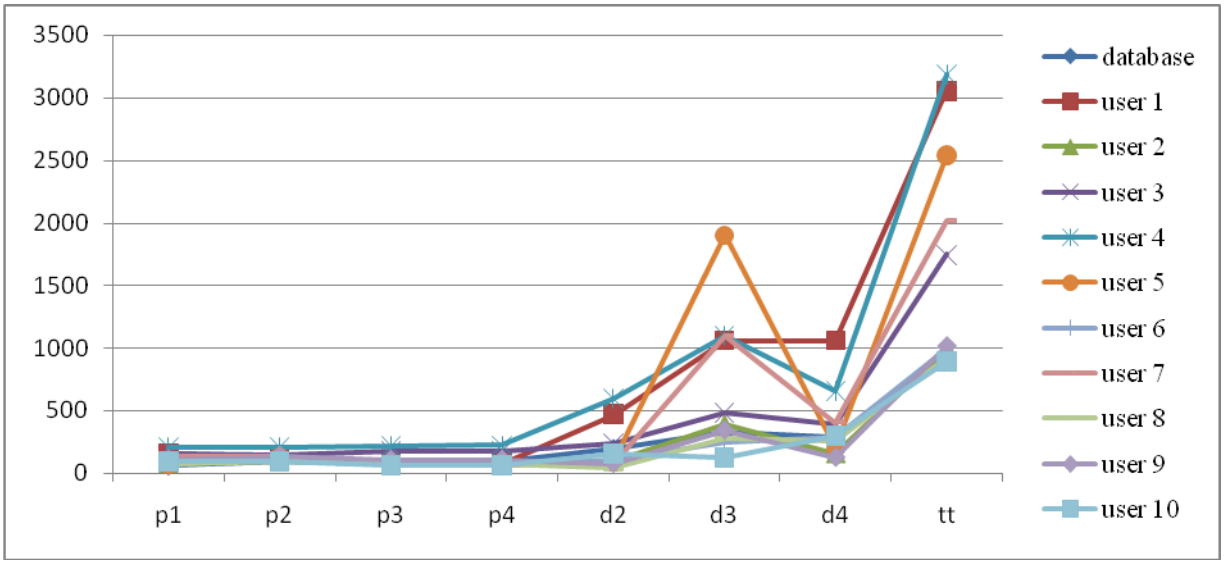

Fig. 7: Relationship between value stored in database and values of 10 Users for table 2.

V. CONCLUSION

This paper emphasizes is on the importance of keystroke dynamics for desktop. The implementation of keystroke dynamics on desktop is cost effective and compatible as integration of external hardware is not required.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

The conclusion of this thesis is based on comparing the data stored of a user with the login input for authentication. Keystroke Dynamics is a two factor security biometric security, hence, for a successful login, firstly password should be known and secondly, typing rhythm should be match .In human behavior security system of any keypad requires to make a programming. In another method of biometrics we require hardware but human behavior method we generate a secure key to protect our password. This key is generating according to human behavior for e.g. when user give password he use his typing speed to fill the password. The key is generated by programming (java application) to calculate different times in millisecond.
The main drawback of this project is different types of keyboard. But we work on this project and will find the solution for that and can be better advancement of this keystroke dynamics. If we make all keyboards of same style, same features then it gives better results.

REFERENCES

1. Mariusz Rybnik, Piotr Panasiuk & Khalid Saeed "User authentication with Keystroke dynamics using Fixed Text" University of Bialystok Marii Sklodowskiej Curie 14, 15 097,978-07695-3692- 7/09 $25.00 © 2009 IEEE.
2. Saurabh Singh, Dr. K.V.Arya "Key Classification: a New Approach in Free Text Keystroke Authentication System" Invertis University Bareilly, India, 978-1-4577-0856-5/11/$26.00 © 2011, IEEE.
3. Mudhafar M.AL-Jarrah "An Anomaly Detector for Keystroke Dynamics Based on Medians Vector Proximity" Department of Computer Information Systems, Middle East University, Amman, Jordan, VOL 3, NO. 6, © 2009-2012 CIS Journal.
4. Killourhy, K. & Maxion, R.,"Comparing anomaly-detection algorithms for keystroke dynamics",IEEE/IFIP International Conference on Dependable Systems & Networks, 2009. DSN'09, pp. 125– 134.2009
5. Killourhy, K. & Maxion, R. "Keystroke biometrics with number pad input",IEEE/IFIP International Conference on Dependable Systems & Networks, 2010. DSN'10
6. Hocquet, S. Ramel, J.-Y. & Cardot, H, "Fusion of methods for keystroke dynamic authentication". autoid, 0, 224–229.2005
7. Heather Crawford "Keystroke Dynamics: Characteristics and Opportunities" Department of Computing Science Sir Alwyn Williams BuildingUniversity of Glasgow Glasgow, 978-1- 4244 7550 6/10/$26.00 ©2010 IEEE.
8. S. J. Shepherd, "Continuous authentication by analysis of keyboard typing characteristics", Proc. IEEE European Convention on Security and Detection, vol. 16-18, May 1995, pp. 111- 114.
9. R. V. Yampolskiy, "Motor-Skill Based Biometrics," In Assuring Business processes, Proceedings of the 6th Annual Security Conference, Ed. G. Dhillon. Global Publishing, Las Vegas NV, USA. April 11-12, 2007.

AUTHOR PROFILE

Swarna Bajaj- M. Tech. in CSE (2010-2013), YCOE Talwandi Sabo, Punjabi University Patiala., B. Tech. IT, JCDMCOE Sirsa, Haryana, KUK.,Degree awarded by Dr. APJ Abdul Kalaam Azad, former President of India.

Sumeet kaur is currently a Ph.D. candidate in computer science. Her research interests include Area of password security. She works as Assistant Professor at Faculty of Yadvindra College of Engineering, Talwandi Sabo, Bhatinda, India. Her Publications are more than 25.

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)