

A Keystroke Dynamics Based Authentication System

Ravi Kiran ^[1], Sarita Soni ^[2]

Department of Computer Science
Babasaheb Bhimrao Ambedkar University, Lucknow
Uttar Pradesh, India

ABSTRACT

The requirement of authentication is not limited to PIN and password at present time. Here required a high level of security who is found by keystroke biometrics. In this review paper we want to know the keystroke methods and sketch a common conclusion. After applied this mechanism we can enhance and improve the security of various systems.

Keywords:- Static Authentication, Keystroke Dynamics, Soft Biometrics, Security.

I. INTRODUCTION

Keypress is a authentication system which is based on keystroke dynamics which identifies users, based on their typing pattern. If we have any authentication related problem then it seems to be ultimate solution for it. In the typing rhythm of a person, the keystroke dynamics is uncopiable, reliable, unique and even adaptive to changes. It is not boomed at that time inspite of the benefits over normal biometrics solutions which are decumbent to forged. Some times this technology is quite but some considerable number of research is done in this field. It needs a lot of training, they can be counterfeit which is the major defect of physical and biological biometrics. In the cast of fingerprint and iris scans the advancement of this technology has become very easy to forged.

One of the main problem in most recent information systems alongside with data storage and processing is allowed to access permissions. It allows the access permissions of faculty members within the organization and also prevent unauthorized access by intruder. If the user wants to enter in the system and the user is not authorized then there are exist key problems in information systems.

II. LITERATURE REVIEW AND BACKGROUND STUDY

Systematic literature review is a method for conducting bibliographic reviews in a formal way, following well defined steps, which allows the results to be reproducible. In addition, the protocol adopted for the conduction of the review must assure its completion. This review method is commonly used in other areas, mainly in Medicine and has several reported benefits, like less susceptibility to bias. In the area of Computing, this method of review is more disseminated in Software Engineering. The application of the systematic review involves three major phases: planning, conduction and presentation of results. In the first phase, a review protocol is

returned references. References used for the extraction of information are called primary studies, while the review is a secondary study. Finally, the third phase defines the way to present the results and the final report is done. The items comprehended in each of the three phases.

The Previous methology inhances many features which is collected untill the user types and modles constructed with these features. We can describes in detail of these approaches from some of the details overview which is given below.

A. Key Press Duration

In this approach, the model is the vector X of n elements, each element corre-sponding to one of the keyboard keys and represented by the pair (M_k, D_k) : M_k is the mean dwell time during which the key k is depressed (key press duration) and D_k is the standard deviation for key k .

B. Press and Release Sequence

This approach assumes that the user entering the password sometimes presses the next key before releasing the current key (this leads to a so-called “swap”). A user model is constructed by observing the sequence in which keys are pressed and released and calculating the number of “swaps”. FAR and FRR produced by this method are highly dependent on pairs of users participating in the assessment.

C. Relative Typing Speed

The rate of relative typing is normally assumed the similar type of any pair of keys, regardless of the text which is typed. It is therefore proposed to measure the typing rate for pairs of keys and apply it as a user model. The user model is constructed by measuring the distance between vectors of key

pairs ordered by typing speed. The distances between two vectors of the same user were on average value.

D. Use of Right and Left Shift Keys

It can be used only for authentication because of the different people use the right and left shift key varitly. Users were divided into 4 classes based on experimental data: those who use only right or only left Shift, and those who give preference to the right or the left Shift, but also use the other key.

E. Method for Short Alphabetic or Numeric Passwords

In the calculation, which is done by different three techniques and the key press duration are used as a model. The learning algorithm is the multiclass linear SVM, because it demonstrates the best performance on simple data structures. The test subjects were divided into two groups for data collection: one group was aware of the ongoing experiment, the other not.

III. METHODOLOGY

This work uses one-class classification approach coupled with immune algorithms for identification purposes in keystroke dynamics. The key here is a deep analysis and through understanding of data that helps in preprocessing and extraction of more refined features; after that rank transformation is applied to improve the recognition.

Using classification approach the immune algorithm is uses for identification purposes in keystroke dynamics. It uses key for deep analysis and knowing of raw data, the another feature of this is preprocessing and extraction of data and for improved of this recognition we uses transformation.

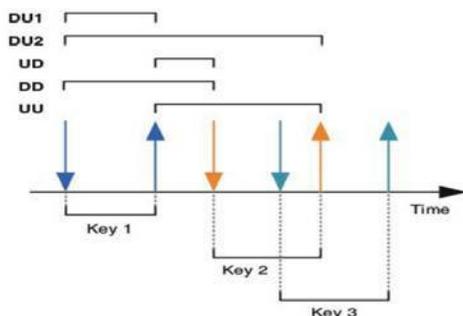


Fig 1. Feature extraction

HERE:

1)DU1: It is the time difference between the key press and the key released. It is known as Dwell Time and denoted by the

DU1. This feature work on the time and calculated with the respect of time untill the key is pressed.

Time difference between the instants in which a key is pressed and released. This feature represents the time that the key keeps pressed and is also named by some authors as dwell time.

2)DU2: When we press a key and press a another key without releasing previous key, it shows the time difference between a continuous key is pressed and the next key is released.

Time difference between the instants in which a key is pressed and the next key is released.

3)UD: It is show the time difference between releasing a key and after that press a key now. This is known as Flight time. We can say that instantly a key released and the next key is pressed, using this we can find the time difference.

Time difference between the instants in which a key is released and the next is pressed. This feature is also known as flight time.

4)DD: It is knows the time difference between a instantly a key is pressed and the next key is pressed.

Time difference between the instants in which a key is pressed and the next key is pressed.

5)UU: It is show the time difference with the respect of time. It calculated the time difference between a key is released and the next key is releasing.

Time difference between the instants in which a key is released and the next key is released.

Using typing pattern and feature extraction it creates a profile of typing signature or characteristics of typo behaviour. Handling the dimensionality is ineluctable in keystroke dynamics using transformation.

IV. CONCLUSION

Since the onset of the technological era and the boom of internet there have been identity crises, wherein people have been using fraudulent methods to fake identities. Today, there exists no authentication system which cannot be misled. For example, consider the following problems:

- Phone patterns can be snooped upon and so can be email passwords.
- Even 2-step verification can be cracked by stealing the phone of the user.
- Furthermore, there exists enough media depicting on how to copy fingerprint and iris scans.

ACKNOWLEDGMENT

We would like to thank our colleagues and for their feedback on the earlier version of this paper and we would

also thanks to our guide and faculty for their help and guidance on this paper and their views.

REFERENCES

- [1] Dharmendra Singh, Bhawnesh Jaggi, Himanshu Nayyar, Amit Kumar, “Presskey- A Keystrokes Dynamics Based Authentication System” International Journal of Advanced Research in Computer Science, Volume 8 No. 5, May- June 2017, pp. 2665-2670.
- [2] V. Yu. Kaganov, A.K. Korolev, M. N. Krylov, I. V. Mashechkin, M. I. Petrovskii, “Machine Learning Methods In Authentication Problems Using Password Keystroke Dynamics”, Computational Mathematics and Modeling, Volume 26 No. 3, July 2015, pp. 398-407.
- [3] Ahmed Mahfouz, Tarek M. Mahmoud, ahmed Sharaf Eldin, “A survey on behavioral biometrics authentication on smartphones”, Journal of Information Security and Applications, Elsevier, 2017, pp. 28-37.