International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 3 | Issue 3 | ISSN : 2456-3307

A Survey on Keystroke Dynamics Based Authentication System

Ravi Kiran, Sarita Soni
Department of Computer Science Babasaheb Bhimrao Ambedkar University Lucknow, India

ABSTRACT

In the keystroke dynamics, we face many types of error and problems in user authentication. In this new types of static authentication method where we found the selective data or information is described the user keystroke. By the experiments of this authentication problem we applicable to substantiated and optimize the condition for the selected and implemented of the method. In this approach, we only discuss the limitation, strength, facts which are combined the behavioral biometric trait. Finally, in this research field, we face the different types of open research problems and challenges.

Keywords : Behavioral Analysis, Static Authentication, User Authentication, Keystroke Dynamics, Verification.

I. INTRODUCTION

Keystroke dynamics is the main fact in the most recent information systems alongside with processing and data storage for access license granting. If we have the permissions then we stop to access unauthorized access by the intruder and also permit right access within the organization or staff members. Keystroke dynamics provides the legally access to the system which user wants in authentication problem.

Here, different types of techniques are present to solve the authentication problem. The most powerful and popular methods are used in recent information system i.e. password authentication. The only user can permit to access the system authentication by the use of the special string of known symbol. In addition to obvious advantages - passwords are simple to implement and their use is very widespread, password authentication suffers from essential shortcomings: the user may forget the code string or reveal it to other users; if the password is too short or too simple, it can be found by direct enumeration or by dictionary-based enumeration. All this casts serious doubts on password use in high-security systems.

Authentication by means of electronic and digital signatures (EDS) is free from the last shortcoming. However, it is impossible to ensure secure storage of closed keys in this way, because they are stored using other access control tools.

For these reasons, many effective security systems rely on biometrics to identify the user. Biometric systems fall into two categories. One category includes systems using features that differ for natural reasons among different individuals: fingerprints, retina scans, voice patterns, body temperature chart, etc. These systems are effective but quite costly because they require special equipment. The second category includes systems that analyze user behavior; they are based on user experience and skills. They do not require any special equipment and are simple to introduce. One of such systems analyzes user keystroke dynamics [3].

CSEIT1833658 | Received : 17 April 2018 | Accepted : 28 April 2018 | March-April-2018 [(3) 3 : 1930-1934]

II. LITERATURE REVIEW

Mainly for buying the internet based applications, the modern technology gives various services to the peoples for easy to use. In this fast developing technology, we need an approach to enhance our security system. In this, The use of biometric that takes into account the calculation of physiological and behavioral of masses.

In the system, we learn various points and proposed a model which increases the security of our systems. For a person the behavioral biometrics (typing pattern, signatures) is unique. To using press key intends feather it provides a powerful security system which is most unbreakable by the intruder.

A detailed review of related work:

I. Flight Mining for Keystroke Dynamics Authentication (KDA).

In the form of keystroke dynamics, it uses password and username method for knowing the additional measurement of keystroke dynamics profile creation for the authenticating users, it uses a selected method careful which is keystroke dynamics analysis.

For creating a profile of users, it used keystroke data as username. Selected letters converted to a flight way and the username works as a point. Based on flight difference users authentication will be done after flight profile is created. Typo behavior can be used for increasing real system security with the help of profile creation but it can be different in different situations.

II. Accenting typing signature in keystroke dynamics using the immune algorithm.

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 thorough understanding of data that helps in preprocessing and extraction of more refined features; after that rank, a transformation is applied to improve the recognition.

Using classification approach the immune algorithm is used for identification purposes in keystroke dynamics. It uses a key for deep analysis and knowledge of raw data, another feature of this is preprocessing and extraction of data and for improved of this recognition we use transformation [4].

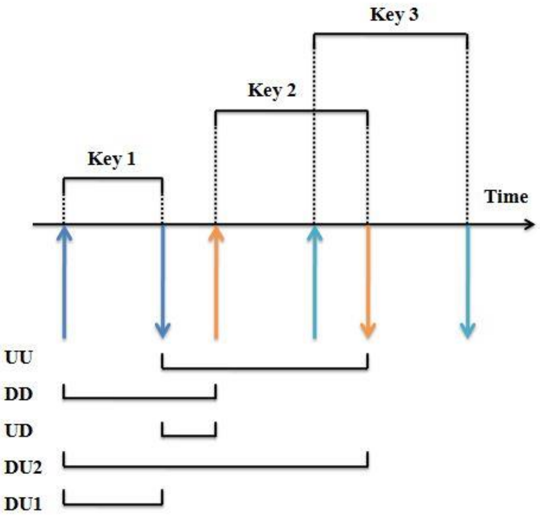

Figure 1. Feature extraction

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 works on the time and calculated with the respect of time until 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 another key without releasing the 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 shows 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 known the time difference between an 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 shows the time difference with the respect of time. It calculated the time difference between a key is released and the next key is releasing [1].

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 behavior. Handling the dimensionality is ineluctable in keystroke dynamics using transformation.

III. User Authentication Using Free Write Strings by Various Input Devices in Keystroke Dynamics :

We should not use minimum predefined letters but we use different types of input devices, for solving compound problems of keystroke dynamics authentication which is based on free and long write strings. It works and based on three important questions, which are :

- ✓ The given authentication algorithms are suitable to the condition of string lengths and input device.
- ✓ The achievement of the authentication is altered by the length of the string.
- ✓ The achievement of the authentication is based on the use of different types of input device.

12 one-class classifier is the method by which the enemy can get the answer to the above-pointed questions, for the application scenario the multi-class classifier would be idealistic but it gives the sharpened result. Instead of desires customization used with other input devices, we used a keyboard as an input device which is working good and used different types of methods. Enough achievement is bringing off by the size of reference and string keystrokes. The length of the string keystrokes is reduced the authentication error if we increase at least one factor of reference keystroke. When we used the adapted admeasurements then we found the minimum fault rate in authentication.

IV. Consecutive Keystroke Dynamics: Another aspect of biometric appraisal:

This is a root to briefly appraisal a biometric consecutive keystroke dynamics system: this system is consecutively loaded and monitor the data of rhythm behavior of a user so that the system is always whether the user is arbitrated present or not, the system can be cinched if another user ascertains the system. The static system relies on the count of wrong decisions made by the user but on the other hand, the continuous system needs to work faster and with accurate results to identify the impostor quickly. Detection of the imposter as soon as possible with minimum keystrokes increases the trust and performance of the system.

III. METHODOLOGY

A 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 defined, in which research questions are specified along with search strategies. After that, in the second phase, the review protocol is applied and the Information is extracted from the 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 methodology enhances many features which are collected until the user types and models constructed with these features. We can describe in detail of these approaches from some of the details overview which is given below.

A. KeyPress Duration

In this approach, the model is the vector X of n elements, each element corresponding 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. 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 the 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 variety. It can be used only for authentication because of the different people use the right and left shift key variety. 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. 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 [2].

IV. CONCLUSION

Since the onset of the technological era and the boom of the 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 emailed passwords.
- ✓ Even 2-step verification can be cracked by stealing the phone of the user.
- ✓ Furthermore, there exist enough media depicting on how to copy fingerprint and iris scans.

V. REFERENCES

[1]. Prof. 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.

[4]. Ravi Kiran, Sarita Soni, "A Keystroke Dynamics Based Authentication System", International Journal of Computer Science Trends and Technology, Volume 6 Issue 2, Mar-Apr 2018, pp. 53-55.

[5]. P.H. Pisani, A.C. Lorena, "Emphasizing typing signature in keystroke dynamics using immune algorithms," Applied Soft Computing Volume 34, September 2015, pp 178–193, Elsevier Press, DOI: 10.1016/j.asoc.2015.05.008

[6]. D. Shanmugapriya, G. Padmavathi, "Virtual Key Force-A New Feature for Keystroke," J. International Journal of Engineering Science and Technology, Vol. 3 No. 10 October 2011, pp. 738-743.

[7]. A. K. Jain, R. Bolle, and S. Pankanti (editors), Biometrics: Personal Identification in a Networked Society, Kluwer Academic Publishers, 1999.

[8]. K. Wangsuk, T.A. Amornkul, "Trajectory Mining for Keystroke Dynamics Authentication," Procedia Computer Science, Volume 24, 2013, Elsevier Press, pp 175-183, DOI: 10.1016/j.procs.2013.10.041

[9]. R. Thanganayagam, A. Thangadurai, "Hybrid Model with Fusion Approach to Enhance the Efficiency of Keystroke Dynamics Authentication," Proc 3rd International Conference on Advanced Computing, Networking and Informatics, Oct 2015, SIST vol 43, Springer Press, pp 85-96, DOI: 10.1007/978-81-322-2538-6_10

[10]. G. Jagadamba, S.P. Sharmila, T. Gouda, "A Secured Authentication System Using an Effective Keystroke Dynamics," Proc Emerging Research in Electronics, Computer Science and Technology, 2013. LNEE vol 248 Springer press, pp 453-460, DOI: 10.1007/978-81-322-1157-0_46