2nd International Conference on Emerging Trends in Engineering, Science and Management
Indian Federation of United Nations Associations, New Delhi (India) (ESM-17)
13th August 2017, www.conferenceworld.in ISBN: 978-93-86171-59-7

Keystroke Dynamics Approach for User Authentication

Assistant. Professor Vandana

S.D.S.P.Memorial College for Women, Rayya (India)

ABSTRACT

User authentication is an important part of the problems related to computer and system security i.e. the process or action of verifying the identity of a user or process. Biometrics is the science and technology of authentication by identifying the living individual's physiological or behavioral attributes. One of such behavioral measurement is ***Keystroke dynamics*** *which utilizes the manner and rhythm in which each individual type. To authenticate user based on their typing samples, it is required to find out the resemblance of a typing sample of user regardless of the text typed. In this paper we focus on a biometric technique that aims to identify users based on analyzing habitual rhythm patterns in the way they type.*

Keywords- Biometrics, Keystroke dynamics, User authentication

I. INTRODUCTION

Today the dependence on computer technology and Internet information has increased, hence authentication and security has become a vital issue. Personal identification is necessary to protect the information of a system and to give access or modify data by only authorized people. Authentication is the process or action of verifying the identity of a user or process. There are three approaches of user authentication i.e.-

1.1 Object based: In this approach, to identify the user of a smart card or some key is required strong user identification techniques like combination of password with the tokens are needed. If the user forgets their details such as PIN the card get locked after some number of incorrect attempts.

1.2. Knowledge based: In this approach, to access the information passwords are the most commonly used tools but the flaw is that generally the individual chooses very easy passwords that can be easily guessed or hacked.

1.3. Biometric based: In this kind of a system the user has to give personal physical characteristics like fingerprints. The reason is because biometrics is directly linked and dependent on the user while the password or token can be used some other person.

II. BIOMETRIC BASED AUTHENTICATION

Biometric authentication is an automatic method that identifies a user or verifies the identity based upon the measurement of his or her unique physiological traits or behavioral characteristics. The Physiological Biometrics depicts those features that describe who the user is depending on the physical attributes e.g. fingerprints, Iris and retina scanning. For this additional hardware required. The Behavioral Biometrics is based on typing pattern, Voice recognition and Signature style and there is no need of any extra hardware. This study will focus on Behavioral biometric technique i.e. Keystroke Dynamics.

Keystroke dynamics is a promising biometric technique to recognize an individual based on an analysis of his/her typing patterns. It provides a natural choice for secure “password-free” computer access with no

additional hardware required. Simply, we can say that Keystroke dynamics refers to the habitual patterns or rhythms an individual exhibits while typing on a keyboard input device. It enables a cost effective, user friendly, and continuous user authentication with potential for high accuracy.

Keystroke dynamics is governed by a person's neurophysiological pathway to be highly individualistic; it can also be influenced by his or her physical and psychological state. As a "behavioral" biometrics keystroke dynamics exhibits instabilities due to transient factors such as fatigue, emotions, stress, and drowsiness. It also depends on some external factors, such as the specific keyboard device used, possibly due to different layout of the keys. As such, keystroke data need to be collected at multiple sessions to assess the robustness of various approaches. It was shown that the frequently used word tends to have better typing timing consistency.

III. NEED OF KEYSTROKE DYNAMICS

Keystroke dynamics is part of a larger class of biometrics known as behavioral biometrics; their patterns are statistical in nature It is a commonly held belief that behavioral biometrics are not as reliable as physical biometrics used for authentication such as fingerprints or retinal scans or DNA. But the reality is that behavioral biometrics use a confidence measurement instead of the traditional pass/fail measurements. Moreover, unlike other biometric systems, which may be expensive to implement, keystroke dynamics is almost free. For-example- A person at gun-point might be forced to get start-up access by entering a password or having a particular fingerprint, but then that person could be replaced by someone else at the keyboard who was taking over for some bad purpose or an employee might violate business rules by sharing their password with their secretary, or by logging onto a system but then leaving the computer logged-in while someone else he knows about or doesn't know about uses the system. Keystroke dynamics is one way to solve such problems. The advantage of using behavioral biometrics such as keystroke dynamics is that it can be collected even without the knowledge of the user. Human-computer interactions play an important role in keystroke dynamics

IV.. LITERATURE REVIEW

Recently, keystroke dynamics has become an active research area due to the increasing concerns of cyber security and access control.. Several techniques came into existence since then. Brief review of these techniques is as follows:

N. Chourasia has introduced an additional layer of security for the authentication of the user, Keystroke Dynamics. The security can be implemented in android phones or any other smart phones through which internet is accessible as well as online transactions can be performed. Dataset was collected to measure the performance and evaluation procedure was developed. A mathematical model was presented before implementation.

Hussain et al, in his study 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.

Ahmed et al. (A. A. Ahmed and I. Traore, 2014) presented a new approach for the free text analysis of keystrokes that combined monograph and digraph analysis. A neural network had been used to predict missing digraphs based on the relation between the monitored keystrokes. The heterogeneous experiment involved 53 users, the follow-up experiment in a homogeneous environment considered only 17volunteers. The results obtained from this research were promising with reduced error rates.

The use of keystroke dynamics for verification and identification has a long history and can be dated back to the 1970s. Since then, numerous template-matching and machine-learning algorithms have been reported to tackle the classification problem. These approaches can be broadly classified into four categories: statistical method based on distance metrics, neural networks, statistical machine-learning methods, and many other algorithms.

Sluganovi et al (I. Sluganovi, A. Karlovi, P. Bosilj, M.Šare, and S. Horvat, 2012) focused on building a system that would provide an additional authentication layer besides the standard password protection and successfully store the typing dynamics of various users passwords .The artificial neural network output was used to reach to the decision about the user's identity. The artificial neural network had been trained on samples of genuine user as well as impostor samples in order to learn how to distinguish between a genuine user and an intruder. For each user-password pair a separate neural network was constructed .An application for this purpose was implemented in C# for data collection purpose and live testing of the trained network, a MATLAB application was also developed to train the neural network and gather network performance data.

V. HOW IT WORKS?

The keystroke rhythms of a user are measured to develop a unique biometric template of the user's typing pattern for future authentication. With keystroke dynamics, the biometric template used to identify an individual is based on the typing pattern, the rhythm and the speed of typing on a keyboard. The raw measurements used for keystroke dynamics are dwell time and flight time.

- **Dwell time** is the time duration that a key is pressed
- **Flight time** is the time duration in between releasing a key and pressing the next key

When typing a series of characters, the time the subject needs to find the right key (flight time) and the time he holds down a key (dwell time) is specific to that subject, and can be calculated in such a way that it is independent of overall typing speed. The rhythm with which some sequences of characters are typed can be very person dependent. "). The recorded keystroke timing data is then processed through a unique neural algorithm, which determines a primary pattern for future comparison. Data needed to analyze keystroke dynamics is obtained by keystroke logging. Normally, all that is retained when logging a typing session is the sequence of characters corresponding to the order in which keys were pressed and timing information is discarded.

VI. SUITABILITY OF KEYSTROKE DYNAMICS

The behavioral biometrics such as keystroke dynamics is less reliable than physiological biometrics. We use the following 7 criteria to evaluate the suitability of keystroke dynamics:

1. Collectability- An important advantage of keystroke dynamics is that there is no special hardware needed as with other biometrics, a standard computer keyboard is sufficient.

2. Universality- This biometric solution can be used by all individuals that are able to use a keyboard.

 ISBN: 978-93-86171-59-7

3. Circumvention- It is certainly difficult, if not impossible to mimic another person's typing rhythm. Electronically capturing using keylogging software is possible, thus implementing this biometric solution requires that data security is guaranteed from the input (keyboard) to the matching algorithm.

4. Uniqueness- This biometric solution can be used by all individuals that are able to use a keyboard. Unlike physiological biometric factors, there can be no such thing as an absolute match with behavioral biometrics. Therefore it is difficult to discuss uniqueness of a typing pattern.

5. Permanence- A major problem with keystroke dynamics is that a subject's typing rhythm varies considerably in between days and even within the same day. There are numerous reasons for this: tiredness, switching computers / keyboards, mood, influence of alcohol and medications, etc.

6. Performance- Behavioral biometrics has higher variations because they depend on a lot of (external) factors such as ergonomics, fatigue, mood, etc. This causes higher FAR and FRR when compared to solutions based on a physiological biometric factor such as fingerprint recognition.

7. Advantages of Keystroke Dynamics

- The keystroke dynamics can be used by any person who knows how to use a keyboard
- Every individual type in a unique manner. Therefore typing pattern of two users cannot be same. Thus it provides more cyber security
- Compared to written signatures typing pattern cannot be reproduced. Most security systems allow limited number of incorrect attempts. After few incorrect attempts they block the account.
- Compared to physiological biometric systems such as fingerprint, Iris detection Keystroke dynamics does not require any extra hardware. Thus implementation and deployment cost is low.
- As long as user interacts with the computer system, keystroke pattern can be constantly monitored.

8. Applications of Keystroke Dynamics

Keystroke dynamics can be used for authentication, as well as Surveillance**.** Some of the Companies which develop software products applying keystroke dynamics are:

- Typing DNA built and AI engine able to match any two typing patterns with unprecedented accuracy. It's easy to use keystroke dynamics authentication API is suitable for securing logins, enforcing reset passwords, detecting intruders and online biometric authentication for user behaviour analytics, multifactor authentication, user identification, eLearning and fraud prevention. They also provide a continuous authentication app, for Windows and Mac, also based on keystroke dynamics.
- ID Control is a dutch company developing strong but affordable authentication solutions, some of which use keystroke dynamics. Their software integrates with MS Windows logon, Citrix, VPN and many others.
- BehavioSec is a swedish company specialized in continuous authentication systems, this is software which monitors activity on a computer to make sure that it is the genuine account owner who is using the computer. BehavioSec uses not only keystroke dynamics but also mouse dynamics and the general way in which the user interacts with the computer.

9. Problems with Keystroke Dynamics

- **Temporal** variation- One of the major problems that keystroke dynamics runs into is that a person's typing varies substantially during a day and between different days. People may get tired, or angry, or have a beer, or

 ISBN: 978-93-86171-59-7

switch computers, or move their keyboard tray to a new location, or use a virtual keyboard, or be pasting in information from another source (cut-and-paste), or from a voice-to-text converter. Because of these variations, any system will make false-positive and false-negative errors.

- **Legal and regulatory issues**- The use of key- logging software may be in direct and explicit violation of local laws. This could have severe penalties including jail time.

VII. CONCLUSIONS AND FUTURE WORK

User authentication is a major problem in gaining the access rights for computer resources. Keystroke dynamics is a behavioral biometric approach to enhance the computer access rights. It verifies the individual by its keystroke typing pattern. Keystroke biometric is based on the assumption that the typing pattern of each user is unique. Different methods such as neural network, pattern recognition algorithms, data mining techniques can be applied to analyze the keystroke patterns. Keystroke finds its applications in several crucial areas like online examinations, ATM, mobile phones

There are a number of challenges that need to be overcome in order for it to become an effective biometric. However, it has tremendous potential to grow in the area of cyber-security and remote monitoring since it is non-intrusive and a cost-effective biometric.