User Verification by Keystroke Dynamics

[1]Manisha Chaudhary, [2]Mr. Amit Arora
[1]Research Scholar, [2],Professor
[1]Electronics and Communication Engineering [2] Electronics and Communication Engineering
[1] Marudhar Engineering College, Bikaner, India.

Abstract: In the age of massive information transfer, security and privacy are primary concerns. The most commonly used security ensuring techniques are static passwords. The high vulnerability of these techniques have led to the development of biometric techniques for user authentication. Keystroke dynamics is a part of behavioral biometrics which identifies and verifies a user based on his/her typing patterns. The authentication by keystroke dynamics does not requires additional hardware for authentication and cannot be imitated or copied easily. The aim of this paper is to demonstrate a user verification system by using keystroke dynamics.

Index Terms – **User Verification, Behavioral biometrics, Key stroke dynamics.**

I. INTRODUCTION

In modern world security of personal data is very important. Many procedures have been designed to prevent the access of illegitimate user. Fig 1.1 shows the increasing number of identity theft in social media. In this project we have designed software which will do the same. In this project we have used a technique Known as keystroke dynamics. Keystroke dynamics is a process of verification of user based on his/her typing rhythm on keyboard. A user interface is created on devices for human interaction and based on his typing rhythm we verify if the user is legitimate or not.

This technique has added one step further in the field of user verification. The typing rhythm of every user is considered to be different so it can be used as parameter for verification. Earlier many techniques were used for user verification as given:-.

1. Based on Knowledge[2]:- It represent to something a user knows (like PIN) so in this technique we use the knowledge of the person to verify him/her. But as we know a user can forgot something so this process has disadvantage and it can be stolen as normally a person keel his name or birthday etc. as a password so it can be guessed and may be used in wrong way.
2. Token:- **:-** It is a kind of an object which a user carries physical with him/her for verification. ATM[3] is a very good example of this technique. But as the user carries it always with (him when he needs to verify him) then there is chance of theft so user may find it difficult to keep it safe all the time. Authentication RFID cards[4] and One Time Passwords(OTP)[5] also fall under this category.
3. Biometrics[4]:- It refers to some specific behavior or physiological characteristics that is uniquely associated to a person. The physiological biometrics refers to person's figure print[5], face[6], and iris[7]. These biometrics are very accurate in identifying a person. But as these are very costly to so it cannot be used everywhere.

Behavioral biometrics[8] are the way people speak, write, type, walk. This type of biometrics can be used to identify the person even without his knowledge or it can be used to identify even when a person is doing his work. As it is a behavior of a person so a person need not to do some extra work for his verification.

The authentication technology for Keystroke dynamics[9] can be protected from multiple assaults by password. With their typing pattern, this method is based on human behavior. Authentication is the method used to verify a user's identity as it generally happens in the initialization of the scheme, known as original authentication. A user's authentication includes three basic pieces of information about who you are, what you have and what you know If all this basic data becomes right and only users are admitted to the scheme.

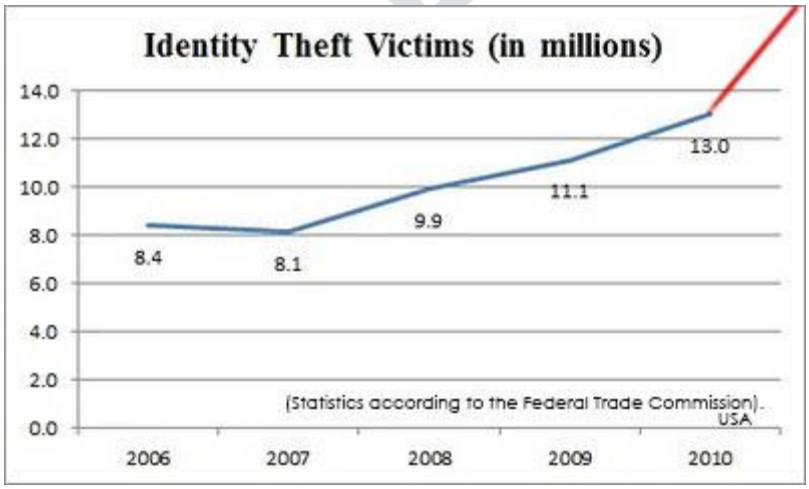

Fig 1.1 Increasing rate of identity theft[1]

II. RESEARCH METHODOLOGY

The proposed research methodology can be categorized into three sub routines namely ; User Interfacing , Backend processing and User Verification. The details of these subroutines are discussed below:

1. **User interfacing**: In this subroutine the participants or the users who are authorized for the application are given training. The above image shows the user interface which is used for training and data collection. In the interface user is given option to enter his/her name (Textbox) and then he/she is asked to type a keyword "WORK HARD" in the subsequent text box. Then save file button is pressed. Then the user interface will open again the user have option to type as many session as he/she want and when he wants to see the results a option to close(Close Button) the file is given. And then file will be closed and another dialogue box will open in which user will be verified.
2. **Backend Processing**:- When the user typed the given Keyword in first text box at the backend the dwell time and flight time of every characters is extracted. And corresponding to each user we stored the dwell time and flight time in a excel file. Dwell time and Flight time are the features of keystroke dynamics and are related to latency incurred in key press and release events. Dwell time is defined as the duration for which a particular key is pressed by the user. Flight time is defined as the time from releasing the previous key and reaching the next key.

The dwell time and flight time are unique for every user and forms a part of their behavioral biometrics. In our approach dwell time and flight time between each character is extracted. Thus the user profile consists of 9 features of dwell time and 8 flight time. This data is stored along with the user name.

3. **User Verification**: This is the testing phase of our proposed algorithm. The form shown in Fig 2.2 is used for user verification. The user will type the same keyword WORK HARD and click on processing button and then click on output button to see if the user is legitimate. A textbox has been used in which the name of the identified user will be printed.

When the user types the pre-defined string the subsequent features as mentioned in section 2.2 are extracted. These features are compared with the features present in training database by Euclidian distance. A user is said to be identified if the Euclidian distance between the test and train samples is less than twenty percent.

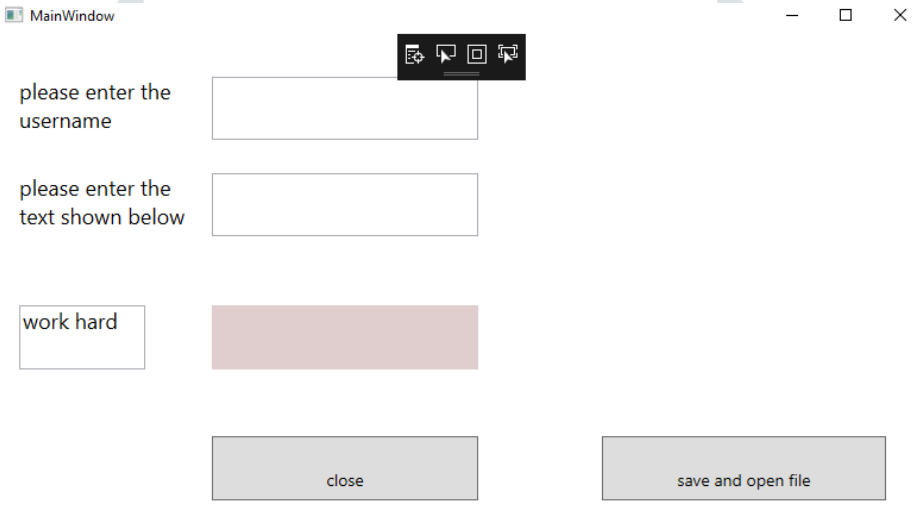

Fig 2.1 :Form for user interfacing

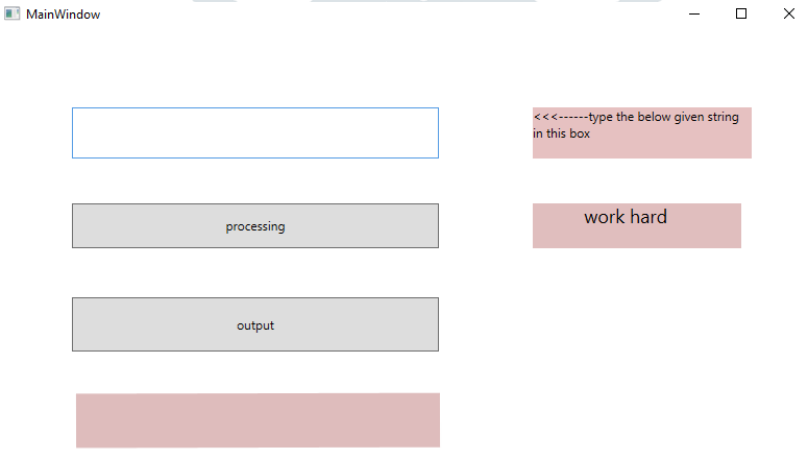

Fig 2.2 Form for user verification

III. RESULT AND DISCUSSION

Based on the above training data we tested the software almost 20 times and in various session and we found legitimate user up to 17 times . So we found the verification accuracy of the proposed system is 85%.

IV. CONCLUSION

User verification system using keystroke dynamics was successfully demonstrated. The features used in the keystroke dynamics are dwell time and flight time. It can be concluded that the developed system shows good accuracy even with limited datasets.The proposed approach is a effective and user convenient way of preventing security breaches.

V. FUTURE SCOPE

In future more the amount of the participants and the number of features extracted can be increased to improve the efficiency of the proposed algorithim. The efficiency can be further improved by integrating the proposed approach with machine learning algorithims.

REFERENCES

[1] A.J. Bernheim Brush, Bongshin Lee, Ratul Mahajan, Sharad Agarwal, Stefan Saroiu, Colin Dixon, "Home Automation in the Wild: Challenges and Opportunities", May 7–12, 2011.

[2] R. Khan, R. Hasan and J. Xu, "SEPIA: Secure-PIN-Authentication-as-a-Service for ATM Using Mobile and Wearable Devices," *2015 3rd IEEE International Conference on Mobile Cloud Computing, Services, and Engineering*, San Francisco, CA, 2015, pp. 41-50.

[3] B. M. Nelligani, N. V. U. Reddy and N. Awasti, "Smart ATM security system using FPR, GSM, GPS," *2016 International Conference on Inventive Computation Technologies (ICICT)*, Coimbatore, 2016, pp. 1-5.

[4] M. Sidorov, M. T. Ong, R. V. Sridharan, J. Nakamura, R. Ohmura and J. H. Khor, "Ultralightweight Mutual Authentication RFID Protocol for Blockchain Enabled Supply Chains," in *IEEE Access*, vol. 7, pp. 7273-7285, 2019.

[5] TZ. Khalid, P. Paul, S. P. Chattopadhyay and A. N. Biswas, "Secure authentication with dynamic password," *2016 IEEE 7th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)*, Vancouver, BC, 2016, pp. 1-7.

[6] D. Bhattacharyya, R. Ranjan, P. Das, T. Kim and S. K. Bandyopadhyay, "Biometric Authentication Techniques and its Future Possibilities," *2009 Second International Conference on Computer and Electrical Engineering*, Dubai, 2009, pp. 652-655.

[7] G. Aguilar, G. Sanchez, K. Toscano, M. Salinas, M. Nakano and H. Perez, "Fingerprint Recognition," *Second International Conference on Internet Monitoring and Protection (ICIMP 2007)*, San Jose, CA, 2007, pp. 32-32.

[8] N. K. Gondhi and E. N. Kour, "A comparative analysis on various face recognition techniques," *2017 International Conference on Intelligent Computing and Control Systems (ICICCS)*, Madurai, 2017, pp. 8-13.

[9] M. Trokielewicz, A. Czajka and P. Maciejewicz, "Iris Recognition After Death," in *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 6, pp. 1501-1514, June 2019.

[10] I. Deutschmann, P. Nordström and L. Nilsson, "Continuous Authentication Using Behavioral Biometrics," in *IT Professional*, vol. 15, no. 4, pp. 12-15, July-Aug. 2013.

.