User Authentication By using Advanced Key Stroke Recognition

Deepika Sharma
Department Of Computer Science
M.Tech
Urvashi Garg
Lovely Professional University
Jalandhar, India

***Abstract*— As Today the most important issue is to provide the security to individuals account access or any other computer access. Mostly security required where password facility is available. Username password is best mechanism for providing user authentication. This paper is based on technique called key stroke recognition for providing user authentication. Key stroke is a biometric characteristic by using which we stop the hackers or imposters to enter into the secured system. It is based on user's typing speed. in this paper the various features of key strokes are considered like key hold time, inter time, ASCII code to detect the use of caps lock, detection of backspace and shift, total time of typing, up and up time and so on. Firstly all these features are calculated when authorized user enter the password and stored in database. When again someone type the password to enter into account then all the above said features are calculated again for this new user and compared them with stored values of trusted users by finding Euclidian distance and token system is used to check whether this user is valid or not. if the distance is according to limit which is set then user is allowed to enter into system .otherwise ,he/she will be considered as imposters**

Keywords*—— *keystroke recognition, authentication, biometrics characteristics, pattern analysis

I. INTRODUCTION

Biometric characteristics are of two type: first one is physiological characteristics that include face, fingerprints, iris, pattern analysis and second characteristic is behavioral characteristics that include handwriting, Keystroke dynamics, gait. In this paper the Keystroke dynamics feature is used to provide user authentication. With increase in technology the use of computer in every field is also increased. As the demand of computer increases day by day, the security issue is also arises. Everyone wants that there system , personal accounts are secured from hackers or imposter like in online banking. to make the system secure various username password facility is provided to each user. but now a days the passwords are also hacked by imposters so all this required a technique that can protect the system from unauthorized user. key stroke recognition is the technique used to protect the system by permitting imposters to enter into system. The system based on keystroke dynamics captured various time durations of key press and key release. these systems are totally based on the typing speed of users. It is data processing technique used to analyses the way of user typing. This technique works by integrating the keystrokes features in existing password and record all the features for original user and store into database and if any imposter unfortunately get login information ,he/she try to login into the system with this login information then our keystroke recognition system denied their access by comparing all features with existing features. The advantage of using keystroke recognition system is that it is cheapest method as it does not require any additional hardware. In this system user has to fill password, when he presses the key all keystroke features are recorded and compared with previously recorded features and then user is allowed to enter into system. All these features help us to distinguish between the different users.

This paper is organized as: section II describes the background study, section III describes Literature survey, section IV explain Conclusion from literature survey and the work which we further continue in our research.

II. BACKGROUND STUDY

In 1990 Joyce and Gupta [7] showed that keystroke method is used to analyze the identity of person. many approaches are available some are simple and some are complex. Some researchers used false rejection rate and give results in acceptance level. Some of them uses key vibration as a basics feature to identify users. Young and Hammon are the researchers that use key stroke pressure as a feature to identify user and deny the access of imposters. but this is most expensive feature as it required special keyboard available in market which is able to calculate the pressure of pressed key. On the basis of this pressure the system distinguished between different users and provides the access to correct user. In one research paper there is one interesting feature is using camera to calculate the pattern for typing. but all these features are expensive one. The simplest feature among all of these is calculating various timing like hold time, total time.

III. LITERATURE SURVEY

In [1] by Yogesh Meena and Urvashi Garg they continued the previous work of [6].They proposed a technique by using keystroke for providing User authentication. For this they used inter time, key hold time and also some other features to find the authorized user. When user starts type the password ,its inter time and key hold time were calculated as well as then compared with the actual values stored in database using Euclidian distance and token system is used to conclude whether the user is valid or not. They succeed in reaching type 2 errors as 0% but type 1 error 30%. Where type 2 error states that unauthorized user is allowed to use resources and type 1 error states that legitimate user is not verified and hi is not able to access his account.

Features used in this paper are:

- Inter time
- Key hold time
- Key type change time
- Number of Backspaces
- Number of Caps
- Number of Shifts

Result of this paper is by using all these attributes they make type 2 error 0% but type 1 error 30% only.

However this can be further improved by minimizing type 1 error and makes its accuracy levels more high.

In [2] by Pin Shen Teh, Shigang Yue and Andrew B.J, Teoh they provide Keystroke Dynamics by using fusion approach. Firstly four types of features are measured on collected data and then changed into similarity scores by using Gaussian Probability density Function and Direction Similarity Measure.

Features used:

- Dwell Time (D1)
- Flight way (D2)
- Pressure of Keystroke
- Sound of Typing
- Difficulty of typing Phrase
- Typing Rate
- Linguistic style
- Frequency Errors

Methodology used:

A. Matching

- Gaussian Probability density Function
- Direction Similarity Measure

B. Fusion approach

- Single Layer Single Expert
- Single Layer Multiple Expert
- Multiple Layer Multiple Expert

Finally **result** of paper represents that combination of proposed fusion method and keystroke features are able to obtain reliable result of 1% of EER.

But there is also some ***cons*** included that not all of the features are reliable. As in order to use keystroke Pressure Feature a separate pressure sensitive Keyboard is required that contradicts the main advantage of Biometrics. Frequency of word errors, difficulty of typing phrase, typing rate are rarely practical as well as there is concern of noise in recording sound of typing.

In [3] by Robert Moskovitch,Clint Feher,Arik Messerman, Niklas Kirschnick, Tarik Mustafic, Ahmet camtepe, Bernhard lohlein,Ulrich Heister,Sebastian Moller, Lior Rokach and Yuval Elovici
They discuss the problem of identity theft and provide the solution for that.

- Features included:
- Key Press Duration
- Relative Key Event Order
- Relative Key Stroke Speed
- Classes of Shift Key
- Mouse Dynamics

Methodology Used:

A. Feature acquisition

B. Feature extraction

C. Classifier

D. Signature Database

By proposing four new metrics and using statistical approach on these metrics they were able to analyze keystrokes of 14 characters long for each user. After that analyses the similarity metrics for generating decision table. With all these things they reached at 97% of accuracy in results.

In [4], the new feature called Virtual Key Force is introduced along with commonly extracted timing features. The features are normalized using Z score method

Features are:

- Dwell time
- Flight time
- Latencies
- Digraph
- Virtual key force

Methodology used:

The entire methodology divided into three phases namely *feature extraction phase, normalization phase, feature subset selection* . For feature subset selection *Wrapper based approach Ant colony optimization- Extreme Learning Machine with analytic network process (ACO-ELM-ANP)* *and Genetic algorithm Extreme Learning Machine with analytic network process (GA-ELM-ANP) are proposed*

From the result of the paper it is observed as *ACO-ELM-ANP* selects less number of features for further processing. In this paper Type 1 error decreases if number of selected features increases.

In [5], they analyzed four features and performed seven experiments by combining these features. The result of experiment is was measured by three types of users namely imposters, legitimate user and observer imposter users

Features used:

- Key code
- Two keystroke latencies
- Key duration

Their approach is when user trying to access a system he indicates an account and types the target string. While user types the string, keystroke data is captured and sample is created and then this sample will be analyzed through classifier that either it belongs to its owner or not.

Result of this paper shown that type 2 error is 1.89% and type 1 error is 1.45%

IV. CONCLUSION FROM LITERATURE SURVEY

From all literature survey we have seen that Type 1 error i.e. sometime authorized user is not verified and he/she is not allowed to access resource, is not completely removed.

So my research work is to add additional features in [1] to increase accuracy rate and to remove or minimize Type 1 error which is 30% in this paper.

For this purpose we used some additional features to remove errors of previous paper and continued the work of [1]. So new Features or metrics are trying to involved in order to remove the type 1 error.

Keystroke features are:

- *Key hold time*: duration of time when one key is pressed and then released is called key hold time or dwell time.

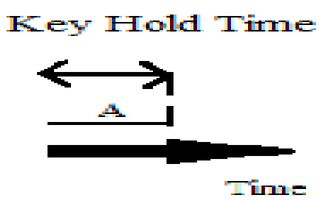

Fig 1. Key hold time

- *Key inter time*: time taken between one key is released and other is pressed.

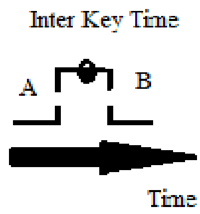

Fig 2. Inter key time

- *Up and up time*: the duration of time taken between one key is released and other key is released.

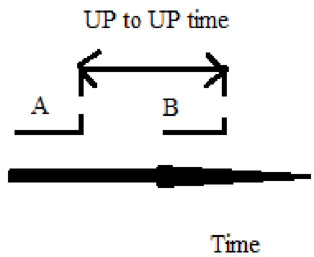

Fig 3. Up to Up tme

- *Total time*: It is the total time taken by user to type the whole password.
- *Use of ASCII code*: to detect whether it is alphabet or numeric key we take help of ASCII code and also detect the use of caps lock.
- *Detection of shift key:* this feature is used to detect when shift is pressed or how many time it is pressed.
- *Use of backspace key*: this feature is used to detect when shift is pressed or how many time it is pressed.
- *Key pressed and Key released time*

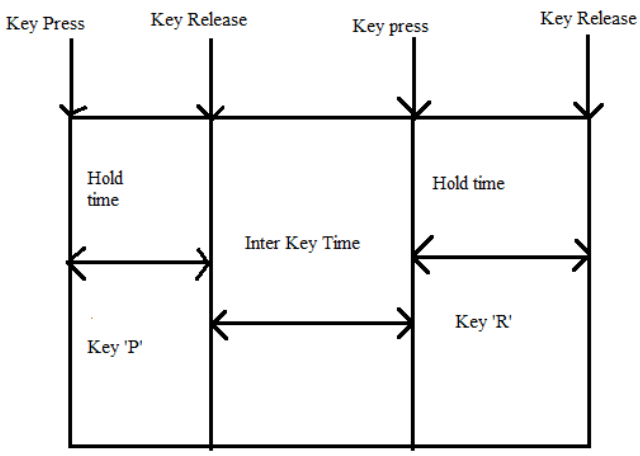

Fig 4. Explaining all key values

REFERENCES

[1] Yogesh Meena and Urvashi Garg, "User authentication using keystroke recognition,"

[2] Pin Shen Teh, Shigang yue and Andrew B.J. Teoh, "Feature fusion approach on keystroke dynamics efficiency enhancement," International

Journal of cyber- security and digital forensics,the society of digital information and wireless communication,2012

[3] Robert Moskovitch,Clint Feher,Arik Messerman, Niklas Kirschnick, Tarik Mustafic, Ahmet camtepe, Bernhard lohlein,Ulrich Heister,Sebastian Moller, Lior Rokach, and Yuval Elovici, "Identity theft,computer and behavioral biometrics,"

[4] D.Shanmugapriya and Dr.G.Padmavathi, "A wrapper based feature subset selection using ACO-ELM-ANP and GA-ELM-ANP approaches for keystroke dynamic authentication*,"* International Conference on Signal Processing,image processing and pattern 2013

[5] Lívia C. F. Araújo, Luiz H. R. Sucupira Jr., Miguel G. Lizárraga,

Lee L. Ling and João B. T. Yabu-Uti , " User authentication through typing biometrics features," in IEEE transaction on signal processing, vol.53,no.2,feburary 2005

[6] Mariusz Rybink and Piotr Panasiuk, "User authentication with keystroke dynamics using fied text,"conference on biometrics and kansei engineering 2009

[7] Rick Joyce and Gopal Gupta, "Identity authentication based on keystroke latencies," communications of ACM,1990

[8] J. R. Young and R. W. Hammon. *Method, "*Apparatusfor

verifying an individual's identity," United States Patent US

4,805,222, February 14, 1989.

[9] Shimon modi ,Dr. stephen J.Elliott, "Keystroke dynamics verifications using a spontaneously generated password" in IEEE 2006