International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 05 Issue: 04 | Apr-2018 www.irjet.net p-ISSN: 2395-0072

KEYSTROKE DYNAMICS FOR USER AUTHENTICATION

Priyanka Namnaik[1], Rajeshree Kurale[2], Sanyukta Mahindrakar[3]

[1,2,3]*Department of Information technology, Shah and Anchor Kutchhi Engineering College*

***Abstract*—** In this paper, authentication method is based on keystroke along with the current username and password system. a multifactor authentication scheme using the keystroke dynamics. The scheme is composed of two keystroke patterns levels. In this first level, the speed of each user's password is measured depending on the comparisons between the registered speeds with different calculated thresholds. In the case of large deviations in the typing speeds, the user must transit to the second authentication level. In this level, the user decrypts ciphered thresholds by using his/her private key. The objective of this paper is to provide a strong authentication method and to assign a high accepted value of the typing speed by training the user to type his/her password 100 times as a pretext before the actual registration level . In this case, the system results in a high precise speed values. The system is analyzed using different statistical measurements.

Keywords: Security, Authentication, keystroke, typing speed.

I. INTRODUCTION

One of the important challenges in user authentication is security and privacy. Furthermore, authentication plays an important role in preserving security and privacy of applications, data or resources, especially, in wide spread networks, internet, cloud services and even standalone desktop applications. It is use for protect shared data from unauthorized persons. In other words, an authentication mechanism determines how user is identified and verified to gain access.

Verification of user's identity is the most important goal of authentication [2]. Passwords are adopted as the most widely used security mechanism. It is obvious that, passwords (something the user knows) are not a very secure mechanism for authenticating users because of its limitation, as well as, it is difficult to confirm that the demand is from the rightful owner. Strong method of authentication should cover one or several factors of identification to improve security. Keystroke dynamics is the process of analyzing and measuring the style in which any user types the elements of his/her secret information by the keyboard. This process is either done at either during a complete session, which is called continuous keystroke dynamics or during login time or after a predetermined period of time which is called static keystroke dynamics.

There are 3 main step in keystroke dynamic : data collection, feature extraction and pattern classification. In data collection, raw data is collected and the registered to include all typed keys, related timing information and key events (press or down key, and release or up key) in profile.

Feature extraction:

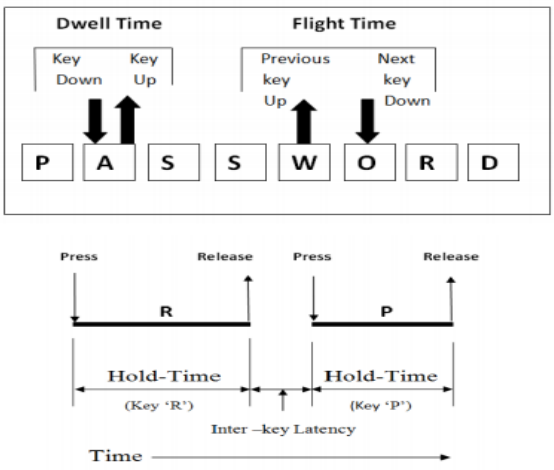

Fig 1.Dwell time and Flight time

There are several keystroke features, but some of the essential features extracted by researchers are :

- **Session time** is the total time spent by the user on the system. Session time is calculated by computing the difference between the starting time and user response times.
- **Keystroke latency** is the time interval between the key release of the first keystroke and the key press of the second keystroke. However, the latency of longer n-graphs (n > 2) is defined as the time interval between the down key events of the first and last keystrokes that make up the n-graph.
- **Dwell Time** is the time (in milliseconds) between a key press and a key release of the same key.
- **Frequency of error** is the use of backspace key and delete key. This rate may provide evidence of a state of confusion, as individuals who tend to delete are more likely to be confused.

II. PROPOSED SYSTEM

A. Overview

This section presents the proposed method in for user authentication using keystroke dynamics. There are different parameters for measuring keystrokes of application users; keystroke duration is considered as an attribute to measure keystrokes of uses. As shown in fig. 3.1, this method

is multi-factor authentication. It uses username/ password as well as keystrokes authentication to identify users.

B. New User Registration:

The process is shown in fig. 3.1 for the registration of the first time user. User has to set the username and password along with a long Sample Text already presented to the user. The username – password binding will be stored in the database. Also, the Dwell Time and Flight Time of the password entered will also be stored. The password, keystroke dynamics (dwell time and flight time) of the password and the sample text will be used for authentication of the user later.

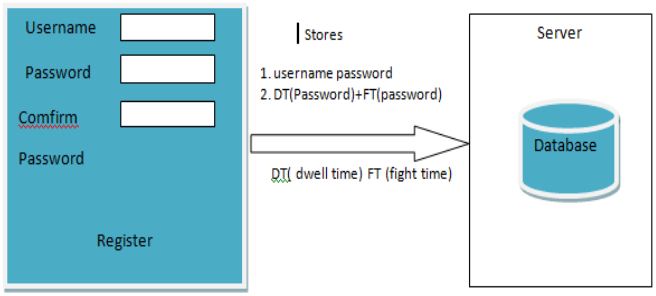

Fig B: New User Registration

C. User Login Procedure:

When a user wants to login to the system, he needs to enter the username and password which will be checked by the system. Apart from this, the system will also calculate the values of the keystroke dynamics of the entered password and will compare it with the ones stored in the database. If the match is within an acceptable limit then the second level of authentication is done. For the third level of authentication, the user has to type a phrase displayed on the screen in a window which will be a random challenge to the user. The keystroke dynamics of this challenge will be compared with that of stored values of the Sample Text from the Registration phase.

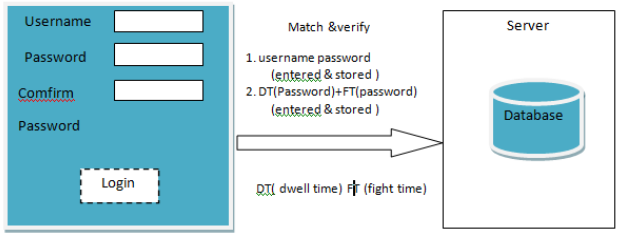

Fig C: User Login Procedure

III IMPLEMENTATION DETAILS

1. Registration Module:

a. Enter Username: It is checked in the username module and if username already exists, user has to change its username and register with a username which is available.

b. Enter Password: After entering a unique username, user is supposed to enter his choice of password and the password is encrypted and stored in a module known as password module and along with password it also stores the factors (flight time, dwell time and total time taken to enter the password) of keystroke authentication.

c. Registration: A registration module is created which links to various modules that are username, password.

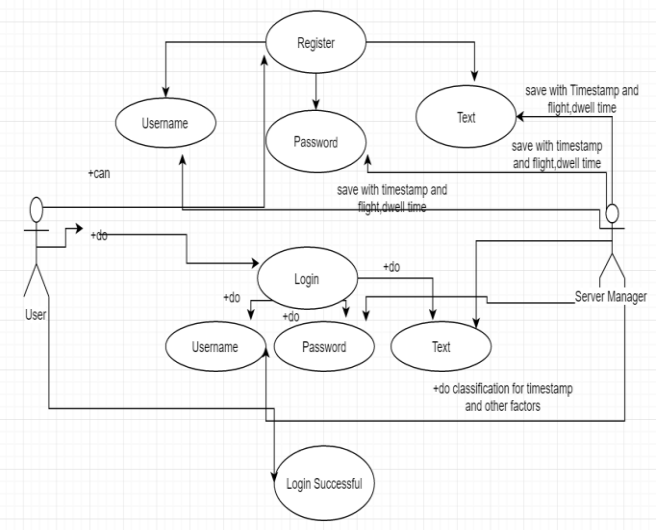

Fig 3:Registration Procedure

2. Login Phase

a. User enters his username and password: Username and password are matched with username and password module, if username matches, corresponding password is checked and if it matches the biometric factors of keystroke authentication stored in module, it proceeds to next step of login. In order to match the factors, we need to temporarily store the flight time, dwell time and total time when user enters his password during login in the login module.

b. If all factors and details match, login is successful.

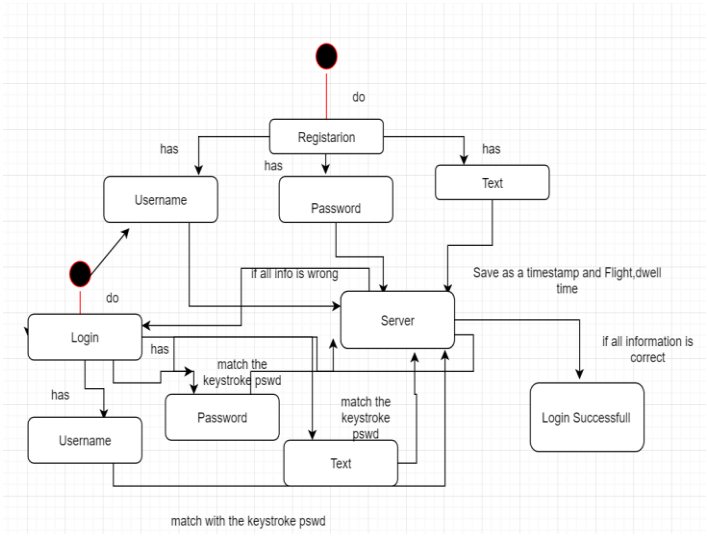

Fig 2:Login Procedure

HARDWARE AND SOFTWARE SPECIFICATIONS

Hardware Specification:

Processor : Any Processor above 1.9GHz.

RAM : 2 GB.

Hard Disk : 10 GB.

Input device : Standard Keyboard and Mouse.

Output device : VGA and High Resolution Monitor.

Software Specification:

Operating System : Windows7

Language : Java

Database : MySQL 5.0 & Above

Tool : JDK 1.5 & Above, Eclipse IDE

IV. ALGORITHM

Various features to be extracted to implement the algorithm is calculated using following equations:

- **Session time =** Starting time – User response time
- **Flight time =** ∑Releasing time of key 1 – ∑pressing time of key 2
- **Dwell time =** ∑Releasing time of key – ∑pressing time of same key.
- **Keystroke latency** = ∑Releasing time of key 1 – ∑pressing time of key 2 per sentence.

.

After the feature extraction and feature selection phase, the next phase is the classification phase where the matching between the template stored and sample provided during the session takes place. There are various methods used for classification. These classification algorithms are pattern reorganization based algorithms and decision tree.

V. PAGE DESIGN OF THE PROPOSED AUTHENTICATION MODULE

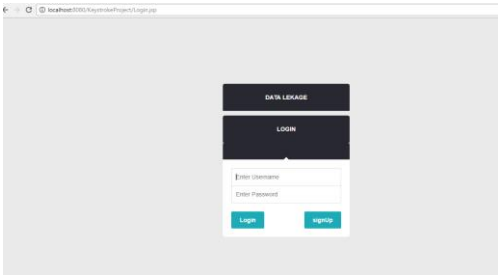

Fig 4.1 sign up page of the proposed authentication module

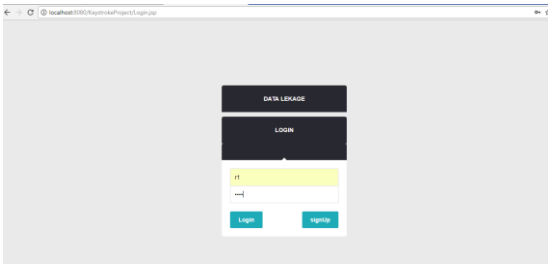

Fig4.2 login page of the proposed authentication module

VI.SCOPE

The password based authentication system is used almost everywhere. With this we can comfortably used Keystroke based authentication as the keyboard is already present, either physical or virtual. Any other factor may require additional hardware like smart card reader or biometric sensors. This flexibility provides an advantage to deploy this mechanism virtually anywhere wherever authentication is required.

VII. CONCLUSION

The keystroke and mouse features are combined and provides a high level security using keystroke parameters called as dwell and flight time. These keystroke parameters to provide high level of security. The combination of dwell and flight time with single click shows better results. The accuracy of combination of keystroke and mouse authentication shows more than 85%. The future scope includes the identification of other parameters and the use of another algorithm to improvise the level of security and implementation of keystroke on touch screen system (LAPTOP) and use of pressure keyboard.

REFERENCES

1. Gil David, Anomaly detection approach to keystroke Dynamics Based User Authentication,2017,ISCC..

2. Sahurdi, Novianto Badi Kurniawan , Keystroke Dynamics for authentication using dynamics time warping, 2016, Jaka Sembiring School of Electrical Engineering & Informatics, Bandung, Indonesia.

3. Jordan Amman,Analysis of Strong Password Using Keystroke Dynamics Authentication in Touch Screen Devices, 2016, Cybersecurity and Cyberforensics Conference.

4. yaw marfo missah ,keystroke dyanamic as an additional security measured to passwaord security on web based application ,2016