Authenticate User by Keystroke Dynamics

Nandini Chourasia
ME Student, Department Of Computer
MIT COE, Kothrud
Pune, India

Prof. Dr. Prasanna Joeg
H.O.D. Department of computer
MIT COE, Kothrud
Pune, India

Abstract—: **In the past few year the number of internet users are increasing exponentially, so the amount of data over internet is also increasing. As the data is increasing unfortunately the attacks on that data are also increasing. So to protect that data from misuse we need to authenticate the user. As the every authorized user has their own username and password for verification and to access their accounts, for more authentications we need an extra step. So the keystroke dynamics is being used to improve authentication process and help to increase security for data. In this paper, we look at several processes for keystroke to enhance user authentication. Our objective is to collect a keystroke-dynamics dataset, to develop a table for evaluation of typing pattern, and to measure the threshold and according to the variation of that threshold, results can be detected that the user is authorized or not. All the four key latencies and dwell time is used for making data set. That dataset is used to calculate degree of variance of the user and to detect the authorization of the user.**

Keywords— *keystroke dynamics, false rejection rate, false acceptance rate, virtual key force, metric proposal, partial access full access, no access.*

I. INTRODUCTION

Now-a-days the use of technology is increasing at very high rate. Every individual depends mostly on internet, and user their confidential information over the internet . Therefore more security on authentication of the user is required.[1] Once the login details have been exposed to a illegal user they have complete access to the system in a transparent manner and can easy access the authorized user's account, and can misuse those information such things may result in direct financial loss and information security leaks.[2]

Authentication is the process to prevents the unauthorized access over the account of authorized user by verifying the claimed identity.[7].User authentication is classified in three classes: knowledge based authentication, object or token based authentication and biometric based authentication.

Fig 1 shows the various users' authentication processes i.e. knowledge based, object based and biometric based.

- The knowledge based authentication refers to what the user is already aware for accessing their personal account i.e. password or PIN.
- The object or token based refer to what the user posses i.e. ID-card, token.
- Biometric based depends on the behavioral and physiological characteristic of the user i.e. figure prints, keystroke dynamics.[1][7].

Currently, there are two major forms of biometrics first those based on physiological attributes and second those based on behavioral attributes.

Physiological biometrics integrate a measurement of some physiological feature such as validation of user from fingerprints, retinal blood vessel patterns detection and iris patterns detection into an automated authentication schema such type of biometric is also known as static biometrics.

Behavioral biometrics extract and integrate information about human behavior such as variations in our speech pattern, signature and the way we type into the authentication, and is also known as non static biometric. So to enhance computer security biometric is used [2][5][7].

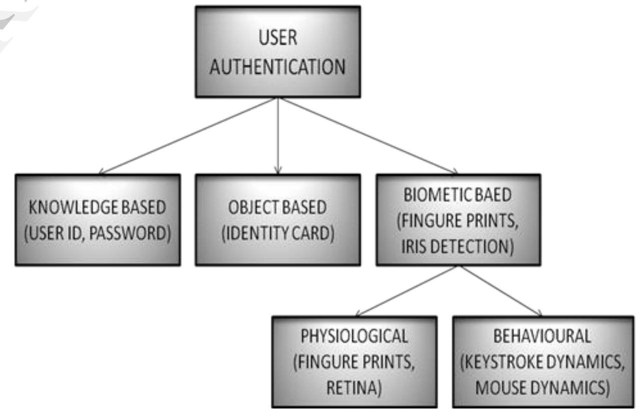
USER AUTHENTICATION
KNOWLEDGE BASED (USER ID, PASSWORD)
OBJECT BASED (IDENTITY CARD)
BIOMETIC BAED (FINGURE PRINTS, IRIS DETECTION)
PHYSIOLOGICAL (FINGURE PRINTS, RETINA)
BEHAVIOURAL (KEYSTROKE DYNAMICS, MOUSE DYNAMICS)

Fig: 1 User Authentication Processes

Keystroke dynamics-refers to the art and science of recognizing an individual based on the analysis of typing patterns of the user. Typing pattern includes such factors as the time user takes to type the login ID and password, how long user take to depress a key and how long user take to type successive keys [5].To provide security key stroke dynamics is being used. User access to the systems is secured through possession of a login ID and password.

II. Related Work

A. *KEYSTROKE DYNAMICS*

Key stroke dynamics define as the process of analyzing the user by the typing pattern of the user and by monitoring the keyboard input patterns and identify the user by their habitual typing pattern. Keystroke dynamics refer to the typing pattern and behavior of the user it distinguish the user on the bases of the key press duration, typing rate, typing pressure. Keystroke dynamics is a form of digital verification of the user [3][10].

Keystroke dynamics or typing dynamics refers to the automated method of identifying identity of an individual based on the manner and the rhythm of the typing of the user. **Keystroke dynamics** is behavioral biometric, this means it is based on what he user do.

As this process is used for the authentication of the user it is having some advantages as well as disadvantages.

ADVANTAGES

a)Uniqueness

Keystroke event measure up to nanoseconds. So it is very difficult to copy typing pattern of an individual at such high accuracy [2].

b)Low Implementation and Deployment Cost

Traditionally physiological biometric is use for authentication of the users i.e. fingure prints recognization etc. For implementation of physiological biometrics extra hardware is required which reqiued extra cost. But keystroke dynamics doesn't depend on the hardware, only software is required for implementation[1].

c)Transparency

In many situation the user doesn't know that they are provided with an extra layer of authentication. This simplicity is useful for the user who is not having the technical knowledge[6].

d) Universality

Keystroke dynamic biometric is used by all individuals that are able to use a keyboard in Smartphone or computer's virtual key board.

e) Circumvention

It is very difficult, and is impossible to copy another individual's typing patterns. Keystroke dynamics is a process of electronically capturing user typing patterns and the keys that user uses while typing and the pattern of users' typing, thus implementing this biometric solution requires that data security is guaranteed from the input (keyboard) to the matching algorithm.

DISADVANTAGES

a)Low Accuracy

Keystroke dynamic authenticate the user by the typing rhythm of the user, but if any external injury cause to the user due to which the typing rhythm of the user don't match then the system will not accept the authenticate user also[1].

b) Performance

Behavioral biometrics has higher variations because they depend on factors such as tiredness, mood, etc. This causes higher False Acceptance Rate and False Rejection Rate.

B. *FEATURES OF KEYSTROKE DYNAMICS*

Keystroke dynamics have several different feature to detect authenticate user.

- Latency between two key stroke
- Duration of keystroke, hold time
- Overall typing speed
- Frequency of errors
- Force of hitting key while typing
- Which shift key is used by the user more frequently
- Which key is first released shift or another key?

The most commonly used feature of keystroke dynamics is latency and duration. Fig2 is showing the latencies and dwell time. Here the word 'ADMIN' is taken as an example for explaining more specifically the latencies and dwell time.

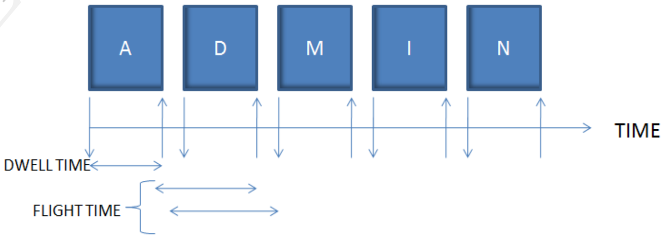

Fig2. Keystroke latency and Dwell time

1) *Latency or Flight Time*

Latency in keystroke dynamics is calculated with key press (P) and key release(R) i.e. P1 is pressing first key, P2 is pressing second key,R1 is releasing first key,R2 is releasing second key. There are four types of latencies for keystroke dynamics L1, L2, L3 and L4 where L1 is press-press, L2 is release-press, L3 is press release and L4 is release.

- PRESS-PRESS: it is the time between two key presses.
  L1=P1-P2
- RELEASE-PRESS: it is the time interval between first key release and second key press.
  L2= R1-P2
- PRESS - RELEASE: it is the time interval of second key press and first key release.
  L3= P2-R1

- RELEASE- RELEASE: it is the time interval between two key releases.
  L4= R1-R2

The above are the four latency that is considered by the user while typing, and used to calculate the typing pattern of the user.[1][2][6]

2) Duration or Dwell Time:

Dwell time (D1) is the time taken by the user in pressing and releasing of the single key [7]. Figure 2 illustrates the key press duration and latency of key press.
D1=P1-R1

The most commonly adapted metrics to evaluate the authentication of the user are false acceptance rate (FAR) and false rejection rate (FRR) [2][6]. The false rejection rate refer to rate the legitimate user is denied access and the false acceptance rate is denoted as the rate illegal user is given access [6]. For this the data sample of the user are collected irrespective of the backspace, delete key usage. Then key press, key release and relative keystroke speed is calculated. And the metrics are made on both the features i.e. FRR and FAR. The main advantage of this feature is the more trials taken from user gives more accurate results [11].

Now the keystroke dynamics have become an active research due to increase of the unauthorized access. To improve the accuracy of the keystroke virtual key forces feature is used, as compared to other feature of keystroke virtual key force is new; the virtual key force is based on the typing speed and behavior of the user on the keyboard. It measures the time taken by the user between releasing one key and pressing another key. Virtual key force is determined from the key complexity. The key complexity is calculated by key position and key distance. Based on the key complexity the average time interval of releasing a key and pressing another key is calculated [7].

Basically keystroke dynamics is used for authentication on mobile phones. This application is developed for the Android OS with SDK14. It focuses on both the scenario first on alphabets and second is on numeric on different type of keyboard layout [4].

However keystroke dynamics is suitable method for the user authentication based on user typing pattern and difference between the typing styles of the user [10].

III. IMPLIMENTATION

The proposed model is divided into two phases. In first phase the user has to complete their login process and in second phase the user is authenticated by using keystroke dynamics is performed.

In first phase the verification of the user is done, the user have to input their user ID and password. The user ID and password of the user are verified, if it is true then it will process else the user have to again input their user ID and password.

In another phase the authentication of the valid user is done. Here the typing pattern and the typing speed of the user is match from the threshold that is present in the database.

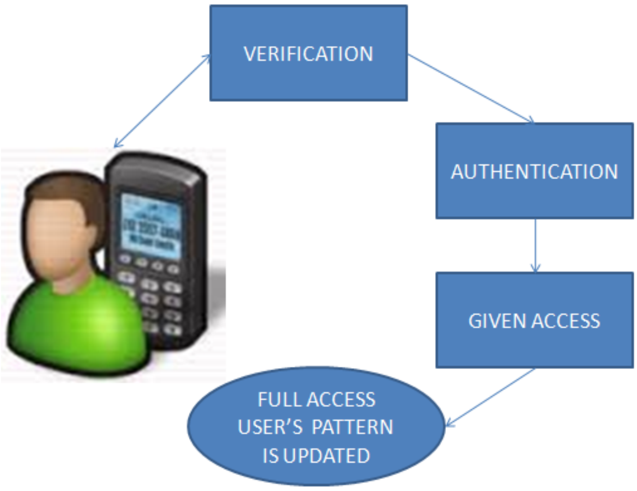

Figure3: Implementation Design

According to the degree of variance from the threshold value the access to the user is provided. The user whose degree of variance is very low from threshold value given full access and the typing pattern and speed of the user is updated in the table for further authentications, the user whose variance is above threshold given no access and the user whose variance is within the threshold have given partial access and no updated is performed for no access and partial access user on the table. Full access user and no access user is give access to the account, where as no access user is not given any access to the user.

A. DATA FLOW

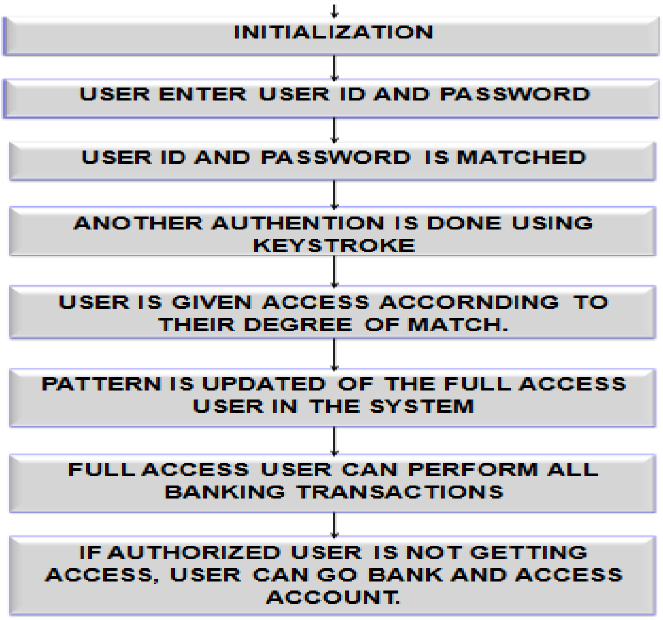
INITIALIZATION
USER ENTER USER ID AND PASSWORD
USER ID AND PASSWORD IS MATCHED
ANOTHER AUTHENTION IS DONE USING KEYSTROKE
USER IS GIVEN ACCESS ACCORNDING TO THEIR DEGREE OF MATCH.
PATTERN IS UPDATED OF THE FULL ACCESS USER IN THE SYSTEM
FULL ACCESS USER CAN PERFORM ALL BANKING TRANSACTIONS
IF AUTHORIZED USER IS NOT GETTING ACCESS, USER CAN GO BANK AND ACCESS ACCOUNT.

Figure4: Data Flow Diagram

The above figure shows that the way data flow in the proposed system.

As the user initializes the process user have to enter user ID and password, if password is matched then authentication is performed using keystroke dynamics. According to the degree of variation the access is provided to the user.

B. Steps Of Implimentation

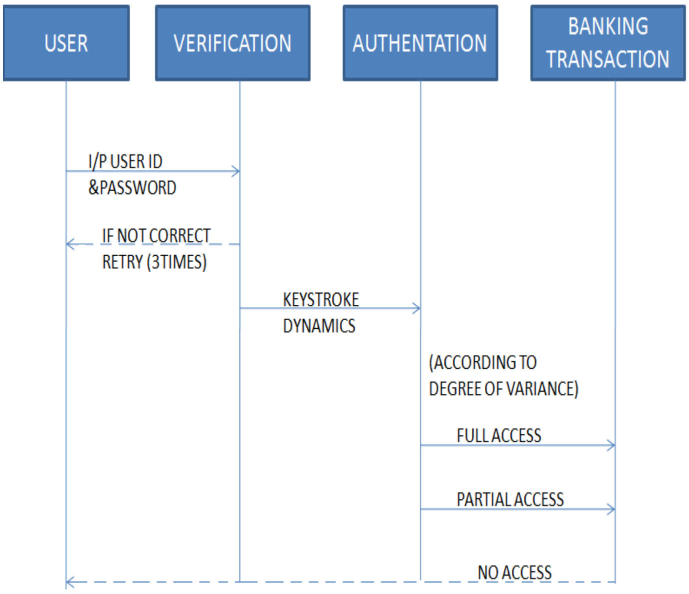

Figure5: Implementation Process

Step1: it is the initial state where the new user will register themselves and the user have to type their user ID and password ten time and these pattern will be upload in the table which is used to calculate the threshold for matching the typing pattern.

The existing user has to input their user ID and password.

Step2: The verification process of the user is done i.e. the characters of the user ID and password of the user is matched.

If the user ID and password of the user is incorrect then user has to again input their user ID and password. And 3 trails is given to the user, if in that 3 trails user don’t able to input the correct user ID and password then account is blocked.

Step3: In this step the keystroke dynamics is done i.e. the typing pattern of the user is matched from the threshold that is fixed for the user.

Step4: According to the degree of variance from threshold the access is provided to the user.

i. Full access: User is give full access of the banking transactions. The variance is very less or nearly nil from standard typing pattern.

ii. Partial access: User is given partial access of the banking transaction i.e. user can’t perform transactions only can see the account details. The variation is not high from the standard typing pattern.

iii. No access: User is given no access for banking transactions. The variation is very high from standard typing pattern.

Step5: The typing pattern of the full access user is updated in the table and again the standard typing pattern is calculated of the user.

IV. Result Analysis

This paper introduced keystroke dynamics which is an additional layer of security for the authentication of the user. The unauthorized users can easily access the account of an authorized user, if unauthorized came to know the user ID and password of the authorized user. Whereas keystroke dynamics depend on the typing pattern of the user. And it is very tough to copy the typing pattern of the user.

This process don’t always gives the correct result , here we are trying to reduce false acceptance rate and false rejection rate.

V. Conclusion and Future Work

By using keystroke dynamics we are trying to provide more secured transaction. The system is proposed to provide more security to the account. Only authenticate user can access the account their accounts. This application can be used in android phone or Smartphone through which we can access internet and can perform transaction. Keystroke dynamic is replacing the knowledge based and token based authentication system. However the keystroke dynamic is more reliable, having low cost for implementation, transparent, the user doesn’t recognize the in background keystroke dynamics is being preformed. The user who is not of technical background can easily access because it doesn’t required any technical knowledge. This system doesn’t require any extra hardware for implementation this software can be easily downloaded and accessed.

Acknowledgment

Authors thank Dr. Prasanna Joeg, Head of Computer Engineering Department, and MIT College of Engineering, Pune (MH); for his kind support in providing laboratory infrastructure facility required for this research work.

References

[1] Pin Shen, Andrew Beng Jin Teoh and Shigang Yue, “A Survey of Keystroke Dynamic Biometrics,” The Scientific World Journal Volume 2013, Article ID 408280,24

[2] Pin Shen The, Shigang Yue, Andrew B.J.Teoh, “Feature Fusion Approach On Keystroke Dynamics Efficiently Enhancement,” International Journal Of Cyber-Security And Digital Forensic(IJCSDF) 1(1):20-31, 2012

[3] Yu Zhong, Yundin Deng, Anil K. Jain, “Keystroke Dynamics for User Authentication,” International Journal of Computer Science & Information Technology(IJCSIT) Vol 4, No 3 March 2012

[4] Matthias Trojahn and Frank Ortmeier, Volkswagen AG, Wolfsburf, Germany, “Biometric Authentication Through A Virtual Keyboard For Smartphone,” International Journal of Computer Science & Information Technology(IJCSIT) Vol4, No 5, October2012

[5] Mudhafar M. Al-Jarrah, “An Anomaly Detector For Keystroke Dynamics Based On Median Vector Proximity,” Journal Of Emerging Trends In Computing And Information Sciences VOL3, NO. 6 June 2012

[6] Sally Dafaallah Abualgasim, Izzeldin Osman, "An Application of the Keystroke Dynamic Biometric for Securing PINs and Passwords," World of Computer Science and Information Technology Journal(WCSIT) Vol 1, No 9, 398-404, 2011

[7] D. Shanmugapriya, DR. G. Padmavathi, "Virtual Key Force- A New Feature For Keystroke," International Journal Of Engineering Science And Technology(IJEST) Vol.3, No.10 October 2012

[8] Maximiliano Bertacchini, Carlos E. Benitez and Pablo I. Fierens, "User Clustering Based On Keystroke Dynamics," Congreso Argentino De Ciencias De La Computación CACIC2010-XVI

[9] Luciano Bello, Maximiliano Bertacchini, Carlos Benitez, Juan Carlos Pizzoni and Marcelo Cipriano, " Collection And Publication of a Fixed Text Keystroke Dynamics Dataset," Congreso Argentino De Ciencias De La Computación CACIC2010-XVI

[10] Kenneth Revett, Florin Gorunescu, Marina Gorunescu, Marius Ene, "A machine learning approach to keystroke dynamics based user authentication," Int. J. Electronic Security and Digital Forensics, Vol.1 No. 1, 2007

[11] Edmond Lau, Xia Liu, Chen Xiao, and Xiao Yu, "Enhanced User Authentication Through Keystroke Biometrics," International conference on biometrics dec 9, 2004

[12] Fabian Monrsone, Aviel D. Rubin, "keystroke dynamics as a biometrics for authentication," preprint submitted to Elservier Preprinter march1,2000

[13] Kevin S. Killourhy , Roy A Maxion, "Comparing Anomaly-Detection Algorithms For Keystroke Dynamics," Cornegies Mellon University PA 15213

[14] N.M. Gunathilake, A.P.B. Padikaraarachchi, S.P. Koralagoda, M.G.Jayasundara, "Enhancing the Security of Online Banking System via Keystroke Dynamics," SLIIT Colombo, 2012

[15] Luciano Bello , Maximiliano Bertacchini , Carlos Bentez , Marcelo Cipriano, "Collection And Publication Of Keystroke Dynamics Dataset," CACIC 2010

[16] Fabian Monrose , Aviel D. Rubin, "Keystroke Dynamics As A Biometric For Authentication," Preprint submitted to Elsevier Preprint, march 2009

[17] M. Karanan, N. Krishnaraj, "A Model to Secure Mobile Device Using Keystroke Dynamics Through soft Computing Techniques," International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue- 3 July, 2012.