AUTHENTICATION OF THE USER BY KEYSTROKE DYNAMICS FOR BANKING TRANSACTION SYSTEM

NANDINI CHOURASIA

Computer Department: MIT COE, Pune

Abstract- In the past few decades the data usage from internet has been increased at very high rate. The online payment and banking transactions also increased exponentially. But unfortunately the attacks on that data and transactions are also increasing. As the every authorized user has their own username and password to access their personal accounts, but as these details can be misused by an authorized user so there is a requirement of additional authentication step. The keystroke biometric is more efficient to authenticate the user and provide more security. Keystroke biometrics is based on the assumption the the typing pattern of each user is unique. In this paper, we are looking forward at several processes for keystroke biometrics to enhance user authentication. Our objective is to collect a keystroke-dynamics dataset, to develop a repeatable evaluation procedure, and to measure the performance of a range of detectors so that the results can be compared more accurately. All the four keystroke latencies and dwell time is used for making data set. That dataset is used to degree of variance of the user and to detect the authorization of the user.

Keywords- Keystroke Biometrics, False Acceptance Rate, False Rejection Rate, Full Access, Partial Access, No Access, Virtual Key Force, Metric Proposal.

I. INTRODUCTION

The use of the banking system is increasing exponential day by day. The society depends mostly on internet, there is more confidential information is used by the user over internet. Therefore we need more security and the authentication of the user. So that only authorized user can only able to access the account [1]. As the login details have been exposed to an unauthorized, then that unauthorized user have complete access to the authorized user's account in a transparent manner and such things may result in direct financial loss and secured information may leak. Authentication is the process to prevent the unauthorized access on the authorized account of the user [7].User authentication is classified in three classes: knowledge based, object or token based and biometric based. Fig1 1 shows the various user authentication classifications which are knowledge based, object based and biometric based. The authentication of the user is done on (i)The knowledge based authentication refers to what the person knows i.e. user ID & password. PIN code etc. (ii)The object or token based refer to what the user posses i.e. ID-card, token etc. (iii) Biometric refers to the identification of humans by their characteristics. Biometrics is used in computer science as a form of identification and access control. It is also used to identify a person from the group from their habitual patterns. Biometric identifiers are the distinctive, measurable characteristics used to label and discriminate the person from other. Biometric identification is depend on the behavioral and physiological characteristic of the user i.e. figure prints, keystroke dynamics.[1][7].

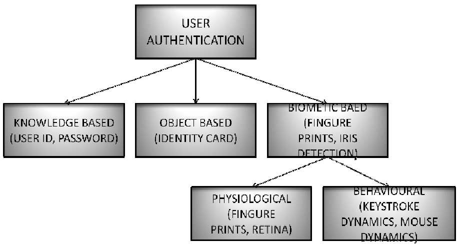

USER AUTHENTICATION
KNOWLEDGE BASED (USER ID, PASSWORD)
OBJECT BASED (IDENTITY CARD)
BIOMETIC BAED (FINGURE PRINTS, IRIS DETECTION)
PHYSIOLOGICAL (FINGURE PRINTS, RETINA)
BEHAVIOURAL (KEYSTROKE DYNAMICS, MOUSE DYNAMICS)

Figure1: Classification of the Authentication Process

Currently, there are two major forms of biometrics first is physiological biometric it is based on physiological attributes i.e. Iris Detection etc and second is behavioral biometric it is based on behavioral attributes i.e. keystroke dynamics, signature detection, etc.

Keystroke dynamics is referring to the art and science of recognizing an individual based on an analysis of their typing patterns. Typing pattern of an individual includes many factors such as the length of time it takes to type the login and password, how long the individual required to depress a key and how long it take to type successive keys [5].To provide an additional layer of 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

2.1. KEYSTROKE DYNAMICS

Key stroke dynamics define as the process of analyzing user by the way user type by monitoring the key board inputs in attempt to identify them 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][18].

The Keystroke dynamics process is used for the authentication of the user. As every process has their advantages with some disadvantages this process is also having some advantages as well as disadvantages.

2.1.1. ADVANTAGES

a) Uniqueness
The typing pattern of every user is unique. So to check uniqueness of the keystroke of the user, it measure up to nanoseconds. So it is very difficult to copy one's keystroke pattern at such high accuracy [2].

b) Low Implementation and Deployment Cost
In traditional physiological biometric such as finger print recognizer we need extra hardware and software for implementation. Where as in keystroke dynamics doesn't depend on the hardware, only software is required for implementation, it runs at a backend of the system without any interruptions [1].

c) Transparency and simplicity
In many situations 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 because for using the keystroke one doesn't required any technical knowledge. [6].

d) Replication Prevention
As the typing of the user differ from user to user. So nobody can easily copy the typing pattern of another user. So it prevents the replication of the typing pattern [6].

2.1.2. 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].

2.2 FEATURE EXTRACTION

Keystroke dynamics have several different feature to detect authenticate user.

- Latency of key stroke
- Duration of keystroke
- Hold time
- Overall typing speed
- Frequency of errors
- Force of hitting keys while typing
- Which shift key is used by the user more frequently i.e. left shift key or right shift key
- Which key is first released shift or another keys.

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

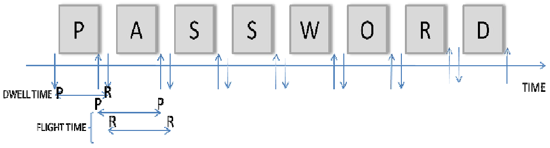


Figure2. Keystroke Latency and Duration

1) Latency or Flight Time
Latency in keystroke dynamics is calculated with key press (P) and key release(R). The latency or flight time is calculated between successive keys. 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 successive key presses i.e. [(time take to press first key) – (time take to press another key)].
L1=P1-P2

- RELEASE-PRESS: it is the time interval between key release and key press i.e. [(time take to release first key) – (time take to press second key)].
L2= R1-P2

- PRESS - RELEASE: it is the time interval of key press and key release i.e. [(time take to press second key) – (time take to release first key)].
L3= P2-R1

- RELEASE- RELEASE: it is the time interval between two successive key releases i.e. [(time take to release first key) – (time take to release second key)].
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 i.e. [(time take to press key) – (time take to release key)]. D1=P1-R1

The most commonly used metrics proposal is to evaluate the authentication of the user is on the false acceptance rate (FAR) and false rejection rate (FRR)

[2][6]. The false rejection rate refer to rate the authorized user is denied access and the false acceptance rate is denoted as the rate unauthorized user is given access [6].

For this the data sample of the users 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 of the user is taken, so that it give more perfect result [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][18].

III. MATHEMATICAL MODEL

Let U be the set of the where all the user is to be authenticated for performing bank transaction and according to the degree of match transaction is performed.

U ={WDB, GIK , GIW , U, A, T}

Notations

WDB: Word Database
GIK: Inter Key press Gap
GIW: Inter Word Gap
U: User
A: User's Account
T: Transaction

Set Theory

WDB = {W1,W2,W3,W4,……. ,Wn }
GIK = {g1,g2,g3,g4……,gn}
GIW = {G1,G2,G3,G4…, Gn}
U = {U1,U2,U3,U4…..,Un}
A = {A1,A2,A3,A4……,An}
T = {T1,T2,T3,T4…….,Tn}

Functions

F1: verification of user
F2: authentication of user

Process

U = Register (user id, password, full name, address, contact number, e-mail, etc.)
Verification [Y/N] = log in (user ID, password);
Authentication [Y/N] = verified (user ID, password)
G = keystroke dynamics (WDB)
g' = Euclidean Distance(G)
i.e. $g' = \sqrt{(g1 - G1)^2 + (g2 - G2)^2}$
Sd = Standard Deviation
Percent authentication (Sd, DB)
Update (Sd, DB)
T = create transaction (user ID, amount transfer, date, time)

IV. IMPLEMENTATION

A. Design

In addition to the verification process keystroke stroke dynamics is used to provide authentication to the user. The fig3 is showing the implementation process of the proposed model. The proposed model is divided into phases. Before the first phase starts the users have to register themselves for performing banking transaction. While registration process, the user has to input their password 10 time so that the typing pattern is analyzed and threshold of the user's typing pattern is detected. In first phase the user have to complete their login process and in second phase the user is authenticated by using keystroke dynamics. 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 .this retry is given to the user only 3 times.

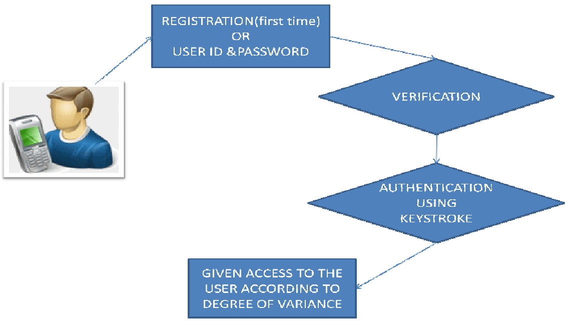


Figure3: Implementation Design

Now, in phase two 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. According to the degree of variance from the threshold value of the user, access of the account to the user is provided.

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.

The typing pattern of the full access user is updated in the table where the typing pattern and speed is stored and threshold is calculated. When the full access user's typing pattern and speed is updated, again the standard typing pattern is calculated for the user.

B. State transition diagram

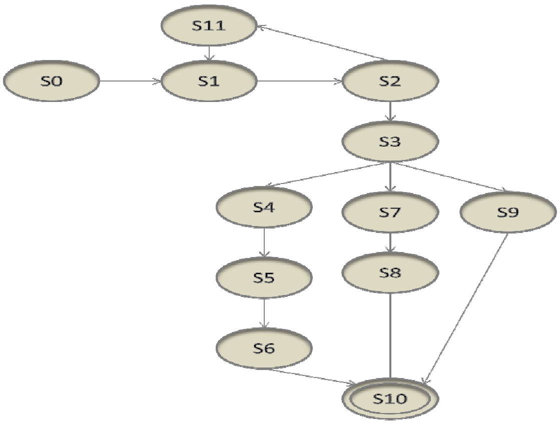


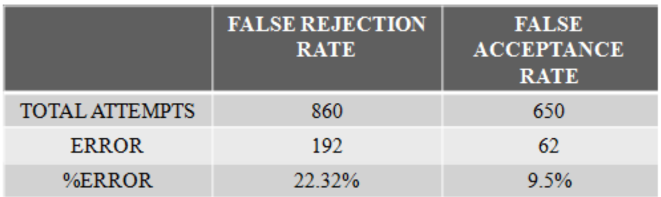
Figure4: State Transition Diagram

S0: (Initial State) User
S1: User Input User Id And Password
S2: Character Are Matched At This State
S3: Keystroke Dynamics
S4: Full Access
S5: Update Is Done On Existing Data
S6: Full Banking Transaction
S7: Partial Access
S8: Partial Banking Transaction
S9: No Access
S10: Retry
S11: End

C. Hardware And Software Requirements

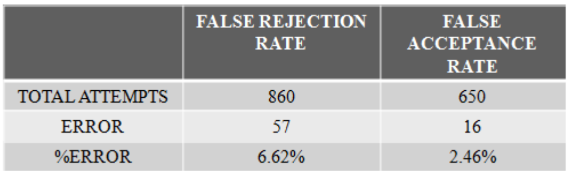
Operating System	: XP or higher version of window
Database	: SQL
User Designer Tools	: Eclipse
Software Component	: JAVA Version 1.6 or Adv. Java
Hard Disk	: 1GB Minimum or onwards
RAM	: 256 MB or Higher
Processor	: Intel P family Or Equivalent
Input device	: Android smart phones, keyboard.

V. EXPERIMENTS



	FALSE REJECTION RATE	FALSE ACCEPTANCE RATE
TOTAL ATTEMPTS	860	650
ERROR	192	62
%ERROR	22.32%	9.5%

Table1: Results for User Authentication By Using Manhattan Distance



	FALSE REJECTION RATE	FALSE ACCEPTANCE RATE
TOTAL ATTEMPTS	860	650
ERROR	57	16
%ERROR	6.62%	2.46%

Table2: Results for User Authentication by Using Manhattan Distance

VI. 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.

Here the user will give their user ID and password, firstly the character are matched for verification of the user. If the user ID and password of the user are correct it will proceed further else it will go to retry, where the user is provided with 3 chances to give correct user ID and password. If in three chances user doesn't input correct user ID and password then the account of the user is blocked. Now, the user who is valid proceed further for the authentication process the user is authenticated with their typing pattern and typing speed and according to the degree of variance the user is provided access to the account. As the keystroke dynamics don't give the positive result always sometime unauthorized user can also given access, so we will improve the algorithm to provide more fair results. From the experimental results the Euclidian distance is much better way to calculate the equal error rate where as Manhattan distance is not giving much accurate results

CONCLUSION AND FUTURE WORK

This paper proposes to provide more security to the account. Only authenticate user can access the account. This application can be used in android phone or Smartphone through which we can access internet and can perform transaction. Authorized user can easily access their account and 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.

As keystroke dynamics doesn't always give the positive results. We are trying to reducing the false acceptance rate and false rejection rate. And till date we have tried two techniques but in future many other techniques can also be used for authenticate the user by using keystroke dynamics.

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.

[18] Deian Stefan, Member, IEEE, and Danfeng (Daphne) Yao, Member, IEEE, "Keystroke-Dynamics Authentication Against Synthetic Forgeries," Rutgers DIMACS REU programs, National Science Foundation grants CNS-0831186 and CAREER CNS-0953638.

★★★