Intrusion Detection System using Keystroke Dynamics and Fuzzy Logic for Touch Screen Devices

Mahalaxmi Sridhar, Amritha Agarwal, Mansi Patel, Candida Rodrigues, Jincy Sam
Don Bosco Institute Of Technology, Kurla(W)
mahalaxmi90sridhar@gmail.com

***Abstract*—Passwords play a crucial role in many mechanisms of user authentication and security. They provide the first line of defence for applications or data stored in devices ranging from computers to mobile phones. Currently,due to tremendous increase in the usage of mobile phones, people tend to store more and more sensitive data on their mobile devices. Passwords are shared by people for various purposes, knowingly as well as, unknowingly. Also, passwords can be predicted easily by sophisticated methods by attackers for the sake of intrusion. Therefore, it is essential to enhance the security of password based authentication.**

In this application, we make use of the users' keystrokes to form a unique signature, which cannot be easily replicated by intruders, thus providing a more stringent form of security. Hence, even if an intruder gains access to the password or PIN, he will not be able to access the system without the users' keystroke biometric features.

***Keywords*—Biometrics, keystroke dynamics, Smart phones, Android, Fuzzy Logic, Security.**

I. Introduction

Smartphones have become a crucial part of modern society. We use it for a variety of purposes ranging from everyday activities to storing and accessing confidential data. Also we might access this data in an unsecure environment such as public places. Since we depend so much on Smartphones to store and process sensitive information, it has become all the more necessary to secure them from intruders.

For user authentication and identification in phone-based applications, there is a need for simple, low-cost and unobtrusive device.Use of biometrics such as face, fingerprints and signature requires additional tools to acquire the biometric which leads to an increase in cost. Use of a behavioral biometric which makes use of the typing pattern of an individual can be obtained using existing systems such as the standard keyboard/touch screen, making it an inexpensive and extremely attractive technique. One of the major advantages of this biometric is that it is non-intrusive and can be applied covertly to existing security systems. The advantage of using behavioral biometrics such as keystroke dynamics is that it can be collected without the knowledge of the user of the phone.

Don Bosco Institute Of Technology, Kurla(W)

II. Literature Survey

Intrusion detection using Keystroke Dynamics and Pi membership function for web applications[1]-Mahalaxmi Sridhar*(2014) was the implementation of Fuzzy logic in web applications. Pi membership function is used here, as a classifier, for efficient output and was proved to better than the other membership functions because the pattern detection doesnt alter that much and it is hardware independent.

Keystroke Dynamics on Android Platform by Margit Antal*(2014)[3]-Demonstrated experimentally that touchscreen based features improve keystroke dynamics based identification and verification. Identification measurements were performed using several machine learning algorithms, out of which the best performers were Random forests, Bayesian nets and SVM in this order.

Keystroke Dynamics for Mobile Phones: A Survey (2012)[4]-A survey of all existing papers on keystroke dynamics for aunthentication, on different platforms and the decision making techniques/classifiers used. Experimented using neural networks.

Keystroke-based User Identification on Smart Phones[2]-Various classifiers were compared but on Symbian OS.(2009)

There has not been any study to measure the performance of keystroke dynamics on smartphones using a real life password. Moreover,the effect of touchscreen features pressure and finger area has not been studied in a realistic environment till 2014.

Hence, in year 2011-2012, 2013-2014 also some of the membership functions were implemented to check the efficiency of the product in terms of FAR (False Acceptance Rate) & FRR (Fault Rejection Rate) to get the better output.[5][7]

A. Where and how it can be used

Analysis of keystroke dynamics can be broadly classified into two types static or structured text and dynamic or free text.

- Static analysis involves analyzing keystroke behavior of an individual on predetermined phrase(s) at certain points in the system. For example, when logging in a system the users typing pattern is analyzed when he/she types the user-id and password. It can also involve the use of a particular phrase which is common for all the users of the system. Static text entry can be deployed in

systems where there is no scope for further text entry. For example, when a user logs in to check his bank accounts online there is usually no further scope of text entry.

- Dynamic analysis involves continuous or periodic monitoring of keystroke behavior. It is first checked when a user logs in the system and continues thereafter. For example, if a person is browsing the web, certain websites maybe frequented by the user. A list of the commonly occurring websites and the typing behavior of the user while entering the string can be stored. In this case, a training phase would be needed where the user types a particular string several times so that a model can be built for that string. During the test phase, as the user types, the string is recorded along with its timing info which can then used for authentication. However, dynamic monitoring may lead to privacy issues due to its intrusive nature.We will be making use of static analysis in the form of password.

B. Fuzzy Logic

In simple terms, Fuzzy logic can be said as a way to reach a goal by going through different paths. Fuzzy logic is a form of many-valued logic; it deals with reasoning that is approximate rather than fixed and exact.

Compared to traditional binary sets (where variables may take on true or false values) fuzzy logic variables may have a truth value that ranges in degree between 0 and 1.

1) Membership Functions: Degree of membership is calculated by a Membership Function. All of the membership functions that exist for fuzzy logic have been implemented previously and the PI MF proved to be better because the pattern detection doesnt alter much and it is hardware independent.[1]

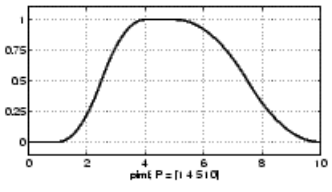


Fig. 1: Pi membership function

This membership function is implemented by using the equation given below:

$$f(x;a,b,c,d) = \begin{cases} 0 & x \leq \text{a} \\ 2*\left(\frac{x-a}{b-a}\right)^2 & a \leq \text{x} \leq \frac{a+b}{2} \\ 1-2*\left(\frac{x-b}{b-a}\right)^2 & \frac{a+b}{2} \leq \text{x} \leq \text{b} \\ 1-2*\left(\frac{x-c}{d-c}\right)^2 & c \leq \text{x} \leq \frac{c+d}{2} \\ 2*\left(\frac{x-d}{d-c}\right)^2 & \frac{c+d}{2} \leq \text{x} \leq \text{d} \end{cases}$$

where, x = Current time
a = Average time - (2*Standard Deviation)
b = Average time Standard Deviation
c= Average time + Standard Deviation
d = Average time + (2*Standard Deviation)

III. Data Acquisition

As a first step towards developing a robust mobile phone user identification system, we developed an application that deals with locking/unlocking of preinstalled applications. We decided to develop the application for Android OS with version 4.4 and above as Android has a relatively large customer base. Majority of the smart phones today have capacitive touch screens. Thus the application is created for smart phones with capacitive touchscreens only.

The installed applications locked using the system cannot be accessed directly but require a password set by the authenticated user. While registering to this application,user biometrics is noted, i.e. all the keys typed by the user along with the pressed/release times of the keys are noted and identification is done using fuzzy logic. Thus, even if an intruder knows the password, unless the biometrics matches, he will not be granted access to the secured applications.

A wide range of data samples were collected for analysing the system. After successfully collecting the dataset, we started the next phase of our research systematically analyzing our raw data to extract useful features for user identification.We observed that some people tend to type faster with less errors as compared to others,while some others type very slowly.Based on this preliminary analysis, we observed that if we can identify a keystroke dynamics feature set that covers all aspects of a persons unique typing pattern, we can actually identify the mobile phone user. Therefore, we extracted 6 features to correctly identify a user hey-hold time, down-down time, up-down time, finger size, average hold time and average finger size.

IV. Feature Selection

A. Feature Sets

The method used to form the signatures include the following features:

- Key hold time: Time between key press and release.
- Down-down time: Time between consecutive key presses.
- Up-down time: Time between key-release and next key press.
- Finger size: Finger size at the moment of key press.
- Average hold time: Average of key hold times.
- Average finger size: Average of finger size.

B. How user will be validated

The block diagram as shown in Figure 1. gives an outline of the operation of the system. After successful registration, when the user logs into the system, it is verified against the database. Based on the correctness of the password and the biometric, the user is either allowed or denied access. If the

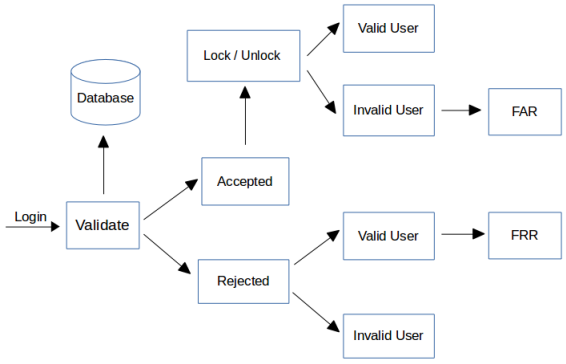
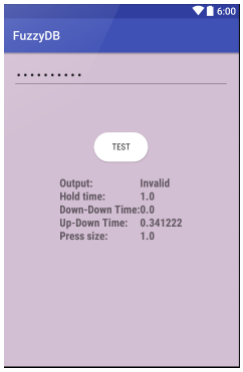
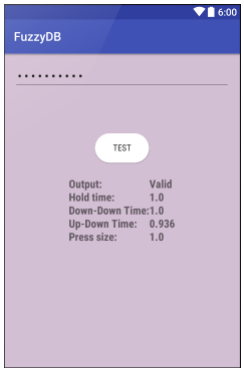


Fig. 2: Block Diagram of IDS



(a) Output for an Intruder



(b) Output for an Authentic User

Fig. 4: System Snapshots

Sr_no	keys_pressed	AHT	ADDT	AUDT	APST
1	3	133	1369	1238	2.0489096641540527e-8
2	3	137.33333333333334	1563.5	1430.5	2.1653249859809875e-8
3	5	137.4	1425	1284	2.3050233721733093e-8
4	3	129.33333333333334	1046.5	918	2.4071106543907753e-8
5	3	140.33333333333334	1331.5	1192	2.505839802324772e-8
6	3	131.33333333333334	1176	1048	2.6028015111622056e-8

Fig. 3: Database Snapshot

valid user is denied access, it is termed as False Rejection. False Acceptance is when an imposter is allowed access. On obtaining access to the system the user can either lock or unlock the applications.

V. Performance Evaluation

The typing pattern was recorded by observing the keystrokes of the users. The timing between the keys and the feature sets used are stored in a database.These parameters were used to generate a signature using the pi membership function, to create a unique signature for each user.

Figure 2 shows the various feature sets - Average Hold Time(AHT), Down-down time(ADDT), Up-down time(AUDT) and the Average press size(APST) of the signature being stored.

After recording 200 signatures for each the group members it was observed that any other person trying to access was denied access to the system. The output for the given scenario is as shown in Figure 3.

If the signature formed is validated .i.e. it matches with the signatures present in the database, the user is allowed access. Figure 4 shows the output of an authentic user.

VI. Conclusion and Future Work

With this application, an approach is presented to implement keystroke dynamics and fuzzy logic as a system to improve smartphone security. PI membership functions are used for validating a user based on behavioural biometrics as its value of FAR and FRR is low and its efficiency is hardware independent. The signature generated by the user is validated and only after verification the user is able to login.

Keystroke dynamics allows for the design of more robust authentication system than traditional based alternatives alone. It is a leap into the new dimensions of the biometric systems which provides foolproof security without the use of a dedicated hardware device.

In future, a simulated clock can be generated which provides increased efficiency in keystroke dynamics as compared to the usage of system clock.The security can also be generalized to free text rather than a static password.Keystroke analysis can also be implemented in security of online accounts and systems.

References

[1] Mahalaxmi Sridhar, Amogh Joshi, Dwarkesh Naik, Udayan Srivastava, Venus Dias *Intrusion detection using Keystroke Dynamics and Pi membership function for web applications*, Department of Information Technology, Don Bosco Institute of Technology, Mumbai, India.

[2] *"Keystroke-based User Identification on Smart Phones"* Saira Zahid , Muhammad Shahzad , Syed Ali Khayam , Muddassar Farooq Next Generation Intelligent Networks Research Center (nexGIN RC) National University of Computer and Emerging Sciences (FASTNUCES) Islamabad 44000, Pakistan School of Electrical Engineering and Computer Sciences (SEECS) National University of Sciences and Technology (NUST) Islamabad 44000, Pakistan saira.zahid, muhammad.shahzad, muddassar.farooq@nexginrc.org,ali.khayam@seecs.edu.pk

[3] 8th International Conference Interdisciplinary in Engineering, INTER-ENG 2014,9-10 October 2014, Tirgu-Mures, Romania. *"Keystroke dynamics on Android Platform"* Margit Antal, Lszl Zsolt Szab, Izabella Lszl

[4] Baljit Singh Saini, Navdeep Kaur and Kamaljit Singh Bhatia *Keystroke Dynamics for Mobile Phones:A Survey* CSE, Sri Guru Granth Sahib World University, Fatehgarh Sahib - 140407,CSE, Lovely Professional University, Phagwara, Punjab, India.CSE, Sri Guru Granth Sahib

World University, Fatehgarh Sahib - 140407, Punjab, India.

[5] Mahalaxmi Sridhar, Siddhesh Vaidya, Piyush Yawalkar, Nigel Lobo, Mitali Gawade *" Intrusion Detection Using Keystroke Dynamics and Fuzzy Logic Membership Functions"*

[6] Mahalaxmi Sridhar, Neeraj Yadav, Narendra Vishwakarma, Nikhil Dhavale, Mohit Nijai *"Intrusion Detection Using Keystroke Dynamics on Virtual Keyboard for Web applications"*

[7] Mahalaxmi Sridhar, Alishia D'souza,Johnelle Rebello, Teby Abraham, Winchell D'souza *"Intrusion Detection using Keystroke Dynamics"*