Strengthening user Authentication using Keystroke Dynamics

Akshat Shah	Parth Shah	Hitarth Shah	Asst. Prof. Chetashri Bhadane,
Department of Computer Engg Dwarkadas J. Sanghvi COE Mumbai, India	Department of Computer Engg Dwarkadas J. Sanghvi COE Mumbai, India	Department of Computer Engg Dwarkadas J. Sanghvi COE Mumbai, India	Department of Computer Engg Dwarkadas J. Sanghvi COE Mumbai, India

***Abstract*-In today's world, the technology has transitioned at such a great extent, that the mobile devices can do all the functions and tasks which were previously done by a personal digital assistant. The mobile phones have the ability to store sensitive and confidential information like digital certificates, financial records and company records, making them primary target for intruders. Thus to secure that, Personal Identification Number (PIN) is used currently, which has limitations from both end user and technological perspective. Therefore, there is a need for non-intrusive and stronger subscriber verification technique. This paper presents the viability of one such technique, the usage of keystroke dynamics to provide an additional layer of security along with PIN. In this paper, we discuss different approaches and methodologies to authenticate users based on their interactions with a mobile phone keypad, comprising a number of investigators into the ability of neural networks.**

Keywords-Authentication; Biometrics; Keystroke; Smartphone

I. INTRODUCTION

Due to technological advancements, the usage of smart phones increased drastically. Smart phones have now become the part and parcel of our home and work environments. Smartphones have enriched capabilities that allow users to store personal and sensitive information like corporate secrets, emails, passwords, credit card details, notes, images etc. [6]. The authentication method used currently makes use of a secret Personal Identification Number (PIN).The problem with such authentication method is that it could be easily decoded and confidential information can be thus accessed easily. Any application or data can be easily accessed through a simple password or PIN, if it is known. Methods like Key logger and social engineering can be used to steal the passwords with alphanumeric letters which are not even in the vocabulary. Moreover, the recent work suggests that an attacker needs only eleven attempts to guess most users passwords [10]. Thus, there is a vital need for robust security mechanisms that safeguard user's data on smart phones. One of the potential approaches is the use of physiological biometric features which are not based on the knowledge of user but based on the user itself. It includes interactive attributes such as retina, fingerprints, hand geometry etc [2].These biometric methods make use of one or more hardware devices in order to recognize a user. Moreover, such authentication methods could be easily compromised and thus security could be easily breached. Another variant to provide authentication is the behavioral biometrics. These methods include keystroke, voice, gait, etc. The behavioral characteristics largely remain unique to a person and do not change drastically. Moreover, it does not require any additional hardware and hence such system can be cost effective. The most common authentication method is the use of PIN. In order to provide an additional layer of security, keystroke dynamics can be used.

II. BIOMETRIC AUTHENTICATION

Traditionally, passwords and PIN were used as measures for authentication. The flaw with such techniques is that it does not identify a user. Nowadays, biometric system is introduced that compares the recorded information attributes of a user in order to identify the user. Biometric authentication is a technique that authenticates a user and identifies its identity based on the physiological or behavioral characteristics of a user. Biometric authentication is a convenient and an accurate method of authentication. One such variant of biometric authentication is Keystroke Dynamics.

A. Keystroke Dynamics:

Keystroke dynamics refers to typing dynamics which is not based on what the user types but it depends on how the user types. Keystroke dynamics is widely used in desktop applications however; integrating it with mobile devices is a modern application [12]. Keystroke authentication can be classified as either static or continuous. Static analysis of keystroke refers to the analysis that is done only at specified times. Dynamic analysis continuously monitors the keystroke patterns during an entire session and provides a tool to detect user substitution after user is authenticated to the system. Different features can be easily extracted from the typing pattern such as dwell time, flight time, multiple digraphs, etc. These features remain fairly unique to a user. More advanced system incorporate pressure sensors to measure on screen pressure applied by finger touch, finger touch size while typing the data can be accessed [13]. Two major quality factors namely, consistency and uniqueness needs to be considered in order to authenticate a user based on keystroke characteristics.

B. Advantages of Keystroke Dynamics

1. Unique: It has the ability to measure timing data up to nanoseconds for keystroke events to precisely identify a user.
2. Low Implementation and Deployment Cost: Keystroke dynamics recognition does not require additional hardware equipments and can be completely implemented by software.
3. Transparency: User may not be aware with the fact that an extra authentication layer using keystroke dynamics is implemented in some systems, as it is implemented at the back end, thus helping users even with no technical background.
4. Reliable: With the involvement of Keystroke dynamics in password authentication scheme, its reliability can be increased.

C. Application of keystroke dynamics

1. Keystroke dynamics provides an additional layer of security to traditional password based system and provide authentication.
2. It is used as a form of surveillance. There exist some software systems which capture user keystroke information while typing without even awareness of the user. This information is further used to analyze that whether the created accounts are shared or are used by different people from genuine user.
3. This technique can be used in online transactions such as online bill payments, fund transfer, account login, etc.

D. Keystroke Dynamics Process:

The general process for Keystroke based authentication methods require following stages

1. Enrolment

In this phase, the keystroke data are processed and stored. This is done using following steps:

- Data acquisition: Information is generated from the keyboard at the authentication device. Then, the existing system records the data and stores it as course of events. These raw data are stored as enrolment samples required for later evaluations [7].
- Pre-processing: Pre-processing is essential as whenever the biometric features are extracted, they cannot be obtained in the same quality every time.
- Feature extraction: Its main function is to select the right features.
- Storage: The extracted data are stored in the database to compare the data during future evaluations. It proves very useful as changes can be easily recognized with the storage of these data.

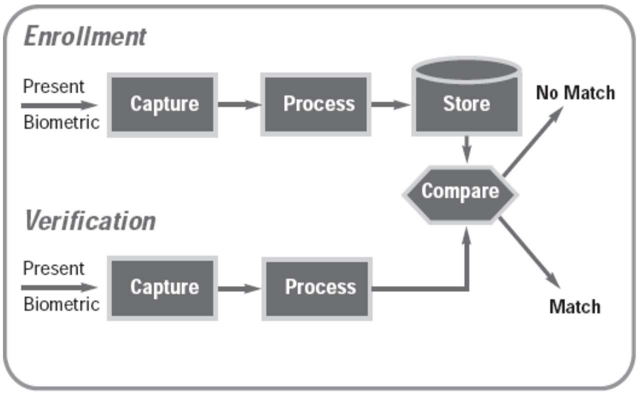

Fig.1 Biometric Authentication System [1]

2. Authentication:

The user can access the system if the data are correctly stored in a database. For this, authentication needs to be done against the system. Authentication phase resembles the enrolment process. The data are stored as samples in the system after the data acquisition phase. In the final steps after the feature extraction, the actual data is compared and classified with the stored data. This is compared based on various biometric modalities like neural networks, distance measures and probabilistic classifier. Biometric authentication has a disadvantage that some users are falsely accepted known as FAR (false acceptance rate) and some people are falsely rejected known as FRR (false rejection rate) [5]. This means that some intruder trying to access the system can be accepted while on the other hand the valid user can be rejected. The error rates should be as low as possible for better results and also needs to be balanced for special cases as both cannot be zero at the same time.

Sometimes, the EER (equal error rate) is evaluated instead of FRR and FAR. This happens when FRR and FAR are equivalent. The main task is to find the right threshold value for comparison and filtering purpose [7]. Some systems require low FAR (high threshold) such that no intruder can get into the system. This is in fact the best solution to make highly secured systems. The systems for which this protection mechanism is used may have a high usability thus it is important that the user does not need to authenticate himself for several times. To achieve this, the threshold needs to be smaller as compared to previous situation and the FRR should be lower as well. Particularly for mobile devices, the second approach is better. Due to these different arising situations FAR and FRR are required.

III. APPROACHES:

A. Feature Selection:

After data are collected from the user, three features are extracted from this data-diagraph, key hold time and error rate. These entities are defined as:

- Key hold time: The difference in time between pressing a key and releasing it.
- Diagraph time: The difference in time between releasing a key and pressing the next one [2].

- Error rate: The number of times backspace key is used [1].

It is relatively easier to identify user on desktops for these three features as compared to mobile as it shows comparatively distinguished feature vector for each user. The results extracted from user working on desktop are easier to segregate and proves relatively simple to classify. However, considering mobile phones, they have extremely diffused feature vectors when the same three features are extracted. Because of multiplexed keys in a 4x3 matrix, user authentication using keystroke dynamics is more challenging on cellular devices [2]. To decrease the data diffusion rate, split the feature "diagraph" into four types of diagraphs as follows:

- Horizontal Diagraph: Time elapsed between releasing a particular key and pressing its neighboring key in the same horizontal line of keys for [4], e.g. key 7 and 8.
- Vertical Digraph: Time elapsed between releasing a key and pressing the neighboring key in the same vertical line of key for [4],e.g. key 2 and 5.
- Non-adjacent Horizontal Digraph: Time elapsed between releasing a key and pressing the next in the horizontal line such that the keys are separated by one or more keys for [4] e.g. key 4 and 6.
- Non-adjacent Vertical Digraph: Time elapsed between releasing a key and pressing the next in the straight up or down line such that the keys are separated by one or more keyfor[4] e.g. key 3 and 9.

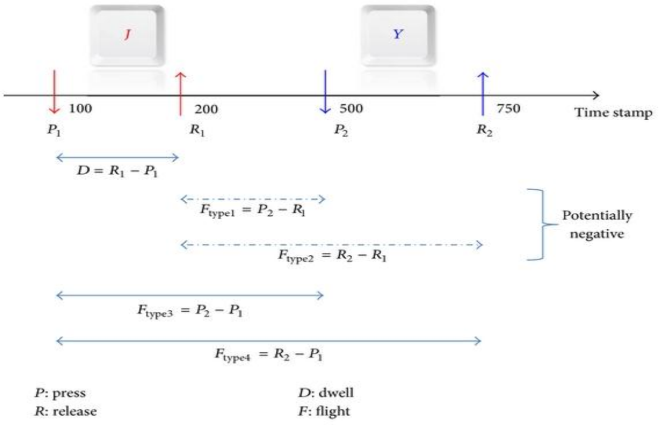

Fig 2. Authentication using dwell time and flight time [2]

For each feature, the coefficient of variation is calculated to determine its randomness and variation in the features' data. After careful evaluation it is observed that the coefficient of variation for key hold time is more or less same as users normally press keys for about same period of time. Thus, classifier is required to properly categorize a user based on this combined feature set that can recognize classification borders for highly fluctuating data which results in diffused usage patterns for different users.

B. *Sensor dynamics:*

Contemporary cellular devices are equipped with a number of sensors that can be used by mobile applications. The Android API, provide applications the authority to use different sensors like gravity, air pressure, humidity, microphone, camera, accelerometer, proximity, light, gyroscope, magnetic and temperature. The primary consideration is on movement sensors, that is gyroscope and accelerometer. The accelerometer computes the acceleration of cellular devices on the X (lateral), Y (longitudinal), and Z (vertical) axes [9]. Applications can access the acceleration values evaluated by accelerometer. On the other hand, the gyroscope measures the alignment (angle) of device around each of the 3 physical axes. Applications can calculate the rate of rotation (radians/sec), orientation (angle) and rotation vector (the orientation of device as a combination of an axis and an angle) values given by the gyroscope [9]. Thus, gyroscope and accelerometer can be widely used in applications where behavioral characterization is required for e.g. location inference and sensor based keystrokes. These techniques have successfully shown that the actions performed by user on cellular device can be accurately recognized by sensor dynamics.

IV. KEYSTROKE DYNAMICS TECHNIQUES

A. *Statistical Algorithm:*

This method adapts the model by retraining the statistical classification algorithm which generates a user model by extracting a set of statistics from the training examples. This algorithm computes some statistics from the training examples (mean, median and standard deviation) for dwell and flight values for specified phrase in whole database [8][10]. These statistical values represent the user model. Afterwards, in the matching phase, this algorithm verifies each attribute of a new example to check if it meets required conditions. For each attribute, which satisfies required conditions, the algorithm updates the score. The classification of a new example is defined by comparing Score to a threshold value. If Score is larger than the threshold, the example is classified as positive (legitimate user), otherwise, as negative (intruder).

Some methods like Double Parallel algorithm is used to retrain classification algorithms to adapt the user model [6]. Any example recognized as positive (legitimate user) that reached a score value above an update threshold is added to a set of examples stored in the window. The classification algorithm is then retrained using the window as an updated training set. After training, the system is tested against trained set. If the accuracy of the obtained results is not satisfying then the network may be trained again using the training data.

B. *Machine learning algorithms:*

- Using fuzzy logic:
  Fuzzy classifiers can provide acceptable accuracies on diffused datasets because they assign a given data point a degree of membership to all available classes. The primary task of fuzzy classification is to determine the boundaries of the decision regions based on the training data points [3] [11]. Once the class-labeled decision regions in the feature space are determined, classification of an unknown point is achieved by simply identifying the region in which the unknown point resides. Since fuzzy logic assigns each data point a degree of membership to different decision regions instead of a single association to a decision region, an accurate and efficient learning mechanism for the diffused mobile phone feature-set is achieved [6].

- Using neural networks:
  Neural network is a technique that mimics the biological neurons for information processing. Neural network is capable of providing an estimation of the parameters without precise knowledge of all contributing variables. A classical neural network structure consists of an input layer, output layer, and at least one hidden layer. Sample data is iteratively fed into the network to produce some outputs based on the current state of its initial predetermined weights. These outputs are compared to the true output, and an error value is computed. This value is then propagated backwards through the network so that the weights can be recalculated at each hidden layer to reduce the error value. The sequence is reiterated until the overall error value falls below a predefined threshold [1].

V. PROPOSED SOLUTION

Neural networks have long been able to solve problems which are not solvable by traditional methods. The advantage of using neural network is that they are flexible throughout different types of datasets. Also, large number of datasets can be considered simultaneously. This data-driven approach is also relatively faster as compared to the statistical approaches. In other words, neural network can be trained specifically for a valid user. Existing statistical models for keystroke dynamics are difficult to be converted into comprehensible forms especially when the number of features increases. Neural networks on the other hand can support multiple features which in the end can still preserve the comprehensibility. Thus because of higher accuracy and other reliable factors we implemented neural networks over statistical approach in our system.

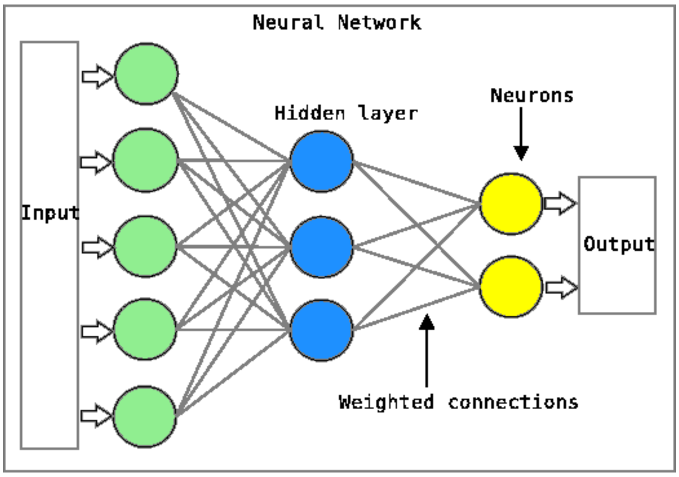

Fig 3. Keystroke dynamics using neural networks [3]

The proposed system operates in 3 sequential phases:

- Enrolment phase: In this phase, the extracted features are fed into the neural network and are trained on this profile. The sample data is iteratively fed into the network based on the current state of its initial pre-determined weights. This output is compared with true output and an error value is computed. This value is then propagated backwards through the network so that the weights can be re calculated to reduce the error value and is re iterated until the overall error value falls below a predefined threshold.
- Detection phase: In this phase, the features are extracted when the user types the password and the neural network differentiates between legitimate users and imposter. If the detector raises an alarm during this mode, the system moves to the verification mode.
- Verification phase: In this phase, the user is asked to enter a remembered PIN. We not only compare the typed characters with the stored PIN but also match how the pin has been typed. Even if the imposter knows the PIN the imposter will still have to enter the PIN using the legitimate user’s keystroke dynamics. This acts as a final line of defense against an imposter.

VI. CONCLUSION AND FUTURE WORK

In this paper, we studied different characteristic of keystroke dynamics for user authentication purpose, various approaches used for determining keystroke patterns and proposed a better solution for keystroke pattern recognition that uses neural network approach. The main advantage of neural network is that they are flexible throughout the different type of datasets and supports multiple features and hence is faster and accurate than various other approaches. Our future work will be to investigate its accuracy and effectiveness to a more complex and challenging test cases and testing on a larger pool of data.

VII. REFERENCES:

[1] Pin Shen The, Andrew Beng Jin Teoh and ShigangYue (2013) A Survey of Keystroke Dynamics Biometrics In: Hindawi Publishing Corporation, article ID 408280,24 pages.

[2] Hataichanok Saevanee, Pattarasinee Bhatarakosol (2008) User Authentication using combination of behavioural biometrics over touchpad acting like touch screen of mobile device In: International conference on Computer and Electrical Engineering.

[3] Mariusz Rybnik, Piotr Panasiuk, Khalid Saeed (2009) User authentication with keystroke dynamics using fixed text In: International conference on Biometrics and Kansei Engineering.

[4] N.L Clarke, S.M Furnell, B.M Lines, P.L Reynolds. Subscriber Authentication for Mobile Phones using Keystroke Dynamics.

[5] M. Karnan, N. Krishnaraj (2012) A model to secure Mobile devices using keystroke dynamics through soft computing techniques In: International journal of Soft computing and Engineering, ISSN:2331-2307, Volume-2, Issue-3.

[6] SairaZahid, Muhammad Shahzad, Syed Ali Khayam, MuddassarFarooq. Keystroke based user identification on Smart phones.

[7] Grant Ho, TapDynamics: Strengthening user authentication on mobile phones with keystroke dynamics.

[8] Yunbin Deng, Yu Zhong, Keystroke dynamics advances for mobile devices using deep neural network.

[9] Cristiano Giuffrida, KarnilMajdanik, Mauro Conti, Herbert Bos. I sensed it was you: Authenticating Mobile users with sensor-enhanced keystroke dynamics.

[10] Matthias Trojahn, Frank Ortmeier (2012) Biometric authentication through a virtual keyboard for smartphones In: International journal of Computer Science and Information Technology,Vol 4, No.5.

[11] P. campisi, E. Maiorana, M. Lo Bosco, A.Neri (2008) User authentication using keystroke dynamics for cellular phones In: IET Signal Processing doi:10.1049/iet-spr.2008.0171

[12] Spillanae R.: ‘Keyboard apparatus for personal identification’, IBM Tech. Discl. Bull., 1975, 17, (3346)

[13] Adams C.W .: ‘Legal requirements for the use of keystroke loggers’. Proc. First Int.Workshop onSystematic Approaches to Digital Forensic Engineering (SADFE05), 2005