ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 5, May 2013

Security System Based on User Authentication Using Keystroke Dynamics

Manpreet Kaur[1], Rajinder Singh Virk[2]
Department of Computer Science and Engineering[1]
Guru Nanak Dev University, Amritsar (Punjab) India[2]

Abstract−Keystroke Dynamics is behavioural biometric used to measure the typing rhythm of the user when an individual types on the keyboard. It is assumed as a robust behavioural biometric. The functionality of this biometric is to measure the dwell time and flight time for changing keyboard actions. The paper focuses on enhancement of security using individual's typing actions to distinguish between authentic and fake users. A Multilayer Perceptron function with a Feed forward Propagation learning algorithm is used to trainindividual's typing actions through keystroke dynamics and cross validation is applied to validate their features.

Keywords−Keystroke Dynamics, Behavioural biometrics, Multilayer perceptron, Typing etc.

I. Introduction

Biometric technologies [1] are defined as automated methods of verifying or recognizing the identity of a living person based on physiological or behavioural characteristics. Biometricstechnologies are gaining popularity due to the reason that when used in conjunction with traditional methods of authentication they provide an extra level of security. Different types of biometrics are widely used for authentication. Biometrics can be classified into two categories: Physiological biometrics and Behavioural biometrics.

*Physiological biometrics*identifies the user based on physiological characteristics, such as fingerprints and eye retina/iris scanning. Implementation of physiological biometrics requires additional tools which lead to an increase in costs.

Behavioural biometrics depends on detecting the behavioural features of the user, such as signature, voice, and keystroke dynamics. Keystroke Dynamics is inexpensive to implement because typing pattern of an individual can be obtained using existing systems keyboard.

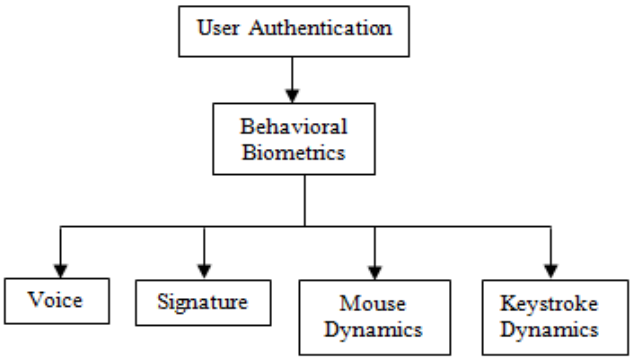

Figure 1. Classification of Behavioral Biometrics

Keystroke dynamics or typing dynamics[2][4] is the process of analyzing the way a user types at a terminal by monitoring the keyboard inputs thousands of times per second, and attempts to identify them based on habitual rhythm patterns in the way they type. It is the detailed timing information when each key was pressed and when it was released as a person is typing at a computer keyboard. The behavioural biometric of Keystroke Dynamics is the manner and rhythm in which an individual types characters on a keyboard or keypad. The keystroke rhythms of a user are measured to develop a unique biometric template of the users typing pattern for future authentication. Raw measurements available from every keyboard can be recorded to determine Dwell time

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 5, May 2013

(the time a key pressed) and Flight time (the time between "key up" and the next "key down"). Key hold time or dwell time [3] is defined as the time for which each keystroke was pressed. The keystrokelatency is the combination of the hold and flight times.In other words, the system verifies how a person types. Keystroke verification techniques [5] can be categorized as either static or continuous.

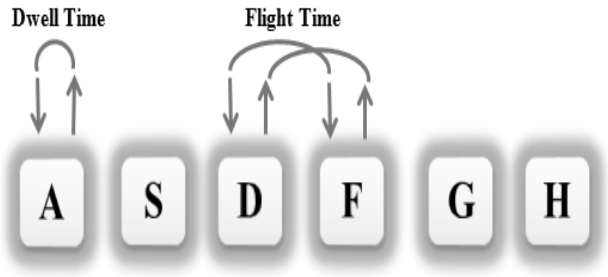

Figure 2. Keystroke Dynamics

Static verification system approaches study keystroke characteristics at a specific time. Continuous verification, on the other hand, examines the user's typing behaviour throughout the interaction time. Time-features can be extracted from keystroke data in many ways, such as studying keystroke latency, duration of key hold, pressure of keystroke, frequency of word errors, and typing rate. However, not all of these methods are widely used. Keystroke solutions are usually measured in three ways: dwell time – how long a key is pressed, flight time – how long it takes to move from one key to another, and key code.

The recorded keystroke timing data [2] is then processed through a unique neural algorithm, which determines a primary pattern for future comparison. Similarly, vibration information may be used to create a pattern for future use in both identification and authentication tasks. Data needed to analyze keystroke dynamics is obtained by keystroke logging.

II. Neural Network Overview

MLP neural network and RBF networks [5] have become the most widely used network architectures in pattern classification problems. The general difference between the two neural networks is that MLP is a more distributed approach compared to RBF, which only responds to a limited section input space.

A. Multilayer Perceptron Network

The MLP is a feed forward neural network pattern [5] that maps groups of input data onto a set of target outputs. Figure 3 shows the structure of the MLP network used in this paper. It consists of three main parts: an input layer, one or more hidden layers, and an output layer.

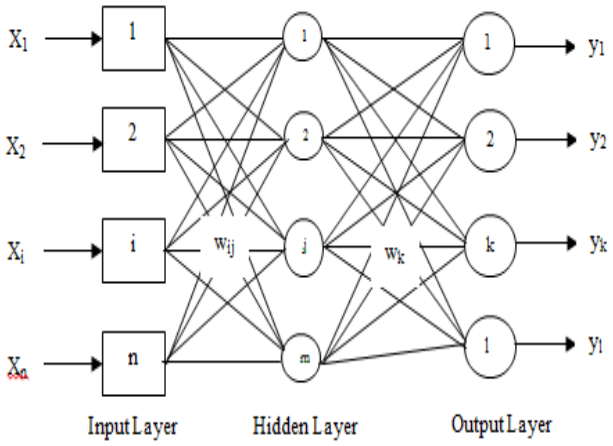

Figure 3. Architecture and signal flow of an MLP neural network [5]

The input layer distributes the input data to the processing elements in the next layer. The second stage is the hidden layer which incorporates the nonlinearity behaviour and the last stage shows the output layer. Input and output are directly accessible, while the hidden layers are not. Each layer consists of several neurons. The architecture in this paper uses only one hidden layer and the structure has an input x1, x2, …,xn and output y. Neurons are connected between different layers using weight and bias.

B. Radial Basis Function (RBF) Network

The popular alternative neural network architecture [5] is RBFN. RBFN normally configured with three different layers; input layer, single hidden layer of units and output layer as shown in Figure 4.

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 5, May 2013

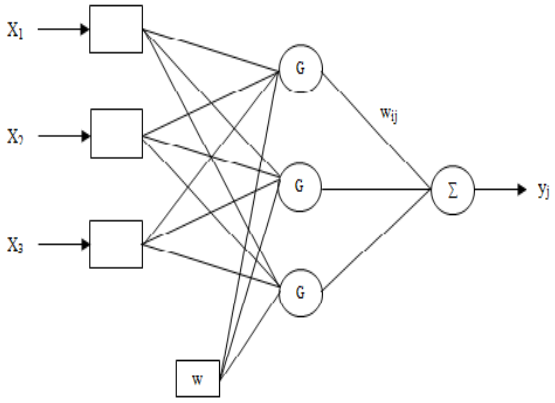

Figure 4. Architecture of RBF neural network [5]

The structure of this network [5] is similar to that of MLP, but it only produces one output. An activation function is used in the single hidden layer from a class of basic functions such as Gaussian and multi quadric. The commonly used basis function is the Gaussian basis function which has the parameter centre and width or spread. A Gaussian basis function monotonically decreases with distance from the centre and are local (give a significant response only in a neighbourhood near the centre) and are more commonly used than multi quadric which have a global response.

III. Related Work

N. Harun et al. (2010) [5] addresses the issue of enhancing systems security using keystroke biometrics as a translucent level of user authentication. The paper focuses on using the time interval between keystrokes as a feature of individuals' typing patterns to recognize authentic users and reject imposters. A Multilayer Perceptron neural network with a BP learning algorithm is used to train and validate the features. The results are compared with a Radial Basis Function neural network and several distance classifier method used in literature based on EER.

Mohammad S. Obaidatet al. (1993) [6] presents a new method of identifying computer users based on the individual typing technique of the users. The identification system is a pattern classification system based on a simulation of an artificial neural network. The user types a known sequence of characters, and the inter character times represent a pattern vector to be classified. This vector is presented to the classification system, and the pattern is assigned to a predefined class, thus identifying the user. The system correctly identified 97.8% users at a time. This intelligent system can be used to improve computer security, in addition to the traditional system in a cost effective manner.

A. Sulong et al. (2009) [7] the design and development of keystroke pressure based typing biometrics for individual user's verification which based on the analysis of habitual typing of individuals is discussed. RBFN which is one of the artificial neural networks is used as a pattern matching method. The effectiveness of the proposed system is evaluated based upon False Reject Rate and False Accept Rate. A series of experiment shows that the proposed system is effective for biometric-based security system.

TomerShimshon et al. (2010) [8] proposed a new method that compactly represents the keystroke patterns by joining similar pairs of consecutive keystrokes. This automatically created representation reduces the session size required for inducing the user's verification model. The proposed method was evaluated on 21 legitimate users and 165 attackers. The results were encouraging and suggest that the detection performance of the proposed method is better than that of existing methods. Specifically they attained a false acceptance rate (FAR) of 3.47% and false rejection rate (FRR) of 0% using only 250 keystrokes.

AgataKolakowska (2010) [9] presents a solution used to collect training data and extract features for a user authentication system based on the keystroke dynamics. Then a few approaches which might be applied to authenticate users basing on the keystroke rhythm are presented. These approaches are going to be tested in order to choose an efficient method to be applied as a part of a biometric security system for mobile workstations, which is being created within the framework of the SART -2 project.

H. Saevanee et al. (2008) [10] proposed behavioural manners of users over the touchpad acting like touch

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 5, May 2013

screen that is able to detect the finger pressure. These behaviours are keystroke dynamics and the finger pressure. The finding has shown that, the finger pressure gives the discriminative information more than keystroke dynamics with the k-NN analytical method. Moreover, using only the finger pressure produces high accuracy rate of 99%.

Chun-wei Tseng et al. (2010) [11] proposed an integrated technique approach to enhance user identification. They adopt keystroke dynamics as a biometric to strength conventional password mechanism and keep these characteristic values into RFID cards as pattern template for user identification.

Shallen Giroux et al. (2009) [12] ,presents a new approach to keystroke analysis that uses key press interval ratios to authenticate users. Participants in this study registered their passwords into a specially-designed analysisprogram. Keypress ratios were calculated, and neural network techniques were employed to obtain a mapping between patterns and the correct user. Results indicate that authentication through keypress ratios achieves high true acceptance rates, while also maintaining low false acceptance rates, which are particularly important in high-security applications. The approach presented here is suitable for incorporation into agent-based networked security systems.

IV. Problem Definition

This research work focus on providing better security system by analysing the typing behaviour of individualsusing keystroke dynamics. Main emphasis of this is to recognize typing behaviour of the users using FFNN with MLP to achieve more secure system.

Keystroke Dynamics is becoming popular in real time security systems. The methods developed so far are less efficient than proposed technique. This paper deals with typing behaviour of individuals using MLP and it also validates the features of users using cross validation in order to give more secure and efficient system than previous system.

V. Proposed Algorithm

The following algorithms are used in order to create new users and for authentication of users by matching data with the previously stored data of users in order to check whether they are authentic users or intruders.

A. New User Creation

Step1. Firstly, Users have to enter valid user name.

Step2. Then, Validity of user is checked by matching entered username with existing user's database to generate unique and valid username.

Step3. Finally, User clicks on create button after entering password and data successfully saved in database with typing behaviour of user.

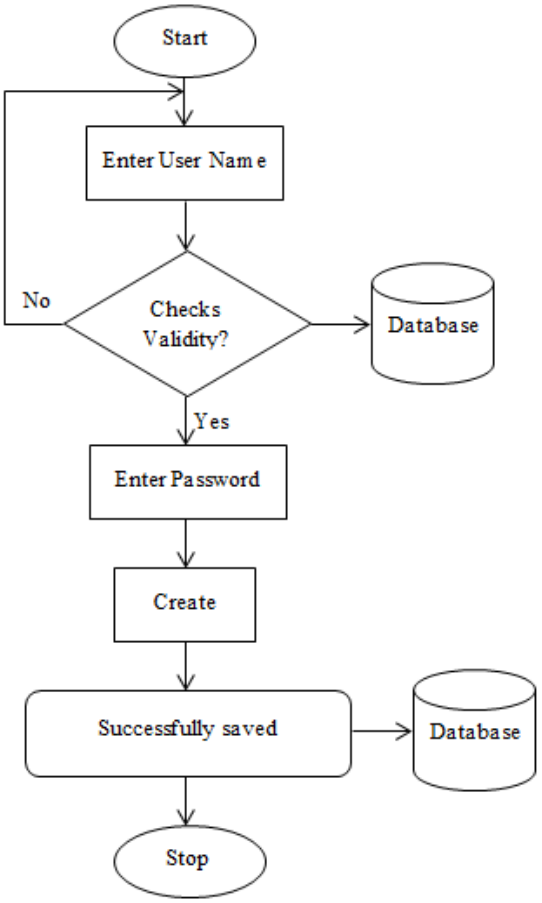

Figure 5. Flowchart for new user creation

B. User Authentication

Step1. User enters his user name and password previously created.

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 5, May 2013

Step2. If entered user name and password typing behaviour does not match with previously saved data in database then again repeat step1.

Step3. If entered user name and corresponding password typing rhythm matches with existing database then user is successfully logged in.

Step4. Successfully logged in user is authentic user other is intruder.

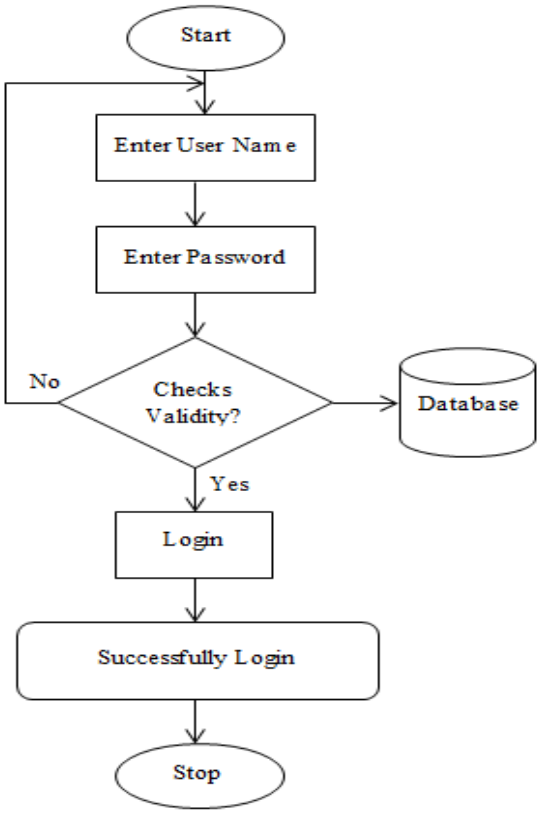

Figure 6.Flowchart for user's authentication

VI. Design And Methodology

A. Collection of Data

First step in our work is to create real time front end in Microsoft Visual Studio to grasp the behaviour of the users using Microsoft Access as a backend. When the user first time enter his password his behaviour is grasped in the DB and when the user again or next time enter his password his behaviour is checked by checking it with the previous DB stored in the Microsoft Access. If it is matched with the existing DB then the login is successful, otherwise the login is unsuccessful. We can also lock the system by providing the maximum attempts to the user to enter his password against the login ID. In this way, I collect sample data in order to evaluate the behaviour and performance of users.

B. Neurons Training Using Neural Network

Finally, train the collected data from different users using Weka tool. Multilayer perceptron (MLP) function is used for the purpose of training previously collected data. Afeed-forward ANN architecture was selected. Cross validation was applied to validate the features of different users in order to detect the genuine users and imposters.

VII. Experimental Results

A. Using Weka

First of all, open the Weka Simulator and add the database file in it. Choose the MLP function to Train the Data which is generated in the Microsoft Access.After that train the database using the MLP function and set the GUI of that function true. Then train the network using the two different sets i.e one set for training the data and other set for testing the data. Output of the function depends upon the various parameters like learning rate, momentum, validation threshold etc. as shown in fig. 7. Hence, the training time varies with varying of these parameters.

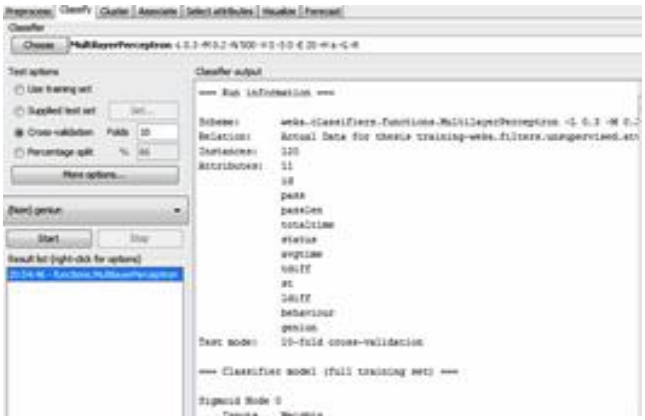

Figure 7: Training using the MLP function

B. Using Matlab

Matlab provides the facility to train the network by using the "nntool" command. Then, set the input data, target data and the network in it.After setting the input, target and network train the network as shown in fig. 8.

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 5, May 2013

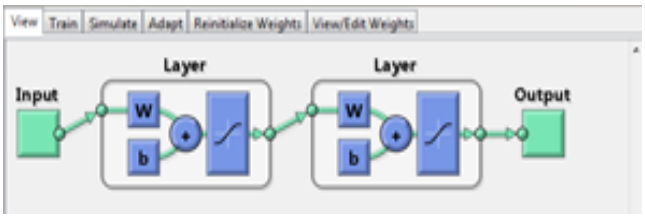

Figure 8: Network used in Matlab

The following are the various parameters used while training in the neural networks, shown in fig. 9.

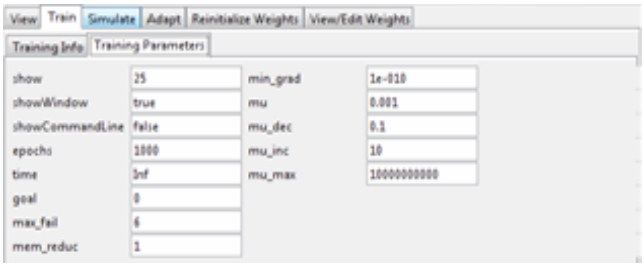

Figure 9: Various parameter used in Training (Matlab)

Finally, Training will be done using the above parameters and the performance depends upon the parameters used in it. At the end, the plot is performed and shown that the mean square error is reduced as the number of epochs increases. Performance graph is shown in fig. 10.

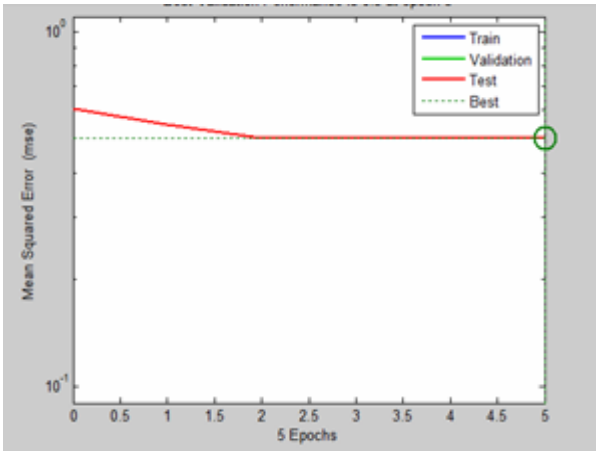

Figure 10: Performance graph

VIII. Conclusion

This proposed model based on Keystroke Dynamics using neural network provides advance level of security to the critical systems where security is one of the major concern. This model does not require the extra hardware like the biometric systems so overall cost cutting and economic cost in use. With this method, multiplelevel of security can be enforced to those systems where security is the major concern.In near future work will be extended for real time behaviour using embedded system.

Acknowledgement

The Authors are thankful to all reviewers for their valuable comments which help in improving the quality of paper.

REFERENCES

[1] Mrs. D. Shanmugapriya, Dr. G. Padmavathi, "A Survey of Biometric keystroke Dynamics: Approaches, Security and Challenges", *(IJCSIS) International Journal of Computer Science and Information Security*, Vol. 5, No. 1, 2009

[2] Wikipedia, Keystroke Dynamics, http://en.wikipedia.org/wiki/Keystroke_dynamics

[3] Salil P. Banerjee, Damon L. Woodard, "Biometric Authentication and Identification using Keystroke Dynamics: A Survey", *Journal of Pattern Recognition Research* 7 (2012) 116-139 July 10, 2012.

[4] FabianMonrose, Aviel D. Rubin, "Keystroke dynamics as a biometric for authentication", *Future Generation Computer Systems* 16 (2000) 351–359 3 March, 1999

[5] N. Harun, W. L. Woo and S.S. Dlay, "Performance of Keystroke Biometrics Authentication System Using Artificial Neural Network (ANN) and Distance Classifier Method", International Conference on Computer and Communication Engineering, 11-13 May 2010, Kuala Lumpur, Malaysia,2010 IEEE.

[6] Mohammad S. Obaidat and David T. Macchiarolo, "An On-Line Neural Network System for Computer Access Security", *IEEE TRANSACTIONS ON INDUSTRIAL ELECTRONICS*, VOL. 40, NO. 2, APRIL 1993IEEE.

[7]A. Sulong, Wahyudi and M.D. Siddiqi, "Intelligent Keystroke Pressure-Based Typing Biometrics Authentication System Using Radial Basis Function Network", *International Islamic University Malaysia (IIUM)*, Kuala Lumpur, Malaysia, 2009 IEEE.

[8] TomerShimshon, Robert Moskovitch, LiorRokach, Yuval Elovici, "Continuous Verification Using Keystroke Dynamics", *International Conference on Computational Intelligence and Security*, 2010 IEEE.

[9]AgataKolakowska, "Generating Training Data for SART-2 Keystroke Analysis Module", *Proceedings of the 2nd International Conference on Information Technology*,June 2010, Gdansk, Poland.

[10] H. Saevanee, P. Bhatarakosol, "User Authentication using Combination of Behavioral Biometrics over the Touchpad acting like Touch screen of Mobile Device", *International Conference on Computer and Electrical Engineering*, 2008 IEEE.

[11] Chun-wei Tseng, Ting-yi Lin, Feng-jung Liu, "Design and Implementation of a RFID-based Authentication System by Using Keystroke Dynamics", *Department of Information Management*, Cheng Shiu University, Taiwan, 2010 IEEE.

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 5, May 2013

[12] Shallen Giroux, R. Wachowiak-Smolikova, "Keypress Interval Timing Ratios as Behavioral Biometrics for Authentication in Computer Security", *Department of Computer Science and Mathematics*, Nipissing University, *North Bay*, 2009 IEEE.

Biography

Manpreet Kaur is currently Pursuing M.tech in Computer Science and Engineering from Guru Nanak Dev University, Amritsar. Completed B.tech in Computer Science and Engineering from College of Engineering & Management, Kapurthala in 2011.Area of interests areComputer Networks, Databases and Neural Networks.

Dr. Rajinder Singh Virk is currently working as Associate Professor in department of Computer Science & Engineering at Guru Nanak Dev University, Amritsar. He has published over 20 papers in referred journals and conferences (India and abroad). His research interests include Query Optimization and Soft Computing.