SmallSEOTools

PLAGIARISM SCAN REPORT

Words	979	Date	May 05,2020
Characters	6219	Exclude Url	

11%	89%	5	41
Plagiarism	Unique	Plagiarized Sentences	Unique Sentences

Content Checked For Plagiarism

Authors Title Contribution 1)David Umphress Department of Computer Science, Texas A&M University, College Station, 2)Glen Williams Department of Computer Science, Texas A&M University, College Station, ->Identity Verification through Keyboard Characteristics This paper proposes that the keystrokes can be static or continuous however continuous verification observes the patter of the user in the entire session of logging which give more security.The keystrokes are calculated as mean latency or average time between two press and score is calculated and from next time the score is calculated and evaluated with the average score. 1)Enzhe Yu Dept. of Ind. Eng., Seoul Nat. Univ., South Korea 2)Sungzoon Cho Dept. of Ind. Eng., Seoul Nat. Univ., South Korea -> GA-SVM wrapper approach for feature subset selection in keystroke dynamics identity verification . Keystroke dynamics vector is created based on typing patterns and trained.Manual cleaning of data results in errors and low accuracy and inconsistencies.Feature selection process which selects the required features and remaining features are ignored and genetic algorithm and SVM is used for results. 1)George R. Widmeyer Department of Information Systems, New Jersey Institute of Technology, 2) Michael L. Recce Department of Information Systems, New Jersey Institute of Technology -> An Investigation into the Efficacy of Keystroke Analysis for Perimeter Defense and Facility Access Pressure related features are brought into consideration.Feature points are obtained using pressure sensors and a biometric keypad was made to do the classification with the keystroke parameters.3 related parameters are considered namely amplitude or peak,peak area and peak sharpness. 1)Purvashi Baynath Electrical and Electronics Engineering, University of Mauritius 2)K.M. Sunjiv Soyjaudah Electrical and Electronics Engineering, University of Mauritius ->Keystroke recognition using neural network Biometric is more complex than password and is unique for each individual. Keystroke which tells about the unique pattern of a particular user.Here dwell time and hold time is used as characteristics and multilayer perceptron is used to train the data.A classifier of neural network to detect the user and evaluate him Motivation The main aim of this lab practical is to learn and apply new model on our dataset and understand the model well enough.LSTM is a common deep learning technique used now and then and plays a vital role in many predictions. Hence this report proposes using a deep learning model called Long Short Term Memory(LSTM) to determine fraud detection.For our approach, the general idea is to extract the desired features of pressure keystrokes by building a pressure sensitive keyboard and time parameters using pyhook library in python and apply different algorithms on the extracted features in order to obtain better fraud detection as nowadays fraud detection is the major concern in many industries Concept LSTM is the concept being contributed through this work of fraud detection technique called Keystroke Dynamics. LSTM have been developed as the short-term memory solution, with internal mechanisms called gates/neurons that can control the flow of information. By doing so, relevant information can be passed down the long chain of sequences to make predictions. With this network, almost all state-of - the-art tests are obtained based on repeated neural networks. In this work we have taken the keystrokes of different users both genuine and fraud.To know the working of Long Short Term Memory and how it is applied on the labelled data to determine this fraud detection called Keystroke Dynamics. Methodology This project contains the following processes. 1)Extracting the time features using a python tool. 2)Extracting pressure features 3)Creating the dataset.and training data with LSTM model and evaluating it 1. Extraction of time parameters: In this step, The capture time or hold time of individual keys and the delay between two keys (the time between the release of one key and the pressing of the other key). The time parameters of the keystrokes are:Different Timing Parameters between consecutive keys A,B Hold Time : key delay between pressed and key released. Press-Press Time: time in between two consecutive presses. Release-Release Time : time between two successive releases. Release-Press Time : time in between the current key release and the next key press. Press-Release Time : time between the current key press and the next key release. There will be many more timing parameters depending on the number of characters in the password. These Key Latencies are calculated using the pyxhook package in python.For simplicity, we have considered the password to be a common name. 2. Extraction of Pressure Parameters: This step involves building the pressure sensitive keyboard. This involves working with the hardware components.e we are to calculate the pressure applied under each key when pressed, We need a long sensor strip which is to be placed under the keys of the same row inside the keyboard.

Such sensor is FSR Interlink-408 as shown in figure. Using this sensor we can calibrate pressure along the length of the strip. It can detect pressure throughout its length. 3. Dataset and applying LSTM : Now we created a dataset of genuine user in which there are a total of 1000 entries labelled as 1. We also created a dataset of fraud users which consists of 500 entries and label as 0. We shuffle both datasets and the new dataset is our final one on which we apply LSTM. .Firstly, we take the pressure and time parameters for the name “shiva” which consists of 23 columns i.e., 23 features of the given password.Then after data preprocessing (shuffling and labelling the data) we split the data to 90% train and 10% test and train the data in batch of 3 and add layers of LSTM and dense layers and Softmax function is used as activation function along with adam optimizer and mean squared error as our loss parameter as it is accurateHere there are 23 features and LSTM models take those features into its network and as per the given data, we can set the number of time steps in the hidden layer to 1.

Sources	Similarity
Which Semantic Web? Frank M. Shipman Department of Computer... catherine c. marshall microsoft corporation 1 microsoft way redmond, wa (425) frank m. shipman department of computer science texas a&m university college station, tx (979) abstract through scenarios in the popular press and technical papers in the research literature, the promise of... https://docplayer.net/103918-Which-semantic-web-frank-m-shipman-department-of-computer-science-texas-a-m-university-college-station-tx-77843-3112-1-979-862-3216.html	20%

New Jersey Institute of Technology | Department of Information... find researchers and browse publications, full-texts, contact details and general information related to the department of information systems at new jersey institute ofarjun banur ananth. new jersey institute of technology.samer nadim karam. new jersey institute of technology. https://www.researchgate.net/institution/New_Jersey_Institute_of_Technology/department/Department_of_Information_Systems/members	20%
(PDF) Keystroke recognition using neural network biometric is more complex than password and is unique for each individual. in this work, the focus is made on the dwell time and flight time of the users' typing to recognize or reject an imposter. for this paper, the recognition rate obtained for the application of chaotic neural network was 99.1%. https://www.researchgate.net/publication/320178246_Keystroke_recognition_using_neural_network	5%