SmallSEOTools

# PLAGIARISM SCAN REPORT

|  |  |  |  |
|---|---|---|---|
| Words | 553 | Date | May 05,2020 |
| Characters | 3638 | Exclude Url |  |

|  |  |  |  |
|---|---|---|---|
| 4%<br>Plagiarism | 96%<br>Unique | 1<br>Plagiarized Sentences | 26<br>Unique Sentences |

## Content Checked For Plagiarism

Abstract Keystroke dynamics, keystroke biometric, typing dynamics and most recently biometric typing, real-time information that describes exactly when each key was pressed and when released as a person typing on a computer keyboard. This report looks at the problem of protecting data from unauthorized access by users. keystroke dynamics.The dataset consists of the pressure and time characteristics typing a common password (“shiva”) of a genuine user and many fraud users and Long Short Term Memory is used to train the dataset where we convert the train data into matrix using horizontal and vertical stack and input that to LSTM model with lstm layers and dense layers using optimizers and loss function including “softmax” activation in LSTM layer and “relu” in Dense layer. Finally we get train accuracy for each epoch and our validation accuracy is around 83% considering all epochs Keywords Keystroke Dynamics, Biometrics, Timing, Pressure characteristics. Introduction Nowadays public IT access is in the works process. An increasing number of web services are emerging. Many countries tend to build an electronic government that will provide and services to their citizens. The level of privacy in such cases services must be of the highest quality. But most of the secret leak information, and cyber attacks occur due to the web and services. The amount of land leaking every year is growing. As of October 2016 biometric authentication is in use 57% of businesses. Biometric images of the figure (finger or iris) is not a secret, so it can be copied by making a physical or digital model (remote validation). Private biometric images contain a secret (password) about it that can provide the highest level of protection. See enter the exposed keystroke power while typing a password phrase. The weak point of the validation method by using the keystroke power for very low reliability decisions made as opportunities for false rejection error (FRR) and false access error is very important to use this method in practice. The keystroke features of the users are calculated to obtain a unique biometric pattern of that user for authentication in the future.The data needed to analyze the keystroke's power is obtained by keystroke entry.There exists different accents of english among different people similarly there exist unique pattern among different users.Though the keystroke depends on physical and mental state it is observed that there exists a consistency while typing words. Literature review Keystroke capabilities have become an active research area due to the growing importance of cyber and computer security or network control. There are two types of authentication that work through these important keystroke steps.In paper[1] these keystroke biometrics recorded are used for the authentication purposes.This paper describes the biometrics can be physical or behavioural out of those keystroke biometrics are one of the features of behavioural. In paper[2] the feature subset selection for the parameters are discussed avoiding manual data preprocessing and reduce typing inconsistencies In paper[3] the only pressure characters are considered for determining the fraud detection and 3 pressure characters and used as parameters In many works, keystroke biometrics research has utilized many existing machine learning and classification techniques.Both classical and advanced classifiers have been used like neural networks [4] In their papers, Bergadano et al.[5] also studied these n-graphs.They have extracted the features using the relative order of times of duration for different n-graphs.

| Sources | Similarity |
|---|---|
| Keystroke dynamics - Wikipedia<br>https://en.wikipedia.org/wiki/Keystroke_dynamics | 10% |