SmallSEOTools

# PLAGIARISM SCAN REPORT

| | | | |
|---|---|---|---|
| Words | 456 | Date | May 05,2020 |
| Characters | 2917 | Exclude Url | |

| 6% | 94% | 1 | 15 |
|---|---|---|---|
| Plagiarism | Unique | Plagiarized Sentences | Unique Sentences |

## Content Checked For Plagiarism

Train data is reshaped into 3D inorder to input into the Long Short Term Memory model.The model consists of LSTM layers and Dense layers, LSTM layer consists of 80 neurons whereas a dense layer has input data shape.Model trains the data in batch size of 3 of 20 epochs where trainloss,train error,validation loss,validationerror are the parameters obtained at each epoch. Experimental work details Programming language :python Libraries used: numpy, pandas, sklearn. Platform : Jupyter notebook Dataset Now we created a dataset of one user(genuine) in which he types the name/password(shiva) in 100 different sessions of a day in which each session contains 10 repetitions making a total of 1000 entries labelled as 1. Time parameters and pressured parameters of the user are named as a column in the dataset and used as an individual feature for that user. The data was not being collected at the same part of the day.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. Contributions The major concept used in this lab work is Long Short Term Memory. I have learned how to apply LSTM on the fraud detection technique called keystroke Dynamics and I have studied a few topics of deep learning. Conclusion and Future work In this report, we propose Keystroke Dynamics using Long Short Term Memory. This method gives better results when compared to applying LSTM/neural networks to the dataset that contain only time parameters.To the validation accuracy of the proposed method(85%) is better in the existing method as the third picture shows the accuracy of existing one(75%).The proposed method works better because the more features are considered which classifies the typing pattern more uniquely . This method can also be applied on large datasets and adding more LSTM and Dense layers according to our requirement. References [1] D.Umphress and G. Williams, “Identity Verification through Keyboard Characteristics”, Int’l J. Man-Machine Studies, Vol. 23, No. 3, pp. 263–273, 1985. [2] E.Yu and S.Cho.“GA-SVM wrapper approach for feature subset selection in keystroke dynamics identity verification”, In Proc. Int’l Joint Conf. on Neural Networks (IJCNN), pp. 2253–2257, 2003. [3] C. S. Leberknight, G. R. Widmeyer and M. L. Recce, "An Investigation into the Efficacy of Keystroke Analysis for Perimeter Defense and Facility Access," 2008 IEEE Conference on Technologies for Homeland Security, Waltham, MA, 2008, pp. 345-350. [4] P. Baynath, K. M. S. Soyjaudah and M. H. Khan, "Keystroke recognition using neural network," 2017 5th International Symposium on Computational and Business Intelligence (ISCBI), Dubai, 2017, pp. 86-90. [5] D. Gunetti and C. Picardi. “Keystroke analysis of free text”, ACM Transactions on Information and System Security, 8(3):312–347, 2005.

| Sources | Similarity |
|---|---|
| Keystroke analysis of free text \| Request PDF<br><br>article in acm transactions on information and system security 8(3):312-347 · august 2005 with 369 reads.keystroke analysis can be done with two different approaches static text and free text. ... ... in free text mechanisms, analysis is done while the user types any text at will.<br><br>https://www.researchgate.net/publication/220593550_Keystroke_analysis_of_free_text | 7% |