**Detection Of Malware Using Deep Learning Techniques**

While working on a text classification challenge utilizing natural language processing, we are interested in a project that involves the identification of malware from datasets. Finding a match with the virus definition dataset, which is periodically updated, allows for the detection of malware. This method of detection signature-based detection. There are numerous machine learning methods developed to recognize new malware. With its feature engineering techniques and incompatibility with a large dataset, this takes too long. Deep learning approaches allow for the entire skipping of this stage. We might detect reoccurring malware patterns by combining this with recurrent neural networks. Also adding this with Recurrent Neural Networks, we could capture recurring patterns in malware.

As the work progresses, we will use two datasets made up of the ICML-09 dataset and the Malimg dataset to assess how well malware viruses can be detected. 9,339 malware samples from 25 different malware families are included in the Malimg collection. And in the ICML-09 data set, there are 3.2 million features and 2.4 million URLs (examples).

|  |  |
| --- | --- |
| Name | ID |
| Saiful Islam | 1731604642 |
| Iftekharul Islam Pranto |  |

Presented By