**Convolutional Neural Network Based Algorithm for Early Warning Proactive System Security in Software Defined Networks**

Software-Defined Networking is an innovative architecture approach in the networking field. This technology allows networks to be centrally and intelligently managed by unified applications such as traffic classification and security management. Traditional networks’ static nature has a minimal capacity to meet organisations business requirements. Software-Defined Networks (SDNs) are the emerging architectures that address a range of networking challenges with new solutions. Nevertheless, these centralised and programmable techniques face various challenges and issues that require contemporary security solutions such as Intrusion Detection Systems. Recently, the majority of this type of security solution has been developed using Machine Learning techniques. Deep Learning algorithms have recently been used to provide more accuracy and efficiency. This paper presents a new detection approach based on Convolutional Neural Network (CNN). The experiments proved that the proposed model could be successfully implemented in a Software-Defined Network controller to detect various attacks with 100% accuracy, achieved a low degradation rate of 2.3% throughput and 1.8% latency when executed in a large-scale network.

**EXISTING SYSTEM:**

* In existing methods analysis of the viability of Logistic regression to detect the behaviour of network traffic by modelling it as a sequence of states that change over time.
* In existing methods verify the performance of Machine learning model based network in classifying intrusion traffics.

**DISADVANTAGES:**

* All the above methods treat the entire network traffic as a whole consisting of a sequence of traffic bytes. They don’t make full use of domain knowledge of network traffics.
* Existing methods treats traffics as independent and ignore the internal relations of network traffics.

**PROPOSED SYSTEM:**

* We propose an end-to-end deep learning model with ml models that is composed of logistic regression and attention mechanism. CNN can well solve the problem of Software Defined Networks and provide a new research method for Early Warning Proactive System
* We compare the performance of ML Modes with traditional deep learning methods, the model can extract information from each packet. By making full use of the structure information of network traffic, the logistic regression model can capture features more comprehensively. 4) We evaluate our proposed network with a real NSL-KDD dataset. The experimental results show that the performance of algorithm is better than the traditional methods

**ADVANTAGES:**

* This method is used to analyse the important degree of packet vectors to obtain fine-grained features which are more salient for malicious traffic detection.
* At the output layer, the features generated by attention mechanism are then imported into a fully connected layer for feature fusion, which obtains the key features that accurately characterize network traffic behaviour.

## SYSTEM REQUIREMENTS

### HARDWARE REQUIREMENTS:

* System : Intel(R) Core(TM) i3-7020U CPU @ 2.30GHz
* Hard Disk : 1 TB.
* Input Devices : Keyboard, Mouse
* Ram : 4 GB.

### SOFTWARE REQUIREMENTS:

* Operating system : Windows XP/7/10.
* Coding Language : Python
* Tool : Anaconda
* Interface : Jupiter notebook. Flask web app