**Malicious Attack Detection by Convolutional Deep Learning Model for Web Applications**

**Madhankumar Y**

A summary by-

*Shashank Agarwal*

**Introduction**

A distributed denial-of-service (DDoS) attack is a malicious attempt to disrupt the normal traffic of a targeted server by overwhelming it with a flood of Internet traffic, by utilizing multiple compromised computer systems as sources of attack traffic.

The major challenges in the field of malicious network activity detection are a huge volume of network traffic, diversity due to new attacks, and reduced performance of low-frequency attacks due to a high imbalance between various classes of attacks.

**Literature Review**

A research in 2017 proposed a security-based watermarking to LEACH routing protocol. Digital watermarking is a trend in security techniques that hides data by using data embedding and data extraction processes. Watermarking technology is integrated into different frames without adding an overheard as in the conventional encryption.

In a 2019 research, particle swarm optimization-based probabilistic neural network (PSO-PNN) was used for the detection and recognition process. UNSW-NB15 dataset was used to validate the proposed solution by characterizing different types of malicious behaviours exhibited by users.

In another research, convolutional neural networks (CNNs) were used to identify and classify grayscale images converted from executable files of malicious code.

**Research Gap**

The http flood attack causes large number of resources to be allotted in response to the few requests from the clients. Existing method’s detection level of DDoS attacks is low.

**Attack Detection Methodology**

KDD cup attack detection database are considered for attack detection and prevention modelling.

1. Initially perform the pre-processing to remove the unwanted data for detection stage.

2. Feature size reduction by Incremental component analysis (ICA) technique, facilitate better generalization, and reducing the learning and operating complexity of the classifiers.

3. Finally, Convolutional Neural Network (CNN) training to detect the DDOS and some attacks from KDD set. The KDD data set is a well-known benchmark in the research of Intrusion Detection techniques.

CNN structure comprises of three-layer capacities:

**1. Convolutional layer:** used to extract the various features from the input images.

**2. Pooling layer:** decrease the size of the convolved feature map to reduce the computational costs

**3. Fully connected layers:** classification of the flattened input images take place.

The output classes were DDOS, Probe, U2R (User to Root) and R2L (Remote to Local (User)).

DARPA’98 is about 4 gigabytes of compressed raw (binary) tcpdump data of 7 weeks of network traffic, which can be processed into about 5 million connection records, each with about 100 bytes.

Encapsulation of all the attributes leads to a delay in detection.