Web Attack Discovery using Deep Convolution Neural Network and Multi-Channel Convolution Neural Network

Yeleti Aarti
Computer Science, JNTUK, AP, India

Yeleti Jyoti
Computer Science, Pragati Engineering College, AP, India

Abstract— The main source of the Internet is the World Wide Web(WWW). In today's scenario, the majority of services are provided by web applications such as information sharing, entertainment, education, etc. With the increase of several services in the Web, the Web has become the main venue for the attackers. Many machine learning methods are developed for discovering web attacks. In this paper two deep learning techniques, Multi-Channel Convolution Neural Network and Deep Convolution Neural Network are proposed which are a special type of Convolution Neural Networks developed for efficiently identifying web attacks.

Keywords - Web attacks, Multi-Channel Convolution Neural Network, Convolution Neural Network

I. Introduction

The World Wide Web(WWW) has become a centre of development in the Information Era. The Web or the Internet is a great convenience to the people, as currently a majority of services are provided by web applications. With the great increase in the number of users for the Internet, the Web has become the main source of attack for cybercriminals[1]. Hackers are focusing mainly on web attacks, as it involves simply modifying the application layer than on traditional computer attacks. Recent studies have shown web attacks have outnumbered traditional computer security concerns.

There are several technical solutions to guarantee web security such as web application firewalls, web intrusion detection systems. There are two basic methods to detect Web attacks, the signature-based [2] and the anomaly-based [3]. The signature-based method builds the detection model from known attacks and any behavior having the corresponding attack signatures is identified as an attack. On the contrary, the anomaly-based method creates a profile from normal behaviors and any violation is identified as an attack. Both the methods must have enough characterization and generalization ability of abnormal or normal behaviors for efficient detection of attacks.

In this paper, we present two deep learning techniques for detecting web attacks that are the Deep Convolution Neural Network and Multi-Channel Convolution Neural Network which are a special type of Convolution Neural Networks.

II. Related Work

1. Zolotukhin et al. [4] have proposed an anomaly detection method for Web attacks through analysis of HTTP logs. The method employs the n-gram models to extract relevant features from three fields in HTTP logs, including Web resources, query attributes and user agents. Correspondingly, three machine learning algorithms are used, namely, Support Vector Data Description (SVDD), K-means, and Density-Based Spatial Clustering of Applications with Noise (DBSCAN)
2. Choras and Kozik [5] have proposed a machine learning approach to model normal behaviors of Web applications and to detect Cyber-attacks. The model is based on information obtained from HTTP requests and consists of patterns that are obtained using graph-based segmentation technique and dynamic programming.
3. Saxe and Berlin [6] have exposed a deep learning approach to several security detection problems including malicious URLs detection. They used Convolution Neural Network with different word embedding's
4. Zhang, Ming, Boyi Xu, Shuai Bai, Shuaibing Lu, and Zhechao Lin[7] in their conference paper proposed a specialized Convolution Neural Network using Word 2Vec word embedding for Web Attack detection
5. Kuang, Xiaohui, Ming Zhang, Hu Li, Gang Zhao, Huayang Cao, Zhendong Wu, and Xianmin Wang[8],in their paper proposed a Deep WAF is proposed that uses CNN and LSTM for detecting Web Attacks

III. Proposed Method

Dataset

The dataset used to discover web attacks is *CICIDS 2017*. The dataset is developed by the Canadian Institute of Cyber Security with the main aim of Intrusion detection and prevention. The CICIDS2017 dataset contains information about different types of attacks such as Distributed Denial of Service, Denial of Service etc., of which in this paper information regarding Web Attacks is considered.

The dataset contains recent information about three types of attacks. They are the Web attack-Brute Force, Web attack- XSS, Web attack- SQL injection. Along with the web attack information the dataset contains information about BENIGN also known as normal human activities. So in this paper, the main motto is to classify the Web attacks from the BENIGN.

Web attackers mainly target the application layer and use the HTTP requests and responses to hack the data. Brute-force attacks are used for attacking and discovering hidden content/pages within a web application. These attacks are usually sent via GET and POST requests to the server. Cross-site scripting (XSS) involves injecting malicious code into a vulnerable web application. In this XSS web attack, the users of the web application are the ones at risk. SQL injection uses malicious SQL code for backend database manipulation to access information that was not intended to be displayed.

3.1 Data Pre-processing

Data Processing involves making data suitable for classification in the deep learning model. To use the CICIDS2017 dataset for classifying Web Attack from BENIGN the data in the dataset should undergo pre-processing. The following are the steps involved in the pre-processing of the dataset.

1. Loading the necessary libraries such as pandas , numpy, matplotlib
2. Loading the dataset
3. Removing redundant data
4. Removing NULL data
5. Tokenizing the data
6. Normalizing the data using Min-Max Normalisation.

3.2 Word Embedding

The CICIDS2017 dataset after pre-processing should pass through word embedding. Word embedding creates a proper association between words. In this, the word embedding used is the GLoVE[9]. GLoVE also known as Global Vectors is developed by Stanford University. The GLoVe is an open-source tool used for word embedding. It takes word –word co-occurrence statistics from corpus and reduces sparse matrix into dense one by matrix factorization. The GLoVE creates vectors that are passed as input to the special Convolution Neural Network Models.

3.3 Model Implemented

3.3.1 Deep Convolution Neural Network (Deep-CNN)

The Deep Convolution Neural Network is one of the extended forms of the Convolution Neural Network. The Convolution Neural Network has a Convolution Layer, Max Pooling, Dense layer. Deep Convolution Neural Network has a structure similar to Convolution Neural Networks, but the difference is that it has more number of convolution and dense layers that makes it more efficient in classifying Web Attacks from BENIGN.

The following are the different layers in the Deep Convolution Neural Networks

1. **Convolution Layer**: The convolution layer is the first layer that extracts features from the embedded dataset. The arguments used in the Convolution layer are filter size which specifies the dimensionality of output space, kernel size which specifies the length of the convolution window. The activation function used in this layer is ReLU. ReLU stands for Rectified Linear Unit. It introduces non-linearity in the model. In the developed Deep Convolution Neural Network the model has not one convolution layer but more number of convolution layers.

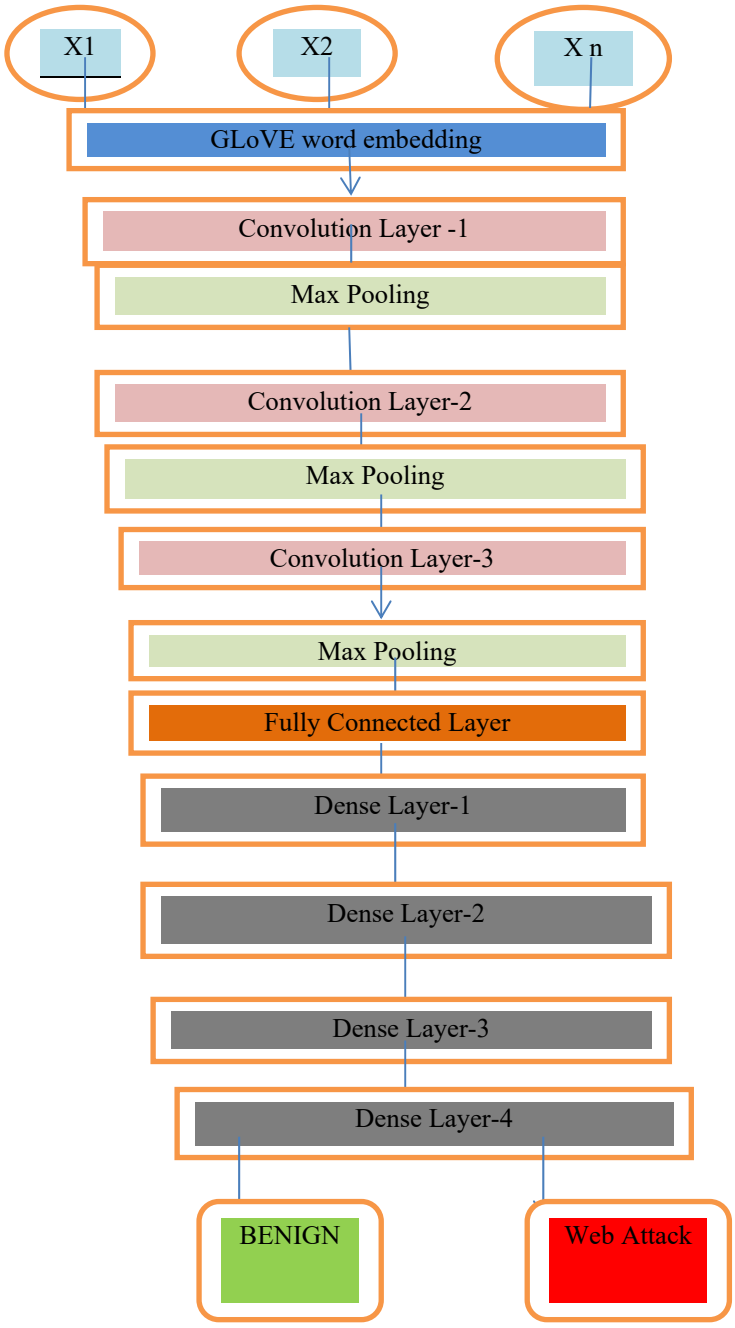

Figure 1: Deep Convolution Neural Network

2. **Polling Layer**: Pooling reduces the number of parameters if the dataset is too large. There are different types of pooling such as Max Pooling, Average Pooling, etc. In the model developed the pooling used is Max Pooling. Max Pooling takes the largest element from the feature map which is generated after Convolution.
3. **Fully Connected Layer**: The Fully Connected Layer is used to flatten the data and fit the data .
4. **Dense Layer**: The Dense Layer is the deeply connected layer which takes as argument filter size.

3.3.2 Multi-Channel Convolution Neural Network

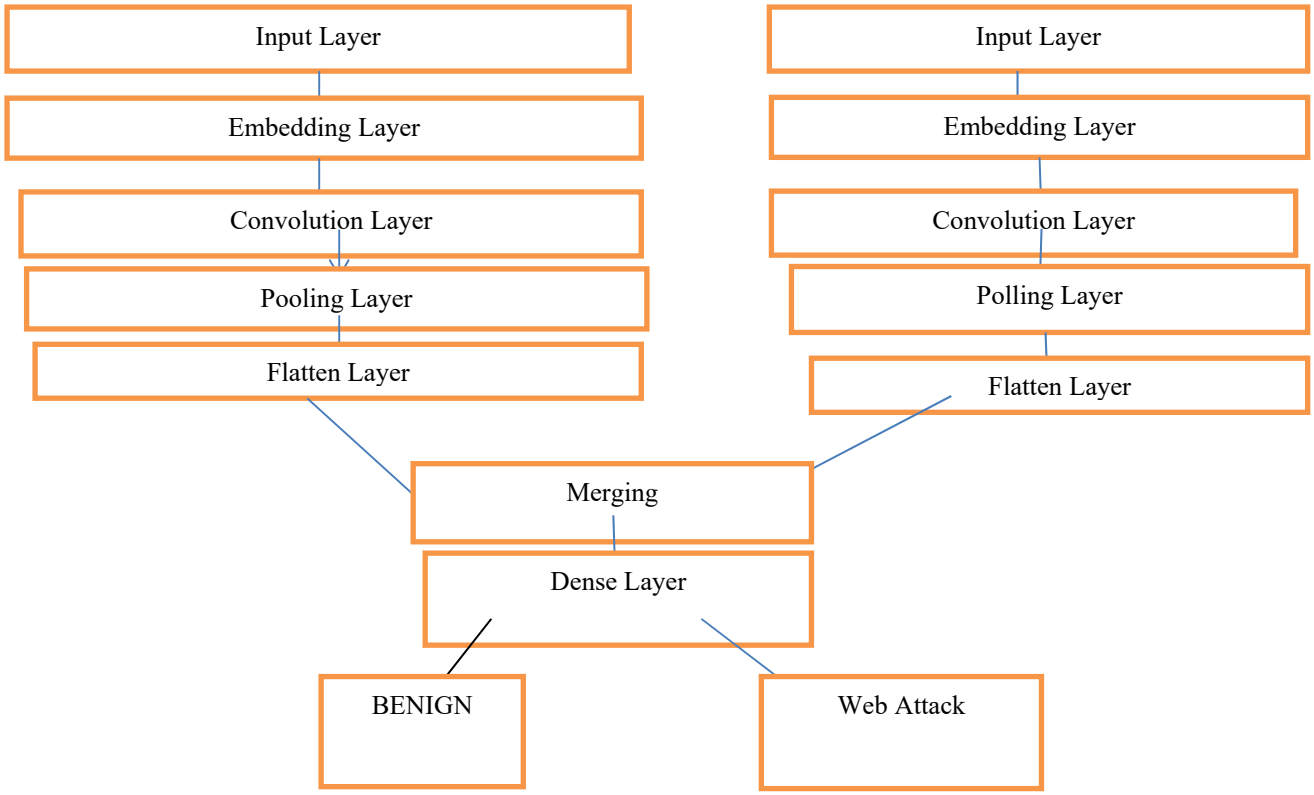

Figure 2 : Multi –Channel Convolution Neural Network

Multi-Channel Convolution Neural Network is a special type of Convolution Neural Network. Multi-Channel Convolution Neural Network involves using standard Convolution Neural Network with different kernel size. The Multi-Channel Convolution Neural Network used for classification of Web Attacks have the following layers as shown in Figure 2

1. **Input Layer**: Input Layer takes the input that are the different features from the dataset
2. **Embedding Layer**: Embedding Layer takes the features of GLoVE
3. **Convolution Layer**: The Convolution Layer takes input from the word embedding layer and convolves it and passes as input to Pooling.
4. **Pooling layer**: The pooling layer consolidates input from the convolution layer.
5. **Flatten Layer**: Flatten layer is used to maintain the dimensionality
6. **Dense Layer**: Dense Layer is used to produce output that's is Web Attack or BENIGN.

In the model developed since individual convolution layers are used, all the flatten layers are merged and passed as input to the Dense layer. The activation function used is RELU. The different kernel sizes are used such as 4, 6, and 8. The last dense layer uses Sigmoid Activation function that is used to classify Web Attack.

IV. Experiment and Results

4.1 Dataset Preparation

The CICIDS2017 dataset used to detect Web Attack contains the following information. It contains 2180 instances of web attack of which 1507 belong to Web Attack Brute Force,652 Web Attack Brute Force,21 Web Attack SQL Injection.

The dataset contains 79 different attributes which contain information about different types of attack. The last attribute is the label which gives the information based if the information is about BENIGN or Web Attack. The BENIGN data collected from the dataset is 6000.The training split is 80% and the test split is 20%.

4.2 Performance and Metrics

The performance metrics used to evaluate the detection of Web Attack are accuracy, precision and recall, and F1score. By using these performance metrics, the extent to which Web Attacks can be correctly classified is analysed.

Based on the information of the confusion matrix the precision, recall,f1-score are predicted [10].

Confusion Matrix: The confusion matrix is used to describe the performance of how well the classification is performed. The confusion matrix consists of values such as true positive, true negative, false positive, and false negative. In the confusion matrix comparison is done between predicted and actual values.

True Positive(TP): It states that both the actual and predicted values are correct.

True Negative(TN): In this, the predicted value is correct but not the actual value

False Positive(FP): In this the actual value is correct but the predicted value is false

False Negative(FN): In this both the actual and predicted values are wrong.

	Predicted values	
Actual values	**True Positive TP**	**False Positive FP**
	False Negative FN	**True Negative TN**

Recall: Recall is the ratio of correctly predicted values to all the values

Recall = True Positive / True Positive + False Negative

Precision: Precision finds the true value from all the truth values

Precision = True Positive/True Positive+ False Positive

F1 Score: The average of precision and recall

F1 Score = (2*Precision*Recall)/ Precision + Recall

The table below represents the performance metrics achieved by the Deep Convolution Neural Network on correctly classifying Web Attacks.

Label	precision	recall	f1-score
0	0.96	0.98	0.97
1	0.98	0.95	0.96

Here label 0 indicates BENIGN and label 1indicates Web Attack. The precision achieved in correctly classifying the Web Attack is 98% and Recall is 95%

The accuracy achieved by Deep Convolution Neural Network are as follows

Training Accuracy : 97.586%

Testing Accuracy: 96.234%

The table below represents the performance metrics achieved by the Multi-Channel Convolution Neural Network on correctly classifying Web Attacks.

Label	precision	recall	f1-score
0	0.96	0.98	0.967
1	0.97	0.96	0.964

Here label 0 indicates BENIGN and label 1indicates Web Attack. The precision achieved in correctly classifying the Web Attack is 97% and Recall is 96%

The accuracy achieved by Multi Channel Convolution Neural Network are as follows

Training Accuracy : 96.723%

Testing Accuracy: 95.554%

V. Conclusion

In this paper, two deep learning techniques using Convolution Neural Networks are proposed to classify and detect web attacks. The two models are Deep Convolution Neural Network and Multi-Channel Convolution Neural Network. The steps involved in implementing both the models are data pre-processing, GloVe word embedding, deep learning model implementation, and result classification. The experiments show that the models proposed can efficiently classify Web Attacks with an accuracy greater than 96%.

The classified data can be used efficiently in various fields to prevent Web Attacks and safeguard the information.

REFERENCES

[1] Symantec Internet Security Threat Report: Trends for July–December 2007. http://eval. symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_exec_summary_internet_ security_threat_report_xiii_04-2008.en-us.pdf.

[2] Axelsson, S.: Research in intrusion-detection systems: a survey. Technical report 98–17, Department of Computer Engineering, Chalmers University of Technology (1998)

[3] Garcia, T.P., Diaz, V.J., Macia, F.G., et al.: Anomaly-based network intrusion detection: techniques, systems and challenges. Comput. Secur. 28(1), 18–28 (2009)

[4] Zolotukhin, M., Hamalainen, T., Kokkonen, T., et al.: Analysis of http requests for anomaly detection of web attacks. In: Proceedings of IEEE 12th International Conference on Dependable, Autonomic and Secure Computing (DASC), pp. 406–411 (2014)

[5] Choras, M., Kozik, R.: Machine learning techniques applied to detect cyber attacks on web applications. Log. J. IGPL 23(1), 45–56 (2015)

[6] Saxe, J., Berlin, K.: eXpose: a character-level convolutional neural network with embeddings for detecting malicious URLs, file paths and registry keys. arXiv preprint arXiv:1702.08568 (2017)

[7] Zhang, Ming, Boyi Xu, Shuai Bai, Shuaibing Lu, and Zhechao Lin. "A deep learning method to detect web attacks using a specially designed cnn." In International Conference on Neural Information Processing, pp. 828-836. Springer, Cham, 2017.

[8] Kuang, Xiaohui, Ming Zhang, Hu Li, Gang Zhao, Huayang Cao, Zhendong Wu, and Xianmin Wang. "DeepWAF: Detecting Web Attacks Based on CNN and LSTM Models." In International Symposium on Cyberspace Safety and Security, pp. 121-136. Springer, Cham, 2019.

[9] https://nlp.stanford.edu/projects/glove/

[10] https://towardsdatascience.com/beyond-accuracy-precision-and-recall-3da06bea9f6c

[11] CICIDS 2017 dataset https://www.unb.ca/cic/datasets/ids-2017.html