كلية الهندسة
College of Engineering
QATAR UNIVERSITY جامعة قطر
Graduate Students, Sciences and Engineering

THE USE OF ARTIFICIAL INTELLIGENCE FOR THE DETECTION OF COVERT CHANNELS ATTACKS

IN NEW GENERATION INTERNET PROTOCOL IPV6

Felwa Al-Senaid, Prof. Sumaya Al-maadeed
Email: fa1003849@qu.edu.qa , s_alali@qu.edu.qa

ABSTRACT

Being instrumental to the Qatar national vision 2030 activities and following up with "Achieving Security, stability and maintaining public safety" objectives, the present paper aims to propose a solution to safeguard the information and monitor internet communications in the region effectively. The increased dependence of internet-based technologies in all facets of life challenges the government and policymakers with the need for an effective shield mechanism against passive and active security violations. The present paper adopted an artificial intelligence-based solution for detecting suspicious communications. Further, a dataset created which was generated by simulating a number of attacks and normal communications was used for the purpose of training and testing the model. The experimental results of training and testing the suggested approach produces an accuracy of 100% with a score of 1 for precision, recall, and F1 score. The project forward a novel, efficient approach for detecting covert channels and suspicion communication.

INTRODUCTION

The proliferation of internet-based technologies and communication channels raises the need for effective security protocols and mechanisms. IPv6, the most recent version of network layer protocol facilitates reliable communication and data transfers over the network. IPv6 was introduced with a 128-bit address, which includes an extension to carry optional internet layer information enables for the steady growth of the internet. Although IPv6 extension header provides supplementary information for passing and processing of internet packets, there is a higher potential for malicious use. The Covert channels are one such security threat emphasizes on secrecy and hidden communication between two IP addresses performed by packet manipulation and would result in security policy violation. The present paper aims to contribute to the discussion of covert channel in IPv6 and propose a new security mitigation mechanism for covert channel. The proposed mechanism will act as a passive warden to an internet data transfer across network connected devices.

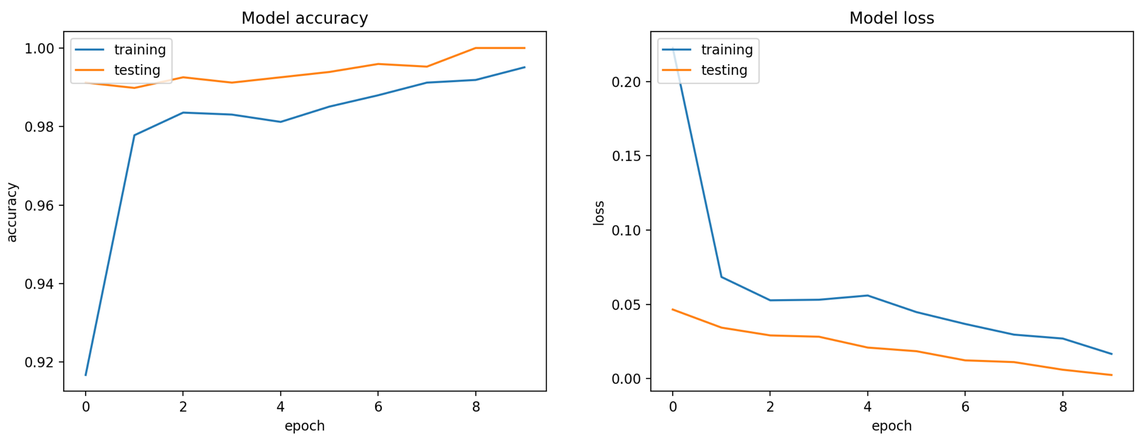
METHODOLOGY

Data Collection: Due to the unavailability of benchmark dataset in IPv6, the present paper generated its own training dataset by capturing the traffic of simulated covert channel attacks developed using oracle virtual GNS3 platform. Subsequently, the dataset has been processed to prepare for training and testing the proposed detection model. Each record in the dataset is a representation of IPv6 and ICMPv6 header fields, described by 9 attributes.

Model Design: For the purpose of research, a multi layer deep learning model is adopted. Essentially, the model is based on a Convolutional Neural Network (CNN) architecture and implemented with a python script and Keras deep learning library. The proposed model has been trained using the dataset to meet the features of an expedient classifier. For examining the performance and efficiency of the model, 10% of the captured dataset was employed for the testing phase.

RESULTS

The quality and the performance of the proposed solution were assessed primarily using four evaluation metrics: accuracy, f1 score, precision, and recall. Fundamentally, a 10-k cross validation approach was adopted for testing the performance of the proposed model. The experimental results indicate an accuracy of 100% which illustrate the productiveness of the model. Further comprising, the results put forward a value of one of F1 score, recall, and precision pointing to the adequacy, efficiency and feasibility of the classifier in the detection of network covert channel attacks.



CONCLUSION

With prevailing security threats and vulnerabilities associated with the advanced networked systems, the present paper aims to explore the novel concept of covert channel attacks detection in IPv6 using artificial intelligence. The proposed model was primarily based on a convolutional Neural Network (CNN) which was further trained and tested using exclusively created dataset. The experimental analysis not only involves the performance assessment of the model, but also training the dataset for gearing up to the subsequent testing phase . The model generated a promising result of 100% accuracy while proving its efficacy. The present paper identifies the need for more advanced research and investigation in the field of covert channel attacks to shield internet users against various complex forms of cyber attacks. Furthermore, there exists a need for contributing to the development of an open-source dataset, which would further facilitate the research community for engaging in IPV6 security research. The current paper foresees more practical applications to the proposed model in the internet security platform.