International Journal of Grid and High Performance Computing
Volume 13 • Issue 1 • January-March 2021

An Ensemble Deep Neural Network Model for Onion-Routed Traffic Detection to Boost Cloud Security

Shamik Tiwari, Department of Virtualization, School of Computer Science, University of Petroleum and Energy Studies, Dehradun, India

ABSTRACT

Anonymous network communication using onion routing networks such as Tor are used to guard the privacy of sender by encrypting all messages in the overlapped network. These days most of the onion routed communications are not only used for decent cause but also cyber offenders are ill-using onion routings for scanning the ports, hacking, exfiltration of theft data, and other types of online frauds. These cyber-crime attempts are very vulnerable for cloud security. Deep learning is highly effective machine learning method for prediction and classification. Ensembling multiple models is an influential approach to increase the efficiency of learning models. In this work, an ensemble deep learning-based classification model is proposed to detect communication through Tor and non-Tor network. Three different deep learning models are combined to achieve the ensemble model. The proposed model is also compared with other machine learning models. Classification results shows the superiority of the proposed model than other models.

KEYWORDS

Cloud Security, Deep Learning, Onion Routing, Tor Network

1. INTRODUCTION

The onion routed or Tor traffic shields the identity of cloud user by communicating his data across diverse Tor servers and by applying encryption that network traffic. Due to these randomised routed it is not easy to trace back to the cloud user. Tor networks are designed to provide confidentiality, autonomy, other network threats to cloud handlers. However, Tor traffic is unsafe for cloud architectures due to the hacking attempts, malwares, DDoS attacks, bypassing security controls, information theft, and other cyber-crime attempts.

The common approaches to block TOR traffic are based on the list of identified malicious IP addresses and list of recognized TOR Exit Nodes. Entering TOR traffic is comfortable to identify in comparison to outgoing TOR traffic since all TOR leaving nodes are widely recognized. It can be examined by the IP address of these nodes. To identify the outgoing TOR traffic is considerably tougher, if not difficult to identify since all entry nodes are not publicly identified. One can examine

DOI: 10.4018/IJGHPC.2021010101

Copyright © 2021, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

by IP address of few incoming network nodes of which the IP is known, however it not so easy to consider all TOR traffic. Due to these difficulties, the machine learning based approaches are more suitable for traffic identification.

These days due to high availability of computational resources, deep learning based classification approaches have become an effective tool for prediction. Deep learning is a sub class of machine learning domain. Deep learning is built upon both supervised and unsupervised learning methods, which are based on Artificial Neural Network (ANN). Its architecture consists of multiple processing layers. Each layer produces nonlinear response, which is generated using the response of previous layer. Deep learning functions by imitating the human brain working for data processing and pattern creation. It uses a network, which is capable of learning from unsupervised data. Due to resemblance of this network with network of neurons in human brain, deep learning is also referred as deep neural network or deep neural learning (LeCun et al., 2015). This work utilizes the Deep Neural Network Model (DNNM) for onion routed traffic detection. The proposed approach is compared with other machine learning models. The performance metrics shows that ensembled DNN based model is superior to other models. The rest of the paper is divided into five more sections. In the subsequent Section and Section 3 the literature review and deep learning models are presented. Section 4 presents the information about used dataset and Section 5 discusses performance metrics, simulation results and result analysis. At the end conclusion is discussed in Section 6.

2. LITERATURE REVIEW

These days machine learning methods and deep learning approaches have revolutionary changed decision making process including the cloud security domain. Deep learning is not a universal tool with the ability to solve all the cloud security problems due to the requirement of large sized training datasets (Najafabadi et al., 2015). Still, there are numerous cloud security problems where the deep learning networks have shown noteworthy enhancements to the traditional security solutions (Papernot et al., 2016). Few cloud security problems are given below where deep learning models have displayed noteworthy enhancements over the traditional machine learning-based approaches (Deng and Yu, 2014; Liu et al., 2017):

1. Network intrusion detection such as scanning, spoofing etc.;
2. Phishing attacks (malicious URL identification);
3. Application attack identification such as OWASP-Top 10 attacks;
4. Malware identification and categorization;
5. Ransomware, spyware recognition;
6. User behaviour study;
7. Suspicious sign-in activity detection;
8. Brute force attack detection and other cloud security related problems.

A network intrusion recognition system supports system to detect network security breaches in the business organizations. Hodo et al. (2017) have presented a nontor traffic detection scheme using the support vector machine and artificial neural network based machine learning models. They have also used correlation based feature selection scheme to reduce the feature dimension.

A deep learning based method for designing such a capable and flexible intrusion detection system is presented by Javaid et al. (2016). Malware has turn out to be a severe threat in the cloud security and confidentiality. Specifically on the common cloud android platform, numerous malicious applications are concealed inside the enormous normal applications, which creates the malware recognition more demanding. A deep learning based dynamic and static analysis for malware detection is given by Yuan et al. (2014). Software Defined Networking (SDN) has appeared to grow into one capable answer

15 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/article/an-ensemble-deep-neural-network-model-for-onion-routed-traffic-detection-to-boost-cloud-security/266216

Related Content

Analysis on the Steps of Physical Education Teaching Based on Deep Learning

Aixia Dong (2023). *International Journal of Distributed Systems and Technologies (pp. 1-15).*

www.irma-international.org/article/analysis-on-the-steps-of-physical-education-teaching-based-on-deep-learning/317937

Scheduling Strategies for Business Process Applications in Cloud Environments

Kahina Bessai, Samir Youcef, Ammar Oulamara, Claude Godartand Selmin Nurcan (2013). *International Journal of Grid and High Performance Computing (pp. 65-78).*

www.irma-international.org/article/scheduling-strategies-for-business-process-applications-in-cloud-environments/102757

Security Standards and Issues for Grid Computing

Athanasios Moralis, Vassiliki Pouli, Mary Grammatikou, Dimitrios Kalogerasand Vasilis Maglaris (2012). *Computational and Data Grids: Principles, Applications and Design (pp. 248-264).*

www.irma-international.org/chapter/security-standards-issues-grid-computing/58748

Monitoring and Controlling Large Scale Systems

Valentin Cristea, Ciprian Dobre, Corina Stratanand Florin Pop (2010). *Large-Scale Distributed Computing and Applications: Models and Trends (pp. 141-167).*

www.irma-international.org/chapter/monitoring-controlling-large-scale-systems/43106

Distributed Dynamic Load Balancing in P2P Grid Systems

You-Fu Yu, Po-Jung Huangand Kuan-Chou Lai (2011). *Cloud, Grid and High Performance Computing: Emerging Applications (pp. 284-298).*

www.irma-international.org/chapter/distributed-dynamic-load-balancing-p2p/54935