Enhanced Bidirectional Encoder Based Classifier Trained Detect Network Intrusion in Big Data Security

Sreeja. S. Nair
Dept of Computer Science
M Tech Student, APJ Abdul Kalam Technological University, Kerala, India

Dr. Smita C Thomas
Dept of Computer Science
Professor, Mount Zion College of Engineering, Kadammanitta, Kerala, India

Ajeesh S
Dept of Computer Science
Assistant Professor, Mount Zion College of Engineering, Kadammanitta, Kerala, India

***Abstract*—With the complexity of network architecture, data Security and the rapid growth of the connection requirements of Internet-connected devices, the traditional architecture eg: complex control, complex software, high line costs, and difficult expansion cannot dynamically handle modern network security in Big Data architecture. Based on the data findings, we collect the perspective of imbalance and high dimensionality of datasets in the area of intrusion detection and propose an oversampling method based on Generative Adversarial Networks (GAN) and feature classification methods. This project proposes a deep learning technology based on a transformer attack-detection model. We grouping the CNN machine learning method and the bidirectional encoder transformer to apply attack detection, The model proposed herein shows better performance in terms of accuracy, recall, F1 score, and AUC indicators. In this project, we build a classifier and train it with adversarial examples for network data, we can use adversarial attacks and successfully break the system. We propose a Bidirectional Encoder based Generative Adversarial Network (GAN) based algorithm to generate data to train an efficient neural network based classifier, and we subsequently break the system using adversarial attacks. Also these approaches extract different features from data messages and adopt machine learning algorithms to analyse and classify the data. The input representation for the transformer encoder is the sum of data key embedding vectors and position embedding vectors of data sequences. The output of the transformer encoder is then fed to a fully connected neural network layer and a softmax layer to generate a probability distribution for each data key in the data key set as the prediction of a trained data key.**

***Keywords*—GAN, CNN, IDS, IAAS, SWFMS, DNN**

I. INTRODUCTION

This In this project, we show that adversarial attacks can be used to defeat machine learning based intrusion detection systems. Specifically, we describe how a classifier yielding very good performance in detecting a network intrusion alert, fails to do so when faced with adversarial attacks. We focus on a dataset of a network intrusion alert system. The dataset has features related to a cyber-event. The first stage of our experiment involves building a robust neural network classifier with the help of GANs. GANs involve two neural networks competing against each other, where one, the generator, is trying to fool the other, the discriminator, with generated adversarial examples. The discriminator, in turn, aims to not get fooled by the generated adversarial examples. We use GANs to generate adversarial examples during the training phase, hoping to make the classifier aware of those adversarial examples. GANs also help us in terms of dealing with the class imbalance problem,which is very common for training a dataset of network intrusion alerts, thereby increasing classification scores for both the classes. In the second part of our experiment we describe how we can use ‘Fast Gradient SignMethod’ to perform adversarial attacks on a classifier with high accuracy. This helps in masquerading the cyberevent samples by perturbing the data slightly, so that to the neural network based classifier it seems that the event is a ‘non-attack’ sample, when in reality it is an ‘attack’ sample. The key contributions of our research are that this paper states that using GANs we can create classifiers which yield very high scores when used to detect network intrusion. To maintain networks as safe and secure, the Intrusion Detection System (IDS) have become very critical. Intrusion Detection Systems (IDS) are designed to protect the network by identifying anomaly behaviors or improper uses. Intrusion Detection systems provide more meticulous security functionality than access control barriers by detecting attempted and successful attacks at the end-point or within the network. Intrusion prevention systems are the next logical step to this approach as they can take real-time action against breaches. To have an accurate IDS, detailed visibility is required into the network traffic. The intrusion detection system should be able to detect inside the network threats as well as access control breaches. IDS has been around for a very long time now. These traditional IDS were rules and signature-based. Though they were able to reduce false positives they were not able to detect new attacks. In today’s world due to the growth of connectivity, attacks have increased at an exponential rate and it has become essential to use a data-driven approach to tackle these issues. In this paper, the KDD data set was used to train the unsupervised machine learning algorithm called Isolation Forest. The data set is highly 12 imbalanced and contains various attacks such as DOS, Probe, U2R, R2L. Since this data set suffers from a redundancy of values and class imbalance, the data preprocessing will be performed first and also used unsupervised learning. For this network traffic based anomaly detection model isolation forest was used to detect outliers and probable attacks the results were evaluated using the anomaly score

II. EASE OF USE

A. *Knowledge Discovery*

(KDD), is the process of uncovering patterns and other valuable information from large data sets. Given the evolution of data warehousing technology and the growth of big data, adoption of data mining techniques has rapidly accelerated over the last couple of decades, assisting companies by transforming their raw data into useful knowledge. However, despite the fact that that technology continuously evolves to handle data at a large-scale, leaders still face challenges with scalability and automation. range of techniques, we can use this information to increase revenues, cut costs, improve customer relationships, and reduce risks.

B. *Big Data Platform*

BIG DATA Big data is data that contains greater variety, arriving in increasing volumes and with more velocity. Simply, big data is larger, more complex data sets, especially from new data sources. These data sets are so voluminous that traditional data processing software just can't manage them. Big data is a field that treats ways to analyze, systematically extract data (information) from, or otherwise deal with data sets that are too large or complex to be dealt with by traditional data-processing application software. Prepare Your Paper Before Styling

C. *Abbreviations and Acronyms*

GAN Generative Adversarial Network
IDS Intrusion Detection System
IAAS Infrastructure as a Service
SWFMS Scientific Workflows Management Systems

D. *Equations*

The objective of this work is to classify a given dataset as either legitimate or malicious and classification problem is binary. Let’s consider a set of dataset U = {(u1, y1),(u2, y2), · · ·(un, yn)} where u represents data set and y represents ’0’ for legitimate and ’1’ for malicious. There are two steps involved in classification procedure, one is appropriate feature representation and second one is prediction function. Feature representation forms n dimensional vector representation xn which can be passed into prediction function as input yn = sign(f(xn)). The main aim is to minimize the total number of misclassification in classification procedure. This can be achieved by minimizing the loss function. This type of loss function can also include regularization term. In this work f is represented as deep learning architectures.

$$adv\_x = x + \epsilon * \text{sign}(\nabla_x J(\theta, x, y))$$

E. *Proposed Method*

The word “ In this Proposed system, the data set contains 38 attacks which are combined into 4 basic attacks classes to provide a more clear and conspicuous visualization of results. NSL-KDD is a cleaned-up version of KDD but the most same number of features and attack types, which is an improvement to a classic network intrusion detection dataset used widely by security data science professionals. Based on the data findings, we collect the perspective of imbalance and high dimensionality of datasets in the area of intrusion detection and propose an oversampling method based on Generative Adversarial Networks (GAN) and feature classification methods. This project proposes a deep learning technology based on a transformer attack-detection model. We grouping the CNN machine learning method and the bidirectional encoder transformer to apply attack detection, The model proposed herein shows better performance in terms of accuracy, recall, F1 score, and AUC indicators. In this project, we build a classifier and train it with adversarial examples for network data, we can use adversarial attacks and successfully break the system. We propose a Bidirectional Encoder based Generative Adversarial Network (GAN) based algorithm to generate data to train an efficient neural network based classifier, and we subsequently break the system using adversarial attacks. Also these approaches extract different features from data messages and adopt machine learning algorithms to analyse and classify the data. The input representation for the transformer encoder is the sum of data key embedding vectors and position embedding vectors of data sequences. The output of the transformer encoder is then fed to a fully connected neural network layer and a soft max layer to generate a probability distribution for each data key in the data key set as the prediction of a trained data key.

These attacks belong to four general categories: DOS, r2I, u2R, and probe attack. Given the descriptions of these attacks, one can observe that DOS attacks are different from other attacks. The primary objectives targeted include:

(1) Design a feature extraction and representation method with Principal Component Analysis (PCA) to reduce the feature dimension for lower memory consumption and computation.

(2) Design an improved Isolation Forest algorithm for lower time cost, which will meet the requirements of having a self-adaption detector radius to speed up the detector generation and having a real time response for reducing the detecting time costs.

(3) Design an multi-levels real time detection model for lower computing consumption, in which the detector generation and optimization processes are deployed in the base station, the data collectors are deployed in the ordinary nodes, the detectors are deployed in the detection node

F. *Components*

Enforcement method retains the security issues components and concerns analyzing all network traffic flows and should provide aim to preserve the confidentiality, integrity, and the technical availability of all systems and information …on the network .When it comes to enforcing protections, network security operates on a defense-in-depth model and follows the principles of the “CIA” triad: The process of auditing network security requires checking back on enforcement measures to determine how well they have aligned with the network security policy. Auditing encourages continuous improvement by requiring organizations to reflect on the implementation of their policy on a consistent basis. This gives organizations the opportunity to adjust their policy and provides better enforcement strategy

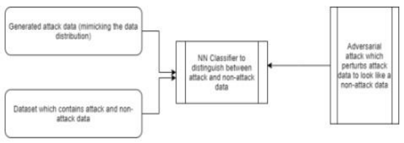
CONFIDENTIALITY – PROTECTING ASSETS FROM UNAUTHORIZED ENTITIES

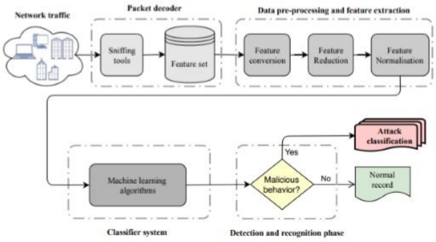
INTEGRITY – ENSURING THE MODIFICATION OF ASSETS IS HANDLED IN A SPECIFIED AND AUTHORIZED MANNER

AVAILABILITY – MAINTAINING A STATE OF THE SYSTEM IN WHICH AUTHORIZED USERS HAVE CONTINUOUS ACCESS TO SAID ASSETS

G. Figures and Tables

ARCHITECTURE DIAGRAM


Generated attack data (mimicking the data distribution)
Dataset which contains attack and non-attack data
NN Classifier to distinguish between attack and non-attack data
Adversarial attack which perturbs attack data to look like a non-attack data



Deep neural networks (DNN) have achieved unprecedented success in numerous machine learning tasks in various domains. However, the existence of adversarial examples raises our concerns in adopting deep learning to safety-critical applications. As a result, we have witnessed increasing interests in studying attack and defense mechanisms for DNN models on different data types, such as images, graphs and text. Thus, it is necessary to provide a systematic and comprehensive overview of the main threats of attacks and the success of corresponding countermeasures. In this survey, we review the state of the art algorithms for generating adversarial examples and the countermeasures against adversarial examples, for three most popular data types, including images, graphs and text. .

ACKNOWLEDGMENT

To bring something into existence is truly the work of ALMIGHTY. I thank GOD ALMIGHTY for making this venture a success. I express my whole hearted thanks to the Management of the college, Mr. Abraham Kalammannil, Chairman, for providing me an opportunity to do my studies in this esteemed institution. I thank Principal Dr. A. Sivasubramanian for providing the facilities for my studies and constant encouragement in all achievement. At the outset I wish to place on record my sincere thanks to quite a few people without whose help, this venture would not have been a success. I would like to express profound gratitude to the Head of the department, Dr. Smita C Thomas for her encouragement and for providing all facilities for carrying out this Project. I express my highest regard and sincere thanks to my Project Guide, Ajeesh S and Project Coordinator, Dr. Smita C Thomas. who provided the necessary guidance and serious advice to carry out this Project. I convey my sincere thanks to all the staff members of the Computer Science department who guided me throughout the entire course.

REFERENCES

[1] Agnieszka Chadzynska-Krasowska Bartek Konarsk Joel Holland Dominik Slezak Andrzej Janusz, Daniel Kałuza. Ieee bigdata 2019 cup: Suspicious network event recognition., 2019.

[2] Mustapha Belouch, Salah El hadaj, and Mohamed Idhammad. Performance evaluation of intrusion detection based on machine learning using apache spark. Procedia Computer Science, 127:1–6, 01 2018.

[3] Security Boulevard. Hacking the hackers: Adversarial aiand how to fightit.https://securityboulevard.com/2020/01/hacking-the-hackersadversarial-ai-and-how-to-fight-it/, January 2020.

[4] Security Boulevard. Why 2020 will be the year artificial intelligence stops being optional for security. https://securityintelligence.com/articles/why-2020-will-be-the-yearartificialintelligence-stops-being-optional-for-security/, January 2020.

[5] Georgios Douzas and Fernando Bac ¸˜ ao. Effective data generation for imbalanced learning using conditional generative adversarial networks. Expert Systems with Applications, 91, 09 2017.

[6] Asmaa Elsaeidy, Kumudu Munasinghe, Dharmendra Sharma, and Abbas Jamalipour.Intrusion detection in smart cities using restricted boltzmannmachines. JournalofNetworkandComputerApplications,135,032019.

[7] K. Eykholt, I. Evtimov, E. Fernandes, B. Li, A. Rahmati, C Xiao, A Prakash, T. Kohno, and D. Song. Robust physical-world attacks on deep learning models. Computer Vision and Pattern Recognition, 2018.

[8] Akash Garg and Prachi Maheshwari. Performance analysis of snortbased intrusion detection system. pages 1–5, 01 2016.

[9] Goodfellow, Jean Pouget-Abadie, Mehdi Mirza, Bing Xu, David Warde-Farley, Sherjil Ozair, Aaron Courville, and Yoshua Bengio. Generative adversarial nets. Advances in Neural Information Processing Systems, 2014.

[10] Ian Goodfellow, Jonathan Shlens, and Yoshua Bengio. Explaining and harnessing adversarial examples. International Conference on Learning Representations, 2015.

[11] Cosimo Ieracitano, Ahsan Adeel, Francesco Morabito, and Amir Hussain. A novel statistical analysis and autoencoder driven intelligent intrusion detection approach. Neurocomputing, 11 2019.

[12] Jayshree Jha and Leena Ragha. Intrusion detection system using support vector machine. 30 International Conference workshop on Advanced Computing, 2013.

[13] Sevcan Korkmaz and Ferhat Karatas¸. Big data: Controlling fraud by using machine learning libraries on spark. International Journal of Applied Mathematics, Electronics and Computers, 6:1–5, 03 2018.

[14] Wenke. Lee and Salvatore Stoflo. A framework for constructing features and models for intrusion detection systems. ACM Transactions on Information and System Security, Vol. 3, No. 4, Pages 227–261, 2000.

[15] CISO MAG. U.s. and europe's cyber readiness numbers stall as cyberattack numbers soar. https://www.cisomag.com/u-s-and-europes-cyberreadiness-numbers-stall-as-cyber-attacknumbers-soar/, January 2020.

[16] Cyber MDX. Real-life cyber-attacks you probably never heard about.https://www.cybermdx.com/blog/5-scary-real-life-cyber-attacksyou-never-heard-about, February 2019.

[17] MIT. 1998 darpa intrusion evaluation dataset. https://www.ll.mit.edu/rd/datasets/1998-darpa-intrusion-detectionevaluation-dataset, February 1998.

[18] Saurabh Mukherjee and Neelam Sharma. Intrusion detection using naive bayes classifier with feature reduction. Procedia Technology, 4:119–128, 12 2012.

[19] David Nguyen, Gokhan Memik, and Alok Choudhary. A reconfigurable architecture for network intrusion detection using principal component analysis. page 235, 01 2006.

[20] Jewish Post. Israel cyber chief: We must protect ai-based vehicles from hacking. https://www.jpost.com/Jpost-Tech/Israel-cyber-chief-We- mustprotect-AI-based-vehicles-fromhacking-615848, January 2020.

[21] BD Tech talks. Ai email phishing prevention. https://bdtechtalks.com/2020/01/01/ai-emailphishing-prevention/, January 2020.

[22] He Tianxing and James Glass. Detecting egregious responses in neural sequence-tosequence models. 09 2018.

[23] Han Xu, Yao Ma, Haochen Liu, Debayan Deb, Hui Liu, and Jiliang Tang. Adversarial attacks and defenses in images, graphs and text: A review. 2015.

[24] Jiong Zhang and Mohammad Zulkernine. Network intrusion detection using random forests.