International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

A Secure Model for Detecting Intruder on Cloud Environment

Himali Gajjar, Dr. Zakiyabanu Malek

Submitted:11/03/2024 **Revised**: 26/04/2024 **Accepted**: 03/05/2024

Abstract: An IDS is a security service that monitors and analyzes network and system events to detect and alert on unauthorized access to system resources in real time or near real time. Unlike a firewall, which sits at the perimeter and acts as a gatekeeper monitoring network traffic and evaluating whether traffic should be allowed into the network or endpoints, an IDS focuses on internal network traffic to detect suspicious or malicious activity. This allows an IDS to detect attacks that originate from within the network as well as attacks that bypass the firewall. A network-based intrusion detection system (NIDS) can protect sensitive data by monitoring the network for unauthorized access attempts. It can detect real-time events such as suspicious activity and alert security personnel so that they can take appropriate measures to prevent data loss or theft. A NIDS can also detect hidden security threats, such as attacks that bypass firewalls and other perimeter security controls.

Keywords: *CNN; convolutional neural network; network security; intrusion detection; deep learning*

1. Introduction

The Intrusion Detection System software uses machine learning to identify network intrusions.IDS monitors a network or system for harmful activity and protects a computer network against unauthorised access by users, including insiders.

The intrusion detector learning task is to create a prediction model (i.e., a classifier) that can discriminate between 'bad connections' (intrusions/attacks) and 'good (normal) connections'.

In this paper we have mainly focus on attacks on database so we have tried to restrict intruder using Cross Site Scripting(XSS), SQL Injection and Command Line Injection(CLI)so in next phase we will understand attacks how to restrict them possibilities followed by accuracy we got.

II. Attacks and it's behaviour

1. Cross Site Scripting :

Cross-site scripting (XSS) is an attack that involves injecting malicious executable scripts into the code of a trusted program or website. In reply, a malicious script may be executed and returned to the attacker.

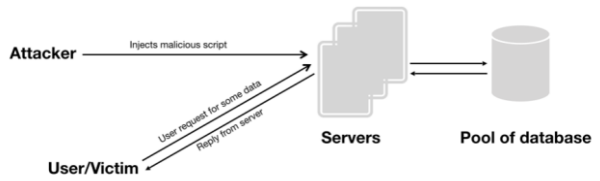

Fig. 1 : Cross Site Scripting

2. SQL Injection :

It's a code injection approach that might damage your database. It is the inclusion of harmful code in SQL queries via website input.

Example :

Input : SELECT * FROM table WHERE user_id = 105

Injection : SELECT * FROM table WHERE user_id = 105 OR 1=1

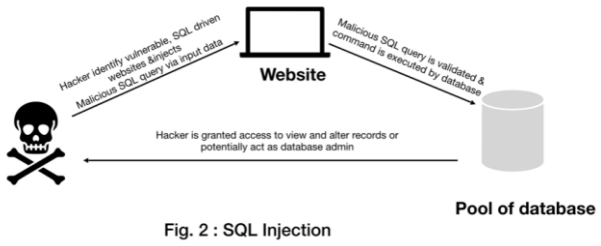

Fig. 2 : SQL Injection

3. Command Line Injection :

Command injection is an attack that targets susceptible applications and executes arbitrary commands on the host operating system. Command injection attacks can occur when an application sends dangerous user-supplied data (forms, cookies, HTTP headers, etc.) to a system shell.

Example :

Attacker try to access host file by pinging

127.0.0.1 & dir

127.0.0.1 | dir

III. Dataset :

A dataset is a structured composition of data, a table at its ease. Data Warehouses are in fact a collection of datasets on different levels of business readiness. The same is obvious for every BI project as it is based on report-ready structured data frames. The architecture and scope of the DW is not that important.

Here we have taken the dataset having multiple attacks like Command Line Injection, SQL Injection & Cross Site Scripting.

An accurate dataset is very important to detect network intrusion detection system so dataset selection is very crucial part.

IV. Developing a model :

The choice of an appropriate algorithm is equally vital while constructing a model. We experimented with many algorithms and datasets, including NaiveBayes, BayesNet, Convolutional Neural Network (CNN), Decision Trees, Random Forest, and KNN, as well as KDD-99, NSL-KDD, and our own dataset.

Based on our experiments, we concluded that the convolutional neural network (CNN) performs perfectly in our model. Convolutional neural networks (CNNs) learn directly from data.

CNNs are very good for detecting patterns in text/images and recognising classes and categories. They may also be very useful for identifying audio, time series, and signal data.

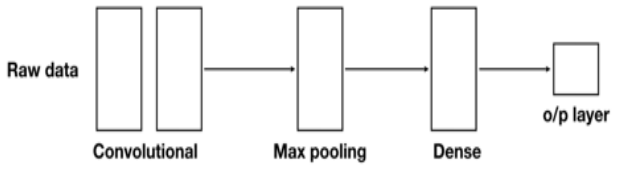

Fig. 3 : Architecture of CNN

Moving to the next part, accuracy of NIDS based on choosing location of model. The model will be kept outside firewall (front facing) because if it will be kept behind firewall than firewall itself has the capability to block attack, no need of machine to be trained and used.

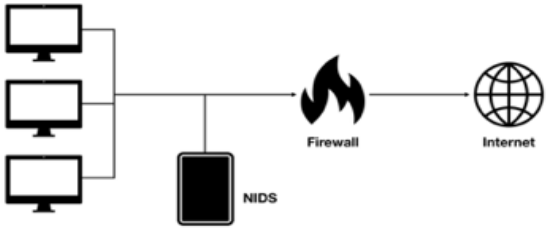

Fig. 4 : Location of NIDS

We opted to work on an anomaly-based intrusion detection system since it can warn you to suspicious or unknown behaviour. Instead of looking for known threats, an anomaly-based detection system use machine learning to educate the system to recognise a normalised baseline. Signature-based detection is often used to identify known threats.It works by utilising a pre-programmed list of known risks and symptoms of compromise.

Our model is divided into five phases where the first phase is raw data process where raw data will be gathered to train our model. After that null, duplicate and missing data will be detected and will be removed to get proper and perfect result. Then the data is labelled and it will create supervised data. Then the data will be converted into into binary language for machine learning process.

The next process is the development of testing and training data. After collecting clean and actual data, the data will be segmented into training and testing data, with the entire data divided into two portions. The fundamental aim of trade and testing data is to train the model using training data and then evaluate its performance using testing data. The primary goal is to determine how effectively the model generalises to the new dataset. Training data is used to train an algorithm or machine learning model to anticipate the outcome for which it was designed.

In the next phase when user try to access the system then at that time and before reaching at the destination it will check user's input with out dataset. If it matches with the dataset having attacks with the help of trained model. After matches requested input with trained model it will detect if attack is present or not. If attack is present then it will generate output of requested input in the form of attack percentage.

V. Result and experiments :

In this section we will have done some experiment on different inputs and their output showing result of our model for detection network intrusion.

To experiment our model first we have taken " or pg_sleep (__TIME__) — as an input.

Below screenshot shows that there is 17.5% probability of having attacks in which probability of having SQL Injection is 47.5%, XSS is having 17.5%.

Attacks	Possibility of attacks
SQL_INJECTION	47.5
XSS	17.5
Command Injection	0.175
LFI & HTML	0

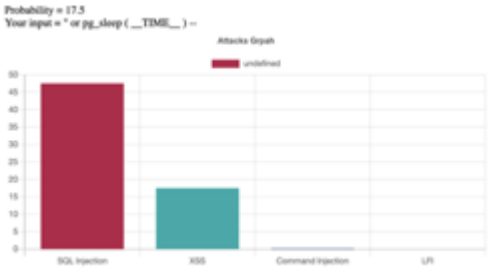

Fig. 5 : Experiments & Results

VI. Conclusion & Future scope :

With our experiments we are concluding that having a ratio of 80% and 20% in the training and testing dataset we are getting highest accuracy of 99.37% with very less false positive rate of 0.19% and having true positive rate of 99.37%. In the future scope we work with multiple attacks and also will work on preventing this attacks.

Author contributions

Himali Gajjar: Conceptualization, Methodology, Software, Field study **Dr. Zakiyabanu Malek:** Guidance

References

[1] https://www.techtarget.com/searchenterpriseai/definition/convolutional-neural-network

[2] https://www.hindawi.com/journals/scn/2020/8891185/

[3] https://ieeexplore.ieee.org/author/37088519064 ,, Said Ouiazzane, Malika Addou, Fatimazahra Barramou, "A Suricata and Machine Learning Based Hybrid Network Intrusion Detection System", Advances in Information, Communication and Cybersecurity, vol.357, pp.474, 2022.

[4] Shweta Gumaste, Narayan D. G., Sumedha Shinde, Amit K, "Detection of DDoS Attacks in OpenStack-based Private Cloud Using Apache Spark", Journal of Telecommunications and Information Technology, vol.4, pp.62, 2021.

[5] Mohammadpour, L.; Ling. T.C; Liew: C.S.; Aryanfar, A. The Survey ofaCNN-Based Network Intrusion Detection. Appl. Sci. 2022, 12, 8162. https://doi.org/10.3390/app12168162

[6] Mohammadpour L, Ling TC, Liew CS, Aryanfar A. A Survey of CNN-Based Network Intrusion Detection. Applied Sciences. 2022; 12(16):8162. https://doi.org/10.3390/app12168162

[7] H. Gajjar and Z. Malek, "A Survey of Intrusion Detection System (IDS) using Openstack Private Cloud," 2020 Fourth World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4), London, UK, 2020, pp. 162-168, doi: 10.1109/ WorldS450073.2020.9210313.

[8] Yogesh Kumar, Rajiv Munjal and Harsh Sharma,".Comparison of Symmetric and Asymmetric Cryptography withExisting Vulnerabilities and Countermeasures" IJCSMS International Journal of Computer Science and ManagementStudies, Vol. 11, Issue 03, Oct 2011.

[9] Mr. Gurjeevan Singh, Mr. AshwaniSingla and Mr. K S Sandha " Cryptography Algorithm Compaison ForSecurity Enhancement In Wireless Intrusion Detection System" International Journal of Multidisciplinary ResearchVol.1 Issue 4, August 2011.

[10] Mr. Gurjeevan Singh, Mr. AshwaniSingla and Mr. K S Sandha " Cryptography Algorithm Compaison ForSecurity Enhancement In Wireless Intrusion Detection System" International Journal of Multidisciplinary ResearchVol.1 Issue 4, August 2011.

[11] D. S. Abdul. Elminaam, H. M. Abdul Kader and M. M. Hadhoud ," Performance Evaluation of SymmetricEncryption Algorithms", Communications of the IBIMA Volume 8, 2009.

[12] Bhaskar Mandal ,Tanupriya, Choudhury, "A Secure Biometric Image Encryption Scheme using Chaos and Wavelet Transformations", International Journal of Advanced Security in Data Analytics and Networks (Special Issue for Recent Advances in Communications and Networking Technology),2016.

[13] "Honeypots: Catching the Insider Threat", available at Lance Spitzner Honeypot Technologies Inc. lance@Honeypots.com.

[14] Karthik Sadasivam, Banuprasad Samudrala, T. Andrew Yang. "Design of Network Security Projects using Honeypots", University of Houston.