As per UGC guidelines an electronic bar code is provided to seure your paper

International Journal for Modern Trends in Science and Technology, 8(09): 80-82, 2022
Copyright © 2022 International Journal for Modern Trends in Science and Technology
ISSN: 2455-3778 online
DOI: https://doi.org/10.46501/IJMTST0809013
Available online at: http://www.ijmtst.com/vol8issue09.html

Deep Learning Based Detection Method for Enhanced Cyber Threat Detection

Dr.D.J.Samatha Naidu | N.Moulish

Annamacharya PG College of Computer Studies, Rajampet, AP-516126.

To Cite this Article
Dr.D.J.Samatha Naidu and N.Moulish. Deep Learning Based Detection Method for Enhanced Cyber Threat Detection. International Journal for Modern Trends in Science and Technology 2022, 8(09), pp. 80-82. https://doi.org/10.46501/IJMTST0809013

Article Info
Received: 20 August 2022; Accepted: 10 September 2022; Published: 17 September 2022.

ABSTRACT

The increased usage of cloud services, growing number of users, changes in network infrastructure. Arising threats, network security mechanisms, sensors and protection schemes have also to evolve in order to address the needs and problems of nowadays users. Computerized fear, which made a lot of issues.Intrusion Detection Systems (IDS) has been made to keep an essential separation from advanced attacks. At this moment, learning the reinforce support vector machine (SVM) estimations.

INTRODUCTION

With the emergence of artificial intelligence (AI) techniques, learning-based approaches for detecting cyber attacks, have become further improved, and they have achieved significant results in many studies. However, owing to constantly evolving cyber attacks, it is still highly challenging to protect IT systems against threats and malicious behaviors in networks. Because of various network intrusions and malicious activities, effective defenses and security considerations were given high priority for finding reliable solutions .

Objective

The Purpose of project is to Designing a Machine Learning Application to provide Intrusion Detection in Internet URL's and Files a which controls different attacks. The proposed approach engages a Bayesian inference theory for cyber attacks detection. For that purpose a directed acyclic network (graph) is built, which is a graphic representation of the joint probability distribution function over a set of variables. In such graph each node represents random variable while the edge indicates a dependant relationship.

SCOPE

The proposed approach engages a Bayesian inference theory for cyber attacks detection. For that purpose a directed acyclic network (graph) is built, which is a graphic representation of the joint probability distribution function over a set of variables. In such graph each node represents random variable while the edge indicates a dependant relationship.

EXISTING WORK

In our previous work, we have introduced an innovative evolutionary algorithm for modeling genuine SQL queries generated by web-application. In this paper we have extended our algorithm with Bayes inference in order to incorporate advantages of signature-based and anomaly-based methods.

Limitations

- Existing tools such as Google Safe Browsing are not enabled on the mobile versions of browsers, thereby precluding mobile users.
- DNS based mechanisms do not provide deeper understanding of the specific activity implemented by a webpage or domain.
- Downloading and executing each webpage impacts performance and hinders scalability of dynamic approaches.

PROPOSED WORK

The proposed approach engages a Bayesian inference theory for cyber attacks detection. For that purpose a directed acyclic network (graph) is built, which is a graphic representation of the joint probability distribution function over a set of variables. In such graph each node represents random variable while the edge indicates a dependant relationship.

Advantages

- Protection from malicious attacks on your network.
- Deletion and/or guaranteeing malicious elements within a preexisting network.
- Prevents users from unauthorized access to the network.
- Deny's programs from certain resources that could be infected.
- Securing confidential information

RELATED WORK

Cyber-attacks are increasing within the cyber world.There ought to be some advanced securitymeasures taken to scale back or avoid the amount of cyber-attacks. There are various attacks like D-Dos attacks, Man within the middle, information escape, PROBE, User-To-Root, Remote-ToLocal. These attacks are utilized by the hackers or intrudersto realize the unauthorized access to any non-public network, websites, information or perhaps in our personal computers

PRODUCT ARCHITECTURE

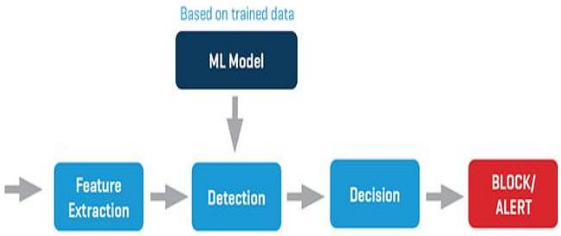


Fig.1.1: System Architecture

MODULES

Data Collection

Collect sufficient data samples and legitimate software samples.

Data Preprocessing

Data Augmentedtechniqies will be used for better performance

Train and Test Modelling

Split the data into train and test data Train will be used for trainging the model and Test data to check the performance

Attack Detection Model

Based on the model trained algorithm will detect whether the given transaction is anomalous or not.

1) Normalization of every data set.

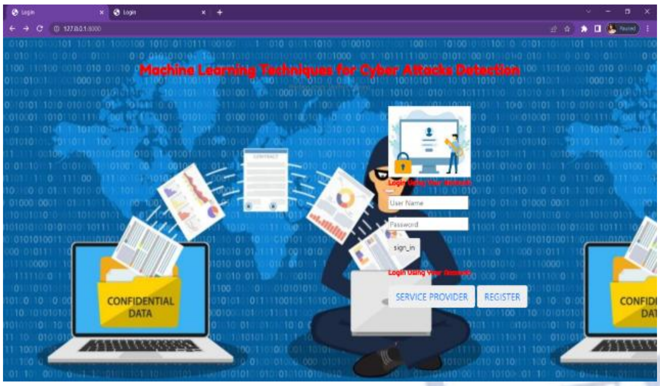
2) Convert that data set into the testing and training.

3) Form IDS models with the help of using RF, ANN, CNN and SVM algorithms.

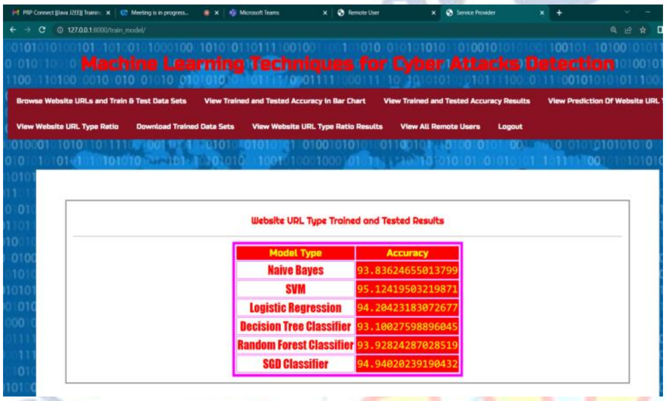
4) Evaluate every model's performances

Sample Screens

Screen 1:Service Provider



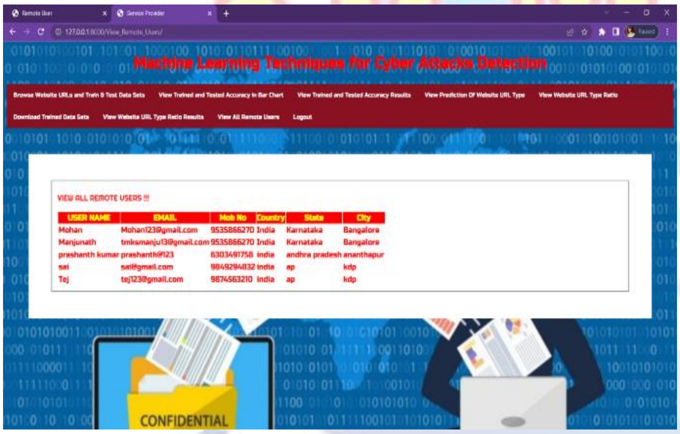
Screen 2: User Login Page


127.0.0.1:8000/train_model/
Machine Learning Techniques for Cyber Attacks Detection
Browse Website URLs and Train & Test Data Sets
View Trained and Tested Accuracy in Bar Chart
View Trained and Tested Accuracy Results
View Prediction Of Website URL Type
View Website URL Type Ratio
Download Trained Data Sets
View Website URL Type Ratio Results
View All Remote Users
Logout

Website URL Type Trained and Tested Results

Model Type	Accuracy
Naive Bayes	93.83624655013799
SVM	95.12419503219871
Logistic Regression	94.20423183072677
Decision Tree Classifier	93.10027598896045
Random Forest Classifier	93.92824287028519
SGD Classifier	94.94020239190432

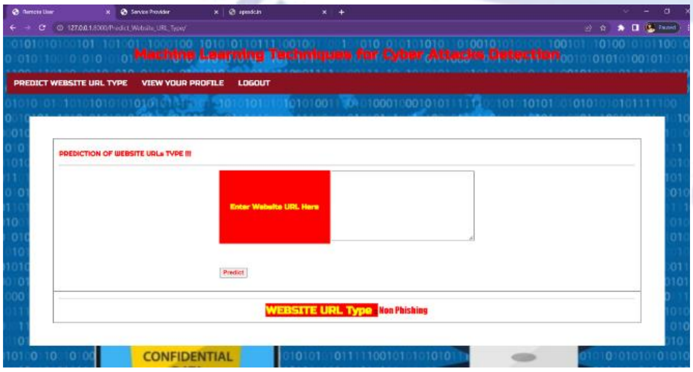
Screen 3: Tested Results using various ML MODULES


127.0.0.1:8000/View_Remote_Users/
Machine Learning Techniques for Cyber Attacks Detection
Browse Website URLs and Train & Test Data Sets
View Trained and Tested Accuracy in Bar Chart
View Trained and Tested Accuracy Results
View Prediction Of Website URL Type
View Website URL Type Ratio
Download Trained Data Sets
View Website URL Type Ratio Results
View All Remote Users
Logout
CONFIDENTIAL

VIEW ALL REMOTE USERS !!!

USER NAME	EMAIL	Mob No	Country	State	City
Mohan	Mohan123@gmail.com	9535866270	India	Karnataka	Bangalore
Manjunath	tmksmanju13@gmail.com	9535866270	India	Karnataka	Bangalore
prashanth kumar	prashanth@123	6303491758	india	andhra pradesh	ananthapur
sai	sai@gmail.com	9849294832	india	ap	kdp
Tej	tej123@gmail.com	9874563210	india	ap	kdp

Screen 4:Chart Showing Train and Tested Accuracy


127.0.0.1:8000/Predict_Website_URL_Type/
Machine Learning Techniques for Cyber Attacks Detection
PREDICT WEBSITE URL TYPE
VIEW YOUR PROFILE
LOGOUT
Predict
CONFIDENTIAL

PREDICTION OF WEBSITE URLs TYPE !!!

Enter Website URL Here

WEBSITE URL Type Non Phishing

Screen 5: Website URL Result

CONCLUSION

At the present time, assessments of help vector machine, ANN, CNN, Random Forest and significant learning estimations reliant upon current CICIDS2017 dataset were presented moderately. Results show that the significant learning estimation performed generally best results over SVM, ANN, RF and CNN. We will use port scope attempts just as other attack types with AI and significant learning computations, apache Hadoop and shimmer advancements together ward on this dataset later on. Every oneofthese estimation assists us with recognizing the digital assault in network. It occurs in the manner that when we think about long back a long time there might be such countless assaults occurred so when these assaults are perceived then the highlights atwhich esteems these assaults are going on will be put away in some datasets.

Conflict of interest statement

Authors declare that they do not have any conflict of interest.

REFERENCES

[1] K. Graves, Ceh: Official certified ethical hacker review guide: Exam 312-50. John Wiley & Sons, 2007.

[2] R. Christopher, "Port scanning techniques and the defense against them," SANS Institute, 2001.

[3] M.Baykara, R. Das , and I . Karado ˘gan, "Bilgi g ¨uvenli ˘gisistemlerindekullanilanarac ̧larin incelenmesi," in 1st International Symposium on Digital Forensics and Security (ISDFS13), 2013, pp. 231–239.