ISSN: 2278-4632
Vol-14, Issue-8, August: 2024

MACHINE LEARNING TECHNIQUES FOR CYBER ATTACKS DETECTION

Guduri Bhavani
Email: guduribhavani14@gmail.com
M. Tech, Department of Computer Science and Engineering.
Annamacharya Institute of Technology and Science, Hyderabad, Telangana, India.

Ramesh Babu Varugu
Email: rameshvarugu82@gmail.com
Assistant Professor
& HOD, Department of CSE.
Annamacharya Institute of Technology and Science, Hyderabad, Telangana, India.

Abstract - Cyber-attacks on the internet have become increasingly sophisticated and frequent, posing significant challenges to cyber security. Traditional rule-based methods for detecting these attacks often struggle to keep pace with the evolving tactics of malicious actors. In this context, machine learning (ML) techniques have emerged as a promising approach for cyber attack detection due to their ability to analyze large volumes of data and identify patterns indicative of malicious behavior. The proposed framework for utilizing machine learning in cyber-attack detection on the internet. The framework integrates various ML algorithms, including supervised, unsupervised, and reinforcement learning techniques, to enhance the detection capabilities against different types of cyber threats. Moreover, the framework incorporates feature engineering and selection methods to optimize the performance of ML models in identifying malicious activities.

Keywords: Cyber Attack; Support Vector Machine; Convolutional Neural Networks; Cyber threats; Machine Learning.

I. INTRODUCTION

The purpose of the study is to differentiate between normal and abnormal network data and how they differ from each other. Machine Learning techniques are being used to train and diagnose if a computer intrusion or hack has occurred. Every classification model can then be used to determine whether the attack is a Distributed denial of service attack. Paxson V. (2020), Support vector machine (SVM) Algorithm, a collaborative learning approach that collects information and identifies trends or can cluster features based on commonality, is an instance of a classification model. Since we can't predict where, how or when a threat will strike, a full-stack intrusion prevention isn't always possible. Hence, our best bet for the time being is early diagnosis that can mitigate the danger of irreversible damage caused by such attacks.

Cyber Attack In the digital age, where interconnectedness prevails, cyber-attacks pose a significant threat to individuals, organizations, and even governments. These attacks can manifest in various forms, from sophisticated hacking endeavors orchestrated by skilled cybercriminals to simple yet effective phishing emails targeting unsuspecting users. Regardless of their complexity, cyber-attacks aim to compromise the integrity, confidentiality, or availability of digital assets.

Issues Surrounding Cyber Attacks

The prevalence of cyber-attacks underscores several pressing issues:

ISSN: 2278-4632
Vol-14, Issue-8, August: 2024

Technological Vulnerabilities: Software bugs, misconfigurations, and inadequate security measures create entry points for attackers to exploit. As technology advances, new vulnerabilities emerge, challenging cybersecurity professionals to keep pace with evolving threats.

Human Factors: Despite the deployment of robust cybersecurity tools, human error remains a significant factor in cyber-attacks. Employees falling prey to phishing scams, neglecting security protocols, or inadvertently disclosing sensitive information can inadvertently facilitate cyber breaches.

Global Impact: Cyber-attacks transcend geographical boundaries, posing a global threat to governments, businesses, and individuals alike. The interconnected nature of cyberspace means that an attack targeting one entity can have cascading effects, impacting numerous interconnected systems.

Resource Constraints: Addressing cybersecurity concerns requires substantial resources, including financial investments in cutting-edge technologies, skilled personnel, and ongoing training programs. However, many organizations, particularly smaller ones, struggle with limited resources, making them more vulnerable to cyber-attacks.

Regulatory Compliance: Governments and regulatory bodies worldwide have introduced cybersecurity regulations and standards to mitigate cyber risks. Compliance with these regulations adds another layer of complexity for organizations, necessitating investments in compliance efforts and risk management strategies.

Types of Cyber Attacks

Cyber-attacks encompass a broad spectrum of tactics and techniques, each tailored to exploit specific vulnerabilities. Some common types of cyber-attacks include:

Phishing: Attackers use deceptive emails, messages, or websites to trick individuals into divulging sensitive information or downloading malware.

Malware: Malicious software, including viruses, worms, trojans, and ransomware, is designed to infiltrate systems, steal data, or cause damage.

Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS): These attacks overwhelm targeted systems or networks with excessive traffic, rendering them inaccessible to legitimate users.

Man-in-the-Middle (MitM): Attackers intercept and potentially alter communications between two parties without their knowledge, enabling eavesdropping or data manipulation.

SQL Injection: By exploiting vulnerabilities in web applications, attackers inject malicious SQL code to gain unauthorized access to databases or execute arbitrary commands.

Cross-Site Scripting (XSS): Attackers inject malicious scripts into web pages viewed by other users, enabling them to steal information or execute unauthorized actions.

ISSN: 2278-4632
Vol-14, Issue-8, August: 2024

Ransomware: This type of malware encrypts files or systems, demanding payment for their decryption, thereby extorting victims for financial gain.

Social Engineering: Attackers manipulate individuals into divulging confidential information or performing actions that compromise security through psychological manipulation tactics.

Zero-Day Exploits: Attackers leverage previously unknown vulnerabilities (zero-day vulnerabilities) in software or hardware to launch targeted attacks before patches or fixes are available.

II. EXISTING SYSTEM

Blameless Bayes and Principal Component Analysis (PCA) were been used with the KDD99 dataset by Almansob and Lomte [9].Similarly, PCA, SVM, and KDD99 were used Chithik and Rabbani for IDS [10]. In Aljawarneh et al's. Paper, their assessment and examinations were conveyed reliant on the NSL-KDD dataset for their IDS model [11] Composing inspects show that KDD99 dataset is continually used for IDS [6]–[10].There are 41 highlights in KDD99 and it was created in 1999. **Consequently, KDD99 is old and doesn't give any data about cutting edge new assault types**, example, multi day misuses and so forth. In this manner we utilized a cutting- edge and new CICIDS2017 dataset [12] in our investigation.

III. PROPOSED SYSTEM

Important steps of the algorithm are given in below. 1) Normalization of every dataset. 2) Convert that dataset 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

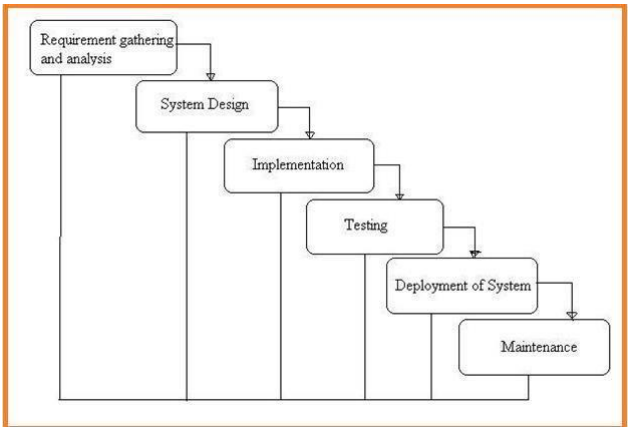
IV. SOFTWARE REQUIREMENTS

The functional requirements or the overall description documents include the product perspective and features, operating system and operating environment, graphics requirements, design constraints and user documentation.

The appropriation of requirements and implementation constraints gives the general overview of the project in regards to what the areas of strength and deficit are and how to tackle them.

- **Python idel 3.7 version (or)**
- **Anaconda 3.7 (or)**
- **Jupiter (or)**
- **Google colab**

V. STRUCTURE OF PROJECT



VI. SYSTEM DESIGN

In System Design has divided into three types like GUI Designing, UML Designing with avails in development of project in facile way with different actor and its utilizer case by utilizer case diagram, flow of the project utilizing sequence, Class diagram gives

ISSN: 2278-4632
Vol-14, Issue-8, August: 2024

information about different class in the project with methods that have to be utilized in the project if comes to our project our UML Will utilizable in this way The third and post import for the project in system design is Data base design where we endeavor to design data base predicated on the number of modules in our project

IMPLEMENTATION

The Implementation is Phase where we endeavor to give the practical output of the work done in designing stage and most of Coding in Business logic lay coms into action in this stage its main and crucial part of the project

TESTING UNITTESTING

It is done by the developer itself in every stage of the project and fine-tuning the bug and module predicated additionally done by the developer only here we are going to solve all the runtime errors

MANUAL TESTING

As our Project is academic Leave, we can do any automatic testing so we follow manual testing by endeavor and error methods Database Design

VII. LITERATURE SURVEY

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

Port Scanning is one of the most popular techniques attackers use to discover services that they can exploit to break into systems. All systems that are connected to a LAN or the Internet via a modem run services that listen to well-known and not so well-known ports. By port scanning, the attacker can find the following information about the targeted systems: what services are running, what users own those services, whether anonymous logins are supported, and whether certain network services require authentication. Port scanning is accomplished by sending a message to each port, one at a time. The kind of response received indicates whether the port is used and can be probed for further weaknesses. Port scanners are important to network security technicians because they can reveal possible security vulnerabilities on the targeted system. Just as port scans can be ran against your systems, port scans can be detected and the amount of information about open services can be limited utilizing the proper tools. Every publicly available system has ports that are open and available for use. The object is to limit the exposure of open ports to authorized users and to deny access to the closed ports

VIII. SOFTWARETESTING

Testing

Testing is a process of executing program with the aim off ending error. To make our software perform well it should be error free. If testing is done successfully it will remove all the errors from the software.

Types of Testing

- White Box Testing
- Black Box Testing
- Unit testing
- Integration Testing
- Alpha Testing
- Beta Testing
- Performance Testing and so on

ISSN: 2278-4632
Vol-14, Issue-8, August: 2024

IX. RESULTS

```
import numpy as np
import pandas as pd
import matplotlib.pyplot as plt
%matplotlib inline
```

```
import itertools
import seaborn as sns
import pandas_profiling
import statsmodels.formula.api as sm
from statsmodels.stats.outliers_influence import variance_inflation_factor
from patsy import dmatrices
```

```
/usr/local/lib/python3.6/dist-packages/statsmodels/tools/_testing.py:19: FutureWarning: pandas.util.testing is dep
recated. Use the functions in the public API at pandas.testing instead.
  import pandas.util.testing as tm
```

```
from sklearn import datasets
from sklearn.feature_selection import RFE
import sklearn.metrics as metrics
from sklearn.svm import SVC
from sklearn.linear_model import LogisticRegression
from sklearn.feature_selection import SelectKBest
from sklearn.feature_selection import chi2, f_classif, mutual_info_classif
```

```
train=pd.read_csv('/content/drive/My Drive/kdd/NSL_Dataset/Train.txt',sep=',')
test=pd.read_csv('/content/drive/My Drive/kdd/NSL_Dataset/Test.txt',sep=',')
```

```
columns=["duration","protocol_type","service","flag","src_bytes","dst_bytes","land",
"wrong_fragment","urgent","hot","num_failed_logins","logged_in",
"num_compromised","root_shell","su_attempted","num_root","num_file_creations",
"num_shells","num_access_files","num_outbound_cmds","is_host_login",
"is_guest_login","count","srv_count","serror_rate","srv_serror_rate",
"rerror_rate","srv_rerror_rate","same_srv_rate","diff_srv_rate","srv_diff_host_rate","dst_host_count","dst_host_sr
"dst_host_diff_srv_rate","dst_host_same_src_port_rate",
"dst_host_srv_diff_host_rate","dst_host_serror_rate","dst_host_srv_serror_rate",
"dst_host_rerror_rate","dst_host_srv_rerror_rate","attack", "last_flag"]
```

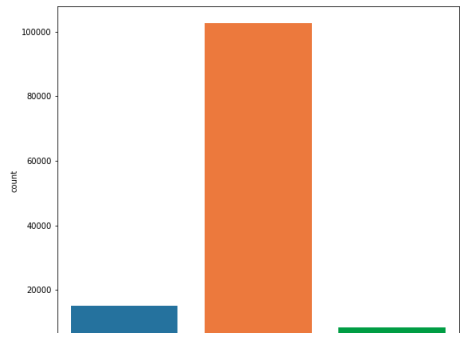
```
train.columns=columns
test.columns=columns
```

```
train.head()
```

	duration	protocol_type	service	flag	src_bytes	dst_bytes	land	wrong_fragment	urgent	hot	num_failed_logins	logged_in	num_compromised	root_s
0	0	udp	other	SF	146	0	0	0	0	0	0	0	0	
1	0	tcp	private	S0	0	0	0	0	0	0	0	0	0	
2	0	tcp	http	SF	232	8153	0	0	0	0	0	1	0	
3	0	tcp	http	SF	199	420	0	0	0	0	0	1	0	
4	0	tcp	private	REJ	0	0	0	0	0	0	0	0	0	

```
test.head()
```

```
# Protocol type distribution
plt.figure(figsize=(9,8))
sns.countplot(x="protocol_type", data=train)
plt.show()
```



Logistic Regression

```
# Building Models
from sklearn.linear_model import LogisticRegression
logreg = LogisticRegression(random_state=0,solver='lbfgs',multi_class='multinomial')
logreg.fit( train_X, train_y)
logreg.predict(train_X)   #by default, it use cut-off as 0.5
```

```
list( zip( cols, logreg.coef_[0] ) )
```

```
logreg.intercept_
```

```
logreg.score(train_X,train_y)
```

Decision Trees

```
train_X.shape
```

```
param_grid = {'max_depth': np.arange(2, 12),
              'max_features': np.arange(10,15)}
```

```
train_y.shape
```

```
from sklearn.model_selection import GridSearchCV
from sklearn.tree import DecisionTreeClassifier, export_graphviz, export
tree = GridSearchCV(DecisionTreeClassifier(), param_grid, cv = 10,verbose=1,n_jobs=-1)
tree.fit( train_X, train_y )
```

```
tree.best_score_
```

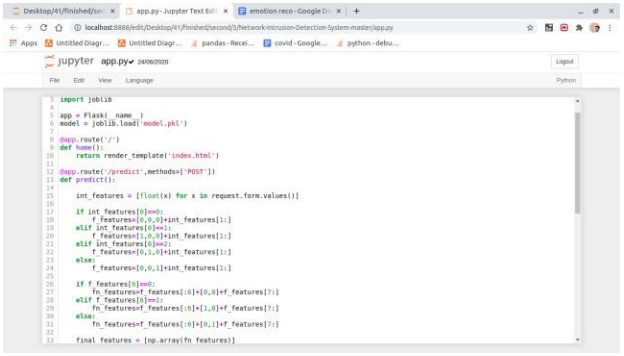
```
tree.best_estimator_
tree.best_params_
```

```
train_pred = tree.predict(train_X)
```

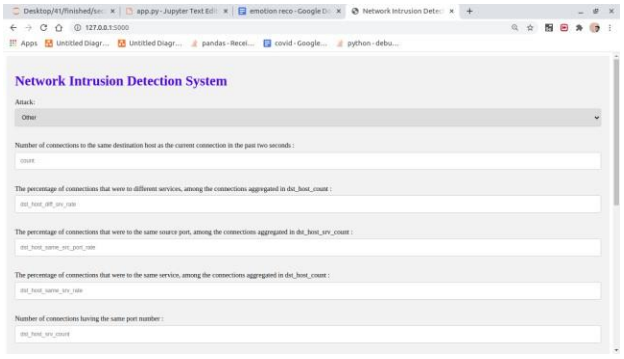
```
print(metrics.classification_report(train_y, train_pred))
```

```
test_pred = tree.predict(test_X)
```

Application



Networking



X. CONCLUSION

Right now, estimations of help vector machine, ANN, CNN, Random Forest and profound learning calculations dependent on modern CICIDS2017 dataset were introduced relatively. Results show that the profound learning calculation performed fundamentally preferable outcomes over SVM, ANN, RF and CNN. We are going to utilize port sweep endeavors as well as other assault types

ISSN: 2278-4632
Vol-14, Issue-8, August: 2024

with AI and profound learning calculations, apache Hadoop and sparkle innovations together dependent on this dataset later on. All these calculation helps us to detect the cyber-attack in network. It happens in the way that when we consider long back years there may be so many attacks happened so when these attacks are recognized then the features at which values these attacks are happening will be stored in some datasets. So by using these datasets we are going to predict whether cyber-attack is done or not. These predictions can be done by four algorithms like SVM, ANN, RF, CNN this paper helps to identify which algorithm predicts the best accuracy rates which helps to predict best results to identify the cyber-attacks happened or not.

XI. FUTURE SCOPE

In enhancement we will add some ML Algorithms to increase accuracy

XII. 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 ˘gi sistemlerinde kullanilan arac¸larin incelenmesi," in 1st International Symposium on Digital Forensics and Security (ISDFS13), 2013, pp. 231–239.

[4] S. Staniford, J. A. Hoagland, and J. M. McAlerney, "Practical automated detection of stealthy portscans," Journal of Computer Security, vol. 10, no. 1-2, pp. 105–136, 2002.

[5] S. Robertson, E. V. Siegel, M. Miller, and S. J. Stolfo, "Surveillance detection in high bandwidth environments," in DARPA Information Survivability Conference and Exposition, 2003. Proceedings, vol. 1. IEEE, 2003, pp. 130–138.

[6] K. Ibrahimi and M. Ouaddane, "Management of intrusion detection systems based-kdd99: Analysis with lda and pca," in Wireless Networks and Mobile Communications (WINCOM), 2017 International Conference on. IEEE, 2017, pp. 1–6.

[7] N. Moustafa and J. Slay, "The significant features of the unsw-nb15 and the kdd99 data sets for network intrusion detection systems," in Building Analysis Datasets and Gathering Experience Returns for Security (BADGERS), 2015 4th International Workshop on. IEEE, 2015, pp. 25–31.

[8] L. Sun, T. Anthony, H. Z. Xia, J. Chen, X. Huang, and Y. Zhang, "Detection and classification of malicious patterns in network traffic using benford's law," in Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA ASC), 2017. IEEE, 2017, pp. 864–872.

[9] S. M. Almansob and S. S. Lomte, "Addressing challenges for intrusion detection system using naive bayes and pca algorithm," in Convergence in Technology (I2CT), 2017 2nd International Conference for. IEEE, 2017, pp. 565–568.

[10] M. C. Raja and M. M. A. Rabbani, "Combined analysis of support vector machine and principle component analysis for ids," in IEEE International Conference on Communication and Electronics Systems, 2016, pp. 1–5.