Balani Infotech Pvt. Ltd.

(Library Information Services)

CIN No: U72300DL2007PTC164136
GSTIN: 09AADCB1970E1ZV

TAX INVOICE

Reverse Charge	: N	Subscription Period	: 01 Year From the Date of Activation
Invoice Number	: BL/n/22-23/71	Exchange Rate	: INR
Invoice Date	: 24-Feb-23	Exchange Rate Base	: INR
State	: Uttar Pradesh State Code 09	Reference No.	: NRIIT/CSE/PO-28/2022-23
		Reference Date	: 23-Feb-23

Details of Receiver | Billed To	Details of Consignee | Shipped to
NRI INSTITUTE OF TECHNOLOGY, POTHAVARAPPADU AGIRIPALLI Andhra Pradesh State : Andhra Pradesh State Code : 37 GSTIN :	NRI INSTITUTE OF TECHNOLOGY, POTHAVARAPPADU AGIRIPALLI Andhra Pradesh State : Andhra Pradesh State Code : 37 GSTIN :

Sr No.	PRODUCT DESCRIPTION	HSN SAC CODE	QTY	RATE	Disc %	TAXABLE VALUE	IGST 18	IGST Amount	TOTAL Rs.
1	DrillBit Plagiarism Detection Software 1000 Document Submissions 1 Admin & 10 Users Accounts 1 Year Subscription Period Cloud-Based Anti-Plagiarism Software Service	998431	1	1,00,000.00/Nos	10	90,000.00	18.00 %	16,200.00	1,06,200.00

TOTAL INVOICE AMOUNT (IN WORDS)

Rupees One Lakh Six Thousand Two Hundred Only.

Total Amount Before Tax :	90,000.00
Total Amount:GST	16,200.00
Total Amount After Tax	1,06,200.00
GST Payable On Reverse Charges :	No

Terms and Condition:

1. The Invoice is valid for paymnet within a period of 21 days from the date of issue . In case of delay in payment the amount shall be payable as per the exchange rate prevalent on the date of receipt of payment .
2. Bank Charges , if any , Shall be borne by the Customer , in case of short payment , order will not be processed .
3 100% advance payment required, after receipt of payment, account required 5-7 working days for the activation
4. Please mention Invoice number in Description / Remarks while making NEFT / RTGS Payment .

Bank Details:

Beneficiary Name	: BALANI INFOTECH PRIVATE LIMITED
Bank Name	: RBL BANK LIMITED
Branch Name	: NOIDA BRANCH (P-7, SECTOR-18, NOIDA)
Account No	: 1383774
RTGS/NEFT Code	: RATN0000114
PAN	: AADCB1970E

For BALANI IN[illegible]ATE LIMITED

Signatory

B-116, Sector-67, Noida - 201301
Distt. Gautam Budh Nagar
Uttar Pradesh
Regd. Office: 119, Vinoba Puri, Lajpat Nagar II
New Delhi-110024

DrillBit

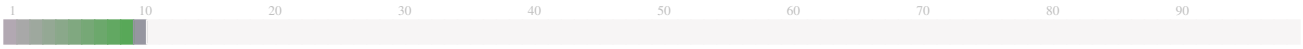
The Report is Generated by DrillBit Plagiarism Detection Software

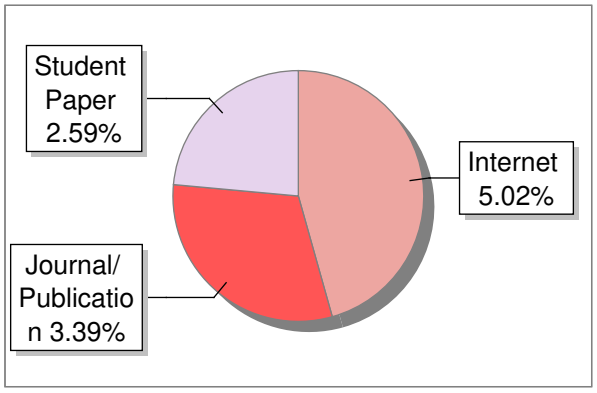
Submission Information

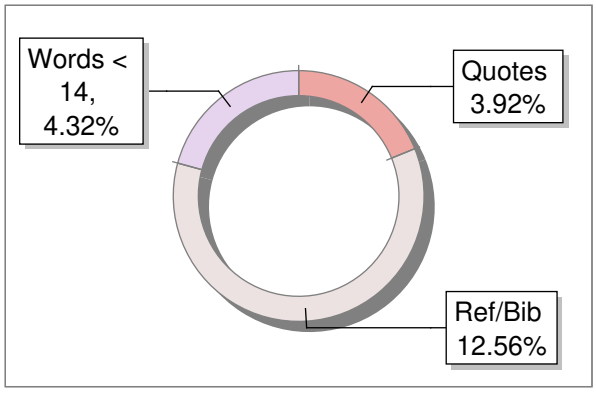
Author Name	M VENKATESWARA RAO
Title	DETECTION OF CYBER-ATTACK IN A NETWORK USING ADVANCED MACHINE LEARNING TECHNIQUES
Paper/Submission ID	1543022
Submitted by	kvsrao@nriit.edu.in
Submission Date	2024-03-18 15:39:25
Total Pages	6
Document type	Article

Result Information

Similarity **11 %**







Exclude Information

Quotes	Excluded
References/Bibliography	Excluded
Sources: Less than 14 Words %	Not Excluded
Excluded Source	**0 %**
Excluded Phrases	Not Excluded

Database Selection

Language	English
Student Papers	Yes
Journals & publishers	Yes
Internet or Web	Yes
Institution Repository	Yes

A Unique QR Code use to View/Download/Share Pdf File

DrillBit

DrillBit Similarity Report

11	9	B
SIMILARITY %	MATCHED SOURCES	GRADE

A-Satisfactory (0-10%)
B-Upgrade (11-40%)
C-Poor (41-60%)
D-Unacceptable (61-100%)

LOCATION	MATCHED DOMAIN	%	SOURCE TYPE
1	Submitted to Visvesvaraya Technological University, Belagavi	3	Student Paper
2	www.dx.doi.org	2	Publication
3	bracu.ac.bd	1	Internet Data
4	www.mdpi.com	1	Internet Data
5	Parallel Systems and Structural Frames Realignment Planning and Actua, by Nahangi, Mohammad - 2015	1	Publication
7	aiscience.org	1	Internet Data
8	springeropen.com	1	Internet Data
10	www.dx.doi.org	1	Publication
11	springeropen.com	1	Internet Data

DETECTION OF CYBER-ATTACK IN A NETWORK USING ADVANCED MACHINE LEARNING TECHNIQUES

Dr. M. Venkateswara Rao[1], B. Ramya[2], A. Kiranmayi[3], Ch. Bhavya Sri[4], G. Deepthi[5]
[1]Head of the AI&ML department, [2,3,4]B. tech Student
Department of CSE, NRI institute of technology, Pothavarappadu, Andhra Pradesh, India

ABSTRACT: In contemporary society, reliance on cyberspace permeates every facet of daily life, leading to an increase in cybercrimes and threats. While novel innovations offer significant advantages to individuals, organizations, and governments, they also introduce vulnerabilities. Critical issues such as safeguarding important data, securing stored information platforms, and ensuring data availability have emerged. Among these concerns, cyber terrorism stands out as a paramount challenge. The proliferation of cyber threats poses significant risks to both individuals and institutions, potentially jeopardizing public and national security. Consequently, the development of Intrusion Detection Systems (IDS) has become imperative to mitigate cyber-attacks. In this study, we employ support vector machine (SVM) algorithms for port scan detection using the latest CICIDS2017 dataset, achieving precision rates of 97.80% and 69.79% respectively.

KEYWORDS: Data Preprocessing, Cyber Attack, SVM, ANN, CNN, Random Forest, CICIDS2017.

INTRODUCTION

The utilization of machine learning has become pivotal in the detection of cyber-attacks, with various algorithms being employed for this purpose. This study endeavours to conduct a comparative analysis of different machine learning methodologies utilized in identifying cyber-attacks, drawing insights from diverse metrics. The foundation of this paper lies in a comprehensive literature review of detection techniques deployed in identifying cyber threats. Emphasis is placed on comparing and contrasting different machine learning algorithms through the presentation of a comparative table. However, our practical experience in investigating unsolicited remote port scans has led us to observe a significant trend: a considerable portion of these scans originates from compromised hosts, indicating potential hostile intent. As such,

considering port scans as potentially malicious and promptly reporting them to the administrators of the corresponding remote networks appears to be a prudent course of action. Nonetheless, the primary focus of this paper remains on the technical intricacies involved in port scan detection, independent of the interpretation or response strategies associated with such scans. Specifically, our attention is directed towards the detection of port scans through network intrusion detection systems (NIDS), while addressing evasion tactics in a manner conducive to real-world implementation within dynamic network environments.

Within subsequent sections, we aim to provide a clear definition of port scanning, supplemented by illustrative examples and an exploration of evasion techniques employed by attackers. A comprehensive review of existing research pertaining to port scan detection is presented, followed by the introduction of proposed algorithms and preliminary data supporting our approach. Furthermore, potential avenues for extending this research are discussed alongside considerations for broader applications. Throughout this paper, it is assumed that readers possess a foundational understanding of Internet protocols, fundamental concepts related to network intrusion detection and scanning, as well as rudimentary knowledge in probability theory, information theory, and linear algebra.

Port scans serve two primary purposes for attackers: information gathering and disruption. While our primary focus lies in the detection of information-gathering port scans, the threat of malicious flooding with excessive information remains a critical consideration in algorithm design. We introduce the concept of a "scan footprint" to delineate the set of port/IP combinations of interest to attackers, distinct from the scan script, which dictates the temporal sequence of exploration.

LITERATURE REVIEW

In the realm of cyber security, Yaokai Feng et al. (2018) introduced a novel machine learning framework aimed at early detection of distributed cyber-attacks. By discerning crucial features from network traffic data, their approach leveraged SVM feature selection alongside a classifier, exhibiting notable efficacy in preempting cyber threats. The study emphasized the pivotal role of feature selection in optimizing algorithmic performance for timely detection of cyber-attacks.

A seminal contribution by R. Christopher (2001), titled "Port scanning techniques and the defense against them,"

disseminated by the SANS Institute, delineates port scanning as a prevalent strategy utilized by adversaries to pinpoint exploitable services for system infiltration. Systems tethered to LANs or the Internet via modems often host services across a spectrum of ports, prompting attackers to conduct port scans to glean information about active services, user ownership, anonymous login support, and authentication requirements. Port scanning entails a systematic probing of individual ports, with response characteristics indicating potential vulnerabilities. The significance of port scanners lies in their capacity to uncover security weaknesses, empowering network security practitioners to bolster system defenses. Conversely, the detection and mitigation of port scans are imperative for safeguarding network integrity. Measures such as restricting access to open ports for authorized users and implementing stringent access controls are essential for fortifying system security against potential intrusions.

Limitations of the current system:

1) Stringent regulatory constraints

2) Complexity poses challenges for non-technical users

3) Resource limitations impede functionality

4) Ongoing necessity for frequent patches

5) Persistent vulnerability to cyberattacks

PROPOSED SYSTEM:

The proposed algorithm entails several crucial steps:

1) Normalization of each dataset.

2) Division of the dataset into testing and training sets.

3) Creation of Intrusion Detection System (IDS) models utilizing RF, ANN, CNN, and SVM algorithms.

4) Evaluation of the performance of each model.

Advantages:

• Enhanced protection against malicious network attacks.

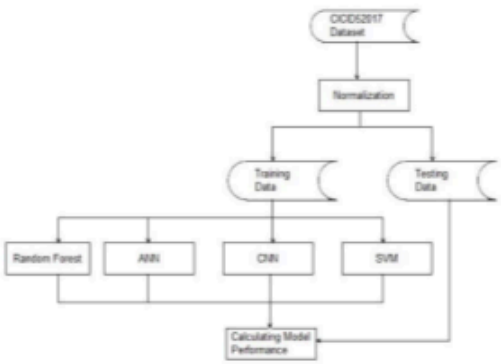
• Identification and removal of malicious elements within an existing network.

• Prevention of unauthorized access to the network by users.

• Restriction of programs from accessing potentially infected resources.

• Enhanced security for confidential information.

SYSTEM DESIGN



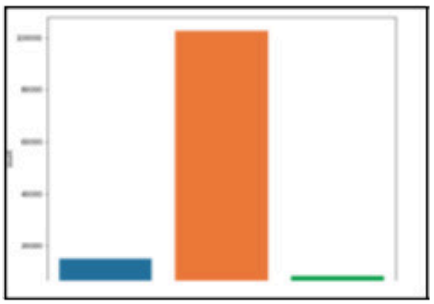
METHODOLOGY

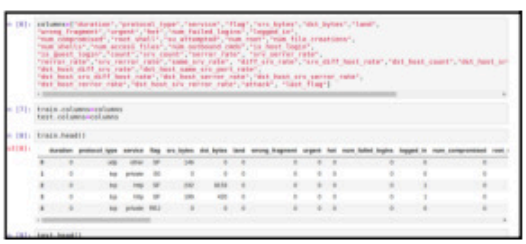
The SVM, ANN, CNN, Random Forest, and deep learning algorithms were applied to detect port scan attempts using the CICIDS2017 dataset. The methodology's flowchart is depicted in the accompanying figure. Initially, 692,703 records from the dataset underwent standardization. Subsequently, these standardized records were divided into a 75% training dataset and a 25% testing dataset. Finally, the models were evaluated using the testing dataset, and their performance metrics were computed accordingly.

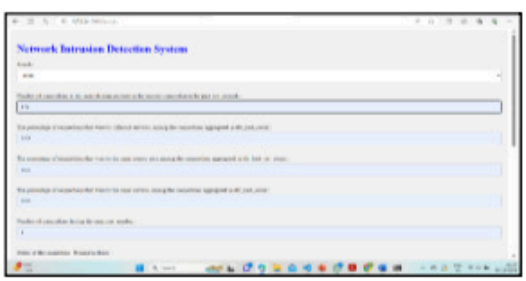
RELATED WORK

1. DDoS Attacks: A Distributed Denial-of-Service (DDoS) Attack floods a server with internet traffic, aiming to disrupt access to linked online services and websites.
2. Malware: Any software or code designed to inflict harm on computers, networks, or servers is categorized as malware or malicious software.
3. Denial-of-Service (DoS) Attacks: During a DoS attack, users are unable to access email, websites, or other resources controlled by a compromised computer or network, though most of these attacks do not result in data loss.
4. Phishing Attacks: Phishing scams attempt to steal user credentials or sensitive data, often by tricking individuals into providing passwords or account numbers, or by deploying malicious files that can infect systems or devices.
5. Ransomware: Ransomware is a sophisticated form of malware that employs strong encryption to hold data or system functionality hostage, exploiting system vulnerabilities.
6. Backdoor Trojans: Backdoor Trojans create a secret entry point on a victim's system, granting attackers full and remote control, which can be utilized for various cybercrimes.
7. IoT-Based Attacks: Any cyber-attack targeting Internet of Things (IoT) devices or networks qualifies as an IoT attack, allowing hackers to compromise devices, steal data, or enlist infected devices in botnets for launching DoS or DDoS attacks.
8. Supply Chain Attacks: Supply chain attacks target trusted third-party vendors providing essential services or software, posing significant risks to the integrity and security of the supply chain ecosystem.

RESULTS:







CONCLUSION

In this project, we aim to leverage port scan attempts alongside other attack types using AI and deep learning algorithms, as well as Apache Hadoop and Spark technologies, based on the dataset at hand. The integration of these advanced algorithms enables us to effectively detect cyber-attacks within networks. Over the years, numerous cyber-attacks have occurred, resulting in the accumulation of datasets containing information about the characteristics of these attacks. By utilizing these datasets, we endeavour to predict whether a cyber-attack has taken place. To achieve this, we employ four algorithms: SVM, ANN, RF, and CNN. This research seeks to determine which algorithm yields the highest accuracy rates, thus facilitating the identification of cyber-attacks with greater precision and reliability.

REFERENCES

[1] Jeyaselvi, M., M. Sathya, S. Suchitra, S. Jafar Ali Ibrahim, and N. S. Kalyan Chakravarthy. "SVM-Based Cloning and Jamming Attack Detection in IoT Sensor Networks." Advances in Information Communication Technology and Computing, pp. 461-471. Springer, Singapore, 2022.

[2] V. Praveena, A. Vijayaraj, P. Chinnasamy, I. Ali, R. Alroobaea et al., "Optimal deep reinforcement learning for intrusion detection

in uavs", Computers Materials & Continua, vol. 70, no. 2, pp. 2639-2653, 2022.

[3] K. M. Sudar, P. Nagaraj, P. Deepalakshmi and P. Chinnasamy, "Analysis of Intruder Detection in Big Data Analytics", 2021 International Conference on Computer Communication and Informatics (ICCCI), pp. 1-5, 2021.

[4] Ajmeera Kiran and D. Vasumathi, "Optimal Privacy Preserving Technique Over Big Data Analytics Using Oppositional Fruitfly Algorithm", Recent Patents on Computer Science, vol. 13, no. 2, 2020.

[5] V. Padmanaban and M.Nalini, Proceedings of the 2019 international IEEE Conference on Innovations in Information and Communication Technology, (2019).

[6] Jeyaselvi, M., M. Sathya, S. Suchitra, S. Jafar Ali Ibrahim, and N. S. Kalyan Chakravarthy. "SVM-Based

Cloning and Jamming Attack Detection in IoT Sensor Networks." *Advances in Information Communication*

Technology and Computing, pp. 461-471. Springer, Singapore, 2022.