International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 12 **Issue:** IV **Month of publication:** April 2024

DOI: https://doi.org/10.22214/ijraset.2024.61352

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue IV Apr 2024- Available at www.ijraset.com

Cyber Intrusion Detection System Using Deep Learning Approach

Reshni S[1], Vadipalli Navateja[2], Vinukonda Naveen[3], Rettadi Ravindra Kumar[4], Kunku Praveen[5]
Kalsalingam of Academy of Research and Education, Krishnanakovil, Tamilnadu

Abstract: Technological developments in network communications have led to a remarkable increase in network traffic and an explosion in the use of linked devices across a number of commercial fields. Systems for detecting intrusions that can recognize malicious assaults from traffic data might be useful instruments for protecting company assets from illegal access. This project suggests a two-stage architecture for an intrusion detection system, where an auto encoder (AE) and the grey wolf algorithm (GWO) choose features. It is evaluated using the Bot-Iot and NSL-KDD datasets, yielding better accuracy levels for binary and multiclass attack categorization. This method outperforms the latest intrusion detection techniques in terms of categorization using an ideal selection of traffic characteristics.

I. INTRODUCTION

Cybercrime skyrocketed after the swift advancement of technology and globalization of internet networks. The Internet Security Threat Report states (ISTR), over 430 million new malware variants were discovered in 2015, 362 of which were crypto-ransomware. In 2018, the anticipated rates of cybercrime generated 1.5 trillion US dollars. If 2019 has taught us anything, it's that no business is secure from cyberattacks of any size. Cyberattacks are more sophisticated, devious, and focused than in the past. As a result, security measures need to be updated often. To begin with, meta-heuristics are rather basic. Most of them have been influenced by quite basic ideas. Usually, physical facts, animal behaviors, or ideas about evolution serve as the sources of inspiration. Second, flexibility describes how metaheuristics may be applied to many issues without requiring specific modifications to the algorithm's structure. Since meta-heuristics typically treat issues as black boxes, they may be easily applied to a wide range of problems. Third, the processes of most meta-heuristics are derivation-free. Meta-heuristics are a stochastic method to problem optimization, as opposed to gradient-based optimization techniques. To locate the optimal, the optimization process begins with a random solution or solutions; the derivative of search spaces does not need to be calculated. Lastly, when it comes to avoiding local optima, meta-heuristics outperform traditional optimization methods. This is because meta-heuristics are stochastic, which enables them to thoroughly search the whole search space and prevent stagnation in local solutions.

A. Proposed System

Now we are going to discuss about the Software and hardware requirements of our project.

B. Software Requirements

Google Colaboratory - It's a platform for developing machine learning models in python.

C. Hardware Requirements

1) Processor - INTEL CORE
2) RAM - More than 4 GB
3) Hard Disk - 10 GB

D. Functional Requirements

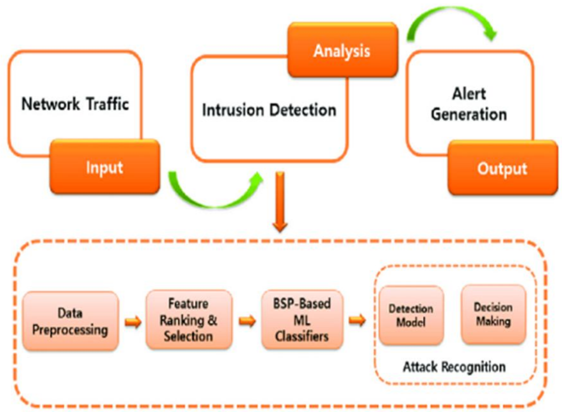
We will now talk about the project's functional and nonfunctionalneeds.

E. Functional prerequisites

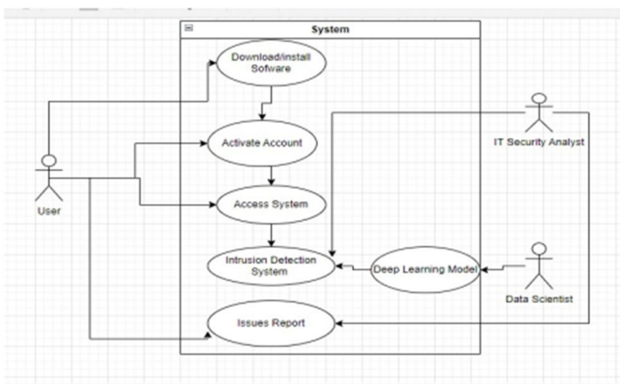
Functional requirements are the particular attributes and qualities that a system or piece of software has to have to fulfill the requirements and anticipations of its consumers.The specifications generally outline the activities and features that the system ought to as well as any restrictions or limits on its ability to fulfill execution.

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue IV Apr 2024- Available at www.ijraset.com

F. Architecture



G. Use Case Diagram



H. Problem Statement

To create a network intrusion detection system that performs well with any data by selecting the best characteristics using a metaheuristic algorithm and a classifier model. The goal is to create a network intrusion detector, a predictive model that can tell the difference between malicious connections—also known as intrusions or attacks—and trustworthy, regular connections.

II. SCOPE OF THE PROJECT

This section addresses the many aspects of our project's scope.

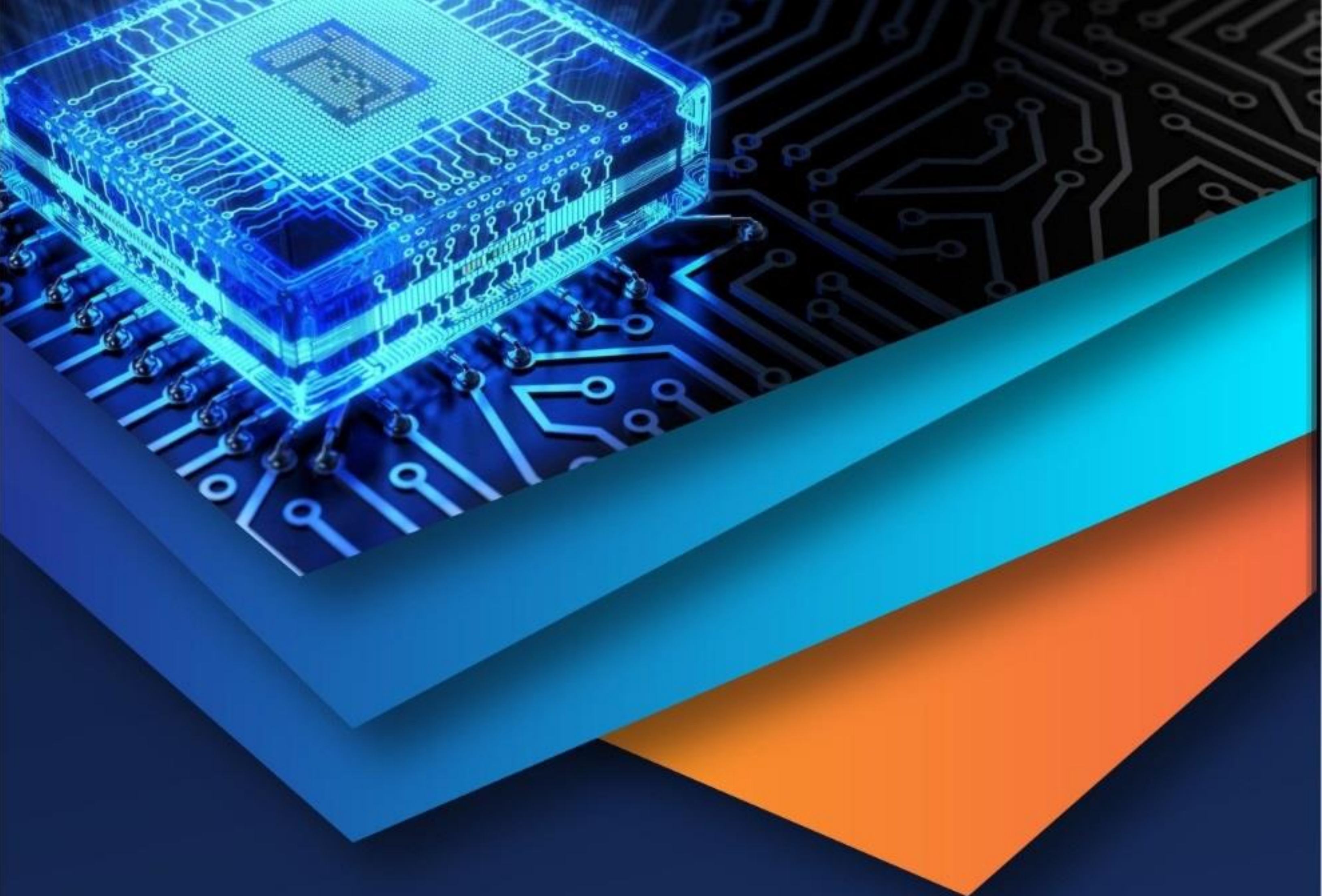
1) *Threat Detection:* Through real-time network traffic analysis, NIDS is able to identify and detect a wide range of security risks, such as viruses, malware, and other cyberattacks.
2) *Early Warning System:* NIDS can function as an early warning system by informing security personnel of questionable activities and sending warnings and notifications in response.
3) *Incident Response:* NIDS can offer important information about the origin, target, and kind of attack in security events. This can aid security personnel in reacting to attacks more skillfully and lessening their effects.Compliance: Through the provision of network activity visibility and the detection of any unwanted access or data breaches, NIDS may assist enterprises in meeting compliance requirements for security and data privacy standards.
4) *Network Optimization:* By locating and fixing problems that might affect network performance and user experience, such as bottlenecks and congestion, NIDS can assist in improving network performance.
5) *Forensic Analysis:* Security teams may perform a thorough examination of security events and acquire evidence for legal or regulatory purposes by using NIDS to record and retain network traffic data for forensic analysis.

These are the various uses for network intrusion detection systems.

a) *Corporate Network Security:* Organizations utilize Network Intrusion Detection Systems (NIDS) to keep an eye on and defend their corporate networks against security threats and cyberattacks. This include identifying and stopping hostile behavior, illegal access, and data breaches.
b) *Cloud Security:* Network intrusion detection systems (NIDS) are used to monitor and defend cloud environments—both public and private—against security risks. This entails identifying and stopping hostile activities in the cloud, including data breaches and illegal access.
c) *Industrial Control system Security:* To keep an eye out for and defend against cyberattacks and other security risks, NIDS are employed in conjunction with industrial control systems (ICS). This include identifying and stopping malware infections, illegal access, and other types of harmful activities that might compromise vital infrastructure.
d) *Security of Mobile Networks:* NIDS are used to keep an eye on and defend mobile networks against security risks. This involves identifying and stopping malware infections, illegal access, and other dangerous conduct on mobile devices for the
e) *Security of the Internet of Things (IoT):* NIDS are used to keep an eye on and defend networks and devices connected to the IoT against security threats. This covers the identification and mitigation of malware infections, unapproved access, and other harmful activities on Internet of Things devices.

REFERENCES

[1] B. R. Raghunath and S. N. Mahadeo, "Supervised and unsupervised ML algorithm & CNN & recurrent neural networks of deep learning algorithms," IEEE, 2018.
[2] S. Lim and S. Kim, "AE, GWO algorithms & UNSW-NB15 dataset used," 2019.
[3] Yang, Y., Zheng, K., Wu, C., & Yang, Y. "Conditional variational autoencoder (ICVAE) with a deep neural network (DNN): UNSWNB15 and NSL-KDD datasets are used" 2019.
[4] Sultana, J., & Sadaf, K. "Autoencoder (AE) and Isolation Forest (IF) deep learning approach",2020.
[5] Panda, M., Abraham, A., Das, S., & Patra, M. R."Filter and wrapper techniques: Mix decision trees, random forests, and support vector machines",2021.
[6] Moizuddin, M. D., & Jose, M. V. "Swarm optimization (PSO) algorithm & KDDCup99 dataset",2022.
[7] "Anomaly Detection in Network Traffic Using Deep Autoencoder and Grey Wolf Optimization Algorithm" by H. Mirzaei, H. Amintoosi, and M. Nourian. IEEE Access, 2021.
[8] "A Hybrid Network Intrusion Detection System Using Autoencoder and Grey Wolf Optimization" by S. M. Abbasi, M. S. Rezvani, and H. R. Shahriari. Journal of Cybersecurity and Privacy, 2021.
[9] "An Efficient Hybrid Intrusion Detection System Based on Autoencoder and Grey Wolf Optimization Algorithm" by H. Mirzaei, H. Amintoosi, and M. Nourian. Journal of Ambient Intelligence and Humanized Computing, 2021.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY