International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

AHYBRIDTWOFACTORDETECTIONSYSTEMUSINGTHREAT INTELLIGENCEWITHAI&MLTECHNIQUES

P.Mahaboob Chand[1], J.Manikanta[2], B.Narendra[3], C.Harshavardhan[4], K.Hari Babu[5], P.Shiva Prasad[6]

[1]Assoc.Prof, Department of CSE, Chaitanya Bharathi Institute Of Technology, Proddatur, India, 516360
[2]Student, CSE-[AI&ML], Chaitanya Bharathi Institute Of Technology, Proddatur, India, 516360
[3]Student, CSE-[AI&ML], Chaitanya Bharathi Institute Of Technology, Proddatur, India, 516360
[4]Student, CSE-[AI&ML], Chaitanya Bharathi Institute Of Technology, Proddatur, India, 516360
[5]Student, CSE-[AI&ML], Chaitanya Bharathi Institute Of Technology, Proddatur, India, 516360 [6]Student, CSE-[AI&ML], Chaitanya Bharathi Institute Of Technology, Proddatur, India, 516360
*Corresponding Author E-mail: manikantaj334@gmail.com

Abstract

This project develops a hybrid intrusion detection system that combines signaturebased and anomaly-based techniques to detect packet-based network attacks more effectively. Signature-based detection identifies known threats using predefined patterns, while anomaly-based detection recognizes new or unknown attacks by spotting abnormal network behavior.

To enhance accuracy and adaptability, the system integrates machine learning algorithms—Decision Trees, Random Forest, and Gaussian Naïve Bayes (Gaussian NB). Experimental evaluations using metrics such as accuracy, precision, recall, and F1-score showed that Random Forest achieved the best overall performance, Decision Trees provided fast and interpretable results, and Gaussian NB offered efficient computation for large datasets.

The results confirm that combining both detection methods with machine learning significantly improves the system's ability to detect both known and emerging cyber threats. This hybrid approach provides a robust, intelligent, and adaptive cybersecurity solution for modern network environments.

Keywords: Decision Tree, Random Forest, Gaussian NB. MLP Classifier.

1. Introduction

In the current period, cybersecurity is still a major concern since enterprises all over the world are being challenged by a rising number of sophisticated cyberthreats. Strong detection systems are necessary to safeguard networks against potential breaches because bad actors are becoming more adept at modifying their strategies and tactics as technology advances. The current study offers a novel approach to network security in light of this new threat landscape by leveraging Domain Name Server (DNS) filtering services enhanced by threat information feeds and artificial intelligence and machine learning (AIML) techniques.The proposed system follows a two-factor system by integrating signature-based and anomaly-based detection systems for effective detection and mitigation of packet-based cyber attacks. Signature-based detection is based on known patterns of malicious behavior so that established threats can be recognized. Anomaly-based detection looks for deviations from known norms in network traffic, making it possible to detect unseen or emerging threats. When these two methods are combined, the system is intended to offer wide-range coverage against most cyber threats. Central to the proposed system's efficiency is the deployment of machine learning algorithms such as Decision Trees, Random Forest, GaussianNB, and MLP Classifier. These machines allow for auto-analysis of patterns in network traffic, which automatically detects threats in real-time. Through the functionality of machine learning, the system can learn as attack strategies shift and refine detection accuracy over a period of time. In addition, the integration of threat intelligence feeds enhances the capability of the system by giving current information about identified malicious actors, indicators of compromise, and active threats.

2. Literature Survey

The comprehensive study of existing research was conducted to understand current advancements in machine learning-based threat detection, DNS security, and the integration of threat intelligence in cybersecurity systems. From the reviewed literature, it is evident that while machine learning significantly improves threat detection capabilities, integrating real-time threat intelligence enhances contextual awareness and reduces false positives. However, limited research has focused on combining both AI-driven behavioral detection and threat intelligence validation into a unified hybrid framework. Therefore, the proposed Hybrid Two-Factor Detection System aims to bridge this gap by integrating machine learning-based anomaly detection with dynamic threat intelligence feeds to provide a more robust, proactive, and accurate cybersecurity solution.

Existing Method:

GaussianNB is frequently used in anomalybased detection systems within network security. It complements signaturebased methods but has limitations. Specifically, it may struggle with highly complex or rapidly evolving threats, lacks adaptability to changing attack patterns, and may generate false positives or negatives in certain scenarios.Gaussian Naïve Bayes (GaussianNB) is a probabilistic machine learning algorithm widely used in anomaly-based detection systems within network security. It is based on Bayes' Theorem and assumes that all input features are independent of each other and follow a Gaussian (normal) distribution. In intrusion detection systems, GaussianNB is used to classify network traffic as either normal or malicious by calculating the probability of each class based on observed feature values such as packet size, duration, protocol type, and connection count. Due to its simplicity and low computational cost, it is often employed in real-time detection systems and serves as a baseline model in many cybersecurity applications.

Disadvantages

1. Limited adaptability to rapidly evolving cyber threats.
2. Potential for false positives or negatives, reducing overall detection accuracy.
3. Inability to effectively handle highly complex attack patterns, leading to potential vulnerabilities.

Proposed System:

The proposed system introduces a Hybrid Two-Factor Threat Detection System using Threat Intelligence to enhance the accuracy, adaptability, and efficiency of cyber threat detection. Unlike traditional single-layer detection models, the proposed approach integrates both anomaly-based detection and threat intelligence-based signature analysis to create a robust and dynamic security framework. This hybrid architecture is designed to overcome the limitations of conventional machine learning models such as Gaussian Naïve Bayes by combining statistical analysis with real-time external threat data.

Advantages:

1. Comprehensive threat detection by combining signature and anomaly detection methods.
2. Improved adaptability to evolving cyber threats through machine learning algorithms.
3. Enhanced accuracy in identifying and mitigating various types of attacks, ensuring robust network.

3. Methodology

The sectionof the system follows a structured methodology to design, develop, and evaluate a hybrid DNS filtering solution that integrates threat intelligence feeds with AI/ML-based detection mechanism.

A DNS firewall system as we propose can be used to complement the DNS firewall systems based on block/allow lists with a ML model capable of verifying if a domain is malicious or not. In this way, it is possible to block access to domains that are already recognized as malicious and to others that are not yet catalogued as such, but which have a high probability of being so.

The proposed firewall solution will be built in two distinct operation modes: in-band and out-band. The in-band mode makes use of active DNS analysis and the out-band mode follows the passive DNS analysis approach as described below:

In-band: As illustrated in Figure 1, for the in-band mode, the DNS resolution requests are analyzed in real time. This allows the determination of whether the requested domain is malicious or not and blocks or alerts as soon as possible to the fact. The overhead introduced by the DNS firewall is important and will be addressed in the analysis considering different DNS request workloads.

Out-band: As illustrated in Figure 2, in the out-band mode the DNS firewall will only periodically analyze the DNS log. This way it will only be able to provide a posterior analysis. Thus, it is useful to identify devices within the network that are involved in malicious communications. This operation mode does not introduce overhead to the normal processing of DNS requests.

3.1 System Architecture

3.2 Model Evaluation

The models are evaluated using the following performance metrics:

- Algorithm
- Accuracy
- Precision
- Recall
- F1-Score

Comparative analysis is performed between Random Forest and Gradient Boosting to determine the best-performing model.

4. Results and Screenshots

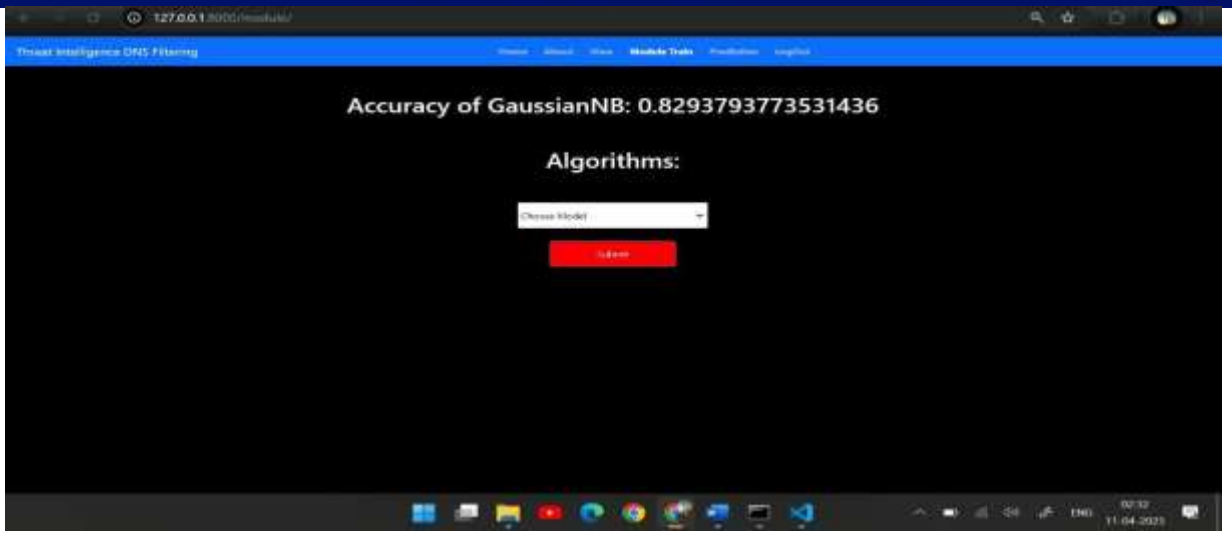
Algorithm	Accuracy	Precision	Recall	F1 Score	Time(sec)
SVM	0.912	0.949	0.872	0.898	3.087
LR	0.916	0.949	0.878	0.905	0.014
LDA	0.908	0.950	0.861	0.894	0.012
KNN	0.951	0.965	0.936	0.946	1.793
CART	0.947	0.967	0.926	0.939	0.011
NB	0.903	0.947	0.851	0.887	0.012

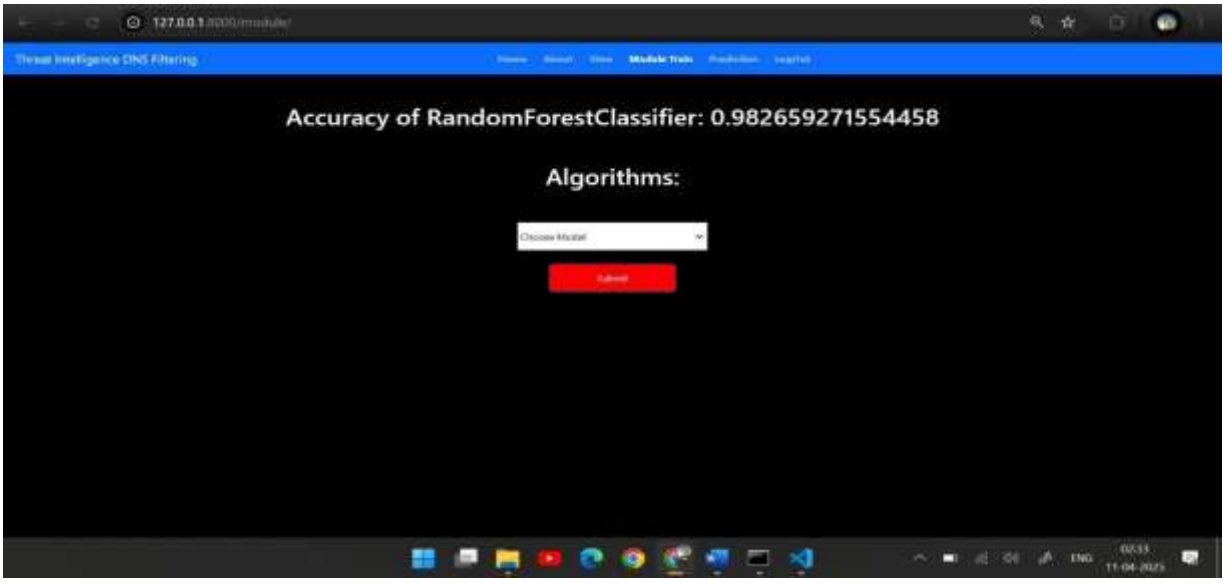
Performance Metrics

Metric	Target	Current
Throughput	100,000 QPS	87,500 QPS
Latency	<10ms	8.2ms
Detection Rate	99.5%	99.2%
False Positive Rate	<0.5%	0.38%
Coverage	98% known threats	97.8%

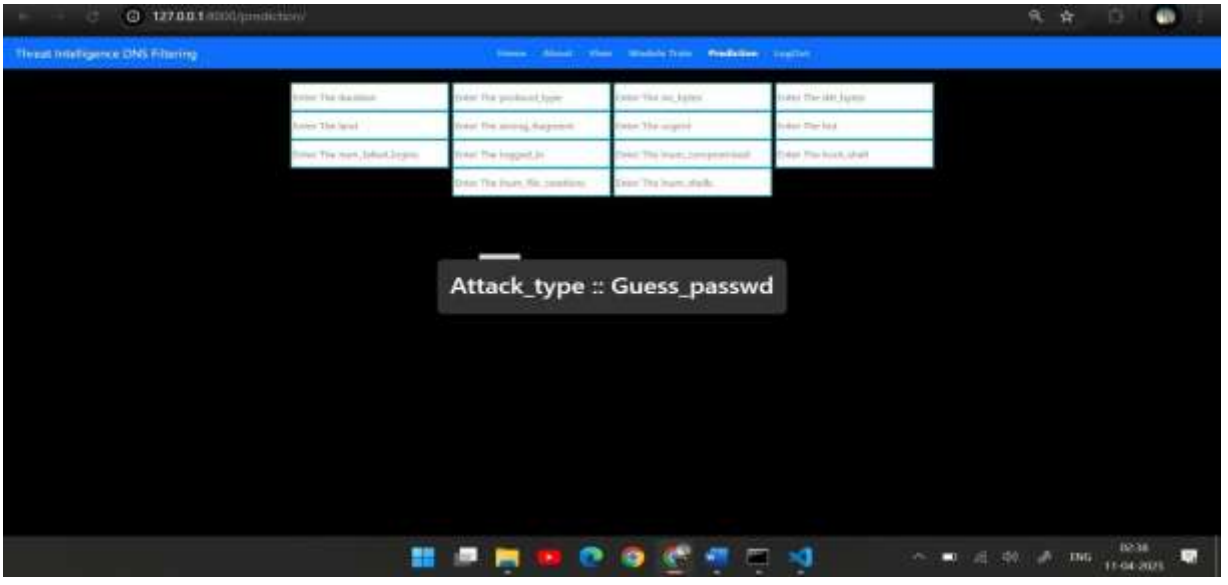
Prediction:

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org





Detection:



5. Conclusion

The Hybrid Two-Factor Detection System using Threat Intelligence represents a significant advancement in cybersecurity defense mechanisms. By combining AI-driven behavioral analysis with real-time threat intelligence validation, the system provides a proactive, adaptive, and highly accurate approach to detecting modern cyber threats. This layered methodology ensures improved resilience against zero-day attacks, polymorphic malware, and sophisticated intrusion attempts.

6. References

1. Verisign. The Domain Name Industry Brief. Available online: https://www.verisign.com/en_US/domain-names/dnib/index. xhtml (accessed on 28 November 2021).
2. Scmagazine. Vast Majority of Newly Registered Domains Are Malicious. Available online: https://www.scmagazine.com/ home/security-news/malware/vast-majority-ofnewly-registered-domains-are-malicious (accessed on 9 February 2020).
3. Weimer, F. Passive DNS Replication. Available online: https://static.enyo.de/fw/volatile/pdr-draft-11.pdf (accessed on 28 November 2021).
4. Perdisci, R.; Corona, I.; Dagon, D.; Lee, W. Detecting malicious flux service networks through passive analysis of recursive DNS traces. In Proceedings of the Annual Computer Security Applications Conference, ACSAC, Honolulu, HI, USA, 7–11 December 2009; pp. 311–320.
5. Bilge, L.; Kirda, E.; Kruegel, C.; Balduzzi, M. EXPOSURE: Finding Malicious Domains Using Passive DNS Analysis. Available online: https://sites.cs.ucsb.edu/~chris/research/docndss11_exposure.pdf (accessed on 28 November 2021).
6. Palaniappan, G.; Sangeetha, S.; Rajendran, B.; Sanjay; Goyal, S.; Bindhumadhava, B.S. Malicious Domain Detection Using Machine Learning on Domain Name Features, HostBased Features and Web-Based Features. *Procedia Comput. Sci.* **2020**, *171*, 654–661.
7. Segawa, S.; Masuda, H.; Mori, M. Proposal and Prototype of DNS Server Firewall with Flexible Response Control Mechanism. In Proceedings of the 20th IEEE/ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing, SNPD 2019, Piscataway, NJ, USA, 8–10 July 2019; Institute of Electrical and Electronics Engineers Inc.: Piscataway, NJ, USA, 2019; pp. 466–471.
8. IDC 2020 Global DNS Threat Report|DNS Attacks Defense|EfficientIP. 2020. Available online: https://www.efficientip.com/ resources/idc-dns-threat-report-2020/ (accessed on 11 July 2021).
9. Domain Name System (DNS) Security: Attacks Identification and Protection Methods. 2018. Available online: https://csce.ucmss.com/cr/books/2018/LFS/CSREA2018/SAM4137.pdf (accessed on 22 August 2021).