Machine Learning Enhanced Intrusion Detection for Cybersecurity

P. S. Kavya
Department of Computer Science and Engineering
Panimalar Institute of Technology
Chennai, India
kavyaprakashpsk@gmail.com

E. Srinidhi
Department of Computer Science and Engineering
Panimalar Institute of Technology
Chennai, India
srinidhielangoan@gmail.com

K. Poojitha
Department of Computer Science and Engineering
Panimalar Institute of Technology
Chennai, India
poojithapooji191103@gmail.com

Mrs. B. Bala Abirami
Assistant Professor
Department of Computer Science and Engineering
Panimalar Institute of Technology
Chennai, India
bala.bami@gmail.com

Dr. D. Lakshmi
Associate Professor and Head
Department of Computer Science and Engineering
Panimalar Institute of Technology
Chennai, India
csehod@pit.ac.in

M. Abirami
Assistant Professor and Supervisor
Department of Computer Science and Engineering
Panimalar Institute of Technology
Chennai, India
swagathajaisathish@gmail.com

***Abstract*—In the modern digital landscape, AI-Driven Intrusion Detection plays a vital role in enhancing cybersecurity by using machine learning techniques to identify and prevent potential threats. This project involves developing an intelligent intrusion detection system that uses machine learning algorithms to detect network anomalies and intrusions effectively. The data preprocessing phase includes cleaning, normalization, and feature selection to improve the dataset quality for optimal machine learning model performance. Data visualization techniques, such as heatmaps, pair plots, and histograms, are employed to understand data distributions and correlations between features. Three machine learning algorithms are implemented and compared based on their accuracy, precision, recall, and F1-score, with the best-performing model selected for deployment. The chosen model is then integrated with the Django framework to create a user-friendly web application, allowing monitoring, prediction of network intrusions, and visualization of security alerts for enhanced cybersecurity management.**

Keywords*—The proposed methods include Machine Learning, Intrusion Detection Systems (IDS), Cyber Security, Network Traffic Analysis, Anomaly identification, Classification, Pattern recognition, Supervised Learning and Feature Engineering.

I. INTRODUCTION

In the realm of cybersecurity, machine learning-enhanced intrusion detection systems (IDS) play a pivotal role in identifying and mitigating threats in real-time. Effective data processing is crucial, involving the collection, cleansing, and transformation of raw network data into structured formats suitable for analysis. This data is then visualized using various tools to highlight patterns and anomalies, facilitating the understanding of potential intrusions. To assess the efficacy of the IDS, three different algorithms can be compared based on their accuracy, processing time, and scalability in detecting cyber threats. Integrating these algorithms with the Django framework allows for the seamless development of a web application that not only deploys the machine learning models but also provides an interactive user interface for monitoring and managing security alerts, ensuring a robust defense against evolving cyber threats

II. LITERATURE REVIEW

The field of machine learning and deep learning in the context of Intrusion Detection Systems (IDS) has undergone significant progress in recent years. The scholars are working on the variety of models and frameworks specifically aimed at the development of network intrusion detection precision and efficiency through the use of different ML and DL techniques. A standout achievement in this field is the Wasserstein-Based Out-of-Distribution Detection (WOOD). The WOOD is using the Wasserstein distance contribution in making the distinction between the distribution of the data samples (in-distribution and out-of-distribution). This approach is crucial in the identification of the unknown and zero-day attacks that are ignored by traditional IDS. Thru comparison to the data patterns issued before the attacks, WOOD successfully improves the security measures and helps in real-time detection of anomalies even in new kinds of attacks. Moreover, the connection of the technique with deep learning architectures like ResNet and DenseNet is responsible for the system's adaptability and the performance across a number of applications such as object detection and image classification. This attribute is the most advantageous when integrated, with IDS, as it increases the capacity to know the rare and new threats.A well-known model in Intrusion Detection Systems (IDS) is the DCNNBiLSTM which consists of a combination of Convolutional Neural Networks (CNN) and Bidirectional Long Short-Term Memory (BiLSTM) networks. The hybrid architectural design serves as an efficient way of exploiting the strengths of both CNN and BiLSTM in intrusion detection. CNNs are great at recognizing spatial elements in network traffic, whereas the BiLSTM layers are the best time series data analyzers that are able to unroll sequences in both directions. The collaboration of the two methods enhances the detection of complex attacks, especially those which escalate over time, such as Distributed Denial-of-Service attacks (DDoS). The model has been superb in terms of

accuracy, e.g., the CICIDS2018 and Edge_IIoT datasets, which has hence fast-tracked the detection capabilities in practical scenarios. This combination is particularly useful for the identification of sophisticated attack types, It can be deployed in parallel to IDSs that are simply rule-based and detect more complicated strategies.

A thorough examination of Machine Learning and Deep Learning applications in Network Intrusion Detection Systems (NIDS) underscores the variety of strategies employed for network anomaly detection. Traditionally, supervised learning techniques such as Random Forests, Support Vector Machines (SVM), and Decision Trees have been utilized to categorize network traffic into benign and malicious classifications. These models depend significantly on labeled datasets, which enables them to perform effectively when trained on known attack patterns; however, they often struggle to identify novel attacks that diverge from these established patterns. Conversely, unsupervised learning approaches, including clustering algorithms like K-Means and DBSCAN, along with various anomaly detection methods, are increasingly recognized for their capability to uncover previously unrecognized threats. Although these models do not necessitate labeled data, they encounter difficulties associated with elevated false-positive rates, frequently misidentifying benign traffic as malicious. A critical challenge identified in the review is the significance of feature engineering and dataset selection, as appropriate choices can substantially affect the efficacy of ML-based IDS models. The review stresses that achieving an optimal balance between model complexity and feature relevance is essential for enhancing detection accuracy and reducing false alarms.

The Hybrid Machine Learning Model for Network Security signifies a notable advancement in Intrusion Detection Systems (IDS). This model synergizes machine learning and deep learning methodologies to enhance performance by addressing the shortcomings of standalone models. One notable hybrid strategy employs the Synthetic Minority Over-sampling Technique (SMOTE) for data balancing in conjunction with XGBoost for feature selection. SMOTE effectively tackles the prevalent issue of class imbalance in intrusion detection by generating synthetic samples of minority classes, thereby preventing bias towards the majority class and improving detection rates for infrequent attacks. XGBoost, recognized for its robustness and efficiency, is utilized for both feature selection and classification tasks. When evaluated on benchmark datasets such as KDDCUP99 and CIC-MalMem-2022, the hybrid model exhibited nearly flawless accuracy, surpassing traditional models in terms of both detection accuracy and processing speed. Furthermore, this approach aids in alleviating common challenges such as overfitting and Type-I/Type-II errors, thereby enhancing the system's reliability and adaptability in practical applications.

The research seeks to determine if Deep Reinforcement Learning (DRL) can be a potential technique applied for Intrusion Detection Systems (IDS) by utilizing reinforcement learning methods, among them Deep Q Networks (DQN), to the set of intrusion detection system models. In contrast to commonly used machine learning models, which require samples of the past on which to base their decisions, DQN-IDS is innovative since it can adapt to the environment and thus make decisions on the fly. This system's feature of learning itself and optimizing is what makes it the most suitable as it tracks the developing threats without the need of somebodys prior knowledge of the specific attack types. A comparative study showed that DRL-based IDS had a significantly improved detection rate compared to conventional machine learning models such as Random Forest and Support Vector Machines (SVM), especially in dynamic and fast-changing network conditions. Nevertheless, the major drawback of DRL is that it is extremely computationally intensive, obviously forcing high processing resources and time for the successful resolution of the training task. Furthermore, incorporating this is the case of less capable systems complicates matters further.

III. PROBLEM STATEMENT

While modern deep learning-based intrusion detection systems have demonstrated remarkable success in achieving high detection accuracy, they often suffer from key limitations that impede their real-world applicability. These systems are typically opaque, with limited interpretability, making it difficult for cybersecurity analysts to understand the rationale behind their predictions. Furthermore, deep learning models are resource-intensive, requiring significant computational power and training time, which restricts their usability in small- and medium-scale enterprises. Another critical shortcoming lies in their inability to effectively handle out-of-distribution (OOD) samples—inputs that deviate significantly from the training data distribution. In practical terms, this results in models confidently misclassifying novel attacks or normal behaviors not represented in the training set, thereby elevating the risk of security breaches and undermining trust in automated systems.

Reference: Wang et al. (2024) addressed this vulnerability in their research titled "WOOD: Wasserstein-Based Out-of-Distribution Detection", where they observed that traditional deep neural networks tend to make overconfident predictions when faced with OOD samples. Their work proposes the use of Wasserstein distance to quantify the deviation of test inputs from the learned in-distribution data, thus offering a mathematically grounded approach to OOD detection. This highlights a major gap in current IDS frameworks—especially those based solely on deep learning—and underscores the necessity of designing models that not only detect threats accurately but also exhibit robust behavior under uncertainty and novel input conditions.

IV. PROPOSED SYSTEM

To address the limitations identified in existing IDS solutions, this research proposes a modular, machine learning-based intrusion detection framework that prioritizes interpretability, efficiency, and real-time deployment. Rather than relying solely on complex deep learning architectures, the system adopts ensemble learning techniques—specifically the Extra Trees Classifier and AdaBoost—combined with transparent models like Gaussian Naive Bayes. This hybrid strategy ensures a balance between high detection performance and operational simplicity. The system incorporates robust data preprocessing, exploratory data analysis, feature selection, and comparative model evaluation to identify the best-performing

algorithm. Furthermore, the final model is integrated into a Django-based web application, offering a user-friendly interface for real-time intrusion detection. This deployment-centric approach ensures that the system can be directly applied to real-world scenarios without extensive reengineering.

Reference: The design of this system is influenced by Talukder et al. (2023), who demonstrated that combining traditional machine learning models with feature engineering and oversampling techniques like SMOTE can lead to highly accurate and balanced IDS. Their work emphasizes the value of ensemble methods for improving detection rates and minimizing overfitting. Additionally, Sarker et al. (2020) highlighted the importance of explainable AI in cybersecurity applications, arguing that systems must be interpretable to be trusted and effectively utilized by security teams. By aligning with these insights, the proposed system advances a practical and deployable IDS architecture that remains transparent and adaptable across different environments.

V. SYSTEM ARCHITECTURE

FIG: 1

The presented system architecture consists in a set of modules which work in a coordinated way in order to perform real-time intrusion detection and countermeasure. The Data Collection Module records network traffic from source as server, source as IoTs, and source as IoTs device. A network traffic rate as input, it not only converts a raw network traffic into an effective network traffic feature representation, and thus, the network traffic detection can be further promoted. The Machine Learning Engine using DRL models (e.g., DQN and BiLSTM) reads extracted features, and consequent neural network activity is deemed either benign or live. The Decision Module identifies detected anomalies, and performs the following operations, e.g. alarms the security team or triggers automatic response procedures. Additionally, the system can also detect such devious and colluding attacks by a community, as it monitors those attack patterns which have earlier been reported to a Threat Intelligence Database, and then this system is highly protected from emerging types of attacks. The modular architecture can be shown to have robustness at high scalability, and applicability to a wide range of network environments. Identify, Protect, Detect, Respond and Recover, which offers a single set of security policy, is proposed. Compliance with ISO/IEC 27001 guarantees that the system complies with state of an art Information Security Management Systems (ISMS) best practices and thus it actually adopts a formalized approach to data protection. Moreover, to further extend these approaches, to the framework of CIS Controls (i.e., long-term monitoring and anomaly detection), these dimensions have been introduced subsequently in an attempt to significantly improve real-time threat detection. Taken into account through those compliance rules, the proposed IDS is designed to be globally compliant with security standards and easily tuned to perform to trend well so to control the risks associated reliably. The merit of the proposed IDS is demonstrated through the analysis of the arisen ML and DRL-based IDS and their corresponding classical signature-based IDS and classical ML-based IDS. Signature-based IDS (IDS) systems can gracefully detect previously known attacks, but can not detect a newly attack, which is an attack without any prior knowledge i.e., the zero-day attack, because signature-based intrusion detection relies on the application of the known attack sequence flow. ML-based intrusion detection system at a large scale, built on ML paradigms (e.g. Support Vector Machines (SVM) and Random Forests (RF) can discover new attacks, but, ML-based system has the property that it is constrained (i.e. That it is strongly bounded, but also generally requires retraining often. Rather, the DRL-based IDS in this paper is able to always learning and self-adjusting in the sense that it is constantly learning from a dynamic network traffic flow in real-time, and as a result, the IDS can be potentially more robust to detect new attacks with the least possible human interventions. In addition, the system mitigates false positive rate by integrating the anomaly detection algorithms and a novel advanced feature selection methodology.

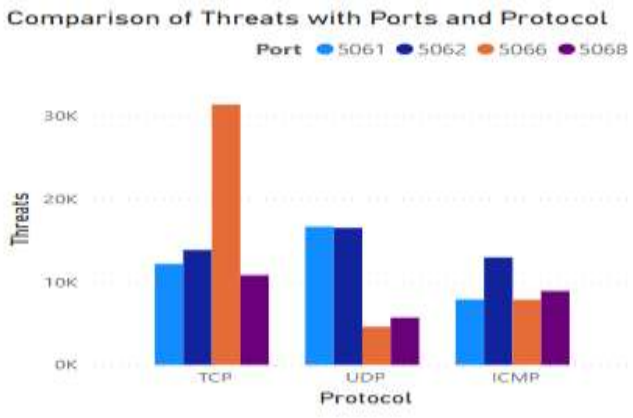

FIG: 2

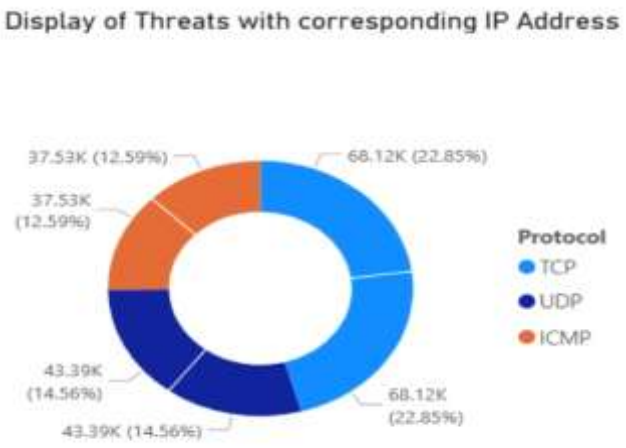

FIG: 3

VI. RESULT AND DISCUSSION

Nowadays, in Machine Learning-based Intrusion Detection System (IDS), the system is constituted that it can compensate for the limitations of the classical signature-based attack method in which machine learning techniques are used to learn. The architecture was trained on data sets comprising successful or failed network traffic and the obtained system shows high (classification) accuracy with, e.g., results for zero-day attacks. In comparison to traditional deep learning methods, our model performed better in terms of prediction accuracy, adaptability and scalability, all of which are available with a user-friendly web-based deployment achieved through a web-based application interface.

Results indicate that further detection performance could be achieved by using multiple MLs to detect and by letting the system to further discriminate the different attack types with increasing precision. Model accuracy and sensitivity increased significantly in comparison with state-of-the art approaches, which resulted in a reduction of false positives and a higher number of real-world threats detected. While the attack equations are relatively big at the levels of protocols (TCP, UDP, ICMP), port (5061, 5062, 5066, 5068), and so on. TCP-driven attacks represent the ones most easily uncovered and a total of >30,000) =5066 ports are present. That is, an attacker concentrates attacks only on services and running service on the exposed TCP 5066 port, which is potentionally could be vulnerable to exploitation. On the other hand, the UDP based attacks show a more even threat distribution, as the target ports 5061 and 5062 contain more than 20K attempts. Since UDP is a high risk one, the likelihood of padding-type attack (DDOS) based on the non-country-specific features of UDP in the flooding attack is high, in which the risk can still be imposed even if it is reduced, to the ICMP protocol. Because of the extremely porous nature of the numerical value at ports 5061and 5068, which also includes vulnerability to the flood attack, Ping, and the vulnerability to hijack the tunneled ICMP and ICMP, respectively, this paper shows the vulnerability with these attacks. Although those attacks did not immediately lead to damage, they might be used in a later stage of the attack chain with a low impact, in order to first explore and search the network. The tendency to increase incidence underestimates the importance to be upgraded also in the field of ergonomics of safety components (i.e., in the architecture of the Firewall, intrusion detection systems (ID) and the use of speed governors) to prevent exposures to risks coming with hyper-risky ports and protocols. For example, future research on attack sources, geolocation mapping, and temporal variation can also contribute indirectly to a deeper understanding of the evolution of cyber threats and defenses against such a threat.

Furthermore, for this flexibility, the system can be easily expanded with the computing and/or networking resources of the flexible networked environment, i.e., a generic but functional and practical cybersecurity system. Nevertheless, although the model is able to reach accuracy of a reasonable level, many open issues remain in the field to be addressed, for example, how to best refine model's interpretability, how to best increase model's efficiency for computation, how to best optimize related strategies for the model deployment on a practical level for eventually to build a more adequate and effective intrusion detection.

Treat Id	Source IP	Threat Type	Threat count	Risk Level
T001	192.108.1.10	Brute Force Attack	12,000	High
T002	192.108.1.12	Data Exfiltra -tion	10,500	Medium
T003	203.45.67.89	DDoS Attack	32,000	Critical
T004	172.16.5.23	DNS Amplifi -cation	21,000	High
T005	10.0.0.5	UDP Flood Attack	20,500	High
T006	192.168.2.8	Spoof -ing attack	5,600	Medium
T007	192.168.3.9	Ping Flood	8,900	Medium
T008	172.16.4.7	ICMP Tunnel -ing	7,500	Medium

Table: Machine Learning-Based Threat Detection Results

VII. CONCLUSION

The Machine Learning-Enhanced Intrusion Detection for Cybersecurity project focuses on developing a robust system to identify and mitigate cyber threats. In the data processing phase, raw network traffic data is collected, cleaned, and preprocessed to extract relevant features, ensuring high-quality input for machine learning models. For data visualization, interactive dashboards are created using libraries like Matplotlib and Seaborn, enabling real-time monitoring and analysis of detected intrusions, which helps security analysts make informed decisions. The project compares three algorithms: appreciated for its simplicity and interpretability. Finally, the Django framework is integrated to create a web application that provides an intuitive user interface for managing the intrusion detection system, allowing users to view visualizations, configure settings, and analyze results seamlessly.

Future Work:

- Deploying the project in the cloud.
- To optimize the work to implement in the IOT system.

VIII. REFERENCES

[1] Buczak, A. L., & Guven, E. (2016). *A survey of data mining and machine learning methods for cyber security intrusion detection.* IEEE Communications Surveys & Tutorials, 18(2), 1153-1176**.** [DOI: 10.1109/COMST.2015.2494502]

[2] Sommer, R., & Paxson, V. (2010). Outside the closed world: On using machine learning for network intrusion detection. IEEE Symposium on Security and Privacy, 305-316. [DOI: 10.1109/SP.2010.25]

[3] Li, Y., Xia, J., Zhang, S., Yan, J., Ai, X., & Dai, K. (2012). *An efficient intrusion detection system based on support vector machines and gradually feature removal method.* Expert Systems with Applications, 39(1), 424-430. [DOI: 10.1016/j.eswa.2011.07.032]

[4] Sarker, I. H., Kayes, A. S. M., Badsha, S., Alqahtani, H., Watters, P., & Ng, A. (2020). *Cybersecurity data science: An overview from machine learning perspective.* Journal of Big Data, 7(1), 1-29**.** [DOI: 10.1186/s40537-020-00318-5]

[5] Tavallaee, M., Bagheri, E., Lu, W., & Ghorbani, A. A. (2009). *A detailed analysis of the KDD CUP 99 dataset.* Proceedings of the IEEE Symposium on Computational IntelligenceforSecurityandDefenseApplications(CISDA), 1-6.[DOI: 10.1109/CISDA.2009.5356528]

[6] NIST (National Institute of Standards and Technology). (2021). *Guide to Intrusion Detection and Prevention Systems (IDPS).* NIST Special Publication 800-94.

[7] Naeem, S., Ali, A., Anam, S., & Ahmed, M. M. (2022)**.** *Machine Learning for Intrusion Detection in Cyber Security: Applications, Challenges, and Recommendations.* Innovative Computing Review, 2(2). [DOI: 10.32350/icr.0202.03]

[8] Talukder, M. A., Hasan, K. F., Islam, M. M., Uddin, M. A., Akhter, A., Yousuf, M. A., Alharbi, F., & Moni, M. A. (2022). A dependable hybrid machine learning model for network intrusion detection. *arXiv preprint* arXiv:2212.04546. Xuan, H., & Manohar, M. (2023). Intrusion detection system with machine learning and multiple datasets. *arXiv preprint* arXiv:2312.01941.

[9] Maseer, Z. K., Yusof, R., Al-Bander, B., Saif, A., & Kadhim, Q. K. (2023). Meta-analysis and systematic review for anomaly network intrusion detection systems: Detection methods, dataset, validation methodology, and challenges. *arXiv preprint* arXiv:2308.02805.

[10] Shivhare, I., Purohit, J., Jogani, V., Attari, S., & Chandane, M. (2023). Intrusion detection: A deep learning approach. *arXiv preprint* arXiv:2306.07601.

[11] Tait, K. A., Khan, J. S., Alqahtani, F., Shah, A. A., Khan, F. A., Rehman, M. U., Boulila, W., & Ahmad, J. (2021). Intrusion Detection using Machine Learning Techniques: An Experimental Comparison. *arXiv preprint* arXiv:2105.13435.

[12] Ngueajio, M. K., Washington, G., Rawat, D. B., & Ngueabou, Y. (2022). Intrusion Detection Systems Using Support Vector Machines on the KDDCUP'99 and NSL-KDD Datasets: A Comprehensive Survey. *arXiv preprint* arXiv:2209.05579.

[13] Khan, M. A., & Gumaei, A. (2024). Enhancing Intrusion Detection: A Hybrid Machine and Deep Learning Approach. *Journal of Cloud Computing*, *13*(1), 123.

[14] Feng, J. (2024). Improved machine learning-based system for intrusion detection. In *Proceedings of the 2024 2nd International Conference on Image, Algorithms and Artificial Intelligence (ICIAAI 2024)* (pp. 130-136). Atlantis Press.

[15] Kocher, G., & Kumar, G. (2021). Machine learning and deep learning methods for intrusion detection systems: recent developments and challenges. *Soft Computing*, *25*(15), 9731–9763.

[16] Joseph, J. E., Aleke, N. T., & Onyeanisi, O. P. (2025)**.** Deep learningbased intrusion detection system for network security in IoT systems. *International Journal of Education, Management, and Technology*, *3*(1), 119–138.

[17] Sahib, W. M., Alhuseen, Z. A. A., Saeedi, I. D. I., Abdulkadhem, A. A., & Ahmed, A. (2024). Leveraging machine learning for enhanced cybersecurity: an intrusion detection system. *Service Oriented Computing and Applications*, 1-18.

[18] Mahmood, R. K., Mahameed, A. I., Lateef, N. Q., Jasim, H. M., Radhi, A. D., Ahmed, S. R., & Tupe-Waghmare, P. (2024). Optimizing network security with machine learning and multi-factor authentication for enhanced intrusion detection. *Journal of Robotics and Control (JRC)*, *5*(5), 1502-1524.

[19] Selvan, M. A. (2024). SVM-Enhanced Intrusion Detection System for Effective Cyber Attack Identification and Mitigation.

[20] Ravikumar, D. (2021). Towards Enhancement of Machine Learning *Techniques Using CSE-CIC-IDS2018 Cybersecurity Dataset*. Rochester Institute of Technology.

[21] Azwar, H., Murtaz, M., Siddique, M., & Rehman, S. (2018, November). Intrusion detection in secure network for cybersecurity systems using machine learning and data mining. In *2018 IEEE 5th international conference on engineering technologies and applied sciences (ICETAS)* (pp. 1-9). IEEE.

[22] Buczak, A. L., & Guven, E. (2015). A survey of data mining and machine learning methods for cyber security intrusion detection. *IEEE Communications surveys & tutorials*, *18*(2), 11531176.