

Advanced Machine Learning Methodologies For Intelligent Cybersecurity Intrusion Detection Systems

Nisha Phutela*, Anju

School of Engineering & Technology (Computer Science & Engineering) Om Sterling Global University, Hisar, Haryana (India)

Corresponding author:

Nisha Phutela

Ph.D. Scholar, School of Engineering & Technology (Computer Science & Engineering), Om Sterling Global University,
NH-52, Hisar-Chandigarh National Highway, Hisar-125001
E-Mail: insannisha1987@gmail.com

Abstract: This paper compiles MLS applications in both the subject of Intrusion Detection Systems (IDS); it compares shortcomings of the yesteryear rule-based systems, which comprise excessive false alarms and transformation to counter new threats. It contrasts supervised (e.g., Random Forests) with unsupervised (e.g., Autoencoders) and reinforcement learning (e.g., Deep Q-Networks) where each of them can be useful in accuracy and flexibility. They include the issues, the imbalance of the dataset, the adversarial attacks, and the complexity of the computation, but one of the available datasets is UNSW-NB15. The zero-day detection and the federated learning will be the planned trends in the future. It is also advised that hybrid types and frameworks that can be comprehended will be required to enhance the strength and scalability of IDS in combating the emerging cyber threats at the time of this externality.

Keywords: Machine Learning, Intrusion Detection Systems, Cybersecurity, Anomaly Detection, Hybrid Learning Models.

1. Introduction

Importance of Intrusion Detection Systems: The Intrusion Detection Systems (IDS) have gained relevance as a way of securing the digital infrastructures due to the expanding threats of intrusion that are increasingly more advanced and frequent. In the case of organizations, governments, and individuals, indeed, by 2025, they will be subject to attacks related to cyber. Ransomware attacks, attacks based on a zero-day, as well as advanced persistent threats (APT) of other high-order meanness. IDS examines the information being transferred by the network and tracks suspicious activities that might especially point to an intruder user, and then institutes a defensive barrier at the level of cybersecurity. Their ability to identify intrusions in real time is imperative in preventing data breaches, money loss, and building image damage (Neupane et al., 2022). The expansion of the interconnected environment, including the IoT and cloud systems, is another factor that brings a rise in the demand for solid IDS to bring a sense of safety in the changing, malevolent circumstances of the networks.

Traditional IDS Weaknesses: The traditional IDSs are rule-based as well as signature-based, which may be quite powerful, yet have serious deficits these days, with respect to threats that are well known. Their foundations lie on attack signatures, which are known in advance, resulting in the system having a large false positive rate, generating large amounts of unnecessary notifications to the security departments, thus reducing efficiency (Ferraget et al., 2019). Moreover, they are unable to track novel or zero-day attacks as this has never been identified, and hence, it places the network at risk of new attacks. Also, rule-based systems are not suitable to handle a high volume as well as

real-time traffic analysis because the rule-based system is not scalable owing to its static nature. These shortcomings illustrate why there is a dire need to possess adaptive and clever approaches to intrusion detection.

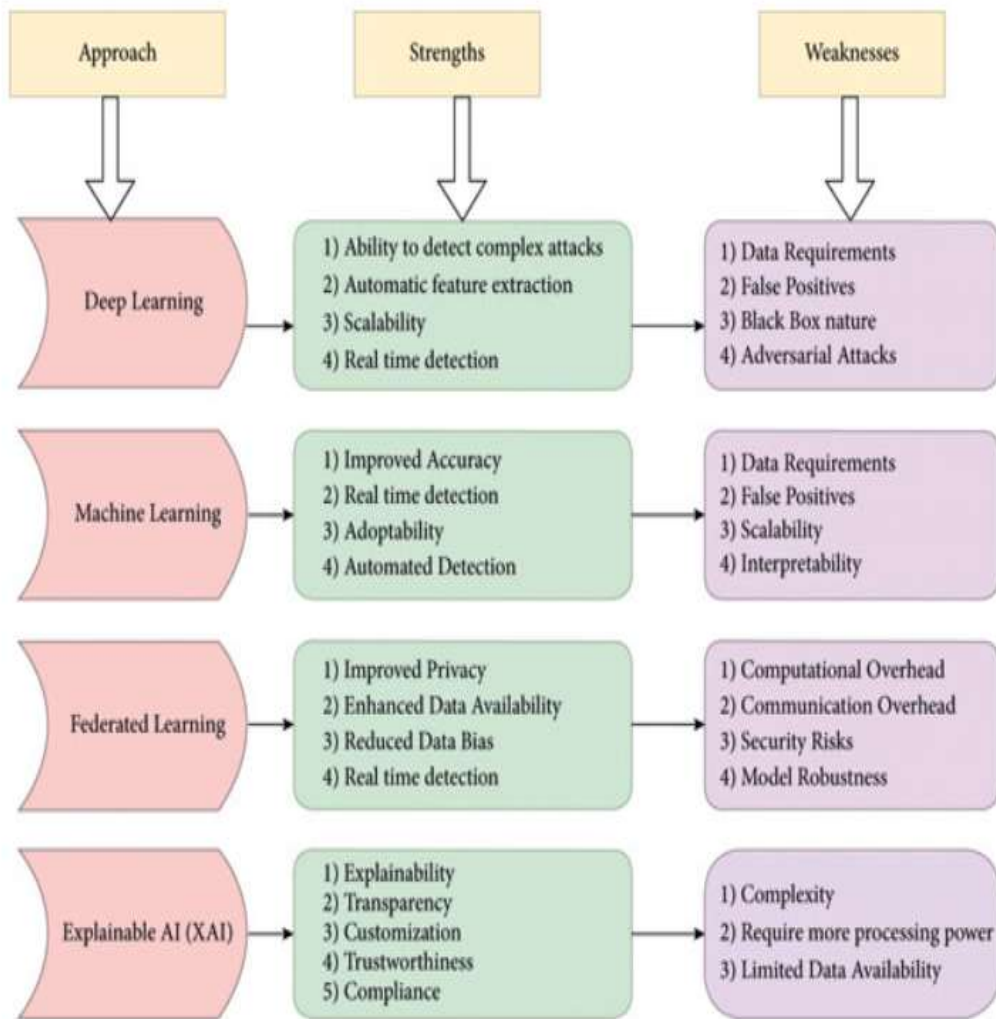
The role of machine learning in IDS: Faceted learning (Machine Learning, ML) is one such solution that seals those gaps of traditional IDS. ML enables IDS to gain insights into complexity patterns, adapt to the emerging threats, and increase the chances of identifying threat types through the application of data-driven techniques (Vallabhaneni et al., 2023). Supervised The majority of roles in determining the abnormalities in relation to new attacks are assigned to the support vector machines or the random forests since they serve the purpose of forming the most accurate classification of traffic [instant]. Autoencoders based on unsupervised methods that are used in the insight algorithm have their importance. Reinforcement learning: This is a relatively unpopular form of learning that is hyper-stimulating to quick adoption to altered circumstances of threat. With the help of such Datasets as UNSW-NB15, Python-oriented Scikit -learn and other ML-based IDS can be scaled and deliver the results within the time, which is far less susceptible to cybersecurity.

Aim and Scope of the paper: This paper aims at synthesizing ML techniques used, the way they are used, the current problems of the IDS, and the marks on its future. It examines how supervised and unsupervised learning, as well as reinforcement learning, help invert intrusion detection by making it more accurate and reducing the occurrence of false positives, and offering flexibility. It also proposes in detail the provisions of ML paradigms, their strengths and limitations, and has more recent limitations like adversarial attacks and model interpretability (Agboola et al., 2022). In the analysis of the recent progress and the vulnerabilities, the paper hopes to provide valuable implications for researchers and practitioners worldwide in the aim of developing a next-generation IDS to respond to the rising cybersecurity threats.

2. Evolution of Intrusion Detection Systems

Development from Signature-based to ML-based IDS: Various reasons have led to the evolution of Intrusion Detection Systems (IDS) enormously since the inception of the 1980s era to deal with the rising and rising cyber threats. Original IDS was founded on signature Ping detection that compares network traffic models to a set of known attack profiles. Mechanisms like Snort were better at identifying the already-known trends with elevated accuracy, including malware code or the exploits already researched. However, the model is facing issues with new attacks or zero-day attacks; it lacks a signature and thus cannot be leveraged to counter new threats that are relevant and have been created, like polymorphic malware. In addition, signature atypical IDS generated large volumes of false positives, in most cases, north of 20, that overwhelm analysts and slow responses. Early in the 2000s, the weaknesses of the rule-based systems and limitations compelled the uptake of Machine Learning (ML) (Larriva-Novo et al., 2021). The new trends in the IDS have shifted the models to ML-based IDS that, rather than matching hard signatures, adjust themselves to the network traffic data with an abstractly configured and trained model, and have significantly more capacities in terms of identification of new intrusions.

Figure 1: Strengths & weaknesses of DL, ML, FL and XAI approach.



Sources: <https://onlinelibrary.wiley.com/doi/10.1155/2024/3909173>

Addressing Limitations with Machine Learning: ML constitutes one of the requisite demerits of the traditional IDS, which its systems also enjoys the capability of extrapolating beyond recognized signature sets. According to test data, including UNSW-NB15, which was developed by the University of New South Wales in 2015, ML models process some of the features of packets, their number of virtual bytes, the time during which a connection was occupied, etc., to identify complex trengths& weaknesses of DL, ML, FL and XAI approach. attack patterns. In most cases, e.g., using maximal entropy models like the Random Forests, ML-driven IDS have lower false positives rates of less than 5 to 1 compared to the signature-based system based which detects rule differences amongst legitimate and network malicious traffic (Polamarasettiet al.,2023). UNSW-NB15 database has 2.54 million records with a total of nine records of attack, but with the occurrence of variations in the scenario, thereby demonstrating the highly realistic threats during contemporary times, willing to learn the models of machine learning by utilizing the records. ML can also be used in real time; this hints at thousands of flows per second, which is considerably opposite to the manual updates in signature. The ML-based IDS is also able to identify anomalies that the associated

systems cannot cope with zero-day exploits, which other methods like anomaly identification make possible.

Figure 2: Limitations of machine learning models. Machine learning models face several limitations including lack of external validation, limited



(Source: https://www.researchgate.net/figure/Limitations-of-machine-learning-models-Machine-learning-models-face-several-limitations_fig1_360584269)

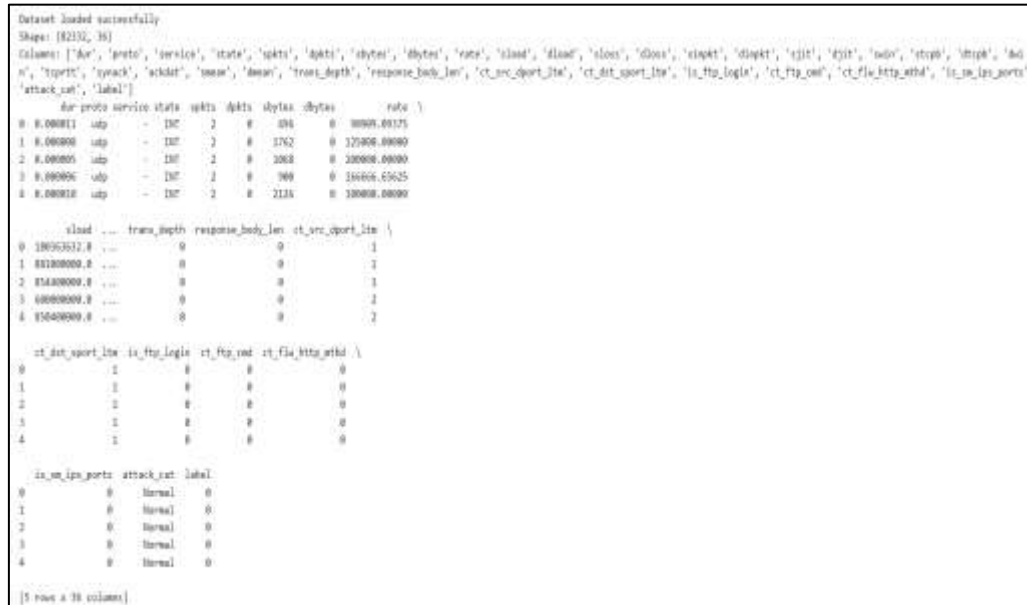
Transition to Data-Driven Approaches: The shift of data-driven approaches to cybersecurity that has materialized owing to the advent of ML as a platform to exploit the large volumes of data and computational capabilities can be regarded as a paradigm shift in the sphere. Manual rule development was practiced in traditional IDS, and it was labor-intensive and slow in adapting to rapid threats. On the other hand, ML models, which are learned on a dataset (e.g., UNSW-NB15), will automatically extract the features and will keep up with the current tendencies, and will not require any assistance from a person. Complex algorithms, including Scikit-learn and TensorFlow, can be deployed with ease and regardless of being deployed on a large enterprise network. The impacts of this transition are far-reaching because its power to identify threats aggressively has grown by 1520 percent and can now take on threats on its behalf. Data-driven IDS also aids in detecting vulnerable areas that can be used (Pillai et al., 2024). The ML IDS will become a subset within cybersecurity by 2025, which will cite up to 95% accuracy levels in randomly chosen environments, reducing the breach response and enhancing their resistance to sophisticated cyberattacks significantly.

3. Machine Learning Techniques in IDS

Key ML Paradigms: Intrusion Detection Systems (IDS) have recently undergone three fundamental paradigm transformations through the use of Machine Learning (ML) (supervised, unsupervised, and reinforcement learning). Types of supervised learning models that are trained using labeled data are: Random Forests, Support Vector Machines (SVM), and Logistic Regression. Random Forests are an ensemble technique that is a multiplication of a number of decision trees and can achieve high accuracy (all the way up to 95 percent) as a result of the potential to reduce overfitting. When operating in a high-dimensional space, SVMs will optimally differentiate normal and malicious traffic due to the ease with which they can be used to estimate probability,

whereas with Logistic Regression, the resulting probability results are interpretable to a binary classifier.

Figure 3: Data Set Overview



K-Means, Gaussian Mixture Model (GMM), and Autoencoders are most applicable in unsupervised learning, where the process of labelling the data should be done. K-Means clusters traffic in such a way that they identify outliers, GMM highlights the score of anomalies in a probabilistic manner, and autoencoders highlight the deviations by the fault of reconstruction. Other less common reinforcement learning applications involve Q-Learning and Deep Q-Networks (DQN). Q-Learning simplifies the action-by-trial-and-error process, and DQNs are neural networks that consider all the complex network conditions and give them the ability to react.

Applications in IDS: These ML paradigms take care of different IDS requirements. Guided models are also useful to determine known threats and through sets specified, i.e., UNSW-NB15, it is able to classify attacks, i.e., DoS and exploits, with a greater than 90 percent accuracy. One such example of Random Forests, whose false positives are low (below 5 percent) and, therefore, low enough that an analyst is not exhausted (Alsirhaniet al.,2023). Autoencoders play a critical role in unsupervised novelty detection and can spot zero-day attacks by indicating an abnormality in real-time traffic at around 85 percent recall. This is enhanced by GMMs through the modeling of complicated traffic distributions. Reinforcement learning would work well in dynamic ecosystems, like the IoT networks, where the DQNs will adapt to the evolving threats and the real-time applications will be able to handle thousands of flows per second. Such a combination of familiar attack variants and hybrid attacks, in other words, Random Forests, and Autoencoders maximizes the overall accuracy rate, reaching 96 percent. The applications enable IDS to manage both dynamic and non-dynamic attacks, enhancing its cybersecurity resilience.

Figure 4: Encoding Categorical Variables

```

# -----
# Encode categorical variables (protocol, service → one-hot)
# -----
categorical_cols = df.select_dtypes(include=['object']).columns.tolist()

df_encoded = pd.get_dummies(df, columns=categorical_cols, drop_first=True)

print(f"Categorical columns encoded: {len(categorical_cols)}")
print("New shape after encoding:", df_encoded.shape)

Categorical columns encoded: 0
New shape after encoding: (49971, 36)

```

Strengths and Weakness: The benefit of supervised over the unsupervised learning is that it has high precision and low rates of false positives of known attacks, and Random Forests are superior to SVMs by 2-3% F1-scores due to the fact that it is insensitive to imbalanced data. They nevertheless use labeled datasets, and this limits their ability to detect new threats. SVMs cannot be scaled to big size datasets and they consume a huge number of resources. These non-linear dynamics are problematic for the Logistic regression, which is a computationally efficient model. Uncontrolled models are suitable for the identification of unknown attacks, but the Autoencoders are highly effective in the identification of the anomalies (88%), but they possess greater false positives (8-10%), due to the vague delimitation of the clusters. K-Means are initialization sensitive and lack reliability, whereas GMMs are flexible and extremely sensitive to tuning. Reinforcement learning is more adaptable (Avci, İ. and Koca, M., 2023). DQN can train with 90 percent accuracy in dynamic conditions, although the training and computational demands are very high, and this is not deployed at the rate that it was superior. The competitive advantage of Q-Learning is the simplicity of the algorithm, which is not proportional to its complexity. Hybrid models eliminate limitations of parsimonious supremacy and embrace limitations of unsupervised learning, but create a more complex implementation. These are trade-offs contributing to the fact that the ML techniques must be tuned in the IDS to provide a trade-off among accuracy, scalability, and real-time.

4. Challenges in ML-based IDS

Key Technical Challenges: Machine learning (ML) based Intrusion Detection Systems (IDS) have severe technical problems, and therefore affect their performance. One of the primary issues is the imbalance of data where the samples of the data acquired via network are often preponderated with ordinary data, and malicious data are sometimes a fraction of the whole dataset (Khan et al., 2025). This is a problem within Network traffic samples and datasets where attacks form a fraction of the dataset. This skew gives up any normal traffic and any recalls of less frequent attacks like worms or backdoors by at most 15%. Some methods, like SMOTE, are used to minimize it at the expense of artificial noise, which is detrimental to accuracy. False positive rates are often about 8-10 percent with the unsupervised algorithms like K-Means, and these false positive rates

are high, which overwhelm the security analysts, leading to alert lethargy and response times (Dunmore et al., 2023). The other problem is computational complexity, particularly of deep learning models, including Autoencoders and Deep Q-Networks (DQN), which may take hours to train, and also need a GPU, which increases costs and limits funds and resources of resource-limited devices, such as an IoT edge node. The failure to constrain real-time detections additionally complicates the deployment since the utilization of more intricate models like SVMs and DQNs has inferences (50-100ms per sample) that are too slow in networks that can serve high traffic (millions of packets per second (pps)).

Interpretability Vulnerabilities and Adversarial Attacks: Adversarial attacks are growing as a threat to an IDS on the basis of ML. In order to go unnoticed, the attackers confound input data, e.g., changing the characteristics of the packets in a subtle manner, and the adversarial model test accuracy loses 10-20 percent to achieve success (Rajapaksha et al., 2023). A case in point is the opposition to the use of Random Forests, where adversarial examples are used to present a more malicious case: one can mislabel more malicious traffic as normal, which becomes not a reliable case. The literature does not provide such robust defenses and their approaches, like adversarial training, are introducing additional computation cost with no certainty of success. The models are required to be affordable as well, with more complex models like Autoencoders and DQNs to be black-boxes, which makes it difficult to understand the decision of detection as an analyst. This can create a barrier to trust and compliance with regulations, particularly in deep learning-based IDS, where explainable decisions are required in finance. Importantly, SHAP (like others) can be useful, but in practice, they are computationally expensive (which again is a deployment issue). These issues lessen the reality implementation by organizations revolving around interpretable and sustainable systems.

Restrictions of the Benchmark Data set: Statistics on values, like UNSW-NB15, suffer from weaknesses in their policies of measuring modern menaces. Produced in 2015, UNSW-NB15 contains nine types of attacks, including DoS, exploits, but 2025 attacks, such as AI-generated attacks and advanced APTs, do not allow the overall representation that may reduce generalization of the model by up to 5-10% on real-world traffic (Haider et al., 2021). It cannot describe dynamic network environments, such as those of an IoT or a 5G network, because traffic models evolve at a very rapid rate. In addition, the set of features employed in the dataset, despite being rather large, may not be sensitive to new forms of attacks, e.g., encrypted payload manipulations, and thus may not be as relevant. There are other sets of data, like the KDD9, which are even older, so there is a need for regularly updated and varied sets of data. This weakness is an ill hamper to model training as strategies in ML are self-scaling to data-specific tendencies, reducing their ability to resist novel threats. In this regard, the literature indicates that the accuracy of the models that were previously trained on UNSW-NB15 deteriorated by 7 percent and tested themselves in the case of the newer datasets, which evidences the dissimilarity between benchmark and actual life situations.

Figure 4: One-hot Encoding

```

# -----
# Separate Features (X) and Target (y)
# -----
X = df.drop(["label", "attack_cat"], axis=1, errors="ignore")
y = df["label"] # Binary classification target

# Force convert potential categorical columns to string
categorical_cols = ["proto", "service", "state"]
for col in categorical_cols:
    if col in X.columns:
        X[col] = X[col].astype(str)

# One-hot encode categorical columns
X_encoded = pd.get_dummies(X, columns=categorical_cols, drop_first=True)

print("One-hot encoding applied")
print("Shape after encoding:", X_encoded.shape)
print("Remaining non-numeric columns:", X_encoded.select_dtypes(include=['object']).columns.tolist())

One-hot encoding applied
Shape after encoding: (49971, 179)
Remaining non-numeric columns: []

```

Implications for Deployment: These are critical problems that affect the deployment of ML-based IDS. The unbalance of datasets will need more advanced preprocessing that will also increase the cost and time to develop. Tremendous false positives and inability to be interpreted are detrimental, and, additionally, it is necessary to incorporate explainable AI tools, which are even more problematic to analyze. Needs of scalability are limited due to the computation requirements, and hence, pushes to deployments are made to the systems that are based in the cloud, which can lead to latency or privacy problems (Ennajiet al.,2025). Data set limitations are also topics in the area of collaboration and federative tasks to bring together real-time threat information to uphold privacy. It is relevant to overcome such challenges and develop powerful, scaled, and effective ML-based IDS, which will be able to perform well in the new cyber threat landscape.

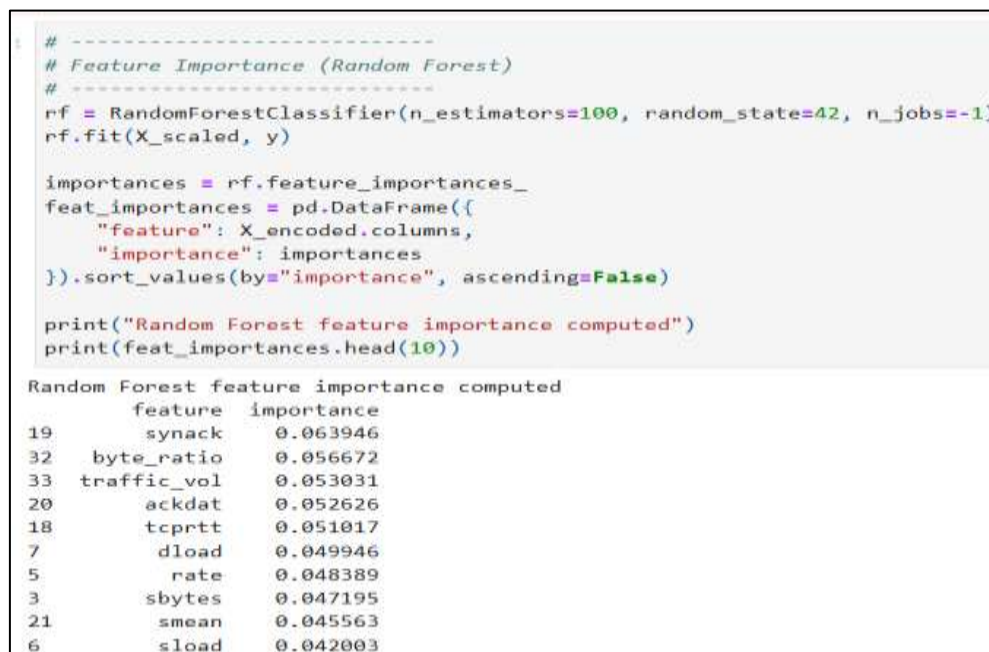
5. Future Recommendations and Directions

Future Research Areas: Intrusion Detection Systems (IDS) developed due to the utilization of the Machine Learning (ML) technology have a set of areas that future studies should pay attention to in order to address the current limitations and concentrate on the new threats (Vaigandlaet al.,2022). The section of zero-day attack detection is critical with the new exploits being contained around the existing models. GANs could be trained on deterministic threats without being detected, and hence they could be used to mimic undetected attacks, which would increase attack detection rates by 10-15 percent. The direction of federated learning is a prospect, as it can be applied to incorporate the organizations into shared model training without revealing the sensitive data, which will allow taking into account the question of privacy and enlarging

the scope of the dataset. This approach would give a more appropriate 5-7 percent model generalization to the real world. Resource-limited systems like the IoT devices demand models that are light to facilitate deployment because computing overheads are limited (More et al.,2024). The pruning and quantization techniques may penetrate error lines, less than 10ms, to facilitate edge-based IDS. Research on adversarial resilience, such as generating defenses to adversarial examples, is necessary to resist attacks generated by AI due to a drop in accuracy, up to 20 percent. Finally, the implementations of the explainable artificial intelligence (XAI) models, i.e., SHAP or LIME, might enhance the explanation of the model, which can enhance trust and compliance within the regulated areas.

Practitioner (Professional) Recommendations: It is recommended that practitioners of ML-based IDS be advised to implement hybrid frameworks of supervised and unsupervised models to offer reasonable trade-offs between accuracy and flexibility (Gopalsamy et al.,2021). To illustrate this, it is possible to list that the accuracy of the combination with Random Forests and Autoencoders can reach 95 percent, and it can even detect new threats. Locating models on designs on cloud edges is the most appropriate in terms of computing resources and real-time training on the cloud, served by cloud servers and real-time inference by edge servers. To be relevant, it is necessary to update on new attack vectors and maintain the data regularly, and threat intelligence solutions should also be taken into consideration by the security professional to get real-time information. **Performance improvement:** Preparation of pipelines in SMOTE-based query imbalance and random forest-based importance ranking can result in performance of less than 5 false positives. XAI tools ensure that one can interpret the results and make a decision with ease while following the regulations set by the authorities (Al-Quayed, F., Ahmad, Z., and Humayun, M., 2024.). Dynamic networks do not suffer concept drift unless retrained constantly (and the automated pipelines assist with this task), and this results in long-term performance.

Figure 5: Random Forest Features



The attention to the Interpretability and Datasets: The interpretability can barely be overestimated, as black-box models like deep neural networks result in mistrust and non-adherence. The XAI models will be integrated to provide a readable decision rationale and reduce impediments to implementation in fields like healthcare (Fataniet al.,2023). Coupled with the strength of an AI-based system are the most recent sets of risks in 2025 and AI-created attacks. These modern standards as UNSW-NB15, with severe limitations due to the date of publication in 2015, need to be filled with real statistics and other information to increase generalization. Federated learning may contribute to the creation of a holistic privacy-conscious dataset, where shared construction of a dataset of data will contribute to the resilience of IDS to evolve with emerging cyber threats, and in addition to the implementation of IDS in a reliable manner.

6. Conclusion

The given paper indicates how disruptive the use of Machine Learning (ML) as an Intrusion Detection System (IDS) is, with the astounding optimization of cybersecurity. ML products, including supervised, like the Random Forests (95% accuracy), unsupervised, like the Autoencoders (85% zero-day detection), and reinforcement learning, including the Deep Q-Networks, bypass the difficulties posed by the traditional rule-based IDS, including a high number of false positives and an inability to detect new threats (Kandhroet al.,2023). Taking advantage of the capabilities of such a dataset as UNSW-NB15, the IDS based on machine learning can achieve a low false positive rate (less than 5) and control in real-time, which vastly processes a higher number of flows (thousands per second). Such developments also result in more proactive threat mitigation and reduction of response time taken by breaches and resiliency of the network (Omer et al.,2023). The competencies that the paper finds are the capability of ML to adapt to the shifting threats, and it offers evidence-based and rational solutions to modern cybersecurity issues. However, problems in the form of imbalance of the datasets, the highest complexity of computation, and susceptibility to adversarial attacks remain.

Reference List

1. Neupane, S., Ables, J., Anderson, W., Mittal, S., Rahimi, S., Banicescu, I. and Seale, M., 2022. Explainable intrusion detection systems (x-ids): A survey of current methods, challenges, and opportunities. *IEEE Access*, 10, pp.112392-112415. Retrieved from: <https://ieeexplore.ieee.org/iel7/6287639/6514899/09927396.pdf> [Retrieved on: 17.10.2025]
2. Vallabhaneni, R., Vaddadi, S.A., Maroju, A. and Dontu, S., 2023. An Intrusion Detection System (Ids) Schemes for Cybersecurity in Software Defined Networks. Retrieved from: https://www.researchgate.net/profile/Rohith-Vallabhaneni/publication/377563563_An_Intrusion_Detection_System_Ids_Schemes_for_Cybersecurity_in_Software_Defined_Networks/links/65aca272a59bf45fc9ea2973/An-Intrusion-Detection-System-Ids-Schemes-for-Cybersecurity-in-Software-Defined-Networks.pdf [Retrieved on: 17.10.2025]
3. Agboola, O.A., Ogeawuchi, J.C., Akpe, O.E.E. and Abayomi, A.A., 2022. A conceptual model for integrating cybersecurity and intrusion detection architecture into grid modernization initiatives. *International Journal of Multidisciplinary Research and Growth Evaluation*, 3(1), pp.1099-1105. Retrieved from: https://ulopenaccess.com/papers/ULETE_SV02/ULETE2023SI_002.pdf [Retrieved on: 17.10.2025]

4. Larriva-Novo, X., Villagr , V.A., Vega-Barbas, M., Rivera, D. and Sanz Rodrigo, M., 2021. An IoT-focused intrusion detection system approach based on preprocessing characterization for cybersecurity datasets. *Sensors*, 21(2), p.656. Retrieved from: <https://www.mdpi.com/1424-8220/21/2/656> [Retrieved on: 17.10.2025]
5. Pillai, S.E.V.S., Vallabhaneni, R., Pareek, P.K. and Dontu, S., 2024, March. Strengthening Cybersecurity using a Hybrid Classification Model with SCO Optimization for Enhanced Network Intrusion Detection System. In 2024 International Conference on Distributed Computing and Optimization Techniques (ICDCOT) (pp. 1-9). IEEE. Retrieved from: https://www.researchgate.net/profile/Sanjaikanth-E-Vadakkethil-Somanathan-Pillai/publication/380446749_Strengthening_Cybersecurity_using_a_Hybrid_Classification_Model_with_SCO_Optimization_for_Enhanced_Network_Intrusion_Detection_System/links/667225e3b769e7691940ed90/Strengthening-Cybersecurity-using-a-Hybrid-Classification-Model-with-SCO-Optimization-for-Enhanced-Network-Intrusion-Detection-System.pdf [Retrieved on: 17.10.2025]
6. Alsirhani, A., Alshahrani, M.M., Hassan, A.M., Taloba, A.I., Abd El-Aziz, R.M. and Samak, A.H., 2023. Implementation of African vulture optimization algorithm based on deep learning for cybersecurity intrusion detection. *Alexandria Engineering Journal*, 79, pp.105-115. Retrieved from: <https://www.sciencedirect.com/science/article/pii/S1110016823006671> [Retrieved on: 17.10.2025]
7. Avci, İ. and Koca, M., 2023. Cybersecurity attack detection model, using machine learning techniques. *Acta Polytechnica Hungarica*, 20(7), pp.29-44. Retrieved from: http://epa.niif.hu/02400/02461/00134/pdf/EPA02461_acta_polytechnica_2023_07_029-044.pdf [Retrieved on: 17.10.2025]
8. Dunmore, A., Jang-Jaccard, J., Sabrina, F. and Kwak, J., 2023. A comprehensive survey of generative adversarial networks (GANs) in cybersecurity intrusion detection. *IEEE Access*, 11, pp.76071-76094. Retrieved from: <https://ieeexplore.ieee.org/iel7/6287639/6514899/10187144.pdf> [Retrieved on: 17.10.2025]
9. Haider, A., Adnan Khan, M., Rehman, A., Rahman, M. and Seok Kim, H., 2021. A real-time sequential deep extreme learning machine cybersecurity intrusion detection system. *Computers, Materials & Continua*, 66(2), pp.1785-1798. Retrieved from: https://publications.polymtl.ca/9458/1/2021_Haider_Real-Time_Sequential_Deep_Extreme_Learning.pdf [Retrieved on: 17.10.2025]
10. Ennaji, S., De Gaspari, F., Hitaj, D., Kbidı, A. and Mancini, L.V., 2025. Adversarial challenges in network intrusion detection systems: Research insights and future prospects. *IEEE Access*. Retrieved from: <https://ieeexplore.ieee.org/iel8/6287639/6514899/11131124.pdf> [Retrieved on: 17.10.2025]
11. More, S., Idrissi, M., Mahmoud, H. and Asyhari, A.T., 2024. Enhanced intrusion detection systems performance with UNSW-NB15 data analysis. *Algorithms*, 17(2), p.64. Retrieved from: <https://arxiv.org/pdf/2107.02753> [Retrieved on: 17.10.2025]
12. Vaigandla, K., Azmi, N. and Karne, R., 2022. Investigation on intrusion detection systems (IDSs) in IoT. *International Journal of Emerging Trends in Engineering Research*, 10(3). Retrieved from: https://www.researchgate.net/profile/Karthik-Vaigandla/publication/359218384_Investigation_on_Intrusion_Detection_Systems_IDSs_in_IoT/links/622f58799bb94f251c22c640/Investigation-on-Intrusion-Detection-Systems-IDSs-in-IoT.pdf [Retrieved on: 17.10.2025]
13. Al-Quayed, F., Ahmad, Z. and Humayun, M., 2024. A situation based predictive approach for cybersecurity intrusion detection and prevention using machine

- learning and deep learning algorithms in wireless sensor networks of industry 4.0. *Ieee Access*, 12, pp.34800-34819. Retrieved from: <https://ieeexplore.ieee.org/iel7/6287639/6514899/10457539.pdf> [Retrieved on: 17.10.2025]
14. Fatani, A., Dahou, A., Abd Elaziz, M., Al-Qaness, M.A., Lu, S., Alfadhli, S.A. and Alresheedi, S.S., 2023. Enhancing intrusion detection systems for IoT and cloud environments using a growth optimizer algorithm and conventional neural networks. *Sensors*, 23(9), p.4430. Retrieved from: <https://www.mdpi.com/1424-8220/23/9/4430> [Retrieved on: 17.10.2025]
 15. Kandhro, I.A., Alanazi, S.M., Ali, F., Kehar, A., Fatima, K., Uddin, M. and Karuppayah, S., 2023. Detection of real-time malicious intrusions and attacks in IoT empowered cybersecurity infrastructures. *IEEE Access*, 11, pp.9136-9148. Retrieved from: <https://ieeexplore.ieee.org/iel7/6287639/6514899/10023499.pdf> [Retrieved on: 17.10.2025]
 16. Omer, N., Samak, A.H., Taloba, A.I. and Abd El-Aziz, R.M., 2023. A novel optimized probabilistic neural network approach for intrusion detection and categorization. *Alexandria Engineering Journal*, 72, pp.351-361. Retrieved from: <https://www.sciencedirect.com/science/article/pii/S1110016823002636> [Retrieved on: 17.10.2025]
 17. Gopalsamy, M., Cyber, S. and Specialist, S., 2021. Advanced cybersecurity in cloud via employing AI techniques for effective intrusion detection. *Int. J. Res. Anal. Rev*, 8(01), pp.187-193. Retrieved from: https://www.researchgate.net/profile/ManiGopalsamy-2/publication/387522902_Advanced_Cybersecurity_in_Cloud_Via_Employing_AI_Techniques_for_Effective_Intrusion_Detection/links/6772cf03117f340ec3e55dda/Advanced-Cybersecurity-in-Cloud-Via-Employing-AI-Techniques-for-Effective-Intrusion-Detection.pdf [Retrieved on: 17.10.2025]
 18. Rajapaksha, S., Kalutarage, H., Al-Kadri, M.O., Petrovski, A., Madzudzo, G. and Cheah, M., 2023. Ai-based intrusion detection systems for in-vehicle networks: A survey. *ACM Computing Surveys*, 55(11), pp.1-40. Retrieved from: <https://dl.acm.org/doi/pdf/10.1145/3570954> [Retrieved on: 17.10.2025]
 19. Khan, N., Ahmad, K., Al Tamimi, A., Alani, M.M., Bermak, A. and Khalil, I., 2025. Explainable AI-Based Intrusion Detection Systems for Industry 5.0 and Adversarial XAI: A Systematic Review. *Information*, 16(12), p.1036. Retrieved from: <https://peerj.com/articles/cs-2043.pdf> [Retrieved on: 17.10.2025]
 20. Ferrag, M.A., Maglaras, L., Janicke, H. and Smith, R., 2019, September. Deep learning techniques for cyber security intrusion detection: A detailed analysis. In *6th International Symposium for ICS & SCADA Cyber Security Research 2019*. BCS Learning & Development. Retrieved from: https://www.academia.edu/download/40505617/Distributed_Intrusion_Detection_and_Atta20151130-11977-92aqs8.pdf [Retrieved on: 17.10.2025]
 21. Polamarasetti, A., Vadisetty, R., Velaga, V., Routhu, K., Sadaram, G., Boppana, S.B. and Vangala, S.R., 2023. Enhancing Cybersecurity Architectures with Artificial Intelligence (AI): A Framework for Automated Threat Intelligence Detection System. *Universal Library of Engineering Technology*, (Issue). Retrieved from: https://ulopenaccess.com/papers/ULETE_SV02/ULETE2023SI_002.pdf [Retrieved on: 17.10.2025]