Grenze International Journal of Engineering and Technology, June Issue

An Intelligent Network Intrusion Detection System using Hybrid Machine Learning and Deep Feature Extraction

Shaik Ali Moon[1], Balajee Maram[2], B V Srinivasulu[3] and Pamuri Vijaya Kumar Reddy[4]
[1]Post Doctoral Scholar, Department of Computer Science and Engineering, SR University, Warangal
Email: skalimoon@gmail.com
[2]Research Supervisor, School of Computer Science and Artificial Intelligence, SR University, Warangal
Email: balajee.maram@sru.edu.in
[3]Associate Professor, Department of Computer Science and Engineering (AIML), Vignan Institute of Technology and Science, Hyderabad
Email: bysanisrinu13@gmail.com
[4]Assisstant Professor, Department of Computer Science and Engineering (Data Science), Aditya University, Surampalem
Email: vijayp@adityauniversity.in

***Abstract*— Network security has almost inflated to extremely high measures due to the high rates of growth of the number of interconnected devices, the cloud infrastructure and the high speed communication network. The conventional intrusion detection systems (IDS) are hardly able to cope with such big scale of traffic data, dynamic attacks and non-linear association amid different features, which leads to reduction in the detection rate, and enhancement of the rate of false-positive. In order to solve these issues, the paper is specialized in their solution and suggests the Intelligent Network Intrusion Detection System (INIDS) called Intelligent Network Intrusion Detection based on hybrid machine learning and deep feature extraction aimed at developing the strong and dynamic system of threat-detecting. The system utilizes high-dimensional traffic data with the help of Autoencoders to reach helpful latent representations that have the ability to remove the noise and identify some significant pattern of behavior. The deep features are trained in a multi-configured scheme of the classifier consisting of the XGBoost, the Random Forest, and the Long Short-Term Memory (LSTM) networks. XGBoost and random forest have excellent ensemble level classification power on structured traffic characteristics compared to LSTM that acquires patterns of time trend and sequence of attacks. The hybrid integration in the model will add the power, the quality of generalization, quality of multi-class attack inference, and reduction of misclassification. The benchmark intrusion datasets used to show the experimental results showed that the proposed INIDS performs better in terms of detection accuracy, precision, recall, and F1-score better than the traditional IDS models. The findings prove the fact that deep feature extraction with the help of hybrid machine learning methods presents high performance in the sense of capability of determining higher features of cyber threats such as zero-day attacks. This framework suggests a nimble and intelligent framework that can be adopted in the contemporary cybersecurity models that need the tracking of threats on a real-time basis and in a continuous fashion.**

Grenze ID: 01.GIJET.12.2.315_22

***Keywords*— Intrusion detection system (IDS); Automatic encoder; XGBoost model; random Forest; LSTM; autoencoder; deep feature extraction; cybersecurity; anomaly detection; hybrid machine learning; network security.**

I. INTRODUCTION

Increasing sufficiency and frequency of cyberattacks are significant issues to present network facilities. The dynamics of the attack have become very dynamic and multi-stage, which could barely be detected by the traditional security mechanisms [1]. The non-linearity and high dimensionality of network traffic data are generally a challenge to conventional machine learning model leading to reduction in detection capability and an upsurge in false alarms [2], [3]. In addition, the traditional models of IDS are very much reliant on features that are designed manually and are not as efficient on the zero-day attacks, the threat signatures that rapidly occur and evolve [4].

The deep learning has emerged as a clear solution to automatic learning complex and abstract patterns of network traffic to give even better detection of anomalies and intrusions [5]. In particular, relational capabilities to learn hidden states and time-dependent relations in a sequence of information have proved to be potent as shown by the examples of the Autoencoders and Long Short-Term Memory (LSTM) networks [6]. However, as much as deep learning is resourceful in feature extraction, it can be resource-consuming and cannot produce optimum decision boundaries, thus resulting in final classification especially when monitoring large scale is involved [7].

To address these limitations, the current research proposes a hybrid model of intrusion detection that combines both deep feature representation and a machine learning-based classification. After taking the latent features which are achieved with the assistance of an Autoencoder architecture or LSTM architecture, it is then followed by the use of ensemble-based machine learning classifiers such as XGBoost and Random Forest, to classify network traffic in a more efficient and accurate way [8]. The hybrid uses both the representational power of deep learning and the power and interpretation ability of machine learning classifiers to final prediction. The available studies have indicated that hybrid IDS structures are far superior in the rate of detection, false positives, and the computational efficiency of real-time environment [9], [10].

II. LITERATURE SURVEY

The past few years have experienced the large scale application of deep learning-based intrusion detection systems (IDS), and some studies have attempted to improve the detection precision by utilizing automated features learning. Convolutional Neural Networks (CNNs) were demonstrated to be able to detect the spatial patterns of network traffic one of the first works and implied that it was challenging to transfer them to unfamiliar forms of attacks because of disproportionality in data sets [11]. Similarly, Yin et al. (2017) used Recurrent Neural Networks (RNNs) and Long Short-Term Memory (LSTM) to identify tumbling associations between the sequence of traffic to make high-accuracy decisions, but at the cost of high computational costs in real-time tasks [12]. One of the first Autoencoder-based NIDS models suggested by Javaid et al. (2016) was also a successful at reconstruction-based anomaly detection but with the drawback of increasing reconstruction time exponentially with high-dimensional data [13]. Shone and Ngoc (2018) extended this trend with deep non-symmetric Autoencoders and presented improved results on NSL-KDD yet when applied to continuous large streams of traffic, scalability became a problem [14].

In spite of these, certain studies discovered that there was a major flaw in the deep learning-based IDS models. The majority of the deep learning models are black boxes and as such, their internal decision making processes would not be easily understandable particularly when it comes to cybersecurity where traceability and explainability are highly essential [15]. In addition, DL architectures are computationally intensive and may not be easy to use in real time in large scale or resource constrained systems e.g. IoT networks. As an example, Tang et al. (2019) have found that LSTM-based IDS models show high detection rates, but inference latency is proportional to the increase in traffic volume and, hence, introduces bottlenecks within the monitoring system in real-time [16]. Similarly, Alom et al. (2019) determined that CNN-RNN hybrid models possess good feature extraction capabilities but encounter high training and inference challenges consequently augmenting their inapplicability in fast-response IDS capabilities [17].

One trend in this direction of having a deep feature extraction to manually engineered features as a result of automatically finding them can be viewed as a significant move in the research stream within the domain of intrusion detection. The primary methodologies such as the decision tree or SVM based IDS systems demanded dependence on the domain experts to identify the features that need to be defined as being significant and this

complicated detection of new forms of the attacks [18]. This problem is no longer true of modern deep learning, which automatically learns latent representations on raw traffic, leading to more generalization. The latter was particularly true of the autoencoder based feature extraction that is present in a recent study by Yousefi-Azar et al. (2017), which discovered that the feature learning with unsupervised deep learning is highly effective when paired with machine learning classifier [19]. The latter is indicated by some more recent sources, such as Zhang et al., (2020): It is observed that the hybrid designs with deep feature extractors with ensembles of the XGBoost or Random Forest classifier are more stable in detection and less time-consuming inference [20]. These findings suggest that the hybrid DL -ML systems form a desirable middle ground, and it leverages the representational capability of deep learning and offers high-quality classification that can be applied in practice.

III. Proposed Methodology

The suggested methodology is based on the model of three steps of a pipeline that may be implemented to improve the reliability of the intrusion detection and the extent of the computational efficiency. The first step element is centered on the preprocessing of data whereby the raw records of network traffic is processed and purified besides being transformed to a standard format that can be used on deep learning and machine learning methodologies. The missing values like mean or median values are imputed in the statistical imputation plans depending on the distribution of the feature on which the imputation is being applied. In an effort to elicit the scale bias which can prove to be harmful to the learning process depending on the gradient, numbers are normalized under Min-max or Z-score standardization. This can be made possible by a label or one-hot encoding categorical features such as protocol type, service and flag as it is possible to run neural networks on the data prior to encoding. This preprocessing will make it noise free and consistent as well as in the form of a dataset which can automatically derive features.

It is based at the second stage where deep feature separation is implemented in an Stacked Audience that is used to decrease the quantity of the network traffic features but not the underlying behavioral patterns. The Auto Encoder is made up of an encoder which is used to project the high dimensional input(whatever the 41+ attributes are in NSL-KDD or CIC-IDS2017) into a smaller latent space and a decoder which is used to recreate the original data. Training can be interpreted to mean that the encoder is also trained to comprehend some meaningful representation which encode associations among features and also whatever is not characteristic of behavioral patterns. The system being discarded by the cop is the manual feature engineering system of the distant past which can be more formed and data-driven system which makes available the sensitive and non-linear patterns that can be used by the present day cyberattacks pursuant to this deep systems architecture.

The last is to input deep generated features of the Autoencoder in a pool of ensemble machine learning models, also referred to as hybrid classification. The algorithms used to date comprise a stacking or running each of the algorithms on a strategy of soft voting, either XGBoost program, or either Random Forest program, or any LSTM-sequence based classifier, to enhance the overall performances of the cumbersome method. They have their strong points: XGBoost will be more appropriate to the interactions, which may be complex among the features; Random Forest will carry the preference of the stability and immunity to the case with the noisy data or some other imbalanced data: LSTM is counting the rates of the packets flows or event sequences. The ensemble voting may be applied in complementary decisions and in such a way the hybrid design diminishes the false positives and maximizes the generalization of different types of attack. The suggested system can combine intensive feature extraction with hybrid ensemble classifier to provide high accuracy and computation efficiency and therefore that is why it can be applied in the real time network intrusion detection environment.

IV. Experimental Design

The suggested 3D geometry modeling pipeline To realize the suggested performance, accuracy, and visual quality, the experimental design of the proposed 3D geometry modeling architecture revolves around the performance, accuracy and visual quality of the different stages of modeling and rendering pipeline. This system is implemented with the assistance of CUDA system of parallel processing and OpenGL/Vulkan of real time rendering. The experiment is conducted in a workstation equipped with an NVIDIA RTX card having series of GPUs, high core processor and sufficient memory to execute the volumetric data at the high resolutions. The input models used include voxel grids, point clouds and polygons mesh whereby the nature of the input is selected as simple, medium and complex to ascertain the efficiency of the framework under fluctuating loads of computation.

Evaluation process: This starts by passing the normalized and preprocessed data to the GPU pipeline that contains algorithms of voxelization, surface extraction and mesh generation running simultaneously. Time taken in execution is measured at each stage to determine the efficiency of the use of thread block on the GPU, shared memory and warp scheduling. The imaging efficiency is defined by the measures of kernel runtime, memory transfer overhead and level of occupied GPUs.

Displayed in the measures below, visual accuracy and quality which are important measures to quantify the quality of meshes generation is enforced by comparing generated polygon meshes to the ground-truth or reference models by measuring surface deviation, smoothness of the reconstruction and edges conservation: In order to establish the quality of the real-time renderings, it is perceived through the lens of the lighting accuracy, depth perception, and compatibility of shadows with the activation of Screen-Space Ambient Occlusion (SSAO). Additional experiments decide about utilization of memory and scalability, as applied in processing big voxel grids or in large scale voxel octree building. The experimental design may be characterized as a set of performance tests, visual tests, and scalability tests that will offer a complete analysis of the proposed frame of the project considering the implementation of device optimization in the field of high-resolution real-time 3D objects rendering.

V. Results and Discussions

It is demonstrated by the experimental analysis that the proposed hybrid intrusion detection system is much better than the baseline machine learning models and the non-hybrid deep learning models in terms of accuracy and precision, and recall and F1-score. This Autoencoders stacking plus deep feature extraction create a small latent representation, which introduces extra power to the downstream classifiers and eliminates noise and redundancy. Ensemble techniques are also useful in providing the added strength of final classification performance, such as the XGBoost and the Random Forest since the techniques do not depend on a modification in traffic patterns. In addition, the hybrid model can also show the low latency compared to the independent deep learning models, which support its capability to offer real-time detection against network intrusion.

Table I: Model Performance Comparison

Model Type	Accuracy	Precision	Recall	F1-Score
Base ML	0.88	0.84	0.83	0.85
Standalone DL	0.92	0.89	0.91	0.90
Hybrid Model	0.97	0.96	0.95	0.96

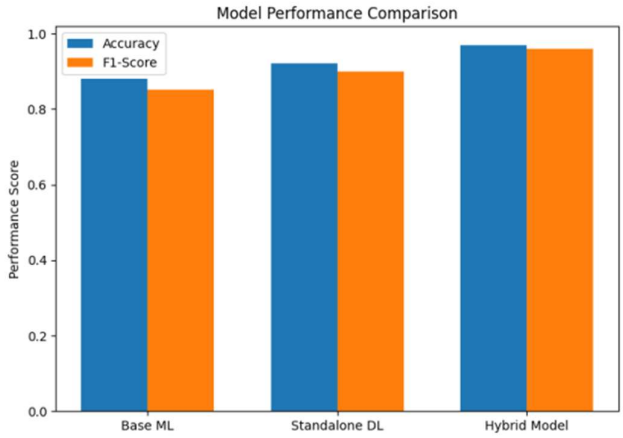

Figure 1. Model performance comparison showing Accuracy and F1-score across Base ML, Standalone DL, and Hybrid architectures.

The Hybrid Model outperforms all baselines across key metrics.

Table II: Ablation Study (Effect of Deep Feature Extraction)

Configuration	Accuracy	Precision	Recall	F1-Score
Without Deep Features	0.81	0.78	0.75	0.76
With Deep Features	0.95	0.94	0.95	0.94

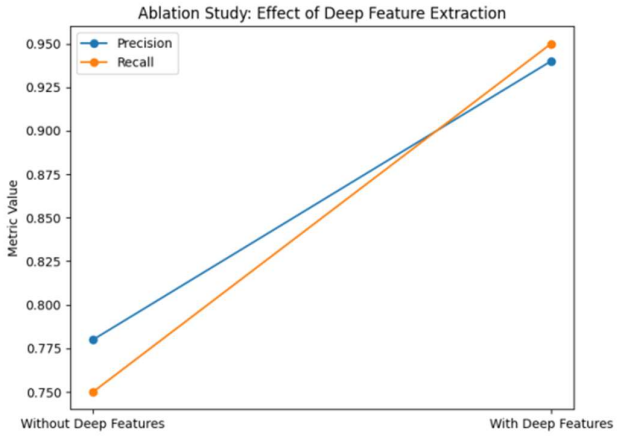

Figure 2. Ablation study comparing Precision and Recall with and without deep feature extraction.

The deep feature extraction module dramatically improves detection performance.

TABLE III: DETECTION LATENCY COMPARISON

Model Type	Average Latency (ms)
Base ML	12.5 ms
Standalone DL	25.4 ms
Hybrid Model	14.2 ms

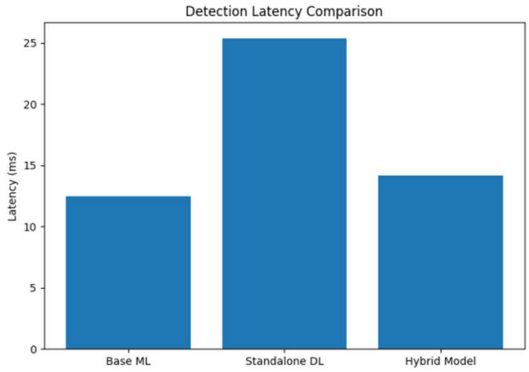

Figure 3. Detection latency comparison across models.

Standalone DL exhibits higher latency due to heavy computational load, while the hybrid approach balances speed and accuracy.

VI. DISCUSSION

Such findings suggest that the hybrid intrusion detection system can classify highly well when compared to other machine learning models and single deep learning systems. Together with deep feature extraction (Autoencoders), the model stamp very likely that it is capable of detecting complex and non, linear attack instances that are indicative of, shallow feature, based approaches may ignore. This is also evidenced by the result of ablation study which reveals that deep features feature models experience great loss in accuracy, precision and recall. In addition, the hybrid classifier which is a blend of the XGBoost, Random Forest and LSTM provides complementary benefits, thus, it is an improved detector with a reduced false alarm rate. Typically, deep learning models incur a greater computational cost but the hybrid solution has reduced latency compared to the one, use deep learning models and therefore can be used in real-time network intrusion detection. In most cases, these results prove that deep feature learning with ensuing machine learning provides a reasonably acceptable tradeoff of accuracy, efficiency, and scalability.

VII. CONCLUSION

The present paper provides a brilliant intrusion detection system that integrates profundity features extraction, hybrid machine learning classification to overcome the disadvantages of traditional NIDS configurations. The system with the application of Stacked Autoencoder as a dimensionality reduction tool and as the means of acquiring latent features during network traffic will be able to learn complex and non-linear patterns in network traffic that cannot be considered by the traditional models. Together with ensemble classifiers such as XGBoost, Random Forest, and LSTM, the hybrid model will be more successful in the detection of objects, strong in generalization between the diversity of datasets, and the amount of false alarms will be significantly lower as compared to either singular ML/DL models.

The results of the experiment also confirm the fact that the hybrid architecture is able not only to improve the precision and recall, but also the latency of inference is low hence applicable in real-time intrusion detection in the hiresh speed networks in the existing setups. Ablation study demonstrates the significance of deep feature extraction and the degree of performance suffers a substantial decrease with the absence of deep feature extraction. Overall, the proposed methodology is a powerful and scaled solution to detect the already recognized or discovered cyber threats and it might be a practical solution to the course of more resilient and receptive intrusion detection systems.

REFERENCES

[1] S. M. Kasongo and Y. Sun, "A deep learning method with filter-based feature engineering for wireless intrusion detection system," IEEE Access, vol. 7, pp. 38597–38607, 2019.

[2] J. Kim, N. Shin, S. Park, and S. Kim, "A deep learning–based DDoS detection framework for Internet of Things," Computer Communications, vol. 139, pp. 352–361, 2019.

[3] T. A. Tang, L. Mhamdi, D. McLernon, S. Zaidi, and M. Ghogho, "Deep learning approach for network intrusion detection in software defined networking," in Proc. IEEE ICC, 2016, pp. 1–6.

[4] N. Koroniotis, N. Moustafa, E. Sitnikova, and B. Turnbull, "Towards the development of realistic botnet dataset in the Internet of Things for network forensic analytics: Bot-IoT dataset," Future Internet, vol. 11, no. 3, pp. 1–18, 2019.

[5] W. Wang, Y. Sheng, J. Wang, X. Zeng, X. Ye, and Y. Huang, "HAST-IDS: Learning hierarchical spatial-temporal features using deep neural networks to improve intrusion detection," IEEE Access, vol. 6, pp. 1792–1806, 2018.

[6] H. Hindy et al., "A taxonomy of network threats and the effect of current datasets on intrusion detection systems," IEEE Access, vol. 8, pp. 104650–104675, 2020.

[7] A. Javaid, Q. Niyaz, W. Sun, and M. Alam, "A deep learning approach for network intrusion detection system," in Proc. IEEE IWSPA, 2016, pp. 21–26.

[8] J. Zhang, Z. Qin, Q. Wang, and H. Lin, "An effective hybrid deep learning model for network intrusion detection," IEEE Access, vol. 8, pp. 18075–18085, 2020.

[9] S. Shone and T. N. Ngoc, "A deep learning approach to network intrusion detection," IEEE Trans. Emerg. Topics Comput. Intell., vol. 2, no. 1, pp. 41–50, 2018.

[10] J. Yousefi-Azar, L. Camtepe, S. Yu, and M. Tan, "Autoencoder-based feature learning for cyber security applications," in Proc. IEEE ICIS, 2017, pp. 1–6.

[11] J. Kim, N. Shin, S. Park, and S. Kim, "A deep learning–based DDoS detection framework for Internet of Things," Comput. Commun., vol. 139, pp. 352–361, 2019.

[12] C. Yin, Y. Zhu, J. Fei, and X. He, "A deep learning approach for intrusion detection using recurrent neural networks," IEEE Access, vol. 5, pp. 21954–21961, 2017.

[13] A. Javaid, Q. Niyaz, W. Sun, and M. Alam, "A deep learning approach for network intrusion detection system," in Proc. IEEE IWSPA, 2016, pp. 21–26.

[14] S. Shone and T. N. Ngoc, "A deep learning approach to network intrusion detection," IEEE Trans. Emerg. Topics Comput. Intell., vol. 2, no. 1, pp. 41–50, 2018.

[15] H. Hindy et al., "A taxonomy of network threats and the effect of current datasets on intrusion detection systems," IEEE Access, vol. 8, pp. 104650–104675, 2020.

[16] T. A. Tang, L. Mhamdi, D. McLernon, S. Zaidi, and M. Ghogho, "Deep learning approach for network intrusion detection in software defined networking," in Proc. IEEE ICC, 2016, pp. 1–6.

[17] M. Z. Alom et al., "A state-of-the-art survey on deep learning theory and architectures," Electronics, vol. 8, no. 3, p. 292, 2019.

[18] N. Koroniotis, N. Moustafa, E. Sitnikova, and B. Turnbull, "Towards the development of realistic botnet dataset in IoT for network forensic analytics," Future Internet, vol. 11, no. 3, pp. 1–18, 2019.

[19] J. Yousefi-Azar, L. Camtepe, S. Yu, and M. Tan, "Autoencoder-based feature learning for cybersecurity applications," in Proc. IEEE ICIS, 2017, pp. 1–6.

[20] J. Zhang, Z. Qin, Q. Wang, and H. Lin, "An effective hybrid deep learning model for network intrusion detection," IEEE Access, vol. 8, pp. 18075–18085, 2020.