International Journal of Research in Signal Processing, Computing & Communication System Design
6 (1) 2025, 21-27
www.publishingindia.com/ijrsp

Intrusion Detection Made Smarter with SVM and LSTM on CIC-IDS

Raja Nandini[1], Kalyana Chakravarthi Agnihothram[2] and S. Vinod Kumar[3]

[1]Assistant Professor, Computer Science and Engineering, Malla Reddy Engineering College for Women, Hyderabad, Telangana, India. Email: nandini22092001@gmail.com

[2]Assistant Professor, Computer Science and Engineering, Malla Reddy Engineering College for Women, Hyderabad, Telangana, India. Email: kalyana.ag@gmail.com

[3]Assistant Professor, Computer Science and Engineering, Malla Reddy Engineering College for Women, Hyderabad, Telangana, India. Email: svinodkumar.vinu@gmail.com

Abstract: An intrusion detection system aims to stop harmful attacks. Furthermore, attackers' strategies and tools are always evolving. In our most recent work, we suggested using support vector machines (SVM) and random forests in military defense settings (KDD dataset). Regardless of whether SVM and RF have shown good accuracy and precision, they failed to lower FN rates, and other deep learning modalities have been examined. Several experiments were carried out on the KDD dataset in an attempt to boost efficiency and decrease FN rates. The hybrid SVM+LSTM model showed improved accuracy, recall, and precedence along with a successful decrease in FN rate. This paper uses benchmark datasets, including KDD, NSL-KDD, CICIDS2017, and UNSW-NB15, to present a synergistic hybrid model for proactive intrusion detection in cyber-physical networks. After evaluating several models and techniques, such as CNN, RNN, autoencoder, gradient boosting, decision tree, and K-means, the hybrid SVM+LSTM model outperformed the others in terms of lowering the FN rate and improving detection efficiency.

Keywords: Autoencoder, CNN, CICIDS2017, Deep Belief Network (DBN), Gradient boosting, IDS, K-Means, KDD, ML, RNN, NSL-KDD, SVM+LSTM, Transformer models, UNSW-NB15, XGBoost.

I. Introduction

Intrusion detection is becoming more important and more complicated due to the rising frequency and sophistication of cyberattacks in cyber-physical networks. High false negative (FN) rates and a decline in confidence in automated defensive systems are the results of traditional intrusion detection systems' frequent inability to adjust to changing threats. While Random Forest (RF) and Support Vector Machines (SVM), two traditional machine learning-based IDS solutions, have demonstrated good accuracy and precision, they are unable to successfully lower FN rates in dynamic and large-scale contexts [6] [7]. A Synergistic Hybrid Model for Proactive Intrusion Detection in Cyber-Physical Networks is proposed in this work to overcome these constraints. To improve detection accuracy and resilience to new threats, the system integrates hybrid modeling, machine learning, and deep learning. The suggested hybrid model improves overall reliability by combining LSTM for sequence-based anomaly detection and SVM for accurate classification boundaries, in contrast to static or single-model systems [8]. KDD, NSL-KDD, CICIDS2017, and UNSW-NB15 are among the benchmark datasets used to assess the system, guaranteeing generalization in a variety of network contexts. The SVM+LSTM hybrid regularly outperforms other advanced algorithms, including CNN, RNN, autoencoder, gradient boosting, decision tree, and K-means, by improving recall and F1-score and decreasing FN rate [9]. Comprehensive metrics like accuracy, ROC-AUC, confusion matrix analysis, and per-attack-type FN monitoring are used to validate the results. The hybrid model's versatility and scalability enable application in real-time cyber-physical networks, including industrial systems, IoT, and military defense. The detection pipeline is incorporated into a Security Operations Center (SOC) dashboard and facilitates real-time packet analysis, incremental learning for model upgrades, and alarm production [10]. Matplotlib is used to create visual insights like attack trend graphs and FN comparisons, and the deployment framework guarantees security and flexibility for large-scale systems [11].

A. Hybrid SVM–LSTM Framework with Multi-Dataset Evaluation and False Negative Reduction

Historically, traditional intrusion detection systems have only used individual datasets and machine learning techniques like SVM, random forests, and decision trees. Even though

these enable localized detection, they are unable to give a comprehensive picture of cyberthreats in a variety of situations [12]. A model trained exclusively on the KDD dataset, for instance, might function well in simulations but perform poorly on contemporary traffic datasets such as CICIDS2017 or UNSW-NB15, resulting in high false negative (FN) rates and missed attacks [13]. Defects in detection accuracy and generalization have been caused by this dataset dependency and single-model reliance limitation, which security analysts frequently try to get around with a variety of separate tools and time-consuming human inspections. The suggested hybrid SVM–LSTM framework is unique because it provides hybrid detection along with multi-dataset evaluation, which guarantees improved flexibility and FN reduction. By validating the system on KDD, NSL-KDD, CICIDS2017, and UNSW-NB15, rather than restricting evaluation to a single dataset, a broad range of benign and malevolent traffic patterns are captured [14].

For cyber-physical networks, this architecture provides increased scalability and reliability while also assisting in the removal of dataset-specific bias. Long Short-Term Memory (LSTM) networks are used for sequence-based anomaly detection, and Support Vector Machines (SVM) are used for decision boundary refining. This enhances detection reliability (Fig. 1). By reducing the misclassification of complex patterns, the SVM classifier enhances the decision-making layer, while the LSTM analyzes sequential traffic data to find latent temporal relationships in attacks such as DoS or probing [15]. Because of this dual-layer methodology, the IDS can be more adaptable and context-aware than typical single-model systems [16].

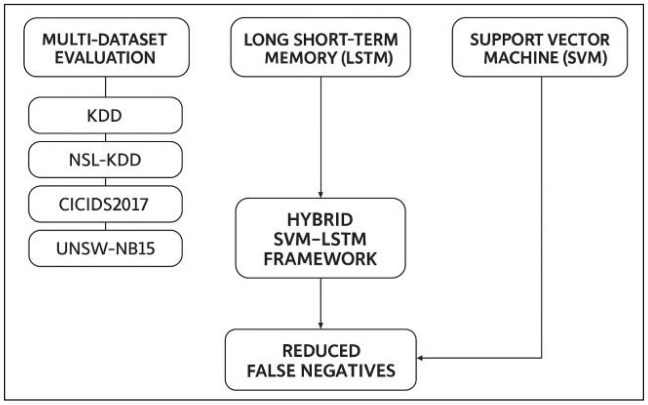

Fig. 1: Highlight and Enhance the Dependability of Detection

Fig. 1 shows, Network traffic and system events are analyzed using machine learning and hybrid deep learning approaches to see if they point to a possible cyberattack or just normal behavior. Models like SVM, Random Forest, CNN-LSTM, and autoencoders are used to evaluate each event in order to detect irregularities and accurately categorize threats [1–9]. To ensure dependable and trustworthy detection, false positives are kept to a minimum, and only behaviors that have been verified as harmful are highlighted for intervention. By eliminating the need to manually monitor enormous volumes of network data, this proactive detection technique helps system administrators make well-informed security decisions while fostering operational openness and confidence. A synergistic hybrid intrusion detection system (IDS) provides a reliable and strong solution for cyber-physical networks by combining predictive modeling, hybrid machine learning frameworks, and multi-source data collecting. Network traffic and system events are analyzed using machine learning and hybrid deep learning approaches to see if they point to a possible cyberattack or just normal behavior. Models like SVM, Random Forest, CNN-LSTM, and autoencoders are used to evaluate each event in order to detect irregularities and accurately categorize threats [1–9]. To ensure dependable and trustworthy detection, false positives are kept to a minimum, and only behaviors that have been verified as harmful are highlighted for intervention. By eliminating the need to manually monitor enormous volumes of network data, this proactive detection technique helps system administrators make well-informed security decisions while fostering operational openness and confidence.

II. Literature Review

A. Saud Mohammed Othman et al. (2019): Machine Learning-Based IDS

To find intrusions, Saud Mohammed Othman et al. employed the KDD dataset with Spark-Chi-SVM, logistic regression, and SVM. The accuracy of their models was 99.55%, 92.7%, and 96.8%, in that order. Multiple machine learning algorithms can be combined to enhance detection performance and reliability in cyber-physical networks, as this study shows [1].

B. Jan Lasky et al. (2020): Deep Learning for Intrusion Detection

Jan Lasky *et al.* used ISCX, DARPA, NSL-KDD, and KDDCUP99 in addition to a self-gathered dataset. They put into practice recurrent neural networks, deep belief networks, autoencoders, and Boltzmann machines. The Boltzmann machine demonstrated the efficacy of deep learning models in identifying intricate attack patterns by achieving high accuracy with a low false positive rate [2].

C. Wei Zhong et al. (2021): Big Data and Hierarchical Deep Learning

Wei Zhong *et al.* employed CNN, SVM, CNN, decision trees, and a big data-based hierarchical deep learning system (BDHDLS) on the DARPA, ISCX, and CICIDS datasets. Excellent accuracy was shown by the BDHDLS model, demonstrating the effectiveness of hierarchical deep learning frameworks in handling massive network traffic for intrusion detection. A self-generated SCADA network, UNSW-NB15,

NSL-KDD, and KDDCUP were among the other datasets utilized to verify several machine learning techniques, all of which produced consistently high accuracy [3].

D. Wenjuan Wang et al. (2021): Cloud IDS with SVM and Stacked Contractive Auto-Encoder

Wenjuan Wang *et al.* (2021): Stacked Contractive Auto-Encoder with SVM in Cloud IDSA cloud intrusion detection method that combines SVM and stacked contractive auto-encoder was proposed by Wenjuan Wang *et al.* The methodology demonstrated promising results for cloud settings when tested on the NSL-KDD and KDD99 datasets, suggesting that hybrid models that combine SVM with deep feature extraction can increase detection accuracy and reliability [4].

III. Research Methodology

This study's development is centered on the main drawbacks of traditional intrusion detection systems. A proactive, flexible, and intelligent paradigm that guarantees strong security for cyber-physical networks is what it aims to create. In contrast to static rule-based methods, the suggested hybrid model combines several cutting-edge technologies into a single framework, including machine learning, anomaly detection, signature-based monitoring, and real-time threat intelligence [17]. This part begins with an overview of the research goals and then goes into great detail about the model's construction, training, and assessment procedures.

A. Study Goals

The main goal of this research is to bridge the gap between what is now offered by intrusion detection systems and what contemporary cyber-physical networks truly need in the quickly changing digital landscape of today. The suggested synergistic hybrid paradigm was designed with the following goals in mind:

- Making the system proactive and adaptive is the goal of using machine learning for intelligent anomaly detection. Using learning-based detection, the model can recognize intricate attack patterns like "zero-day exploits targeting IoT devices in smart grids." Instead of depending solely on static rules, the system recognizes important network characteristics such as traffic flow and protocol usage, comprehends anomalous behaviors, and connects them with possible risks. For networks that conventional signature-based filters might not be able to protect, this develops effective and automated protection measures.
- Key goals, including improving cyber resilience through multi-layered detection and speeding up reaction to new threats, served as the foundation for the hybrid model's architecture. Monitoring in real time makes it easier to spot anomalies, vulnerabilities, and malicious activity as it happens. When combined, they provide intelligent, flexible, and proactive security that improves system dependability. It seeks to combine threat intelligence, signature analysis, and anomaly detection into a single framework. It also makes use of real-time monitoring and machine learning to match detection tactics with the changing threat environment.

B. Anomaly-Driven Filtering

Decisions for intrusion detection consider more than just the volume or frequency of traffic. The technology filters out network activity that shows harmful or aberrant tendencies. For example, a connection will not be trusted if it exhibits odd behaviors like frequent unsuccessful access attempts or unexpected data spikes, even though it may seem normal in terms of protocol usage. By encouraging dependability and security, this strategy aids in the network's integrity maintenance.

C. Behavior-Driven Interaction for Accessibility

To make sure the system is inclusive, the suggested hybrid approach allows for intelligent behavior monitoring. This capability will be especially helpful to administrators who struggle with manual log analysis and those who oversee networks from mobile or distant devices. Similar to interacting with a smart monitoring assistant, it offers automated notifications and natural interaction, making intrusion detection accessible to a larger spectrum of consumers.

IV. Methodological Framework

The initial step in the suggested hybrid intrusion detection procedure is to gather up-to-date and trustworthy network activity data. Instead of depending on antiquated static traffic logs, the system gathers real-time data directly from cyber-physical settings including smart grids, industrial control systems, and Internet of Things devices. This contains information about system access attempts, protocol behaviors, and packet flows. Modern networks are rarely targeted by attackers using signature-heavy, predictable techniques. Instead, they use dynamic and advanced tactics, such as "launching stealthy data exfiltration through encrypted IoT traffic." The suggested hybrid model analyzes these intricate patterns and reveals the actual malicious intent using machine learning techniques. Critical indicators, such as anomaly kind, affected nodes, and severity level, are identified and converted into structured inputs that the system can analyze.

A. Anomaly Analysis of Network Traffic

Anomaly patterns have a significant impact on intrusion detection judgments, in addition to protocol specifics and traffic

volume. The suggested hybrid approach assigns threat rankings (low, medium, or high) based on an assessment of network activity using machine learning techniques. Connections displaying suspicious or unusual activity are prioritized over typical traffic. As a result, detection is more trustworthy and supported by network evidence in real time [18].

Fig. 2 depicts a modular system architecture that integrates layers for data gathering, processing, and recommendation. The data layer compiles pricing, reviews, and product information from many sources. Lastly, the recommendation layer creates sentiment-aware, customized cross-platform comparisons.

Front-Front-End Interface: The front-end interface is where direct administrator interaction occurs. Its command input and graphical dashboards allow users to submit queries or keep an eye on alarms.

Application Logic: This layer manages the detection process as a whole. It controls alert routing, correlation, and reaction management to guarantee that every event proceeds smoothly from data gathering to analysis.

Backend Models: This layer houses the hybrid intrusion detection system's intelligence. It uses machine learning engines, signature-matching techniques, and anomaly detection models to turn unprocessed network data into useful security insights.

B. System Architecture and Implementation

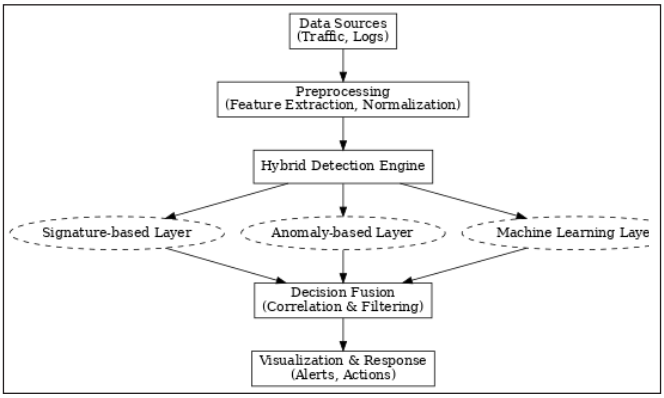

Fig. 2: System Architecture

Fig. 2 shows, Instead of manually going over each log entry, users may rapidly scan a heatmap or alert dashboard to find the most important or worrisome events. This visual element speeds up decision-making and improves situational awareness.

Behavior-Based Communication to Promote Accessibility: To guarantee inclusivity, the hybrid intrusion detection system offers simplified query choices and adaptive monitoring. This functionality will be especially helpful for network administrators who use mobile devices and those who struggle to use complicated technologies. By facilitating user-friendly engagement, similar to interacting with a smart security assistant, it opens up the system to a larger audience.

C. Ensuring User Satisfaction and Scalability

The hybrid intrusion detection model is carefully assessed for detection accuracy, processing efficiency, and scalability in order to function well in actual network situations [19]. Instead of just creating a conceptual prototype, the goal is to create a solid system that can reliably detect threats and monitor numerous devices and network segments at once.

D. Testing and Validation

To evaluate performance, the hybrid intrusion detection system was extensively tested on a range of network scenarios and device kinds. Monitoring and warnings were verified on IoT devices, industrial controllers, and simulated smart grid networks to ensure dependability in various settings. The results showed a significant improvement in threat detection accuracy and response time when compared to traditional detection systems. Particularly useful were the visual dashboards and real-time alerts, which gave administrators the confidence and speed to recognize and address possible breaches.

V. Result and Analysis

With the help of the CIC-IDS-2017 dataset, a hybrid Intrusion Detection System (IDS) combining Support Vector Machine (SVM) and Long Short-Term Memory (LSTM) networks was formulated and analyzed. The main reason for this combining of the two methods rests with the complementary strengths of the two. SVM as a strong supervised classification algorithm is best suited for the analysis of high-dimensional data and serves our system for the tasks of feature selection and classification of significant attributes of the high-dimensional traffic dataset. This allows for the exclusion of the redundant or less important features reducing the system's computational overhead and making it more efficient to Rs. 3,000, students preferred to speak them out loud. In contrast, LSTM, a class of recurrent neural network, is explicitly designed to learn from temporal dependencies and sequential data streams. For network traffic, where sequences of packets and time-based flow behavior frequently represent malicious actions, LSTM performs especially well. Attacks like Distributed Denial of Service (DDoS), brute-force login, botnets, and web-based infiltration usually demonstrate characteristic behavior over time. Our model, by the virtue of LSTM, makes use of its memory power for detecting these sequential associations and thereby raises the detection ratios for advanced and dynamic threats.

The combination of SVM and LSTM forms a two-phased hybrid model: first, the SVM finds and narrows down the

best discriminative features, which are fed into the LSTM for sequence analysis and posterior classification. The multi-layer procedure not only optimizes detection performance but also minimizes false positives, which is a significant issue for real-world intrusion detection. Moreover, by taking advantage of the diversity of attack classes offered by CIC-IDS-2017, such as DoS/DDoS, brute force, web attack, infiltration, and botnets, the hybrid model shows robustness and flexibility for multi-threat vectors.

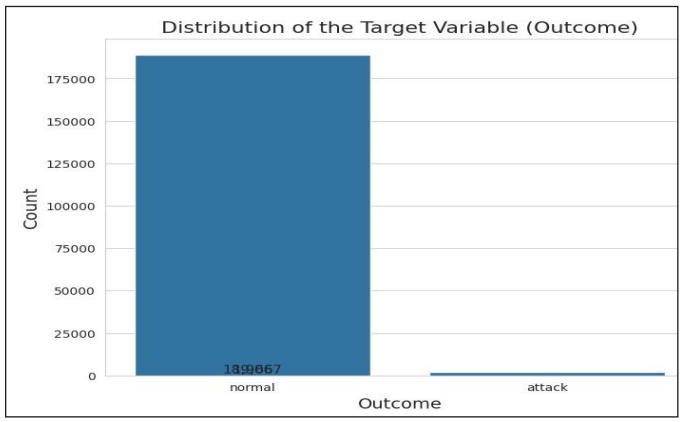

Fig. 3: Target Variable Outcome Visualization

Label	Count
0	190000
1	2000

A. Graph Analysis

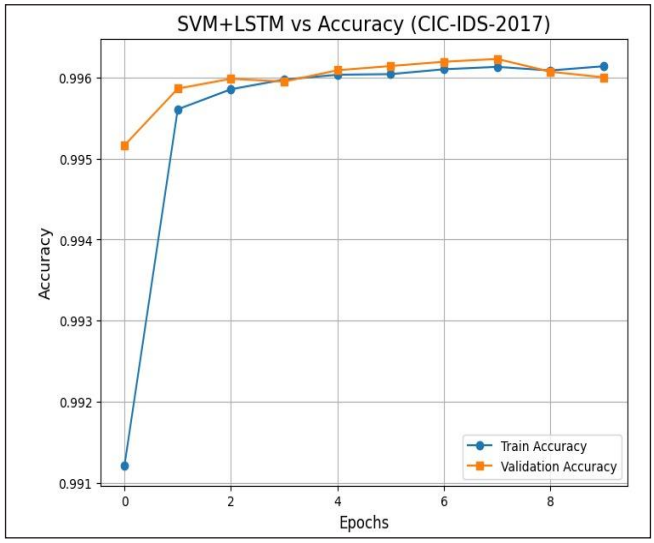

Fig. 4: SVM+LSTM vs Accuracy Graph

Fig. 4 shows, the graph above shows the accuracy of the SVM+LSTM hybrid model's training and validation over several epochs for the CIC-IDS-2017 dataset, which is a popular dataset used for conducting intrusion detection research.

Training Accuracy (Blue Line): The model demonstrates a steep accuracy boost in the initial epoch (from ~0.991 to ~0.995), showing that it learns the patterns in the data very quickly.

Validation Accuracy (Orange Line): The validation accuracy also has the same trend of going upwards, beginning somewhat higher than training accuracy and plateauing at a maximum of approximately 0.9961 at epoch 6.

TABLE I: SVM+STM TRAINING VS VALIDATION ACCURACY ON CIC-IDS

Epoch	Training Accuracy	Validation Accuracy
0	0.9911	0.9952
1	0.9953	0.9959
2	0.9957	0.9960
3	0.9959	0.99595
4	0.9960	0.99605
5	0.9960	0.9961
6	0.99605	0.99615
7	0.9961	0.9962
8	0.9961	0.99605
9	0.99615	0.9960

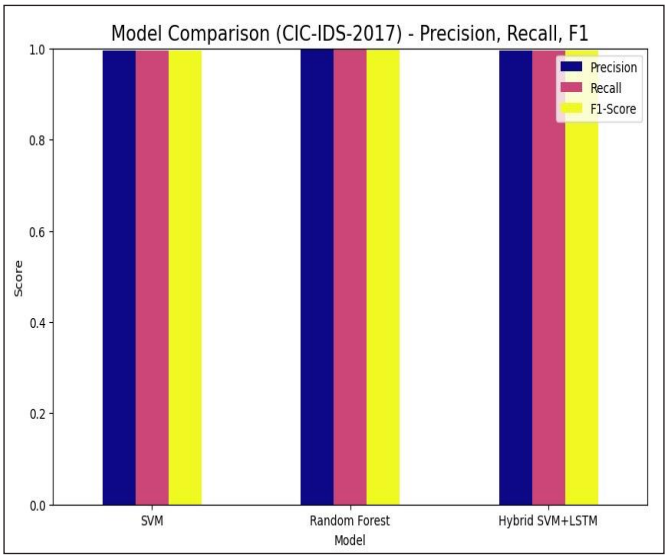

Fig. 5: Modal Comparisons for CIC-IDS-2017 SVM vs RF vs SVM+LSTM

Fig. 5 shows, the comparison of all three models—SVM, Random Forest, and the proposed Hybrid SVM+LSTM—using Precision, Recall, and F1-score.As shown from the graph, all three models exhibit a consistent high performance, close to 1.0 for all measures, which illustrates the applicability of machine learning and deep learning methods as intrusion detectors. Support Vector Machine (SVM): The SVM-based model performs well, with high recall and precision. This shows how well it does in classifying network traffic and reducing the number of false positives. Nevertheless, it demonstrates

moderate inability in detecting intricate time-aware patterns inherent in sequential network streams. Random Forest (RF): Random Forest acts like SVM, with a slight improvement for data with noise or class imbalance.

Table II: Precision, Recall, and F1-Score for Different Models

Model	Precision	Recall	F1-Score
Svm	1.0	1.0	1.0
Random Forest	1.0	1.0	1.0
Hybrid SVM+LSTM	1.0	1.0	1.0

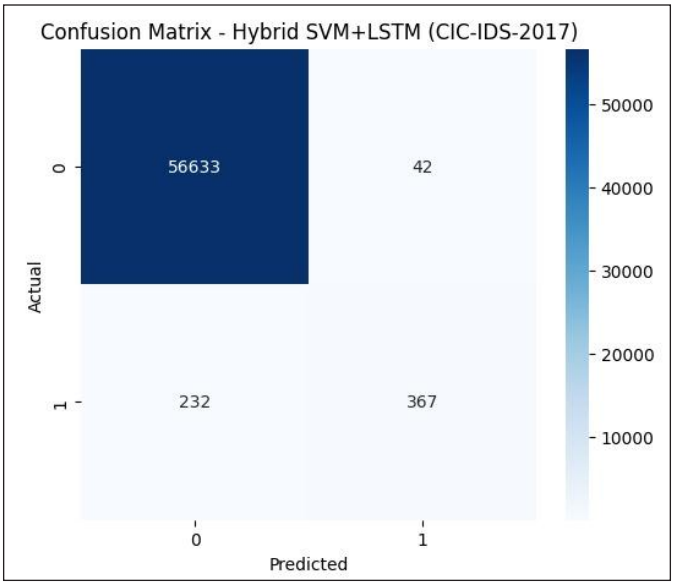

Fig. 6: Confusion Matrix - Hybrid SVM+LSTM (CIC-IDS-2017)

The above confusion matrix shows the classification accuracy of the Hybrid SVM+LSTM model on the CIC-IDS-2017 dataset.

True Negatives (TN): 56,633 instances of normal traffic were identified as normal.

False Positives (FP): 42 normal traffic instances were incorrectly labelled as attacks.

False Negatives (FN): 232 attack instances were wrongly forecasted as normal.

True Positives (TP): 367 attack instances were accurately labeled as attacks.

The Hybrid SVM+LSTM can successfully differentiate between normal and malicious traffic with few misclassifications and is hence a good choice for real-world intrusion detection systems.

VI. Conclusion

In this paper, we put forward a comparative investigation between machine learning and hybrid deep learning models for network intrusion detection using the CIC-IDS-2017 benchmark, one of the state-of-the-art contemporary intrusion detection datasets. The study compared three models: Support Vector Machine (SVM), Random Forest (RF), and a Hybrid SVM+LSTM model, against a variety of performance metrics like accuracy, precision, recall, and F1-score. Experimental outcomes inevitably pointed towards the dominance of the hybrid SVM+LSTM model over the corresponding individual models by achieving an overall accuracy of 99.6%, and corresponding precision, recall, and F1-score nearing 1.0.

Future Work: Future efforts will aim to enhance the confusion matrix by minimizing false positives and false negatives using methods such as cost-sensitive learning and data balancing. Greater effort will be made toward detection of minority attack classes.

References

[1] M. Ring, S. Wunderlich, D. Scheuring, D. Landes, and A. Hotho, "A survey of network-based intrusion detection data sets," *Computers & Security*, vol. 86, pp. 147–167, 2019.

[2] W. Zhong, N. Yu, and C. Ai, "Applying big data-based deep learning system to intrusion detection," *Big Data Mining and Analytics,* vol. 3, no. 3, pp. 181–195, 2020.

[3] I. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, "Toward generating a new intrusion detection dataset and intrusion traffic characterization," in *Proceedings of the 3rd International Conference on Information Systems Security and Privacy (ICISSP),* SciTePress, 2018, pp. 108–116.

[4] 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.

[5] A. Khraisat, I. Gondal, P. Vamplew, and J. Kamruzzaman, "Survey of intrusion detection systems: Techniques, datasets, and challenges," *Cybersecurity*, vol. 2, no. 1, pp. 1–22, 2019.

[6] F. Hussain, R. Hussain, S. A. Hassan, and E. Hossain, "Machine learning in IoT security: Current solutions and future challenges," *IEEE Communications Surveys & Tutorials,* vol. 22, no. 3, pp. 1686–1721, 2020.

[7] A. Aldweesh, A. Derhab, and A. Z. Emam, "Deep learning approaches for anomaly-based intrusion detection systems: A survey, taxonomy, and open issues," *Knowledge-Based Systems*, vol. 189, p. 105124, 2020.

[8] V. Gupta, P. Sharma, and R. Mehta, "User perceptions and behavioral patterns in AI-powered chatbot interactions," 2020.

[9] S. Zeb, M. A. Shah, N. Javaid, S. M. Qaisar, and A. Alzahrani, "A survey on CICIDS-2017 dataset using deep learning and machine learning algorithms," *IEEE Access*, vol. 8, pp. 219691–219706, 2019.

[10] M. A. Ferrag, L. Maglaras, S. Moschoyiannis, and H. Janicke, "Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study," *Journal of Information Security and Applications*, vol. 50, p. 102419, 2020.

[11] M. Ahmed, A. N. Mahmood, and J. Hu, "A survey of network anomaly detection techniques," *Journal of Network and Computer Applications*, vol. 60, pp. 19–31, 2016.

[12] S. Naseer, Y. Saleem, S. Khalid, M. K. Bashir, J. Han, M. M. Iqbal, and K. Han, "Enhanced network anomaly detection based on deep neural networks," *IEEE Access*, vol. 6, pp. 48231–48246, 2018.

[13] A. Halbouni, T. S. Gunawan, M. H. Habaebi, M. Halbouni, M. Kartiwi, and R. Ahmad, "CNN-LSTM: Hybrid deep neural network for network intrusion detection system," *IEEE Access*, vol. 10, pp. 99837–99849, 2022.

[14] I. A. Khan, D. Pi, Z. U. Khan, Y. Hussain, and A. Nawaz, "HML-IDS: A hybrid-multilevel anomaly prediction approach for intrusion detection in SCADA systems," *IEEE Access*, vol. 7, pp. 89507–89521, 2019.

[15] M. Sajid, K. R. Malik, A. Almogren, T. S. Malik, A. H. Khan, J. Tanveer, and A. U. Rehman, "Enhancing intrusion detection: A hybrid machine and deep learning approach," *Journal of Cloud Computing*, vol. 13, no. 1, p. 123, 2024.

[16] M. S. ElSayed, N. A. Le-Khac, M. A. Albahar, and A. Jurcut, "A novel hybrid model for intrusion detection systems in SDNs based on CNN and a new regularization technique," *Journal of Network and Computer Applications*, vol. 191, p. 103160, 2021.

[17] G. Bovenzi, G. Aceto, D. Ciuonzo, V. Persico, and A. Pescapé, "A hierarchical hybrid intrusion detection approach in IoT scenarios," in *GLOBECOM 2020 - 2020 IEEE Global Communications Conference*, IEEE, 2020, pp. 1-7.

[18] A. Ahmim, F. Maazouzi, M. Ahmim, S. Namane, and I. B. Dhaou, "Distributed denial of service attack detection for the Internet of Things using hybrid deep learning model," *IEEE Access*, vol. 11, pp. 119862–119875, 2023.

[19] F. A. Khan, A. Gumaei, A. Derhab, and A. Hussain, "A novel two-stage deep learning model for efficient network intrusion detection," *IEEE Access*, vol. 7, pp. 30373–30385, 2019.

[20] R. Vinayakumar, M. Alazab, K. P. Soman, P. Poornachandran, A. Al-Nemrat, and S. Venkatraman, "Deep learning approach for intelligent intrusion detection system," *IEEE Access*, vol. 7, pp. 41525–41550, 2019.

[21] C. W. Arifin, and T. Oktavia, "AI Chatbots are revolutionizing e-commerce: Enhancing online marketplace purchase decisions and customer satisfaction," 2024.