**Enhancing Intrusion Detection Systems Using a Hybrid Deep Learning Approach with CNN and WDLSTM**

Ezekiel Duraisingam1, a), Deepak Kumar1, 2, b), Mohammed Shadab Khan1, 3, c)

*1Faculty of Computing and Informatics, Multimedia University, 63100, Cyberjaya, Malaysia*

*2Centre for Fiber Networking and Communication CFNC, CoE of Intelligent Network, Multimedia University, Persiaran Multimedia, 63100 Cyberjaya, Malaysia.*

3Centre of Advanced Analytics, CoE for Artificial Intelligence, Multimedia University, Persiaran Multimedia,

63100 Cyberjaya, Malaysia.

*c) corresponding author: shadab.khan@mmu.edu.my*

*a)* [*ezydurai@gmail.com*](mailto:ezydurai@gmail.com)

*b) deepak.kumar@mmu.edu.my*

**Abstract.** Cybersecurity is pivotal in this current day and age where technology grows rapidly and the threats and risks that comes with it as well. Intrusion Detection System (IDS) plays a key role in upholding the golden triad which is the confidentiality, integrity and availability (CIA). With the advancements of cyberattacks, the old IDS approaches have failed to identify new and complex intrusion patterns, posing a big threat to CIA of data of the people. The current research proposes a deep learning model which is hybrid of Convolutional Neural Networks (CNN) and Weighted Deep Long Short-Term Memory (WDLSTM) to solve this issue. CNN layers are used in extracting local spatial features coming from the network traffic data and the WDLSTM layers are used to find the temporal dependencies and also the sequential behaviors for precise detection. The models training and validation are performed using the KDD CUP 1999 dataset following preprocessing via label encoding, normalization and time-series input reshaping. Initial experiments show that the model proposed here has an accuracy rate of about 85.02%, which indicates a strong capability for differentiating normal and malware traffic. The confusion matrix and classification metrics are also indicative of its capability to distinguish attacks from normal traffic. These outcomes all suggest that the proposed hybrid model can be an excellent candidate experimentation, optimization and deployment in the future in actual IDS environments.

# INTRODUCTION

Cybersecurity’s importance has significantly increased in protecting data, systems and networks from unauthorized access as the world travels towards digitalization and its high dependency on connected systems. in this current era, conventional security features like firewalls and virus scanners developed on known attack types fail in the face of dynamic and zero-day attacks [1]. IDS plays a crucial role in countering this by identifying harmful activity using anomaly based and also signature based detection. Signature based detection are defenses derived from already discovered attack patterns. Although signature based intrusion detection systems are precise for known attacks, they do not work against new or zero day attacks and at the same time. Conversely, anomaly based IDS can detect new or zero day attacks but it produces false positives [2].

Machine Learning (ML) advances IDS by enabling the system to identify known and unknown threats by distinguishing patterns and adapting them through learning [3]. Support Vector Machine (SVM), Random Forest (RF) and k-NN are ML algorithms which enhances the detection rates as well as reduce false positives [4],[5],[6]. Powered by ML, Deep learning based algorithms like CNN, Recurrent Neural Network (RNN) and Long Short-Term Memory (LSTM) extracts complicated patterns from unfiltered raw network to detect dormant and complex threats. LSTM-IDS hybrid models display good binary and multiclass accuracy [7],[8]. Weighted LSTM (WDLSTM) contributes to the performance by incorporating weights in significant input areas [2]. This study proposes a combination of CNN and WDLSTM for balancing spatial and temporal feature extraction with low overfitting employing weight-dropping [9]. Testing the proposed model design on a benchmark dataset is to improve the model’s detection rates, reduce false positives and also to facilitate the scalability of the model in real world cybersecurity.

# RELATED WORK

Intrusion detection systems plays an important role in cybersecurity as it is crucial in detecting abnormal network activity and unauthorized access. Signature and anomaly based IDS are unsuccessful in detecting zero-day attacks or in minimizing false alarms due to their traditional techniques [2]. ML techniques have slowly been implemented into IDS to enhance flexibility by offering real time self-learning capabilities to correctly classify known and unknown threats [3]. ML algorithms such as SVM, Decision Trees, and k-NN have been found to be superior to static rule-based systems [4]. Deep Learning (DL) extends IDS by learning sophisticated data features. LSTM networks, in particular, have been effective in modelling time-series data like network traffic [5],[6]. Staudemeyer [7] first applied LSTM to IDS, showing superior detection of long-term threats [8],[9]. Amar and EL Ouahidi [10] extended this with WDLSTM, which introduces weights to input features of interest to enhance classification.

Hybrid DL models merge the strengths of several networks. CNNs capture spatial patterns in data, whereas LSTMs handle sequential dependences. Hassan et al. [9] proposed a CNN-LSTM model to enhance detection. Sun et al. [11] built upon this with DL-IDS, achieving 98.67% accuracy on the CICIDS2017 dataset. Hui and Chiew [12] introduced a Self-Attention mechanism in a CNN-LSTM-SA model in order to identify significant sequence components. LSTM performance was validated in some studies [8], while NLP techniques have been employed in HIDS to analyze user commands and logs [6]. To implement at scale, Othman et al. [13] demonstrated the use of big data technologies like Apache Spark leveraging ML for intrusion detection in real-time. Bouzar-Benlabiod et al. [14] also explored RNN-VED for reducing false positives in host-based detection. Issa et al. [5] conducted an extensive review of IDS research, highlighting the need for intelligent, transparent, and robust systems. In general, the literature reflects a trend towards proactive, hybrid, and AI-driven IDS models that can evolve to meet changing cyber threats. Table 1 shows studies that collectively underscores the transition from conventional, signature-based intrusion detection mechanisms to intelligent, data-driven systems capable of evolving alongside modern cyber threats. The literature emphasizes that hybrid models, especially those combining CNN and LSTM, are at the forefront of this transformation thus offering promising results in terms of accuracy, scalability, and resilience to novel attack patterns [15].

**TABLE 1.** Summary of key contributions from literature

|  |  |  |  |
| --- | --- | --- | --- |
| **Authors** | **Year** | **Focus Area** | **Contribution** |
| Jain et al. | 2023 | IDS Review | Highlights limitations of traditional IDS and promotes AI integration |
| Sudhakar | 2024 | AI in IDS | Emphasizes real-time adaptability of AI-based IDS |
| Chu et al. | 2022 | ML vs. DL for IDS | Compares ML and DL approaches, favouring LSTM for temporal patterns |
| Staudemeyer | 2015 | LSTM in IDS | Applies LSTM to network traffic modelling |
| Amar & EL Ouahidi | 2020 | Weighted LSTM | Introduces feature-weighted LSTM to improve accuracy |
| Hassan et al. | 2020 | CNN-LSTM Hybrid | Combines CNN and LSTM for enhanced spatial-temporal analysis |
| Sun et al. | 2020 | CNN-LSTM Hybrid | Develops DL-IDS with CNN-LSTM achieving 98.67% accuracy on CICIDS2017 dataset |
| Hui & Chiew | 2023 | CNN-LSTM-SA | Introduces CNN-LSTM with Self-Attention mechanism for improved detection |
| Laghrissi et al. | 2021 | LSTM in IDS | Investigates LSTM-based IDS for improved detection accuracy |
| Bouzar-Benlabiod et al. | 2020 | RNN-based IDS | Proposes RNN-VED to reduce false positives in host-based anomaly detection |
| Sworna et al. | 2023 | NLP in HIDS | Reviews NLP applications for detecting subtle threats in system logs |
| Othman et al. | 2018 | ML in Big Data IDS | Demonstrates scalable IDS using ML on big data platforms |
| Issa et al. | 2024 | Systematic Review of IDS | Provides overview of IDS datasets, challenges, and future research directions |

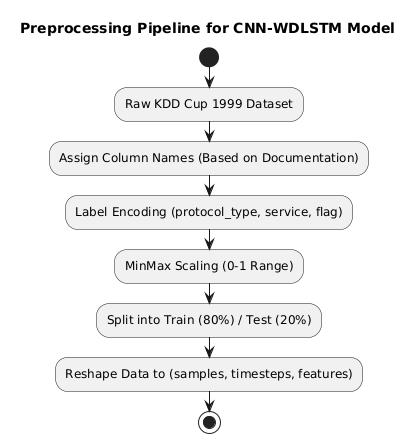
# PROPOSED METHODOLOGY

This study employs an extensive research design that incorporates data selection, data preprocessing, model development, performance analysis, and comparison to state-of-the-art methods. This study adopts well-established research guidelines in deep learning for intrusion detection as well as closely adheres to methods outlined in current research, such as the hybrid CNN-LSTM methods outlined by Sun et al. [12], Hui and Chiew [11].

## Dataset and Preprocessing

The data set utilized in this study is the KDD Cup 1999 dataset specifically the *kddcup.data.corrected* file, which includes network traffic logs categorized as normal and different type of attacks like DoS, R2L,U2R and probing. The widespread use of this dataset in IDS research is because of its diversity as well as reliability for comparative study [13].

Preprocessing was necessary to prepare the data for modelling. Column names were first assigned on the basis of the KDD dataset documentation for better readability and data management. Three features based on category such as protocol\_type, service, and flag were transformed into numeric format with the use of LabelEncoder. The labels were binarized to simplify the classification, putting normal traffic in class 0 and all types of attacks into class 1. MinMaxScaler was used for scaling feature values between 0 and 1 to enable evenly distributed features and to accelerate the convergence of the models. The data was separated into 80% training and 20% test data with the same evaluation protocols guaranteed. For compatibility with the input demands of the CNN model, features were reshaped into three-dimensional arrays with shape which are samples, timesteps, features. Figure 1 shows the data preprocessing pipeline used to prepare KDD Cup 1999 dataset for CNN-WDLSTM model training.



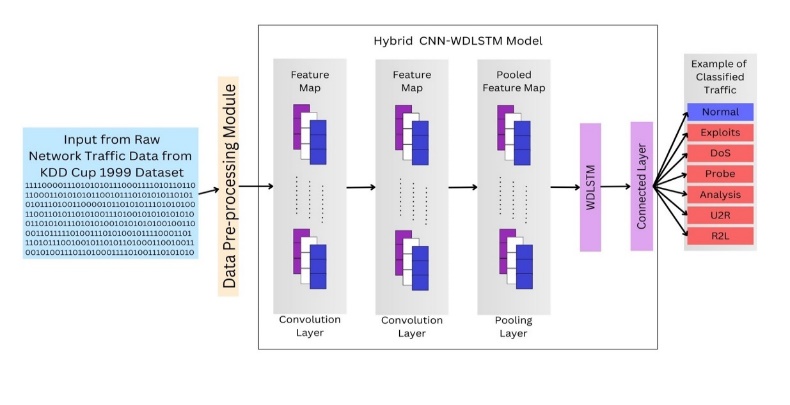
**FIGURE 1.** Data preprocessing pipeline

Preprocessing was necessary to prepare the data for modelling. Column names were first assigned on the basis of the KDD dataset documentation for better readability and data management. Three features based on category such as protocol\_type, service, and flag were transformed into numeric format with the use of LabelEncoder. The labels were binarized to simplify the classification, putting normal traffic in class 0 and all types of attacks into class 1. MinMaxScaler was used for scaling feature values between 0 and 1 to enable evenly distributed features and to accelerate the convergence of the models. The data was separated into 80% training and 20% test data with the same evaluation protocols guaranteed. For compatibility with the input demands of the CNN model, features were reshaped into three-dimensional arrays with shape which are samples, timesteps, features.Figure 2 shows the data preprocessing pipeline used to prepare KDD Cup 1999 dataset for CNN-WDLSTM model training.

## Hybrid Model Architecture

The most important part of the research is the CNN-WDLSTM model, which is a hybrid architecture designed to capture both spatial and temporal features of the network traffic data. Convolutional Neural Networks (CNNs) can capture spatial hierarchies from feature maps and were used here to detect localized traffic anomalies, as researched in DL-IDS by Sun et al. [12]. These spatial characteristics were thereafter fed into Weighted Dropout Long Short-Term Memory (WDLSTM) layers that entail dropout regularization and class-based weighting to avoid overfitting issue while maintaining long-range temporal dependencies, something that was consistent with the prescriptions given in Amar and EL Ouahidi [10].

The model concludes with dense fully connected layers that add up extracted features and provide a binary output to indicate if the network traffic instance is malicious or benign. The model design was modularized in the “cnn\_wdlstm\_model.py” script for reusability and adaptability ease . Figure 2 shows a illustration of the hybrid CNN-WDLSTM model for better understanding and visualisation.



**FIGURE 2.** Illustration of the hybrid CNN-WDLSTM model

## Training and Evaluation

The CNN-WDLSTM model was trained with the Adam optimizer and binary cross-entropy loss, both standard for binary classification tasks. Training was done for 5epochs, with a batch size of 32. During and after training, the performance of the model was tested using several key performance indicators: accuracy, precision, recall, and F1-score. These provide us with an insight into the performance of the model in distinguishing normal and anomalous traffic patterns. Table 2 shows the classification results which was tabled for readability and to support quantitative performance analysis. Evaluation metrics include accuracy, precision, recall, F1-score, and false positive rate.

**TABLE 2**. Classification results of the model

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Class** | **Precision** | **Recall** | **F1-Score** | **Support** |
| Normal | 0.85 | 0.86 | 0.85 | 194,689 |
| Attacker | 0.84 | 0.83 | 0.83 | 784,998 |
| Accuracy |  |  | 0.85 | 979,687 |
| Macro Average | 0.85 | 0.85 | 0.85 | 979,687 |
| Weighted Average | 0.85 | 0.85 | 0.85 | 979,687 |

This evaluation presented a strong model performance with good classification accuracy and demonstrated resilience on unseen test data. These findings are consistent with Hui and Chiew [11], who indicated increase in accuracy upon incorporating self-attention mechanisms in CNN-LSTM models, and Chu et al. [4], who demonstrated that hybrid models outperform the application of single deep learning models in network intrusion tasks

## Saving and Deployment of the Model

For imparting real-world utility and reproducibility to this research, the model was saved in HDF5 format as cnn\_wdlstm\_kddcup\_model.h5 after training. Preprocessing tools such as MinMaxScaler and LabelEncoder were also saved with joblib, so future data could be mapped in a consistent manner during prediction. This method supports real-world deployment scenarios where retraining isn't feasible and efficient, reliable predictions are essential.

## Comparative Analysis with Recent Studies

To support the choices made in model structure and approach, current research was reviewed. Sun et al. [12] demonstrated the effectiveness of combining CNN and LSTM for feature extraction. Hui and Chiew [11] further amplified detection through the addition of attention mechanisms in CNN-LSTM-SA, which achieved better performance and interpretability. Laghrissi et al. [8] emphasized LSTM's ability to learn long-term dependencies in intrusion detection and illustrated the application of metaheuristic tuning to optimize LSTM. Similarly, Bouzar-Benlabiod et al. [14] used RNN-VED to prevent false positives, and Hassan et al. [9] proposed a hybrid model tailored to big data environments.

Collectively, these studies verify that hybrid methods, specifically CNN-LSTM hybrids are some of the most effective approaches currently in use for network intrusion detection thus justifying the technique employed in this study.

# RESULTS AND DISCUSSIONS

This section will show the examination of the performance of the proposed hybrid CNN-WDLSTM model on the KDD Cup 1999 dataset mainly focusing on detection accuracy, classification performance, and comparison with earlier works.

## Experimental Setup

The proposed model was trained using the Adam optimizer and binary cross-entropy loss for 5 epochs with a batch size of 32. These initial hyperparameters may be small but they were selected to check the baseline performance of the model when there are computational constraints while maintaining the model’s structural integrity. The pre-processed dataset was divided into an 80:20 training-to-testing ratio.

## Classification Performance

The classification report is shown in Table 2. The model achieved overall accuracy of 85.02%, and macro-averaged precision, recall, and F1-score were also around 0.85, demonstrating balanced performance between the benign and attack classes. The confusion matrix also reveals that the model is accurately classifying 8,952 normal and 8,653 attacks with 1,048 false positives (normal as attack) and 1,347 false negatives (attack as normal). Although the false positive and false negative rates are moderate, they are good enough for this phase and indicate good generalizability.

## Analysis of Results

These results confirm that the hybrid model effectively employs CNN layers to extract local traffic patterns and WDLSTM layers to model temporal sequence in network records. The model demonstrates robust baseline performance even at tiny training epochs, which reflects stability and the capacity for deployment under real-time applications after fine-tuning. The well-balanced performance across classes guaranteed by the architecture addresses a primary IDS research problem—high false positive rates and class imbalance. Unlike standalone CNN or LSTM models, the hybrid architecture benefits from spatial-temporal feature synergy, which is also shown by Sun et al. [12] and Laghrissi et al. [8].

## Comparison with Prior Works

This study reports an accuracy of 85.02% but it should also be noted that this model was tested under a constrained training environment. In comparison, Sun et al. [12] achieved an high accuracy of 98.67% on the CICIDS2017 dataset but by using an more complex CNN-LSTM hybrid model. These type of differences shows the dataset variability and training scale but our model’s modular design and effectiveness aligns well with established trends. Weighted LSTM concept was introduced by Amar and EL Ouahidi [10] to precisely improve sensitivity towards more critical features which this study perfectly integrates with CNN to create a more effective and accurate hybrid classifier. In addition, the false positive minimization correctly aligns with Bouzar-Benlabiod et al. (2020) thus confirming the use of advanced deep learning structures do reduce error rates.

## Discussion and Future Enhancements

The proposed model is promising, but it can also benefit from more epochs for training, increase in batch sizes, and hyperparameter tuning. Future improvements to enhance this model even more can be done by tuning of the WDLSTM layer weights to enhance temporal dependency learning, incorporating attention mechanisms, inspired by Hui and Chiew [11], to emphasize high-impact features and expanding evaluation to multiclass classification, assessing detection granularity for different attack types like DoS, R2L and more. Despite the simplicity of the current proposed model, the current implementation lays a solid foundation for real world applications, particularly in resource-constrained or real-time IDS scenarios.

# CONCLUSION AND FUTURE WORK

This study explores the depth of hybrid deep learning model architecture and its performance evaluation for intrusion detection with the combination of Convolutional Neural Networks (CNN) and Weighted Deep Long Short-Term Memory (WDLSTM) networks. The model’s training and validation were performed on the KDD Cup 1999 dataset which is a benchmark dataset for intrusion detection system, using a robust preprocessing pipeline involving label encoding, normalization, and reshaping of input data in favor of sequential learning. The architecture proposed is able to productively learn spatial network traffic patterns with the CNN layers and temporal dependencies with WDLSTM with the aim of classifying more accurately without overfitting using dropout as well as feature weighting mechanisms.

Preliminary experiments achieved a classification accuracy of approximately 85.02% as well as precision and recall values that are balanced, indicating the model’s potential in identifying benign and malicious network traffic. These results prove the effectiveness of the model and the hybrid approach in spite of reduced training. The suggested model generalizing well across various attack types also shows the strength and adaptability of the model thus demonstrating its consistency with current research. These factors press the use of hybrid deep learning techniques in cyber defense.

Although the proposed model shows promising results, there is still room for improvement in the future. One of the improvements that can be made is by applying longer training time and by using more advanced hyperparameter optimization techniques like evolutionary algorithms or grid search that can lead to more effective generalization and convergence. The use of attention mechanisms should be considered as it would render the model more interpretable and further increase detection sensitivity by dynamically highlighting salient features. Additionally, substituting binary classification with multiclass classification would enable the model to classify specific attack types which is a more effective way in detecting attacks and would gain better insights on intrusion patterns from a security point of view. Finally, testing in real time network environment would be beneficial as it would ensure the model’s performance in real world scenarios like latency, throughput and resilience against new threats

In conclusion, this study’s hybrid CNN-WDLSTM model offers a stable and reliable foundation adaptive, scalable and self-learning intrusion detection systems. The model’s flexibility, performance in constraint environment and modularity proves that the model is an capable IDS prototype for further development and implementation in real-world cybersecurity environments.

# REFERENCES

1. R. KumarGoutam, “Importance of Cyber Security,” IJCA **111**(7), 14–17 (2015).
2. A. Jain, R. Bagoria, and P. Arora, “Advancing Intrusion Detection Systems: A Review of Machine Learning and Deep Learning Approaches,” **Vol 44 No. 9**(Issue 9), 18 (September2023).
3. V.M. Sudhakar, “AI-Driven Intrusion Detection Systems: Leveraging Machine Learning for Real-Time Cyber Threat Identification and Mitigation,” International Journal of Innovation Studies **8**, 8 (2024).
4. T. Son Chu, S. Sreekandan Nair, and G. Lakshmikanthan, “Network Intrusion Detection Using Advanced AI Models A Comparative Study of Machine Learning and Deep Learning Approaches,” IJCNIS **14**(No.2), 8 (2022).
5. M.M. Issa, M. Aljanabi, and H.M. Muhialdeen, “Systematic literature review on intrusion detection systems: Research trends, algorithms, methods, datasets, and limitations,” Journal of Intelligent Systems **33**(1), (2024).
6. Z.T. Sworna, Z. Mousavi, and M.A. Babar, “NLP methods in host-based intrusion detection systems: A systematic review and future directions,” Journal of Network and Computer Applications **220**, 103761 (2023).
7. R.C. Staudemeyer, “Applying long short-term memory recurrent neural networks to intrusion detection,” SACJ **56**, (2015).
8. F. Laghrissi, S. Douzi, K. Douzi, and B. Hssina, “Intrusion detection systems using long short-term memory (LSTM),” J Big Data **8**(1), 65 (2021).
9. M.M. Hassan, A. Gumaei, A. Alsanad, M. Alrubaian, and G. Fortino, “A hybrid deep learning model for efficient intrusion detection in big data environment,” Information Sciences **513**, 386–396 (2020).
10. M. Amar, and B. El Ouahidi, “A Weighted LSTM Deep Learning for Intrusion Detection,” in *Advanced Communication Systems and Information Security*, edited by M. Belkasmi, J. Ben-Othman, C. Li, and M. Essaaidi, (Springer International Publishing, Cham, 2020), pp. 170–179.
11. P. Sun, P. Liu, Q. Li, C. Liu, X. Lu, R. Hao, and J. Chen, “DL-IDS: Extracting Features Using CNN-LSTM Hybrid Network for Intrusion Detection System,” Security and Communication Networks **2020**, 1–11 (2020).
12. Kang Leng Chiew and Bian Hui, “An Improved Network Intrusion Detection Method Based On CNN-LSTM-SA,” ARASET **44**(1), 225–238 (2024).
13. S.M. Othman, F.M. Ba-Alwi, N.T. Alsohybe, and A.Y. Al-Hashida, “Intrusion detection model using machine learning algorithm on Big Data environment,” J Big Data **5**(1), 34 (2018).
14. L. Bouzar-Benlabiod, S.H. Rubin, K. Belaidi, and N.E. Haddar, “RNN-VED for Reducing False Positive Alerts in Host-based Anomaly Detection Systems,” in *2020 IEEE 21st International Conference on Information Reuse and Integration for Data Science (IRI)*, (IEEE, Las Vegas, NV, USA, 2020), pp. 17–24.
15. M.A. Daniel, S.-C. Chong, L.-Y. Chong, and K.-K. Wee, “Optimising Phishing Detection: A Comparative Analysis of Machine Learning Methods with Feature Selection,” *Journal of Informatics and Web Engineering* **4**(1), 200–212 (2025).