JOURNAL OF SCIENCE TECHNOLOGY AND EDUCATION 13(3), SEPTEMBER, 2025
E-ISSN: 3093-0898, PRINT ISSN: 2277-0011; Journal homepage: www.atbuftejoste.com.ng

Network Intrusion Detection Using Symbiotic Organism Search and Deep Learning

[1]Yakubu Adah, [2]Nurudeen Ibrahim, [3]Hamisu Ismail
[1]*Department of Computer Science,*
[2&3]*Department of Cyber Security*
Nile University of Nigeria, Abuja, Nigeria

ABSTRACT
With the increasing complexity of network environments and the rise in cyber threats, effective and accurate network traffic classification has become crucial for maintaining security and efficiency. Traditional classification methods face challenges in handling large-scale data and class imbalances. This research proposes a novel hybrid approach that integrates the Symbiotic Organisms Search (SOS) algorithm with a Convolutional Neural Network (CNN) to enhance classification performance in flow-based intrusion detection systems. The model utilizes statistical features extracted from TCP flows specifically packets and bytes captured via Wireshark and preprocessed as time-series data. The SOS algorithm is employed to optimize the feature set before feeding it into CNN for classification. Three datasets (USTC-TFC2016, ISCX VPN- nonVPN, and LBNL/ICSI) were used to validate the proposed method. Initial results using only CNN achieved a classification accuracy of 91.27%, but suffered from class imbalance issues, particularly in identifying normal traffic (class 0). The integration of the SOS algorithm significantly improved the model's performance. The final model achieved a remarkable accuracy of 99.19%, precision of 99.28%, and an F1-score of 0.9772. These results confirm the effectiveness of the proposed SOS-CNN hybrid approach in improving classification accuracy.

ARTICLE INFO
Article History
Received: April, 2025
Received in revised form: May, 2025
Accepted: August, 2025
Published online: September, 2025

KEYWORDS
Network Security, Intrusion Detection System, Deep learning, Styling, Symbiotic Organism Search

INTRODUCTION

The rise in security attacks on networks is largely due to the widespread availability of the Internet and interconnected devices, exposing numerous vulnerabilities. These vulnerabilities often lead to intrusions—unauthorized access or data collection—which present major challenges to network administrators. Detecting such intrusions has prompted extensive research, particularly into packet-based and flow-based intrusion detection systems (IDS). While packet-based IDS analyzes full packet content, flow-based IDS focuses on aggregated traffic flows, offering scalability and efficiency, making it the preferred approach (Sperotto et al., 2010).

For many companies, including e-commerce websites, government organizations, defense websites, and other sectors, computer networks and digital information have developed into priceless resources. Considering how well-equipped modern attackers are, these networks are open to attacks. The protection and security of these networks and sites are becoming a highly important and vital issue as a result of the recent rise in network intrusions and network attacks. Intrusion is any series of actions aimed to undermine resource availability, confidentiality, or integrity.

The network administrator would be alerted by an intrusion detection system to take appropriate action against the intrusion, which could involve either hardening the system or preventing similar attacks from happening again. Signature-based intrusion detection systems and

Corresponding author: Yakubu Adah
adahyakubu@gmail.com
Department of Computer Science, Nile University of Nigeria, Abuja, Nigeria.

JOURNAL OF SCIENCE TECHNOLOGY AND EDUCATION 13(3), SEPTEMBER, 2025
E-ISSN: 3093-0898, PRINT ISSN: 2277-0011; Journal homepage: www.atbuftejoste.com.ng

anomaly-based intrusion detection systems are the two most popular forms of IDS currently available. Misuse-based intrusion detection systems are another name for signature-based IDS. Signatures are used by these systems to identify assaults. If signatures are specified in advance, signature-based IDS would ideally detect all attacks with no false alarms. However, signature-based IDS are unable to detect zero-day attacks. In addition, creating a comprehensive database of attack signature is impractical (ÇİMEN, Sönmez, & İlbaş, 2021).

As opposed to signature-based intrusion detection systems, which focus on the system's attack behaviors, anomaly-based IDS create a profile of the system normal behavior, a deviation from the normal behavior will be considered an anomaly(Bostani & Sheikhan, 2017). Many anomaly-based IDS, however, currently suffer from high false positive rate due to the challenges in modeling the complete normal behavior and the difficulties in distinguishing between what constitute a normal and anomalous data (Kamalov, Moussa, Zgheib, & Mashaal, 2020). Despite these advancements, the integration of advanced learning methods with SOS-optimized TCP flows remains underexplored. This research proposes leveraging CNNs with SOS-optimized TCP flows to develop a robust IDS, addressing existing performance gaps and offering a scalable solution for modern network environments. The reminder of this paper is organized as follows: section 2 presents the related work, section 3 discusses the research methodology, section 4 discusses the dataset and experimental set-up while section 5 concludes the research.

related works

Network Intrusion Detection Systems (NIDS) have evolved significantly with the integration of deep learning and hybrid approaches to detect increasingly complex and stealthy cyber threats. Recent studies have explored the fusion of convolutional and recurrent neural architectures to enhance classification accuracy, tackle data imbalance, and ensure robustness in dynamic network environments.

Cao, Li, Song, Qin, and Chen (2022) proposed a hybrid NIDS model that combines Convolutional Neural Networks (CNN) and Gated Recurrent Units (GRU) to improve detection accuracy, particularly in multi-class intrusion scenarios. Their approach integrates ADASYN and RENN for class balancing and applies Random Forest with Pearson correlation for feature selection. The model leverages spatial and temporal dependencies in network traffic through CNN and GRU, achieving enhanced performance on imbalanced datasets.

Nguyen and Watabe (2023) developed A Method for Network Intrusion using Flow Sequence and BERT framework. This study utilizes sequences of network flows and BERT framework to enhance domain adaptation capabilities of NID. Early empirical results indicate improved performance compared to prior approaches, offering a novel method for constructing robust intrusion detection systems.

Du, Yang, Hu, and Jiang (2023) proposed a model for IDS which targets IIoT network environments by integrating CNNs with Long Short-Term Memory (LSTM) networks. This deep learning-based architecture effectively captures both spatial and sequential features in network traffic data. The model demonstrated high accuracy and low false alarm rates on benchmark datasets like KDDCUP99, NSL-KDD, and UNSW-NB15, making it suitable for real-time detection in large-scale IIoT deployments.

In a related effort, a Hybrid Deep-Learning Network Intrusion Detection System (HDLNIDS) was proposed by Qazi, Faheem, and Zia (2023) used a Convolutional Recurrent Neural Network (CRNN) structure with CICIDS-2018 data. This model emphasizes layered feature extraction using CNNs and deep recurrent networks to improve threat detection. The system achieved 98.9% average accuracy, outperforming conventional detection approaches. Shi, Han, and Cui (2023) proposed a Multimodal Hybrid Parallel Network (MHPN) to address the limitations of single-modal NIDS models. This architecture extracts features from both statistical and payload-level modalities using CNN and LSTM in a dual-branch design. Feature fusion and classification

Corresponding author: Yakubu Adah
adahyakubu@gmail.com
Department of Computer Science, Nile University of Nigeria, Abuja, Nigeria.

JOURNAL OF SCIENCE TECHNOLOGY AND EDUCATION 13(3), SEPTEMBER, 2025
E-ISSN: 3093-0898, PRINT ISSN: 2277-0011; Journal homepage: www.atbuftejoste.com.ng

using the CosMargin classifier led to impressive detection accuracy of 99.98% on ISCX-IDS 2012 and CIC-IDS-2017, demonstrating the benefit of multimodal analysis .

Finally, Talukder et al. (2023) developed a hybrid machine learning and deep learning model for NIDS using SMOTE for data balancing and XGBoost for feature selection. The model achieved 100% accuracy on CIC-MalMem-2022 and 99.99% on KDDCUP'99, showing no signs of over fitting. Their study emphasizes the importance of combining ML and DL techniques for scalable and dependable intrusion detection.

Overall, these works reflect a strong trend toward hybrid, deep-learning-based, and multi-modal solutions to meet the growing complexity of network threats. Common themes include addressing data imbalance, improving feature representation, and ensuring generalizability across datasets.

METHODOLOGY

Convolutional Neural Networks (CNN) consist of three primary layers: input, hidden, and output. Designed for solving complex problems, CNNs are increasingly applied in network traffic classification due to their ability to self-optimize through iterative learning. This study proposes a novel method that utilizes CNN in conjunction with the Symbiotic Organism Search (SOS) algorithm for intrusion detection. Network flow features specifically packet and byte counts was be captured using Wireshark and treated as time-series data. The preprocessing steps include:

1. Extraction of all statistical features from the network data
2. Selection of key features (packets, bytes, class label)
3. Data cleaning by removing empty fields
4. Optimization using the SOS algorithm
5. Feeding the optimized data into the CNN

Classification

The CNN configuration for this experiment includes a 70/30 train-test split, 100 epochs, batch size of 500, 12 hidden nodes, and two hidden layers each with 16 neurons.

Datasets

1. USTC-TFC2016 Dataset: Collected in real-time, this 3.71GB dataset includes both malware and benign traffic, with 10 categories each. Packet extraction was done using Wireshark.
2. ISCX VPN-non VPN Dataset: Comprising 28GB of data captured using Wireshark and TCP dump, this dataset contains 14 classes of traffic (e.g., chat, email, file transfer, with and without VPN).
3. LBNL/ICSI Dataset: Featuring over 100 hours of traffic from thousands of hosts, this dataset is used for binary classification (normal vs abnormal). As raw packet data is not available, only flow sizes (packets and bytes) were used in the second phase of experimentation.

This framework aims to improve traffic classification accuracy using optimized flow data and deep learning techniques.

PERFORMANCE EVALUATION METRIC

The evaluation metrics are defined as follows:

1. **Accuracy**: This is expressed as:
$$\text{Accuracy} = \frac{(\text{TP} + \text{TN})}{(\text{TP} + \text{TN} + \text{FP} + \text{FN})} \quad (1)$$
2. **Precision**: This is expressed as:
$$\text{Precision} = \frac{(\text{TP})}{(\text{TP} + \text{FP})} \quad (2)$$
3. **Recall**: This is expressed as:
$$\text{Recall} = \frac{(\text{TP})}{(\text{TP} + \text{FN})} \quad (3)$$

RESULT AND ANALYSIS

Using the CNN model with the first dense layer of 135, second dense layer of 90, last dense layer of 1, with the epochs=100, and batch_size=200, the Training loss VS Epochs is shown in Fig. 1.

Corresponding author: Yakubu Adah
adahyakubu@gmail.com
Department of Computer Science, Nile University of Nigeria, Abuja, Nigeria.

JOURNAL OF SCIENCE TECHNOLOGY AND EDUCATION 13(3), SEPTEMBER, 2025
E-ISSN: 3093-0898, PRINT ISSN: 2277-0011; Journal homepage: www.atbuftejoste.com.ng

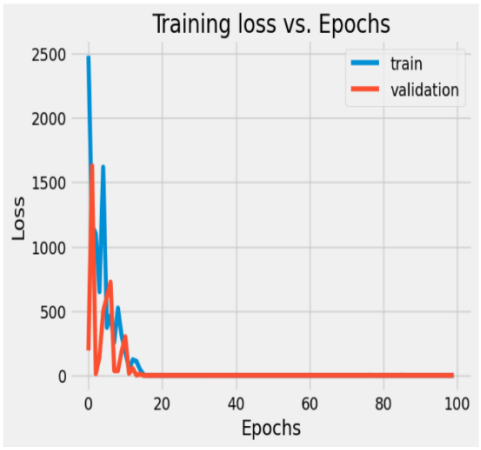

Fig1. Training loss VS Epoch of CNN.

In Fig. 1, for the training and validation as the epochs approached 20, the loss declined close to zero. This showed an excellent training based on the trained dataset Again, Fig. 2, showed the Training Accuracy VS Epochs for the trained dataset.

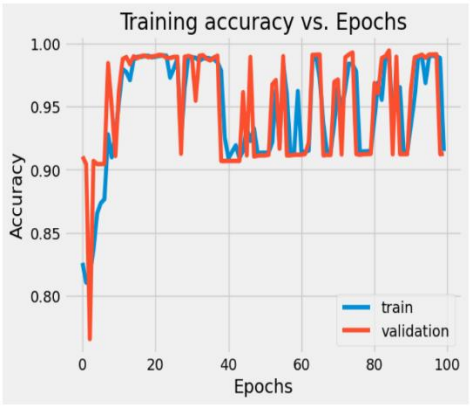

Fig. 2: Training Accuracy VS Epochs of the CNN

Furthermore, the convolutional neural network (CNN) model achieved a high accuracy of 91.27%, indicating that the model correctly classified a substantial proportion of the data. This means the CNN has learned the general patterns and features of the data well, making it effective for the classification task. Even though the accuracy was high, the F1 score of 0.5563 which is a balance between precision and recall, means it could still be fine-tuned to achieve better balance between these two metrics. Furthermore, the precision score of 0.9119 indicates that, when the model predicted a positive class (class 1), it was correct 91.19% of the time. This high precision suggests that false positives are relatively rare, meaning the model is quite accurate when it makes positive predictions. Again, the model's recall of 1.0 is perfect, meaning that the model correctly identified all instances of class 1. This is an outstanding result, indicating that the model does not miss any positive instances.

The combination of the SOS algorithm and CNN has demonstrated a significant improvement in both accuracy and performance compared to typical standalone CNN model. The SOS algorithm, known for its capability to optimize complex problems by mimicking the symbiotic relationship between organisms, likely played a key role in fine-tuning the hyperparameters and optimizing the CNN architecture. This optimization resulted in high precision and recall, making the model highly effective in classifying instances from both classes in the datasets under investigation.

Overall, this research had the final accuracy of 99.19% and precision of 99.82% which indicated that the model is highly effective in making correct predictions, especially for class 1. The model's precision is particularly noteworthy, as it ensures that predictions for class 1 are almost always correct. Also, the high recall of 99.28% for class 1 showed that the model is very good at capturing nearly all instances of class 1, minimizing false negatives.

However, the slight drop in recall compared to precision suggests that a few class 1 instances are still being missed, although a very small number. Despite the performance differences between the two classes, the misclassification rate for class 0 is very low (only 90 misclassified out of 5406), and class 1, although showing a slightly higher misclassification rate (367 misclassifications), still performs excellently with a high number of correct classifications (50792). This shows that the model has achieved a good balance between the two classes, without overfitting to one class, hence well fitted for this purpose.

Corresponding author: Yakubu Adah
adahyakubu@gmail.com
Department of Computer Science, Nile University of Nigeria, Abuja, Nigeria.

JOURNAL OF SCIENCE TECHNOLOGY AND EDUCATION 13(3), SEPTEMBER, 2025
E-ISSN: 3093-0898, PRINT ISSN: 2277-0011; Journal homepage: www.atbuftejoste.com.ng

Classification Report

In this section, the performance of the model in terms of Precision, Recall and F1-Score across datasets.

Table 1. Result

Datasets	Precision	Recall	F1-Score
UDTC-TFC2016	95	96	96
ISCX	98	97	97
LBNL/ICSI	99	98	98

Table 2: Performance Comparison

Technique	Accuracy	F1-Score	Precision	Recall
CNN	91.27%	0.5563	-	-
SOS-CNN	**99.19%**	**0.9772**	**99.82%**	**99.28%**

The values in Table 1 demonstrate that the model consistently achieves high performance across all datasets, with particularly strong results on the LBNL/ICSI dataset.In table below, the performance of our proposed model was compared with the traditional standalone CNN deep learning technique implemented to improve IDS.

CONCLUSION

The combination of Convolutional Neural Network (CNN) model with the Symbiotic Organisms Search (SOS) proved to be highly effective, addressing class imbalance issues and optimizing model parameters to achieve superior performance in both classes. This model demonstrated not only high accuracy but also impressive precision and recall, making it well-suited for real-world classification tasks where reliable predictions are essential. Therefore, the combination of the Convolutional Neural Network (CNN) model with the Symbiotic Organisms Search (SOS) algorithm has demonstrated remarkable performance in the classification task.

REFERENCES

Bostani, Hamid, & Sheikhan, Mansour. (2017). Hybrid of anomaly-based and specification-based IDS for Internet of Things using unsupervised OPF based on MapReduce approach. *Computer Communications, 98*, 52-71.

Cao, Bo, Li, Chenghai, Song, Yafei, Qin, Yueyi, & Chen, Chen. (2022). Network intrusion detection model based on CNN and GRU. *Applied Sciences, 12*(9), 4184.

ÇİMEN, Fethi Mustafa, Sönmez, YUSUF, & İlbaş, MUSTAFA. (2021). Performance Analysis of Machine Learning Algorithms in Intrusion Detection Systems. *Düzce Üniversitesi Bilim ve Teknoloji Dergisi, 9*(6), 251-258.

Du, Jiawei, Yang, Kai, Hu, Yanjing, & Jiang, Lingjie. (2023). NIDS-CNNLSTM: Network intrusion detection classification model based on deep learning. *IEEE Access, 11*, 24808-24821.

Kamalov, Firuz, Moussa, Sherif, Zgheib, Rita, & Mashaal, Omar. (2020). *Feature selection for intrusion detection systems.* Paper presented at the 2020 13th International Symposium on Computational Intelligence and Design (ISCID).

Nguyen, Loc Gia, & Watabe, Kohei. (2023). *A Method for Network Intrusion Detection Using Flow Sequence and BERT Framework.* Paper presented at the ICC 2023-IEEE International Conference on Communications.

Qazi, Emad Ul Haq, Faheem, Muhammad Hamza, & Zia, Tanveer. (2023). HDLNIDS: hybrid deep-learning-based

Corresponding author: Yakubu Adah
adahyakubu@gmail.com
Department of Computer Science, Nile University of Nigeria, Abuja, Nigeria.

network intrusion detection system. *Applied Sciences, 13*(8), 4921.

Shi, Shuxin, Han, Dezhi, & Cui, Mingming. (2023). A multimodal hybrid parallel network intrusion detection model. *Connection Science, 35*(1), 2227780.

Talukder, Md Alamin, Hasan, Khondokar Fida, Islam, Md Manowarul, Uddin, Md Ashraf, Akhter, Arnisha, Yousuf, Mohammand Abu, . . . Moni, Mohammad Ali. (2023). A dependable hybrid machine learning model for network intrusion detection. *Journal of Information Security and Applications, 72*, 103405.

.

Corresponding author: Yakubu Adah
adahyakubu@gmail.com
Department of Computer Science, Nile University of Nigeria, Abuja, Nigeria.