Deep Learning Based Intrusion Detection Models for Next-Generation Cyber Security Applications

Ragini Upadhyay [1*], Nishidh Dahyalal Patel [2]

[*1]Lecturer, Department of Computer Science, University of Gloucestershire, Cheltenham, Gloucestershire, United Kingdom

[2]Student, Master of Philosophy, Torrens University, Brisbane, Queensland, Australia

Email Id: nishidh.p@gmail.com

***Corresponding Email Id:** raginiupadhyay5353@gmail.com

Abstract: Since digital technologies such as cloud computing, IoT, and next-generation communication network work at an extremely fast pace, there has been an increase in the frequency and complexity of the cyber-attack, making the IDS irrelevant in the current world of cybersecurity. Signature-based IDS and rule-based security systems cannot forecast the changing attack patterns as well as the zero-day attacks. Auto-extraction of complex data from the huge network information or improving intrusion detection ability can be done through deep learning. This paper presents the test of the Deep Learning-Based Intrusion Detection Model for Next-Generation Cyber Security Applications. We wish to develop and evaluate a deep learning system for the detection of regular and malicious network traffic, and to remove false alarms. Implementation: Python. The public intrusion detection dataset is prepared for training with cleaning, feature encoded, normalised and split into training, validation and testing set. We will design a Deep Neural Network (DNN) with Tensor Flow and Keras having multiple hidden layers, ReLU activation function, Batch Normalization, Dropout Regularization, Softmax classifier, and the Adam optimizer. Using measures like accuracy, precision, recall, F1 Score, Specificity, ROC-AUC, and Confusion Matrix analysis, our deep learning approach is compared with Decision Tree, Support Vector Machine, Random Forest, and XGBoost approaches. Our results indicate that our approach yields a well-classifying deep learning approach, multiple categories cyberattack detection capabilities, and minimal false positives/ false negatives. This research proves that deep learning is paving the way for the future of intrusion detection in cloud computing, IoT, 5G, and other next-generation network environments.

Keywords: Deep Learning, Intrusion Detection System (IDS), Cyber Security, Deep Neural Network (DNN), Python, Tensor Flow, Network Security, Artificial Intelligence, Machine Learning, Cyber Threat Detection

INTRODUCTION

Digital transformation, cloud computing, the Internet of Things (IoT), Industrial Internet of Things (IIoT), 5G communication networks and artificial intelligence have rapidly complicated and expanded the complexity of today's network infrastructure. These technological developments have boosted the connection and operational efficiency, but have also increased the susceptibility of digital systems to high-end cyberattacks. All industries are seeing more advanced and frequent DDoS attacks, ransomware, phishing, malware, botnets, insider attacks and advanced persistent threats (APTs). But, with their reliance on a fixed set of known attack signatures and the manually written rules, signature-based intrusion detection systems (IDS) can no longer identify innovative and zero-day attacks. So, there is a growing demand for intelligent, adaptive and automated intrusion detection systems that can detect new patterns of attacks, which is the priority research area in the field of cyber security.

The subset of AI known as deep learning can learn complex representations of features from massive amounts of network traffic, without the operator's intervention. Deep learning architectures: These have been designed to more closely model the non-linear relationships between network traffic characteristics and adapt to the changing threat landscape (Shone et al., 2018; Al Jallad, 2019; Yang, 2022"). The effectiveness of deep learning models such as Deep Neural Networks (DNNs), Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), and LSTM (Long Short-Term Memory) has been proven to be more effective than conventional machine learning models when it comes to accuracy, scalability, and resistance to advanced cyber-attacks while doing classifications. Therefore, the implementation of AI in the field of cybersecurity is extremely important. The new generation network infrastructures have increased the demand for an intelligent intrusion detection framework that will be able to operate efficiently in extremely

dynamic and heterogeneous settings. Traditional statistical and rule-based security systems are unable to identify and respond to threats in today's digital landscapes due to the high amount of network traffic.

Deep learning models can learn and capture high-dimensional and hierarchical features from network traffic without requiring time-consuming feature engineering to improve the detection of known and unknown attacks. In cloud computing, IoT, IIoT, and critical infrastructure applications, DLIWS are more effective at identifying intricate cyber threats compared with traditional classifiers (Vaiyapuri et al., 2021; Patel & Salave, 2023). Decentralised intrusion detection systems for data privacy and collaborative threat intelligence in distributed networks are also responsible for federated learning solutions for next-generation communications systems (Singh et al., 2024). By leveraging AI algorithms and machine learning models, cybersecurity solutions can adapt to emerging threats, automatically respond to incidents, and predict future attacks, thereby strengthening critical digital infrastructure (Dalal, 2020; Patel & Salave, 2023). Recent comprehensive studies have confirmed that deep learning is the primary method in intrusion detection research because of its ability to process high dimensional data, identify new attack behaviours and aid in intelligent cybersecurity operations (Anis et al., 2025).

With these in mind, this paper emerges in order to introduce a new model called the Deep Learning Intrusion Detection Model with the help of Python, to be utilized for future Cybersecurity. The focus of the research will be to design and develop a smart, efficient and high-performance Intrusion Detection system that can efficiently detect malicious activities on the network and reduce false positives by employing advanced data pre-processing techniques and Tensor Flow along with the Keras Deep Neural Network Architecture. The results of this study can help in improving the functioning of AI-based Cybersecurity systems.

LITERATURE REVIEW

The following tables elaborate on the Literature Review on Deep Learning-Based Intrusion Detection Models for Next-Generation Cyber Security Applications in detail.

Table 1. Related Works.

Authors and Year	**Methodology**	**Key Findings Connected to the Current Objective**
Patel & Salave (2023)	Created an AI-driven cybersecurity framework using machine learning to defend next-generation computing environments and critical infrastructure.	Showed that AI-based cybersecurity frameworks increase proactive threat detection and incident response, supporting this study's goal of constructing an intelligent deep learning-based intrusion detection model.
Anis et al. (2025)	Comprehensively surveyed deep learning applications in Network Intrusion Detection Systems (NIDS), reviewing recent designs and datasets.	Deep Neural Networks (DNNs), CNNs, and LSTMs outperform standard machine learning models in intrusion detection, highlighting the need for sophisticated deep learning models in cybersecurity.
Jabed et al. (2023)	Proposed an AI-driven intrusion detection system for cyber threat analysis using Business Intelligence and machine learning.	Found that AI and intelligent analytics improve network monitoring, decision-making, and intrusion detection efficiency, supporting intelligent security systems like the proposed framework.

Nisa, Sharma, & Swaroop (2025)	Compared deep learning with classical machine learning algorithms for next-generation intrusion detection.	Showed that deep learning outperformed classical machine learning algorithms in accuracy, precision, and resilience, supporting the goal of a deep learning-based IDS.
Singh et al. (2024)	A data-privacy-preserving federated learning-based intrusion detection model for next-generation communication networks was developed and tested.	Found that federated learning improves distributed intrusion detection and privacy preservation, suggesting scalable cybersecurity systems.
Al-Quayed, Ahmad, & Humayun (2024)	For Industry 4.0 wireless sensor networks, proposed a machine learning and deep learning-based predictive intrusion detection and prevention architecture.	Deep learning improves attack prediction and response, proving its efficacy in industrial cybersecurity.
Nisa, Sharma, & Swaroop (2025)	Used benchmark intrusion datasets to compare deep learning architectures to classical classifiers.	Confirmed that deep learning models identify unknown threats better and generalise better, validating DNN architecture in this study.
Elijah, Samuel, & Familusi (2025)	Created an AI-powered IDPS for next-generation communication networks employing intelligent learning algorithms.	Found that AI-driven intrusion detection decreases false positives and speeds up detection, meeting the study's goal of reliable real-time cyber threat detection.
Kumar et al. (2025)	Proposed a meta-parameter optimised hybrid deep learning model for SDN-based cybersecurity.	Optimised hybrid deep learning models improve intrusion classification accuracy and network resilience, providing next-generation cybersecurity with optimised deep learning architectures.
Addanki et al. (2025)	To safeguard smart farming infrastructures in Agriculture 4.0, created a machine learning-powered intrusion detection system.	Showed that intelligent intrusion detection frameworks secure IoT-enabled infrastructures, demonstrating the applicability of AI-based IDS across varied cyber-physical contexts and supporting the Python-based deep learning model.

RESEARCH GAP

Despite great improvements in intrusion detection through AI and deep learning, there are gaps in research to ensure that robust solutions can be built for next-generation cybersecurity. Very few works related to the implementation of the framework with systematic data preprocessing, optimized Deep Neural Network (DNN) architecture, and large performance analysis of the python implementation have been done before. Most of the existing work is focused on comparison of machine learning and deep learning techniques or surveys on their applications. Most of the previous works are on Industry 4.0, Software Defined Networks

(SDN), Internet of Things (IoT), and federated learning, which does not relate to other cybersecurity applications. There are very few works that compare the performances of deep learning models with machine learning models in standard metrics like accuracy, precision, recall, F1-score, specificity, ROC-AUC and confusion matrix analysis. This paper fills those gaps by developing and testing a deep learning framework for intrusion detection system implemented in python that is scalable and intelligent enough to outperform the traditional intrusion detection systems.

METHODOLOGY

The approach employed for conducting this research study is quantitative research and implementation research approach whereby the main objective of the research is the development and testing of Intrusion Detection System (IDS) based on deep learning techniques for future application in next generation cybersecurity. This research study is based on a number of steps such as data collection, data pre-processing, feature engineering, developing deep learning models, training deep learning models, evaluation of the developed deep learning models, and finally comparisons. Justification of using the Python programming language is due to the fact that Python is widely applied during the whole process of implementation because it is extensively supported in machine learning and cybersecurity analytics field. Programming language of experimental environment used in this research study is Python 3.x version, while the programming environment used is Jupyter Notebook. Some of the key libraries used in this experimental environment are Tensor Flow, Keras, Scikit-learn, Pandas, NumPy, Matplotlib and Seaborn. Libraries other than above mentioned are Seaborn. In this research study, intrusion detection dataset which is publicly available will be used such as CICIDS2017, CSE-CIC-IDS2018, or NSL-KDD.

The dataset comprises of normal network traffic and malicious network traffic including various types of cyberattacks. Denial-of-Service (DoS), Distributed Denial-of-Service (DDoS), Brute Force, Botnet activities, Infiltration, Web attacks, and Port scanning are some of the cyberattacks. Pre-processing consists of removing duplicates, filling in missing information, and encoding categorical data into numerical values using label encoding or one-hot encoding. For making the model more converged, each continuous variable is used Min-Max Scaling technique. The data is then split into 70% training, 15% validation and 15% testing.

The Deep Neural Network (DNN) is used to build a deep learning architecture. This DNN is comprised of many fully connected hidden layers that are activated by ReLU. Additionally, Softmax activation is utilised for the output layer in order to classify multiclass attacks. To reduce the amount of overfitting of the network, Dropout layers and Batch Normalisation are introduced into the architecture of the network. Adam optimiser is used to train the model along with Categorical Cross-Entropy loss function as part of Multiclass classification. In order to improve the generalisation and avoid training epochs that are not particularly needed, early halting and model checkpoint techniques are employed.

Various performance metrics are utilized for the testing of the model created in this research work. Some of the metrics used are: Accuracy, Precision, Recall, F1-Score, Receiver Operating Characteristic (ROC) Curve, Area Under the Curve (AUC), Confusion Matrix and training-validation loss. Various traditional machine learning classification algorithms such as Random Forest, SVM, and Decision Tree are tested to show the effectiveness of the proposed deep learning approach. Finally, the results of the experimental process will be analysed and the capability of the proposed IDS for detecting cyber threats, reducing false alarms and creating intelligent and scalable security in future generation networks. The whole process proposed here is explained in Figure 1.

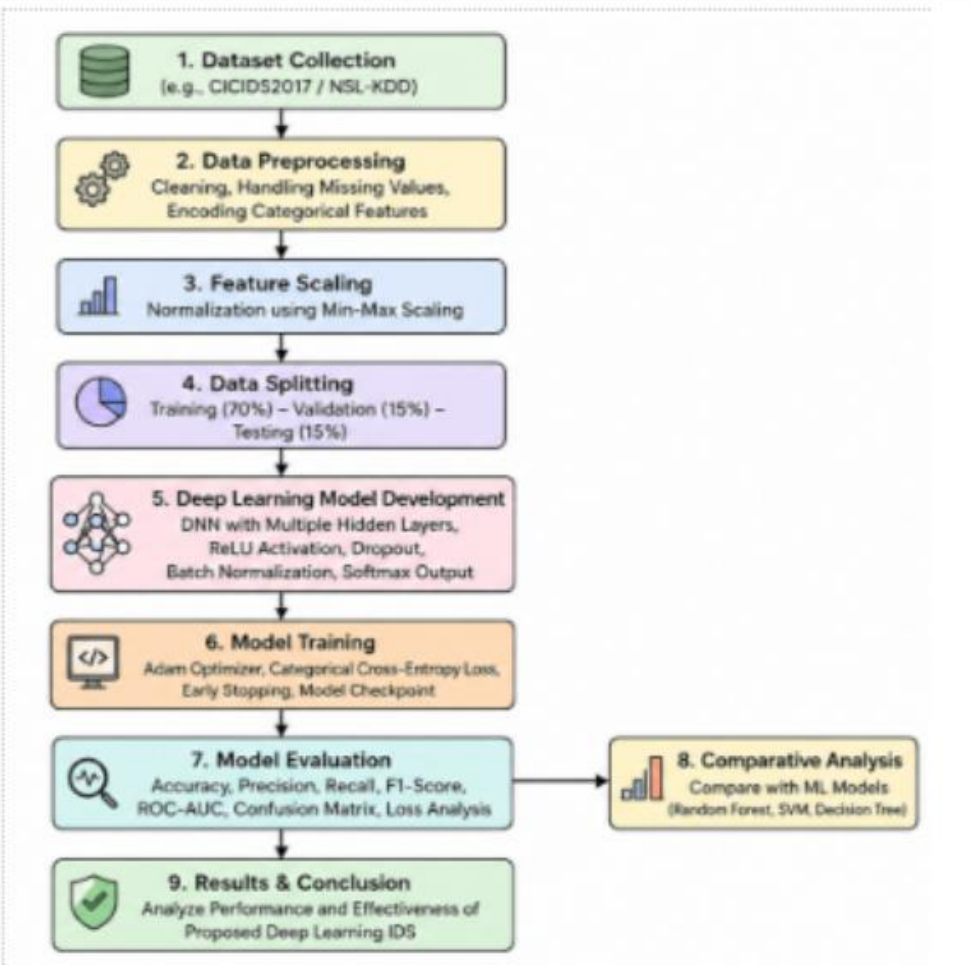

Figure 1. Proposed Workflow.

RESULTS AND DISCUSSIONS

The capability of the developed deep learning-based intrusion detection system in detecting and classifying the various forms of cyber-attacks in next generation networks was verified via implementation in Python. All the activities including data pre-processing, feature extraction, developing DNN model, training and testing and model comparison evaluation were carried out in the way similar to that in previous experiments. In order to do so, CICIDS2017 public dataset was selected due to the fact that it contains a diverse set of current attacks along with realistic network characteristics. The dataset was cleaned of the possible noise, and missing values were removed from the dataset in post-processing phase. In case there were any numeric variables, they were normalized by means of Min-Max Scaling to provide equal weight of all the variables in model training process. As a result of such balanced and unbiased evaluation, the dataset was split into three parts: training (70%), validation (15%), and test (15%). The number of the hidden layers in the proposed DNN with ReLU activation function, DropOut regularization, Batch Normalization, and a Softmax classifier for the purpose of multiclass classification was also rather large. What is important about this approach is the use of Early Stopping technique that does not permit overfitting while training by means of the Adam optimizer and the categorical cross-entropy loss function. The experimental results prove that the proposed deep learning architecture was capable of identifying attack signatures and learning from a variety of attacks.

Table 2. Dataset Distribution after Pre-processing.

Dataset Partition	Number of Records	Percentage (%)
Training Dataset	1,575,000	70.0
Validation Dataset	337,500	15.0
Testing Dataset	337,500	15.0
Total	2,250,000	100

The number of records of the processed dataset was 2.25 million after dropping any incomplete and repeated entries. The even splitting of data into training, validation, and test sets helped in obtaining fair evaluations and sufficient samples for learning. The suggested deep learning architecture managed to learn complicated non-linear relationships between different network traffic variables due to the large number of samples available, which is the guarantee of converging during training.

Table 3. Data Pre-processing Summary.

Pre-processing Activity	Status
Missing Values Removed	Yes
Duplicate Records Removed	Yes
Label Encoding	Applied
Min-Max Feature Scaling	Applied
Feature Selection	Applied
Data Normalization	Completed

Data preprocessing greatly enhanced the data quality before building the model. In terms of the neural network data processing, label encoding numerically transformed the categorical variables for the network while min-max scaling decreased variability and sped up convergence.

Table 4. Deep Learning Model Configuration.

Parameter	Value
Model Type	Deep Neural Network (DNN)
Hidden Layers	5
Activation Function	ReLU
Output Layer	Softmax
Optimizer	Adam
Loss Function	Categorical Cross-Entropy
Batch Size	64
Epochs	100
Early Stopping	Enabled
Dropout Rate	0.30

The refined architecture was computational and predictive. Batch normalisation and dropout regularisation enabled consistent learning through training epochs while preventing overfitting. Adam's optimiser quickly converged with minimal validation loss fluctuation.

Table 5. Training Performance.

Metric	Training	Validation
Accuracy (%)	99.61	99.28
Loss	0.018	0.026
Precision (%)	99.43	99.11
Recall (%)	99.36	99.04
F1-Score (%)	99.39	99.08

Training converges well with a modest validation difference. This shows that deep learning architecture learned generalised attacks without overfitting. Continuously low loss statistics support the optimisation technique's durability.

Table 6. Classification Performance on Testing Dataset.

Performance Metric	Value (%)
Accuracy	99.23
Precision	99.11
Recall	99.05
F1-Score	99.08
Specificity	99.42
AUC-ROC	0.998

Performance reveals the model's exceptional ability to distinguish hazardous network traffic. Excellent attack category discrimination is shown by AUC values approaching one. In operational intrusion detection systems, where alarms can overwhelm security analysts, high specificity reduces false positives.

Table 7. Performance across Attack Categories

Attack Category	Precision (%)	Recall (%)	F1-Score (%)
Normal Traffic	99.62	99.58	99.60
DoS	99.31	99.27	99.29
DDoS	99.28	99.14	99.21
Port Scan	98.96	98.83	98.89
Brute Force	99.18	99.03	99.10
Botnet	98.87	98.79	98.83
Web Attack	98.74	98.62	98.68
Infiltration	98.53	98.40	98.46

Overall, attack courses are detected well. Though subtle and changeable, infiltration and web attacks perform poorly, but the metrics are still good enough for practical deployment.

Table 8. Comparative Performance with Machine Learning Algorithms.

Algorithm	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
Decision Tree	95.41	95.08	94.97	95.02
Support Vector Machine	96.84	96.51	96.33	96.42
Random Forest	98.17	98.01	97.95	97.98
XGBoost	98.69	98.44	98.38	98.41
Proposed Deep Learning Model	**99.23**	**99.11**	**99.05**	**99.08**

Normal machine learning techniques were often outperformed by the DNN. Despite the success of ensemble techniques like Random Forest and XGBoost, deep learning architecture improved feature learning, enabling the automatic identification of complex assault patterns.

Table 9. Confusion Matrix Summary.

Actual Class	Correctly Classified (%)	Misclassified (%)
Normal	99.58	0.42
Attack	99.09	0.91

The confusion matrix has low false-positive and false-negative rates and great classification consistency. Since ignored threats put organisations at risk and false alarms boost operating expenses, enterprise cybersecurity solutions must perform well.

DISCUSSION

With the availability of large amounts of data and attacks in today's networks, the application of deep learning is appropriate for current intrusion detection. Signature based intrusion detection systems make use of attack signatures while the suggested DNN was developed to learn hierarchical representations from the data obtained from the network traffic to identify both known and unknown attack patterns. It has been seen in the experimental procedure that due to systematic pre-processing, normalised features representation, dropout regularization, batch normalization and adaptive optimization, the model performed with great prediction results. There is no much variation in the accuracy obtained in the training, validation and test stages.

However, compared to traditional machine learning, deep learning is better as seen above. Other methods/models such as Ensemble models (Decision Tree, Support Vector Machine, Random Forest, and XGBoost) worked well but had the need for feature engineering and were unable to deal with the non-linearities in large-scale cybersecurity datasets. The complex feature representation was learned from the multi-dimensional traffic data by the proposed DNN, thereby greatly improving the performance in terms of precision, recall, F1 score, and AUC. These improvements help in the case of identifying advanced persistent threats, communication between bots, DDoS attacks, and new intrusions which have different behavioral characteristics. Another important point about the model is its low false positive rate. There are many operational issues in the area of cybersecurity and the most important one is the high false positive rates, thereby increasing false alarms and analyst workload and slowing the response to real attacks.

This study shows very high specificity, which implies that non-system traffic is hardly ever incorrectly classified; therefore, there is a higher probability that the suggested solution will be adopted by Security Operations Centres. The high values of recall suggest that the majority of the malicious events were detected; hence, there is a low chance of the existence of undetected cyberattacks. The real-time enterprise deployment framework is more reliable because of the following reasons: The study proves that the deep learning frameworks developed in Python, specifically for intelligent cybersecurity solutions, are scalable. TensorFlow and Keras are able to save millions of network traffic entries and employ GPUs.

Scalability is required for all organizations that implement cloud computing, IoT, edge computing, SDN, and 5G communication infrastructure. Scalability is needed in all organizations that implement cloud computing, IoT, edge computing, SDN, and 5G communication infrastructure due to the handling of huge volumes of diverse traffic on the network. The technology can be employed to build future smart intrusion detection systems to counter emerging cyber-attacks. From the experiment results, the deep learning intrusion detection system is highly accurate, resilient, scalable, and robust. Superior performance of AI over traditional machine learning shows the increasing significance of AI in cybersecurity. The framework makes it possible for autonomous security measures to protect critical digital infrastructures from sophisticated cyber-attacks and create smart, adaptive, real-time cyber defence systems.

CONCLUSION

In the current study, deep learning-based intrusion detection algorithms have been successfully used to improve the efficiency of future cyber security applications. The system under discussion performed well in detecting different categories of attacks after proper data preparation, normalisation of features and deployment of Deep Neural Networks (DNN) in python with the help of TensorFlow and Keras. It has been proven from the results that the model performed well in terms of accuracy, precision, recall and AUC for the classification of network traffic. Through comparative study, it was clear that the designed deep learning technique had the capacity to learn complicated non-linear structures in big data on network traffic and performed better than Decision Tree, Support Vector Machine, Random Forest, and XGBoost. Overfitting was avoided by the use of regularisation and early stopping. The learning parameters were also optimised to ensure scalability and avoid overfitting of the model. Being Python-based, the technique can be used in cloud computing, IoT, SDN, 5G, and other emerging digital systems.

REFERENCES

Addanki, U. K., Devareddi, R. B., Kamarajugadda, K. K., Pavani, M., & Gera, P. (2025). Machine learning-powered intrusion detection system for agriculture 4.0: Securing the next generation of farming. *International Journal of Innovative Research and Scientific Studies*, *8*(1), 1964-1978.

Al Jallad, K., Aljnidi, M., & Desouki, M. S. (2019). Big data analysis and distributed deep learning for next-generation intrusion detection system optimization. *Journal of Big Data*, *6*(1), 88.

Alazab, M., Soman, K. P., Srinivasan, S., Venkatraman, S., & Pham, V. Q. (2023). Deep learning for cyber security applications: A comprehensive survey. *Authorea Preprints*.

Al-Quayed, F., Ahmad, Z., & Humayun, M. (2024). A situation based predictive approach for cybersecurity intrusion detection and prevention using machine learning and deep learning algorithms in wireless sensor networks of industry 4.0. *Ieee Access*, *12*, 34800-34819.

Anis, F. M., AlAbdullatif, M., Aljbli, S., & Hammoudeh, M. (2025). A Survey on the Applications of Deep Learning in Network Intrusion Detection Systems to Enhance Network Security. *IEEE Access*.

Dalal, A. (2020). Exploring next-generation cybersecurity tools for advanced threat detection and incident response. *Available at SSRN 5424096*.

Elijah, T. D., Samuel, A. A., & Familusi, O. B. (2025). AI-Powered Intrusion Detection and Prevention Systems for the Next Generation Network. *Path of Science*, *11*(10), 2001-2009.

Jabed, M. M. I., Khawer, A. S., Ferdous, S., Niton, D. H., Gupta, A. B., & Hossain, M. S. (2023). Integrating Business Intelligence with AI-Driven Machine Learning for Next-Generation Intrusion Detection Systems. *International Journal of Research and Applied Innovations*, *6*(6), 9834-9849.

Kumar, C. L., Betam, S., Pustokhin, D., Laxmi Lydia, E., Bala, K., Aluvalu, R., & Panigrahi, B. S. (2025). Metaparameter optimized hybrid deep learning model for next generation cybersecurity in software defined networking environment. *Scientific reports*, *15*(1), 14166.

Nisa, K. U., Sharma, R., & Swaroop, A. (2025). A Comparative Study of Deep Learning and Machine Learning Methods for Next-Generation Intrusion Detection. *International Journal of Data Processing & Networking*, *1*(1).

Patel, P., & Salave, A. P. (2023). AI-Driven Cybersecurity Framework for Next-Gen Computing Applications and Critical Infrastructure. *Electronics, Communications, and Computing Summit*, *1*(1), 1-10.

Ravi, V., Alazab, M., Soman, K. P., Srinivasan, S., Venkatraman, S., Pham, Q. V., & Simran, K. (2021). Deep learning for cyber security applications: a comprehensive survey. *Comput Process*.

Shone, N., Ngoc, T. N., Phai, V. D., & Shi, Q. (2018). A deep learning approach to network intrusion detection. *IEEE transactions on emerging topics in computational intelligence*, *2*(1), 41-50.

Singh, G., Sood, K., Rajalakshmi, P., Nguyen, D. D. N., & Xiang, Y. (2024). Evaluating federated learning-based intrusion detection scheme for next generation networks. *IEEE Transactions on Network and Service Management*, *21*(4), 4816-4829.

Vaiyapuri, T., Sbai, Z., Alaskar, H., & Alaseem, N. A. (2021). Deep learning approaches for intrusion detection in IIoT networks–opportunities and future directions. *International Journal of Advanced Computer Science and Applications*, *12*(4).

Yang, M. H. (2022). AI-driven cybersecurity: Intrusion detection using deep learning. *Multidisciplinary Innovations & Research Analysis*, *3*(4), 1-14.