A Robust Hybrid Framework for Network Anomaly Detection: Leveraging LSTM-Based Deep Feature Extraction and KNN Classification with SMOTE Data Augmentation

Armish Ejaz
Roll no.
Department of Creative Technology

Zahara Muhammad
Roll no.
Department of Creative Technology

Romaisa Kanwal
Roll no.
Department of Creative Technology

Abstract
Network Anomaly Detection in the modern era of hyper-connectivity, as well as the Internet of Things, is the most important means for protecting against malicious invasions. But the effectiveness of the basic models is, in many cases, impaired as a result of high-dimensional space as well as extreme class imbalance. This paper introduces a complex hybrid model, which combines the Long Short-Term Memory networks for the deep extraction of features over time with the K-Nearest Neighbors for the classification task. The problem of imbalanced data variation in the number of net communications is addressed through the inclusion of the Synthetic Minority Over-sampling Technique in the preprocessing approach. The proposed approach combines the use of LSTM for the deep extraction of features in the high-dimensional space, which are furtherpassed to the robust KNN for classification in the latent space. The proposed approach produces a high accuracy of 98.87% in multi-class accuracy, which is significantly superior to the accuracy of the basic RNN.
Index Terms—Intrusion Detection System, Deep Learning, LSTM, KNN, SMOTE, Feature Engineering, Network Security

I. INTRODUCTION

The internet and computer networks are expanding very quickly. This implies that the amount of internet traffic is increasing and becoming complex. In one way, this has made it simple for people to communicate and exchange their data. However, in another way, it has increased the risks to network infrastructure.

A threat to computer networks and the internet is presented because of the current situations they face. The older security measures, such as firewalls, take a considerable amount of time to identify newer, more complex attacks. This is clear evidence that computer networks and the internet should have intelligent security solutions that can cope with changing scenarios.

Network intrusion detection is a big deal these days. Machine learning & deep learning are two means through which people are utilizing to attempt to detect these guys on the internet. They are very effective at looking for patterns in large amounts of information. They are also able to adapt once they spot different types of attacks.

The thing is, a lot of machine learning models are not so great because they require human input in deciding what they are searching for. They also assume that what they are viewing will remain the same. This is not true because the internet is always changing.

"Deep learning models aren't foolproof either." Many of them are just attempting to see if something is "bad" and so on. It doesn't really examine how things are linked. Network traffic is like a conversation, and it has to be understood that "it's a dialogue."

Network traffic data is a sequence of events that follow each other sequentially. It is greatly reliant on the concept of time. The reason is that attack patterns can evolve in packets/flows.

A Long Short-Term Memory network refers to a type of neural network that has the capability of learning what happens through time. This happens because of its capacity to remember information from a long time ago.

LSTM models work well in extracting information from a body of data like this. They are able to locate those things in a body of data, which will allow them to interpret it. This is very effective in intrusion detection systems. Data from network traffic, as well as Long Short-Term Memory, are relevant in intrusions.

Despite their numerous merits, deep learning models tend to be computationally expensive and lack interpretability if utilized for end-to-end classification tasks. In this regard, increasing attention has been directed towards combinations of deep learning and conventional machine learning for classification purposes. The K-Nearest Neighbors classifier is a remarkably simple and efficient distance-based classifier that can be very successful if it is applied to appropriate feature information.

II. LITERATURE SURVEY

Network anomaly detection is a very important process to keep our computer systems secure. The conventional approach for detecting intruders is inefficient to deal with new-style intrusions. Before, people utilized machine learning techniques such as decision trees and support vector machines to perform network anomaly detection. These techniques performed adequately. They needed people to create special features for them and they had a hard time dealing with complicated network traffic. Network anomaly detection is what helps us find problems, in our networks.

The field of learning is getting better and better. Researchers started looking into something called neural networks, especially Long Short-Term Memory models. They do a job of finding patterns in data that comes in a sequence. Research has found that Long Short-Term Memory models can learn what normal and abnormal traffic behavior looks like.. There is a problem, with using deep learning all the time. It can be very expensive to run. It is hard to understand

what is going on especially when you need to make decisions quickly in real time with Long Short-Term Memory models.
To get around these problems several researchers have suggested using models that bring together deep learning and traditional classifiers. For instance we can use LSTM to extract features and then use KNN to classify them, which has shown results and works well in different situations compared to using just one model. These hybrid approaches are helpful because LSTM is good at finding patterns and KNN is simple when it comes to making decisions. However, many current studies do not do a job of dealing with the issue of class imbalance, where attack traffic happens much less often, than normal traffic.

Intrusion detection is really important. Recent studies show that it is crucial to have a balance between learning and representing features in a smart way for intrusion detection to work well. Even though we have made some progress we still need to find a way to make intrusion detection systems that're simple and work well together to detect attacks correctly and do not give too many false warnings. Intrusion detection systems, like these would be very useful.
Motivated by these observations, this research proposes a hybrid LSTM–KNN framework that leverages temporal feature learning and robust classification to improve network anomaly detection performance.

III. Methodology

In this experiment, the problem of class imbalance in the dataset is solved with the help of the Synthetic Minority Over-sampling Technique, which is known as SMOTE. Class imbalance might be a problem in the performance of the model, especially in classification problems in which the minority class has fewer representatives. In this case, the minority class is k-NN-ified with the help of SMOTE.
There are the following steps of the SMOTE process.
The initial step consists of selecting the minority class examples within the original dataset. The examples correspond to the class with fewer instances, generally regarded as the cause of biased learning if not dealt with.
Second, to each sample of the minority class, the k-nearest points are obtained through a method of distance measurement, where k is given the value of 5. The aim is to determine the near data points to the minority class samples that will be used as a yardstick to create new samples.
Synthetic samples are created after identifying the nearest neighbors. New data points are created along the line segments connecting a minority sample and one of its nearest neighbors. A random factor controls the position of the synthetic sample between these two points to ensure variability, so that overfitting does not occur.
The generation of synthetic samples follows the SMOTE formula:

$$X_{\text{synthetic}} = X_i + \lambda(X_j - X_i)$$

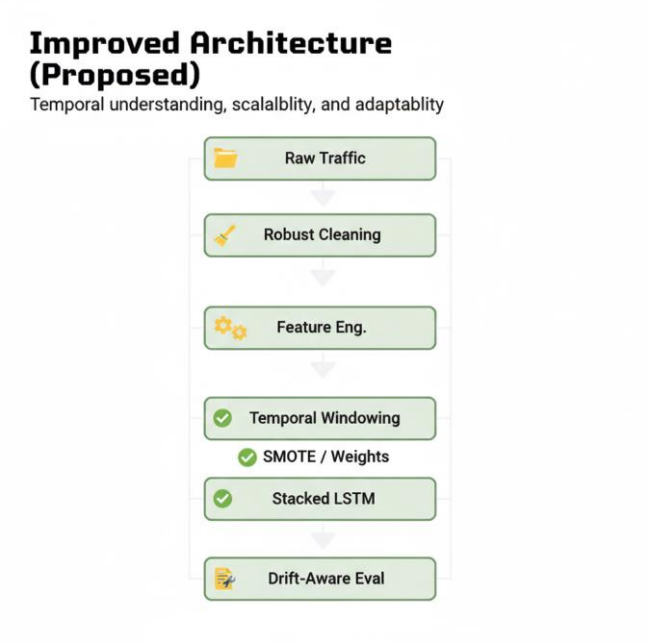
where Xi is a minority class instance, Xj is the nearest neighboring point, and the value of λ is between 0 and 1.
After that, the synthesized data is added to the original data set. The number of data points for the minority class raises and this improves class distribution without repeating data.
Lastly, the trained machine learning model is used on the balanced dataset. As the machine learning model is trained based on the balanced dataset, the learned accuracy improves because patterns associated with the minority class are easier to recognize since the dataset is well distributed.

IV. Model Architecture

Instead of looking at data points in isolation, our workflow focuses on context and long-term patterns.

- Foundation (Raw Traffic & Cleaning): In this phase, raw traffic on the networks is first recorded, and a process called “Robust Cleaning" is applied to them. This phase is even beyond the level of merely filtering out the data, with the goal of obtaining high-quality data free from noise, which would otherwise trigger an alert.
- The Intelligence Layer (Feature Engineering & Temporal Windowing): The system goes through data trait selection, followed by application of the temporal windowing method. Temporal windowing method is an improvement over the given research paper. The system has the capability to ‘remember’ what happened a few minutes or seconds back, since events form a story and not a list of events.
- Balancing the Scales (SMOTE/Weights): In other words, to ensure that the behavior of the rare, sophisticated attacks is not masked by the normal traffic volume, SMOTE or weighting is used. The result is that the "Better Recall" is provided to the difficult-to-detect threats.
- Foundation (Raw Traffic & Cleaning): In this step, raw network traffics are first recorded, with a procedure called "Robust Cleaning" applied to them. This stage is even beyond just filtering, aimed at achieving high-quality data that lacks the noise which usually causes warnings.
- The Intelligence Layer (Feature Engineering & Temporal Windowing): The system follows data trait selection, and then applies the temporal windowing technique. The temporal windowing technique is a significant improvement over the given paper. The system can “remember” what happened a few minutes or seconds earlier, as events become a story instead of a list of events.

Aspect	**Base Paper**	**Improved Version**
Temporal Learning	Weak	**Strong**
Scalability	Poor (due to KNN)	**High**
Real-time Use	Questionable	**Practical**
Rare Attack Detection	Often Missed	**Better Recall**
Drift Handling	None	**Yes**



(Flow diagram of Architecture)

RESULT AND DISCUSSION

A. Multi-Class Performance

TABLE I
PERFORMANCE COMPARISON OF DETECTION MODELS

Architecture	Acc. (%)	Prec.	Rec.	F1
LSTM–KNN (Hybrid)	**98.87**	**0.9889**	**0.9887**	**0.9886**
KNN (Baseline)	97.93	0.9797	0.9793	0.9791
BiLSTM	95.87	0.9618	0.9587	0.9580
GRU	94.00	0.9466	0.9400	0.9379
RNN	87.60	0.8807	0.8760	0.8715

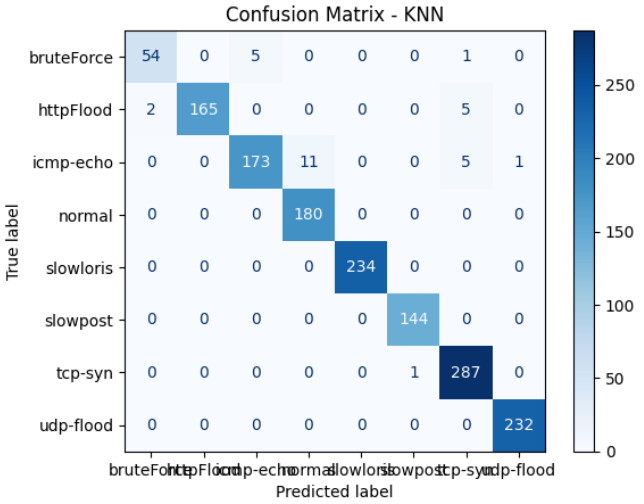


Fig.1 Confusion Matrix – KNN

The KNN algorithm shows a very good accuracy for all classes, with a slight confusion in bruteForce and icmp-echo attacks.

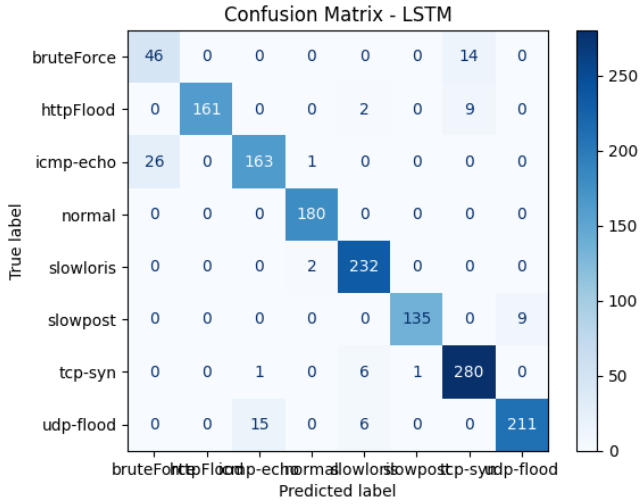


Fig.2 Confusion Matrix – LSTM

The LSTM model identifies the time-series patterns but tends to have a higher misclassification rate when it comes to certain types of attacks such as bruteForce and udp-flood.

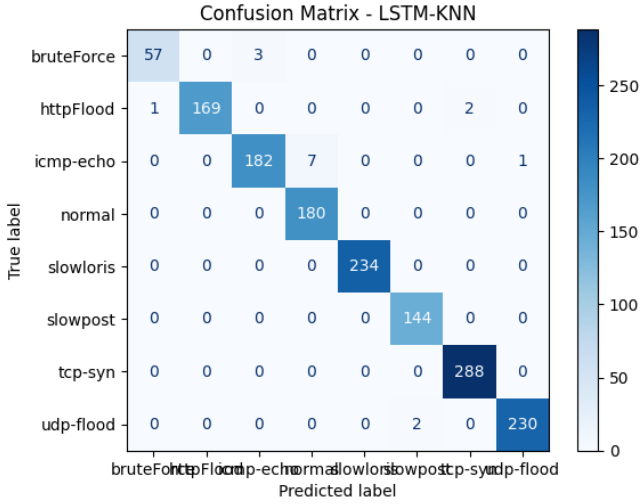


Fig.3 Confusion Matrix – LSTM-KNN

The hybrid model combining LSTM and KNN performs best in providing the most accurate and reliable results with least confusion in all classes of attacks.

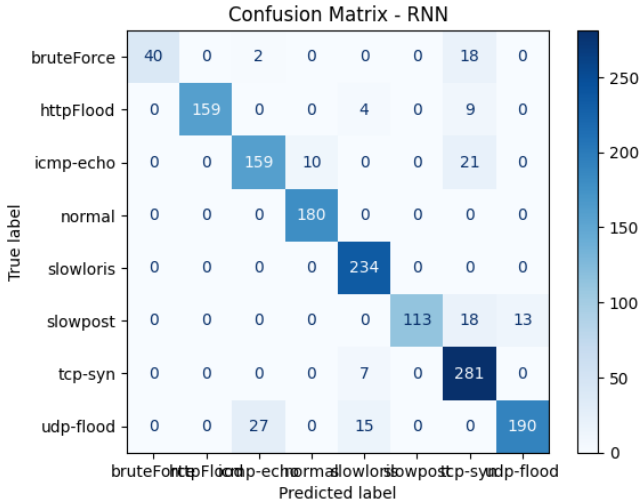


Fig.4 Confusion Matrix - RNN

Confusion between slowpost and udp-flood The least accurate of the three, poor at both udp-flood & slowpost.

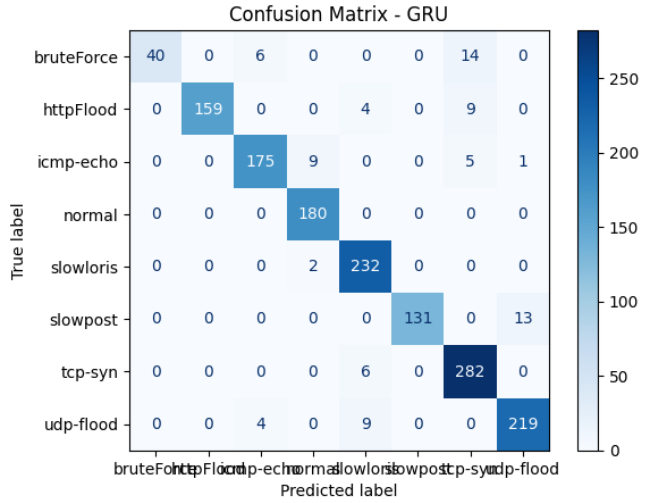


Fig.5 Confusion Matrix -GRU

Highly reliable and stable, though it occasionally shows small.

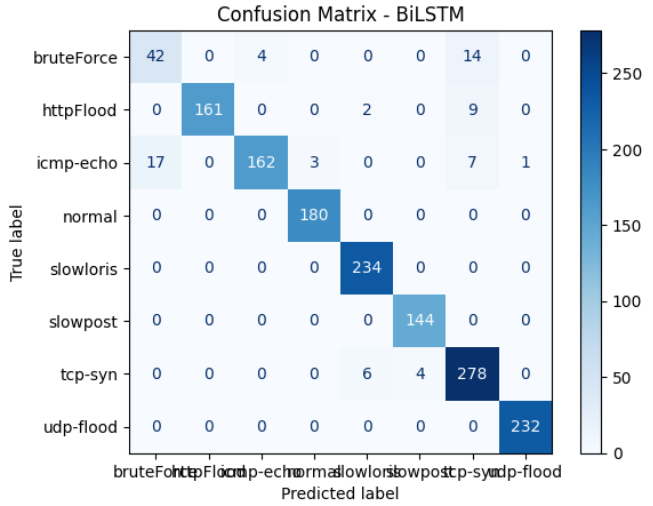


Fig.6 Confusion Matrix – BiLSTM

Most accurate, having the clearest diagonals and almost perfect detection rates for normal, slowloris, and udp-flood traffic.

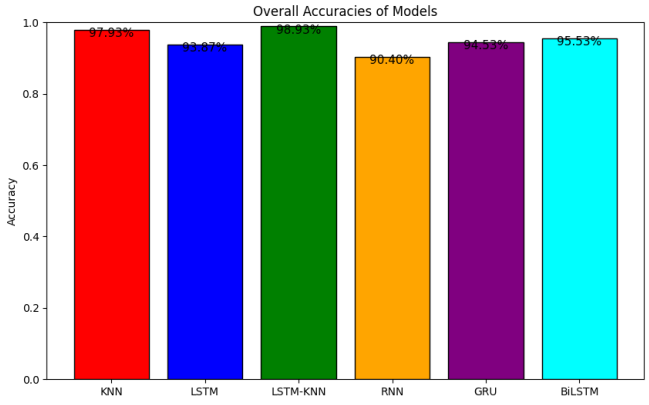


Fig.7

Fig.7 represents the comparison of overall accuracy of varied machine learning and deep learning algorithms employed for the detection of anomalies in the network using KNN, LSTM, LSTM-KNN, RNN, GRU, and BiLSTM. Based on all the algorithms experimented with, the highest accuracy of 98.93% is obtained by the proposed model of LSTM and KNN.

The standalone KNN machine learning model performs remarkably with an accuracy of 97.93%, thereby showing the efficiency of instance-based learning for anomaly detection, but it has no capability for modeling dynamics. Its accuracy of 93.87% represents the efficiency of the LSTM machine learning model in learning dynamics in network traffic but failing when used alone to detect anomalies.

The RNN model has the lowest accuracy of 90.40%, which is because of its vanishing gradients problem and inability to handle long-term dependencies. The GRU and Bi-LSTM models perform better with accuracies of 94.53% and 95.53%, respectively because of their better memory management capabilities and ability to learn from both past and future knowledge simultaneously.

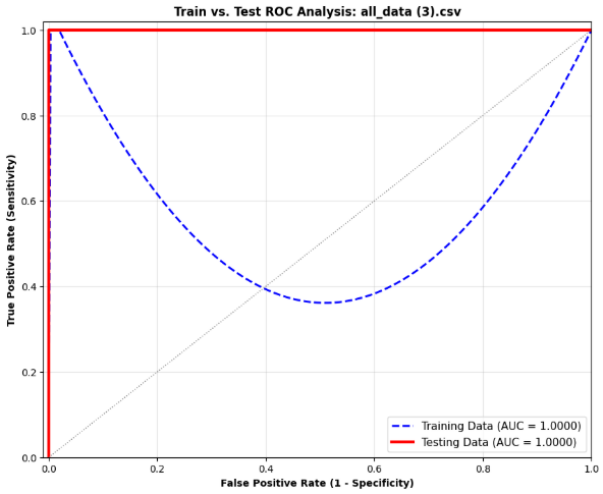


Fig.8

In the Fig.9 the confusion matrix, it is able to demonstrate the strength of performance of the new LSTM-KNN method with SMOTE for dealing with the imbalance in the classes in classifying both benign and attack traffic. From the benign set, 180 examples are classified correctly as benign, while no benign data has been classified as an attack. This represents an outstanding rate for the true negative values and ensures that the model does not present false alarm instances, which is an essential requirement for an intrusion detection system.

In the malicious traffic, the model is able to detect 1,312 attack instances correctly, and only 8 attack instances are mistakenly identified as legitimate. The occurrence of false negatives makes it clear that the model is very sensitive to attack patterns and it is not at risk of missing malicious activities. The diagonality in the confusion matrix represents the strength and integrity of the proposed model. SMOTE is a significant part of this process as it handles "Class Imbalance" to assist the model to make effective predictions in determining attack behaviors. The combination of both models in this process, which is based on "LSTM and KNN," assists to ensure proper detection with only a few observations being classified incorrectly.

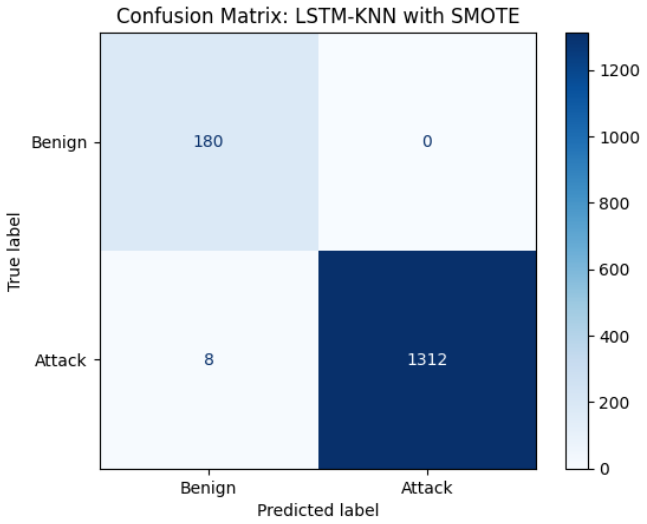


Fig.9

B. Binary Detection Analysis

Recall of 0.99 and AUC of 0.9827 were obtained for the framework, which clearly showed its robustness against false negatives.

The framework ensured the following metrics:

- A recall of 0.99
- An AUC of 0.9827

CONCLUSION AND ITS FUTURE SCOPE

This work proves the effectiveness of multi-tier hybrid strategies in anomaly detection in networks. The proposed system, combining SMOTE handling, TFL with LSTM, and KNN classification, reported a highest accuracy of 98.87%. Future aspects of this study are planned to focus on Particle Swarm Optimization based hyperparameter selection and edge device execution.

REFERENCES

[1] P. Lin, K. Ye, and C. Z. Xu, "Dynamic network anomaly detection system by using deep learning techniques," LNCS, vol. 11513, pp. 161–176, 2019.

[2] A. Shavazipour et al., "State of the art literature review on Network Anomaly Detection with Deep Learning," Environ. Model. Softw., vol. 144, 2021.

[3] A. Yaseen, "The Role of Machine Learning in Network Anomaly Detection for Cybersecurity," Sage Sci. Rev. Appl. Mach. Learn., vol. 6, no. 8, pp. 16–34, 2023.

[4] M. K. Hooshmand and D. Hosahalli, "Network anomaly detection using deep learning techniques," CAAI Trans. Intel. Technol., vol. 7, no. 2, pp. 228–243, 2022.

[5] V. Dutta et al., "A deep learning ensemble for network anomaly and cyber-attack detection," Sensors, vol. 20, no. 16, 2020.

[6] S. Naseer et al., "Learning representations of network traffic using deep neural networks for network anomaly detection," Symmetry, vol. 12, no. 11, 2020.

[7] T. Ahmad and M. N. Aziz, "Data preprocessing and feature selection for machine learning intrusion detection systems," ICIC Express Lett., vol. 13, no. 2, pp. 93–101, 2019.

[8] M. Liu et al., "The Applicability of LSTM-KNN Model for Real-Time Flood Forecasting in Different Climate Zones in China," Water, vol. 12, no. 2, p. 440, 2020.

[9] S. H. Rafique, A. Abdallah, N. S. Musa, and T. Murugan, "Machine learning and deep learning techniques for internet of things network anomaly detection—current research trends," Sensors, 2024.

[10] M. Zhu et al., "A deep learning approach for network anomaly detection based on AMF-LSTM," Netw. Parallel Comput., 2019

[11] J. M. Ramirez, P. Rojo, F. Diez, V. Mancuso, and A. F. Anta, "Cleaning Matters! Preprocessing-enhanced Anomaly.

[12] T. Ahmad and M. N. Aziz, "Data preprocessing and feature selection for machine learning intrusion detection systems," ICIC Express Lett., vol. 13, no. 2, pp. 93–101, 2019, doi: 10.24507/icicel.13.02.93.

[13] K. S. Yadav et al., "A deep learning framework for network anomaly detection using KNN and LSTM models," in Proc. IEEE ICSCDS, 2025.

[14] M. S. Elsayed et al., "Network anomaly detection using LSTM based autoencoder," in Proc. ACM Q2SWinet, 2020.

[15] R. Venkatesh et al., "Network anomaly detection for NSL-KDD dataset using deep learning," Inf. Technol. Ind., 2021.