# Capturing Spatio-Temporal Patterns for Intrusion Detection: A Hybrid CNN-LSTM-GRU Model on the NSL-KDD Dataset

**Dr. B. Chitradevi,**
Assistant Professor,
SRM Institute of Science and Technology (Deemed to be University),
Tiruchirappalli
citradevi.b@gmail.com.

**Dr. B. Balakumar,**
Assistant Professor (Grade III ),
Centre for Information Technology and Engineering,
Manonmaniam Sundaranar University,
Abishekapatti ,
Tirunelveli - 627 012.
balakumarcite@msuniv.ac.in

**Mr.M.Sulthan Alavudeen**
Assistant Professor,
Department of BCA,
G.T.N. Arts College,
Dindigul.
sulthancs2022@gmail.com

**Dr. R. Selvi,**
Assistant Professor,
PG & Research Department of Mathematics,
Thanthai Hans Roever College(A),
Perambalur- 621220.
selvimonishsamy@ gmail.com

**Ms. D. Akilandeswari**
Assistant Professor,
Department of Computer Science,
Thanthai Hans Roever College( A),
Perambalur- 612220
wlsakila@gmail.com

**Vijayakumar Gandhi**
Director, Cyber inline security engineering,
Bengaluru, Karnataka, India.
Vijayakumargandhi4@gmail.com

## Abstract

Intrusion Detection Systems (IDS) are essential for detecting and preventing unauthorized activities in computer networks. This research introduces a DL based IDS framework using the NSL-KDD dataset, employing advanced architectures such as GRU, LSTM, CNN, and a hybrid CNN-LSTM-GRU model. The system addresses both binary and multi-class classification tasks to distinguish between normal and malicious traffic, as well as identify specific attack categories like DoS, Probe, R2L, and U2R. Among the evaluated models, the hybrid CNN-LSTM-GRU approach achieved superior performance due to its ability to capture both spatial and temporal patterns in network data. The results demonstrate that deep learning (DL) significantly enhances the accuracy and robustness of intrusion detection, offering a scalable and intelligent solution for network security.

**Keywords:** Intrusion Detection System, Deep Learning, NSL-KDD, Hybrid CNN-LSTM-GRU Model, Network Security.

## 1. Introduction

The growing complexity and scale of cyberattacks have rendered traditional security mechanisms increasingly inadequate, necessitating the development of intelligent IDS capable of identifying both known and unknown threats in real time. IDS plays a pivotal role in safeguarding network infrastructures by analysing traffic patterns and detecting abnormal or malicious behaviour. Leveraging DL techniques has significantly advanced IDS performance, enabling dynamic feature extraction, adaptive learning, and enhanced detection accuracy. However, the effectiveness of such systems heavily depends on the quality and diversity of training data used to model attack behaviours.

The NSL-KDD dataset serves as a benchmark for evaluating IDS models, addressing critical shortcomings of the earlier KDD Cup 1999 dataset, such as redundancy and class imbalance. It provides a curated set of records representing various attack categories DoS, Probe, R2L, and U2R along with normal traffic, described across 41 extracted features. This dataset enables the development of robust IDS frameworks capable of learning nuanced patterns in network traffic. In this study, the NSL-KDD dataset is utilized to design and validate DL based IDS architectures, focusing on improving detection accuracy, minimizing false positives, and enhancing scalability. The goal is to create a reliable and adaptive detection system aligned with evolving cybersecurity threats in real-world network environments [1].

## 2. Literature review

Alrayes et al. (2024) introduced a CNN based Network Intrusion Detection System (NIDS) integrated with channel attention to enhance anomaly detection. The model was evaluated using the NSL-KDD dataset, which includes 43 features labelled as "attack" and "level." Their approach achieved a high detection accuracy of 99.728%. The channel attention mechanism improved feature prioritization, enhancing the CNN's effectiveness. This method outperformed traditional techniques like RBM, ANN, and ensemble models. The study demonstrates a significant advancement in intrusion detection performance with efficient and adaptable architecture [2].

Le and Huynh The (2025) proposed a DL based NIDS addressing data imbalance using the Synthetic Minority Over-sampling Technique (SMOTE). Their system employs a residual connection convolutional neural network (CNN) and was validated on the NSL-KDD and CIC-IDS2017 datasets. The model achieved a multi-class classification accuracy of 91.40% on NSL-KDD and 99.53% on CIC-IDS2017, with binary classification accuracy reaching 94.15% on NSL-KDD and 99.61% on CIC-IDS2017. The integration of SMOTE significantly improved performance by balancing the dataset. This study demonstrates the efficacy of DL in handling data imbalance in NIDS applications [3].

Sajid et al. (2024) proposed a hybrid intrusion detection model combining Machine Learning (ML) and DL techniques to address the limitations of traditional systems. The model integrates Extreme Gradient Boosting (XGBoost) and Convolutional Neural Networks (CNN) for feature extraction, coupled with Long Short Term Memory (LSTM) networks for classification. It was validated on four benchmark datasets CIC IDS 2017, UNSW NB15, NSL KDD, and WSN DS. The results demonstrated high detection rates with significant accuracy improvements and a low False Acceptance Rate (FAR). The hybrid approach effectively enhanced the system's ability to detect new threats, even with high-dimensional feature space [4].

Imrana et al. (2024) introduced the CNN-GRU-FF method, a double-layer feature extraction and fusion technique, to tackle class imbalance in intrusion detection datasets. The model combines Convolutional Neural Networks (CNN) and Gated Recurrent Units (GRU) with a modified focal loss function, improving performance over

traditional cross-entropy loss. The proposed system was evaluated on the NSL-KDD and UNSW-NB15 datasets, achieving detection rates of 99.68% and 98.22%, respectively, while maintaining low false alarm rates. Compared to seven baseline algorithms, the CNN-GRU-FF method outperformed state-of-the-art intrusion detection techniques, demonstrating significant advancements in accuracy and robustness [5].

Alamro et al. (2025) proposed the MGOADL-CS technique to enhance cybersecurity in IoT-consumer electronics, specifically for drone platforms. The method integrates Blockchain technology with DL, utilizing an Attention Long Short Term Memory Neural Network (ALSTM-NN) for cyberattack detection. The approach employs a Linear Scaling Normalization (LSN) technique for data normalization, an Improved Tunicate Swarm Algorithm (ITSA) for feature selection, and MGO based hyperparameter tuning for optimal model performance. The model was evaluated using the NSL-KDD dataset, achieving a high accuracy of 99.71%. This method outperformed existing approaches, demonstrating significant improvements in attack detection and cybersecurity for dynamic drone environments [6].

Thaljaoui (2025) proposed an optimized hybrid model for Network Intrusion Detection System (NIDS) combining Convolutional Neural Networks (CNN) and Long Short-Term Memory (LSTM) networks, optimized using Bayesian optimization. The model was evaluated using the UNSW-NB15 dataset, a benchmark for intrusion detection in IoT networks. Performance metrics including accuracy, precision, recall, and F1-score were employed to assess the model's effectiveness. The proposed model achieved an accuracy of 98.15%, precision of 97.32%, recall of 98.22%, and an F1-score of 97.77%. A comparative study highlighted its superior performance over traditional methods, validating its effectiveness in securing IoT networks [7].

Abed et al. (2024) proposed a modified CNN-based Intrusion Detection System (IDS) model to enhance the efficacy of detecting network intrusions. Using the UNSW-NB15 dataset, the study applied two feature selection techniques, Principal Component Analysis (PCA) and Singular Value Decomposition (SVD), to improve classification accuracy. The model utilized Ridge Regression (RR), Stochastic Gradient Descent (SGD), and CNN classifiers for both binary and multiclass classification tasks. The results demonstrated that PCA and SVD significantly improved IDS performance, with the RR classifier achieving an accuracy increase from 98.13% to 99.85% for binary classification. This work highlights the importance of feature selection in enhancing IDS effectiveness [8].

El-Ghamry et al. (2023) proposed an optimized CNN-based intrusion detection system (IDS) to mitigate risks in smart farming environments. Using the NSL-KDD dataset, the study applied recursive feature elimination for feature selection, converting the data into square color images for CNN model compatibility. The system was evaluated using CNN architectures such as VGG16, Inception, and Xception, with performance compared to classical machine learning algorithms. The results demonstrated that the Xception

model achieved an accuracy of 98.75%, F1 score of 98.68%, recall of 98.55%, and precision of 98.80%, outperforming traditional machine learning approaches. This approach effectively addresses the security challenges in IoT-based smart farming systems [9].

Kilichev and Kim (2023) explored hyperparameter optimization in 1D-CNN models for network intrusion detection, utilizing genetic algorithm (GA) and particle swarm optimization (PSO) to optimize nine hyperparameters. The study evaluated the models using three datasets: UNSW-NB15, CIC-IDS2017, and NSL-KDD. The results demonstrated significant improvements in performance, with GA and PSO achieving accuracies of 99.31% and 99.28%, respectively, on the UNSW-NB15 dataset. Both optimization techniques showed equivalent results in precision, recall, and F1-score, while varying performance was observed on the CIC-IDS2017 and NSL-KDD datasets. These findings underscore the importance of hyperparameter optimization for enhancing IDS efficacy in addressing evolving cyber threats [10].

Masum et al. (2021) proposed a Bayesian optimization-based framework for automating hyperparameter tuning in deep neural network (DNN) models for network intrusion detection. The study focused on the NSL-KDD dataset, a widely used benchmark in intrusion detection research. The authors reported significant improvements over random search optimization, with their optimized DNN achieving an accuracy of 98.45%, precision of 98.22%, recall of 97.83%, and an F1-score of 98.02%. These results confirmed that the Bayesian optimization method significantly enhances the DNN architecture's effectiveness, providing a more efficient and reliable solution for intrusion detection in modern network environments [11].

Bamber et al. (2025) proposed a DL based intrusion detection system (IDS) to address the growing complexity of cyber-attacks on critical infrastructures. Using the NSL-KDD dataset, they applied Recursive Feature Elimination (RFE) with a Decision Tree classifier for feature selection, followed by the evaluation of several DL models, including ANN, LSTM, BiLSTM, CNN-LSTM, GRU, and BiGRU. Their hybrid CNN-LSTM model achieved an accuracy of 95%, recall of 0.89, and F1-score of 0.94, demonstrating superior performance in distinguishing malicious from benign traffic. These findings validate the proposed IDS's effectiveness and suggest potential for further improvement through ensemble methods [12].

## 3. Materials and Methodology

### 3.1 Dataset Description

The NSL-KDD dataset, developed in 2009 as an enhancement of the original KDD'99 dataset, is widely used for training and evaluating intrusion detection systems. It eliminates redundant and duplicate records, ensuring more balanced class distributions and reliable benchmarking. The dataset comprises three subsets: KDDTrain+ (used for

training), KDDTest+, and KDDTest-21 (both used for testing). Each record includes 41 network traffic features and is labeled as either normal or one of four major attack types: Denial of Service (DoS), Probe, Remote to Local (R2L), and User to Root (U2R). The class-wise distribution across these subsets is provided below:

Table.1. Class Distribution in NSL-KDD Dataset

| Category | KDDTrain+ | KDDTest+ | KDDTest-21 |
|---|---|---|---|
| Total Records | 125,973 | 25,192 | 22,542 |
| Normal | 67,343 | 13,449 | 12,709 |
| DoS (Denial of Service) | 45,827 | 9,234 | 7,749 |
| Probe | 11,456 | 2,289 | 1,867 |
| R2L (Remote to Local) | 995 | 209 | 175 |
| U2R (User to Root) | 49 | 11 | 42 |

### 3.2 Pre-processing

Normalization is a crucial pre-processing step when applying DL models to the NSL-KDD dataset, as the features have different numerical ranges. Min-Max normalization is used to scale all features into the range [0, 1], ensuring uniform contribution across features during model training. This transformation is defined by the equation:

$$x' = \frac{x - x_{min}}{x_{max} - x_{min}}$$

Where $x$is the original feature value, and $x_{min}$ and $x_{max}$ are the minimum and maximum values of that feature in the training set. Applying this normalization improves the learning efficiency and convergence of DL models by preventing features with larger scales from dominating the training process [13].

### 3.3 DL Classification

We used DL classifiers including GRU, LSTM, CNN, and a hybrid CNN-LSTM-GRU model for intrusion detection on the NSL-KDD dataset. GRU and LSTM captured temporal dependencies, CNN extracted spatial features, and the hybrid model combined their strengths. Input features were scaled using Min-Max normalization. These models effectively classified various attack types, improving IDS performance.

#### i. Gated Recurrent Unit (GRU)

The GRU is an efficient variant of Recurrent Neural Networks (RNNs) designed to capture temporal dependencies in sequential data. In Intrusion Detection Systems (IDS), GRUs are highly effective for analyzing network traffic patterns over time, enabling accurate detection of both known and unknown attacks. Unlike traditional RNNs, GRUs overcomes the vanishing gradient problem through gating mechanisms that control the

flow of information. A key component of the GRU is its mechanism for updating the hidden state $h_t$ formulated as

$$h_t = (1 - z_t) \odot h_{t-1} + z_t \odot \tilde{h}_t$$

Here, $z_t$ is the update gate that controls how much of the previous state is retained, and $\tilde{h}_t$ is the candidate activation influenced by the current input and reset modulated hidden state. This update rule enables the GRU to adaptively capture relevant information across time steps, making it highly suitable for detecting dynamic, time-sensitive intrusion patterns in network data [14].

**ii. Convolutional Neural Networks (CNNs)**

CNNs are exceptionally proficient in Intrusion Detection Systems (IDS) owing to their capacity to autonomously extract pertinent information from network traffic data. In the context of IDS, CNNs examine structured data, such as feature maps that depict network traffic flows, to discern malicious from benign patterns. The convolutional layers utilize filters to identify critical properties such as packet sequence and flow duration, aiding in the detection of assaults such DDoS, malware, or illegal access. The CNN design generally comprises convolutional layers, pooling layers, and fully linked layers. The convolution operation is denoted as

$$h_j^{(n)} = \sum_{k=1}^{K} h_k^{(n-1)} * w_k^{(n)} + b_k^{(n)}$$

Where $h_j^{(n)}$ represents the output of the j-th feature map in the $n^{th}$ layer, and $w_k^{(n)}$ denotes the learnable filters. Pooling layers diminish the dimensionality of feature maps, whereas fully connected layers execute the final classification. The optimization is achieved by minimizing the cross entropy loss.

$$E = \frac{1}{m} \sum_{i=1}^{m} \sum_{k=1}^{c} \hat{y}_{ik} \log (y_{ik})$$

Where $\hat{y}_{ik}$ represents the true label, and $y_{ik}$ is the anticipated output. This framework enables CNN based IDS to proficiently categorize intrusions [15].

**iii. Long Short Term Memory (LSTM)**

LSTM networks are advanced variants of Recurrent Neural Networks (RNNs) designed to effectively capture long-range dependencies in sequential data. They are particularly useful in IDS, where detecting complex attack patterns often requires analyzing long sequences of network traffic. LSTMs achieve this through a memory cell and gating mechanisms that regulate the flow of information, allowing the model to retain relevant patterns while discarding noise. The core update mechanism of LSTM is expressed as

$$c_t = f_t \odot c_{t-1} + i_t \odot \tilde{c}_t, \quad h_t = o_t \odot \tanh(c_t)$$

Where $c_t$ is the memory cell, $h_t$ is the hidden state, and $f_t$, $i_t$, and $o_t$ are the forget, input, and output gates, respectively. This gated structure enables LSTMs to maintain and manipulate long-term contextual information, enhancing the model's ability to detect both known and unknown intrusions in dynamic network environments [16].

**iv. Hybrid CNN-LSTM-GRU**

The Hybrid CNN-LSTM-GRU algorithm for intrusion detection initializes a model combining CNN layers for spatial feature extraction and LSTM/GRU layers for capturing temporal patterns in network traffic. The dataset is split into mini-batches, and in each training cycle, the CNN extracts spatial features while the LSTM/GRU processes packet sequences. The Adam optimizer is used for training with class weights for imbalance, and the model is evaluated using a confusion matrix. This process continues for the specified number of cycles, producing a trained intrusion detection model.

**Pseudo code of Hybrid CNN-LSTM-GRU for IDS**

**Input:**

$X_{\text{train}}$ : Features of network traffic (packet headers, flow statistics)

$Y_{\text{train}}$: Labels for attack (binary/multi class)

$X_{\text{test}}$ : Hidden network traffic for validation

$parameter$ : {$I_{ii}$: iterations, $B_i$: batch size, η: learning Rate}

**Output**

Model: Trained CNN-LSTM-GRU intrusion detector

Metrics: {accuracy, F1- Score, Detection Rate (DR), False Acceptance Rate (FAR), confusion metrix}

**Initialize Algorithm**

$b_i$ ← Initialize CNN (for packet/flow features) + LSTM/GRU (for temporal patterns)

$P_i$ ← (Split b in equal parts of $B_i$ )

**For** each cycle $t_i = 1, 2 \ldots z_i$ **do**

{Verify train} ← {$Pt_i$(normal/attack samples), $P_i - Pt_i$}

(t$f_{i,}vf_i$) ← (CNN extracts spatial features from headers,

LSTM/GRU processes sequence of packets in $y_i$)

$nt$ ← Model FIT (Adam t$f_{i,}$ with class weights for imbalance

$rt$ ← Model Evaluate ($nt, vf_i$) using confusion matrix

**End for**

## 4. Results and Discussion

The Network IDS was developed using the NSL-KDD dataset, which contains labelled network traffic for training and testing. DL models including GRU, LSTM, CNN, and a hybrid CNN-LSTM-GRU were used for classification. Min-Max normalization was applied

to pre-process the dataset and scale feature values between 0 and 1 for consistent input across models.

### 4.1 Performance Metrics

Performance metrics are used to measure how well a system or model performs. They provide a standard way to evaluate outcomes and compare different approaches. These metrics help identify strengths, weaknesses, and areas for improvement. Overall, they are essential for monitoring progress and achieving desired goals.

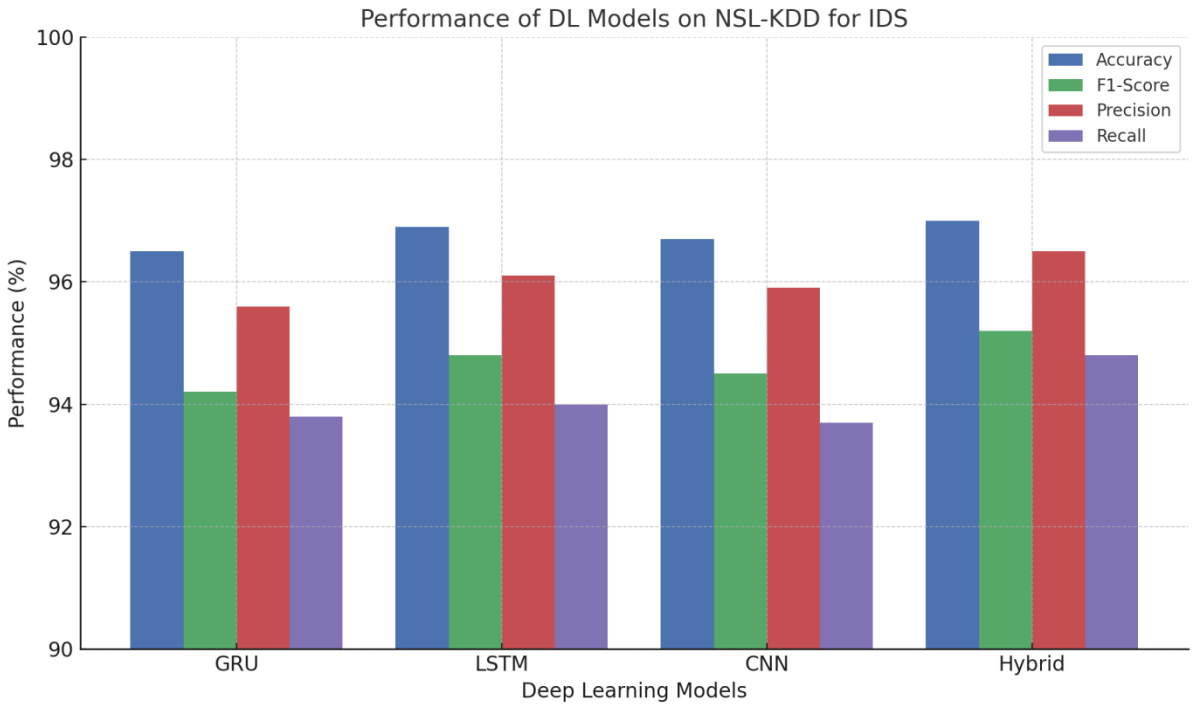
| | |
|---|---|
| **Accuracy** | $Accuracy = \frac{TP + TN}{TP + TN + FP + FN}$ |
| **Precision** | $Precision_c = \frac{TP_c}{TP_c + FP_c}$ |
| **Recall** | $Recall_c = \frac{TP_c}{TP_c + FN_c}$ |
| **F1 Score** | $Recall_c = 2 . \frac{Precision_c . Recall_c}{Precision_c + Recall_c}$ |

### 4.2 Experimental Results

The NSL-KDD dataset was used to evaluate four DL models: GRU, LSTM, CNN, and a hybrid CNN-LSTM-GRU. Performance was assessed using standard metrics including Accuracy, Precision, Recall, and F1-Score. GRU and LSTM captured temporal patterns in the data, while CNN extracted spatial features. The hybrid model combined the strengths of all three architectures and delivered the most consistent performance. These results confirm the effectiveness of DL approaches for intrusion detection.

**Table.5. Performance Metrics of DL Models on NSL-KDD Dataset**

| DL Model | Accuracy (%) | F1-Score (%) | Precision (%) | Recall (%) |
|---|---|---|---|---|
| GRU | 96.5 | 94.2 | 95.6 | 93.7 |
| CNN | 96.7 | 94.5 | 95.9 | 93.8 |
| LSTM | 96.9 | 94.8 | 96.1 | 94.0 |
| CNN-LSTM-GRU (Hybrid) | 97.0 | 95.2 | 96.5 | 94.8 |




The above bar graph presents a comparative analysis of four DL models GRU, LSTM, CNN, and a Hybrid CNN-LSTM-GRU applied to the NSL-KDD dataset for intrusion detection. The models are evaluated using Accuracy, F1-Score, Precision, and Recall. The Hybrid model shows the best performance with 97% accuracy, highlighting its effectiveness in capturing both spatial and temporal features. LSTM and CNN also show strong results, while GRU performs slightly lower across all metrics. The graph emphasizes the improved performance of the hybrid model for intrusion detection using DL.

## 5. Conclusion

In conclusion, the experimental evaluation using the NSL-KDD dataset demonstrates that DL models are highly effective in detecting and classifying network intrusions with significant accuracy. Among the models investigated GRU, LSTM, CNN, and a hybrid CNN-LSTM-GRU architecture the hybrid approach outperformed individual models by effectively capturing both spatial hierarchies and temporal dependencies inherent in network traffic data. The NSL-KDD dataset, with its balanced representation of normal and attack classes, provided a reliable benchmark for validating model robustness. The results affirm that hybrid DL architectures can substantially enhance the performance of IDS by reducing false positives and improving detection rates across various attack categories. These findings underscore the viability of leveraging advanced DL architectures for real-time, intelligent threat detection in modern cybersecurity environments. Future work should explore scalable deployment of such models in distributed and federated IDS frameworks, incorporating continuous learning mechanisms for adaptive defence against evolving cyber threats.

## References

1. Gbashi, Ekhlas & mohammed, Bilal. (2021). Intrusion Detection System for NSL-KDD Dataset Based on Deep Learning and Recursive Feature Elimination. Engineering and Technology Journal. Vol. 39 No. 7 (2021): Engineering & Science Issue /. 10.30684/etj.v39i7.1695.
2. Fatma S. Alrayes, Mohammed Zakariah, Syed Umar Amin, Zafar Iqbal Khan, Jehad Saad Alqurni, CNN Channel Attention Intrusion Detection System Using NSL-KDD Dataset, Computers, Materials and Continua, Volume 79, Issue 3, 2024, Pages 4319-4347, ISSN 1546-2218.
3. T. -T. Le and T. Huynh-The, "Cyberattacks Classification by Tuning Deep Hyperparameters Using Bayesian Optimization," 2025 19th International Conference on Ubiquitous Information Management and Communication (IMCOM), Bangkok, Thailand, 2025, pp. 1-7.
4. Sajid, M., Malik, K.R., Almogren, A. et al. Enhancing intrusion detection: a hybrid machine and deep learning approach. J Cloud Comp 13, 123 (2024).
5. Imrana, Y., Xiang, Y., Ali, L. et al. CNN-GRU-FF: a double-layer feature fusion-based network intrusion detection system using convolutional neural network and gated recurrent units. Complex Intell. Syst. 10, 3353–3370 (2024).
6. Hayam Alamro, Mohammed Maray, Jawhara Aljabri, Saad Alahmari, Monir Abdullah, Jehad Saad Alqurni, Faiz Abdullah Alotaibi, Abdelmoneim Ali Mohamed, Mathematical modelling-based blockchain with attention deep learning model for cybersecurity in IoT-consumer electronics, Alexandria Engineering Journal, Volume 113, 2025, Pages 366-377, ISSN 1110-0168.
7. Thaljaoui, A. Intelligent network intrusion detection system using optimized deep CNN-LSTM with UNSW-NB15. Int. j. inf. tecnol. (2025).
8. Ruqaya Abdulhasan Abed, Ekhlas Kadhum Hamza, Amjad J. Humaidi, A modified CNN-IDS model for enhancing the efficacy of intrusion detection system, Measurement: Sensors, Volume 35, 2024, 101299, ISSN 2665-9174.
9. Amir El-Ghamry, Ashraf Darwish, Aboul Ella Hassanien, An optimized CNN based intrusion detection system for reducing risks in smart farming, Internet of Things, Volume 22, 2023, 100709, ISSN 2542-6605.
10. Kilichev, D.; Kim, W. Hyperparameter Optimization for 1D-CNN-Based Network Intrusion Detection Using GA and PSO. Mathematics 2023, 11, 3724.
11. M. Masum et al., "Bayesian Hyperparameter Optimization for Deep Neural Network-Based Network Intrusion Detection," 2021 IEEE International Conference on Big Data (Big Data), Orlando, FL, USA, 2021, pp. 5415-5424.
12. Sukhvinder Singh Bamber, Aditya Vardhan Reddy Katkuri, Shubham Sharma, Mohit Angurala, A hybrid CNN-LSTM approach for intelligent cyber intrusion detection system, Computers & Security, Volume 148, 2025, 104146, ISSN 0167-4048.
13. Thirimanne, S.P., Jayawardana, L., Yasakethu, L. et al. Deep Neural Network Based Real-Time Intrusion Detection System. SN COMPUT. SCI. 3, 145 (2022).
14. P. Mehrotra and U. Dwivedi, "An Efficient Deep Learning Framwork for Classification and Detection of Anomaly Based Network Intrusion using NSL-

KDD Dataset," 2025 3rd International Conference on Disruptive Technologies (ICDT), Greater Noida, India, 2025, pp. 170-177.

15. Fatma S. Alrayes, Mohammed Zakariah, Syed Umar Amin, Zafar Iqbal Khan, Jehad Saad Alqurni, CNN Channel Attention Intrusion Detection System Using NSL-KDD Dataset, Computers, Materials and Continua, Volume 79, Issue 3, 2024, Pages 4319-4347, ISSN 1546-2218.
16. Imrana, Yakubu & Xiang, Yanping & Ali, Liaqat & Abdul-Rauf, Zaharawu & Hu, Yu-Chen & Kadry, Seifedine & Lim, Sangsoon. (2022). χ2-BidLSTM: A Feature Driven Intrusion Detection System Based on χ2 Statistical Model and Bidirectional LSTM. Sensors. 22. 2018. 10.3390/s22052018.