Journal of Engineering Strategy and Innovation
Volume 1, Issue 1, July – September (2026) Arrived: 28/06/2026: Accepted: 23/06/2026

RESEARCH ARTICLE

# An Intelligent Grey Wolf Optimized Hybrid CNN-LSTM Assisted Multi Layer Cloud Security Optimization And Threat Detection Framework

Kajal Sheth [1], Dheeraj Kumar Bansal [2], K. Madhuvandhana [3]

[1] Department of Energy Engineering University, New York Tech, USA
[2] Program Manager SIEEE Wipro Limited, USA
[3] Research Scholar, Department of Electronics and Communication Engineering, P.S.R Engineering College, Tamil Nadu, India

[1] shethk@ieee.org

***Abstract*— Cloud computing infrastructures are highly vulnerable to advanced attacks due to their multi-tenant structure, distributed nature, and dynamic resource allocation. It has been a serious issue to maintain computing efficiency and robust security in multiple cloud levels. The proposed approach adopts LSTM network for recognizing temporal patterns of attacks in cloud computing traffic data along with CNN for efficient spatial feature extraction. Moreover, GWO algorithm is employed in order to minimize computing cost, tune the parameter values of the model, and increase detection accuracy. Multiple security layers are applied in order to observe and protect cloud infrastructure, platform, and application layers from diverse types of cyber-attacks. Experimental analysis proves that the proposed framework provides better performance than conventional machine learning (ML) and deep learning (DL) models in terms of threat detection, higher precision and recall values, lower false positive rate, and security optimization.**

***Keywords-*** *Grey wolf optimization, convolutional neural network, cloud computing, security, deep learning.*

## 1. INTRODUCTION

The Various electronic devices in the world are now very much linked with the Internet due to the remarkable technological developments witnessed within the last ten years. The use of the internet is widespread in today's world [1]. Although this high level of connectedness provided us with many benefits in our day-to-day lives, it also made our appliances, information systems, and privacy vulnerable to numerous cyberthreats [2]. One of the primary issues with regular computer network communication is network security, and intrusion detection systems (IDS) are crucial in protecting computer networks from cyberattacks [3].

Cloud computing has revolutionized data processing and storage capabilities, but it is still vulnerable to a number of security issues, including advanced persistent assaults, unauthorized access, and data breaches [4]. The inadequacy of current security mechanisms in offering complete security may require a search for innovative solutions. All cyberattacks are harmful to information security. Therefore, network security has become significant in this area of research. There are various approaches to securing network security such as firewalls, encryption, intrusion detection and authentication. The criminal elements in these attacks can be identified through the IDS [5]. In contrast to other security techniques, IDS plays an important role in network security because it can identify attacks in network traffic. Denial of service (DoS), remote to local (R2L), user to root (U2R) and probe are the most common types of attacks [6]. The significance of flexible, intelligent and proactive cyber security models can be seen in the rise in number and sophistication of attacks together with the existence of unpatched systems [7].

An IDS produces reports and alerts on any type of hostile action following the scanning of networks or systems for any malicious actions [8]. The deployment of a highly developed IDS is essential because there are many systems that can cover up any suspicious activity in the network. There are basically two types of IDS; these include network intrusion detection systems (NIDS) and host intrusion detection systems (HIDS) [9]. NIDS will scan and analyze

network traffic by analyzing data packets in a bid to detect any form of anomaly or possible threats. In contrast, a HIDS will monitor activities in other hosts or servers and analyze configuration files and system logs so as to detect any form of unauthorized activity or modifications in the host [10].

Since ML and DL techniques are essential to IDSs, developing an accurate detection mechanism is challenging, and multi-class IDS performance can still be improved. To address these issues, this study presents a hybrid model for advanced threat identification and mitigation using DL coupled metaheuristic optimization. The following is a summary of this study's main contributions.

1. The creation of a CNN-LSTM hybrid architecture that can extract temporal and geographic elements from cloud security datasets.
2. Using GWO to improve security performance and adjust parameters adaptively.
3. The creation of a multi-layer cloud security system that offers complete defense at the platform, data, infrastructure, and application layers.

This is the structure of the rest of the paper. A theoretical foundation for the proposed work is presented in Section II. The suggested multi-layer cloud security framework, Grey Wolf Optimized Hybrid CNN-LSTM, is presented in Section III. The experimental setup and performance evaluation technique, along with the results, are explained in Section IV. Section V brings the task to an end by providing a conclusion.

The ResidualFormer presents a hybrid deep learning network that uses CNN and transformer-based approaches in its encoder and decoder, respectively, to facilitate multi-scale feature learning and robust pattern recognition. The excellent segmentation results indicate the efficacy of hybrid neural networks in dealing with data representation and this encourages the application of such hybrid models for cloud threat intelligence [16]. The Graph-Attention Multi-Agent PPO framework offers flexibility in decision-making through an effective edge resources allocation scheme based on dynamically changing networks. The reinforcement learning approach used to optimize this framework emphasizes intelligent management of the resources, which is directly related to cloud security systems optimization [17]. A CNN-LSTM hybrid architecture was built for detecting different types of faults using spatial feature extraction and sequence learning, and the results showed high accuracy in the detection process. The effective combination of CNN and LSTM architectures shows their applicability for recognizing complicated patterns and relevance in cloud threat detection systems [18]. Combining Retrieval Augmented Generation (RAG) and Knowledge Graphs enhances the reliability and accuracy of the AI system due to the reduction of wrong predictions and improving contextual reasoning. The paper underscores the importance of using different techniques of artificial intelligence for developing decision-making systems, which may enhance cloud security analytics and intelligence in the future [19].

## 2. BACKGROUND

### *2.1. Multi-layer cloud security*

Infrastructure, networks, platforms, applications, and data services are just a few of the interrelated layers that make up cloud computing systems.

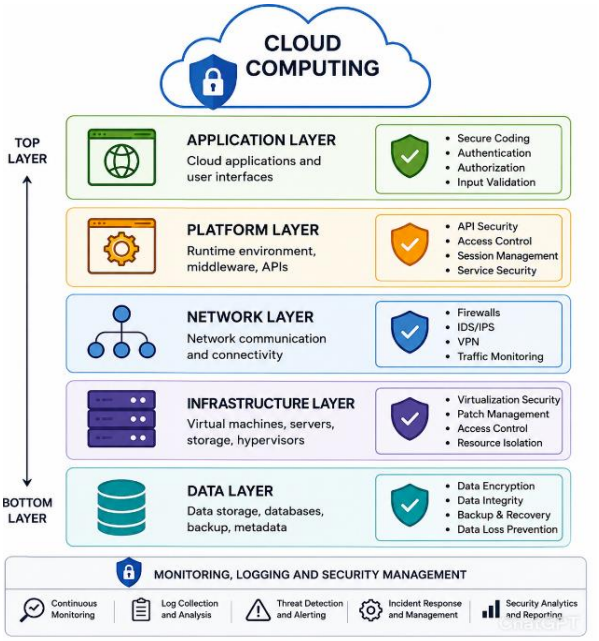


**Figure 1.** Multi-layer cloud security

These layers' dispersed and heterogeneous characteristics expand the attack surface that is vulnerable to cyberattacks Figure 1. Distributed Denial-of-Service (DDoS) attacks, malware injections, privilege escalation, unauthorized access, and data breaches are examples of security issues that can happen at various levels of the cloud architecture. As a result, a successful cloud security framework needs to constantly monitor network traffic, spot malicious activity, and make real-time security choices.

### *2.2. CNN-LSTM Model*

The geographical and temporal attributes of cloud traffic data are efficiently captured by CNN and LSTM architecture. While LSTM learns temporal relationships and sequential attack behaviors, CNN is in charge of extracting discriminative local attributes from network traffic.

#### *2.2.1. CNN based spatial attribute extraction*

CNN uses the convolution operation to automatically identify significant attack patterns.

$$H_f = f(W * X + b) \quad (1)$$

Where $W$ is the filter, $b$ is the bias.

The activation function for the Rectified Linear Unit (ReLU) is used as.

$$f(z) = \max(0, z) \quad (2)$$

To reduce attribute dimensionality, max-pooling is performed as.

$$P_j = \max(H_f) \quad (3)$$

The consequential CNN attribute is represented as.

$$F_{CNN} = \{p_1, p_2, \dots p_n\} \quad (4)$$

Where $n$ is the number of extracted spatial attributes.

*2.2.2. LSTM based temporal attribute extraction*

The LSTM network receives the CNN attribute vector as input for sequential pattern analysis.

The LSTM output in hidden state is

$$h_t = LSTM(F_{CNN}, h_{t-1)} \quad (5)$$

The final LSTM output is.

$$F_{LSTM} = h_t \quad (6)$$

which captures temporal attack behaviors and sequential traffic patterns.

### *2.3. Grey Wolf Optimization (GWO)*

Mirjalili et al. [11] developed GWO, a nature-inspired metaheuristic optimization algorithm that imitates the hunting and social hierarchy of grey wolves. Four groups comprise the population in the grey wolf hierarchy.

- Alphaα. The best possible answer.
- Betaβ. The second-best way to help the alpha wolf.
- Deltaδ. The remaining wolves are guided by the third-best solution.
- Omegaω. The search agents that remain.

Prey encircling, prey attacking, and prey hunting are the three main stages of the optimizing process.

*2.3.1. Encircling Prey.*

Grey wolves adjust their locations based on their estimation of the prey's location. The formula for calculating a wolf's distance from its prey $d$ is.

$$d = |C.X_{best}(t) - X(t)| \quad (7)$$

Where $X_{best}(t)$) is the best prey position, $X(t)$ is the current wolf position, and $C$ is a coefficient vector.The wolf position is updated as.

$$X(t+1) = X_{best}(t) - A.d \quad (8)$$

where $A$ is the control coefficient vector. The coefficient vectors are defined as.

$$A = 2ar_1 - a \quad (9)$$

$$C = 2r_2 \quad (10)$$

Where $r_1, r_2$ are random numbers, $a$ decreases from 2 to 0, allowing the algorithm to gradually shift from global search to local search.

### *2.4. Hunting Mechanism*

The three dominant wolves (α, β, and δ) direct the hunting process. These wolves' separations are calculated as

$$d = |C.X_{best}(t) - X(t)| \quad (11)$$

The candidate positions are obtained as

$$d_\alpha = |C_1 X_\alpha - X| \quad (12)$$

$$d_\beta = |C_2 X_\beta - X| \quad (13)$$

$$d_\delta = |C_3 X_\delta - X| \quad (14)$$

Using these distances, three possible positions are generated.

$$X_1 = X_\alpha - A.d_\alpha \quad (15)$$

$$X_2 = X_\beta - A.d_\beta \quad (16)$$

$$X_3 = X_\delta - A.d_\delta \quad (17)$$

The final position update is

$$X(t+1) = \frac{X_1+X_2+X_3}{3} \quad (18)$$

This tactic preserves population variety while allowing the search agents to converge toward the global optimum.

## 3. PROPOSED GREY WOLF OPTIMIZED HYBRID CNN-LSTM MODEL

The hybrid CNN-LSTM model's hyperparameters, such as learning rate, batch size.

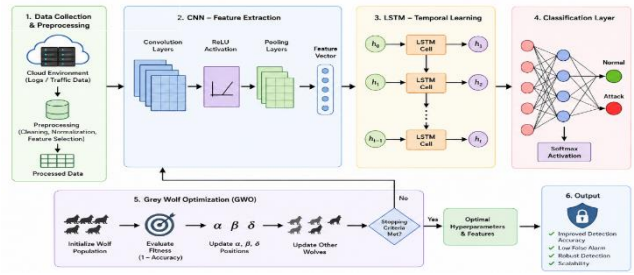


**Figure 2.** Proposed Grey wolf optimized hybrid CNN-LSTM framework

Convolution filter parameters, hidden neurons, and classification thresholds, are optimized in the suggested framework using Grey Wolf Optimization Figure 2. The final attribute representation is created by combining the spatial and temporal information.

$$F_{hybrid} = F_{CNN} \odot F_{LSTM} \quad (19)$$

Where ⊙ denotes attribute fusion

Let the CNN-LSTM hyperparameter vector be represented as.

$$\theta = (\theta_1, \theta_2, \ldots \theta_n\} \quad (20)$$

Where $\theta$ contains all tuneable parameters.

The fitness function $f(x)$is defined as.

$$f(x) = 1 - A_{detection} \quad (21)$$

Where $A_{detection}$ is the detection accuracy defined as.

$$A_{detection} = \frac{P_{true}+N_{true}}{P_{true}+N_{true}+P_{false}+N_{false}} \quad (22)$$

The optimization objective is.

$$\theta^* = argmin\{\theta\}.f(x) \quad (23)$$

where$\theta^*$ represents the optimal CNN-LSTM parameter set obtained by GWO. GWO finds the ideal hyperparameter configuration that optimizes threat detection accuracy and improves the overall performance of the suggested cloud security framework through iterative position updating and fitness evaluation.

The Softmax function is used in the last classification layer to calculate the attack probability.

$$P(y_i) = \frac{e^{z_i}}{\Sigma_{j=1}^{k} e^{z_j}} \quad (24)$$

where K represents the number of classes.

The predicted class label is determined as.

$$y_i^{'} = classification(F_{hybrid}) \quad (25)$$

## 4. SIMULATION RESULTS AND ANALYSIS

### 4.1. *Dataset Description*

The NSL-KDD dataset, which includes examples of both benign and malevolent network traffic, was used to assess the suggested framework. 41 traffic attributes that describe protocol attributes, service details, traffic statistics, and connection behaviors make up the dataset. The dataset was preprocessed prior to training by eliminating duplicate records, managing missing values, encoding categorical attributes, and using Min-Max normalization to guarantee consistent attribute scaling.

### *4.2. Simulation setup*

Python using the TensorFlow and Keras libraries was used to implement the suggested framework. A workstation with an Intel Core i7 processor, 16 GB RAM, and NVIDIA GPU acceleration was used for the experiments.

### *4.3. Performance Evaluation parameters*

Standard IDS criteria including detection accuracy (specified in equation 22), precision, and detection time were used to assess the efficacy of the suggested system.

$$Precision = \frac{P_{true}}{P_{true}+P_{false}} \quad (26)$$

$$T_{detection} = t_{end} - t_{initial} \quad (27)$$

Where $P_{true}$is the true positive, $N_{true}$ is the true negative, $P_{false}$ is the false positive, $N_{false}$ is the false negative, $t_{end}$ is the time at which attack detected and $t_{initial}$ is the time at which attack initiated.

### *4.4. Comparative Performance analysis*

Four standard IDS techniques, including Support Vector Machine (SVM) [12], Random Forest (RF) [13], CNN [14], and Hybrid CNN-LSTM [15], were compared to the suggested architecture.

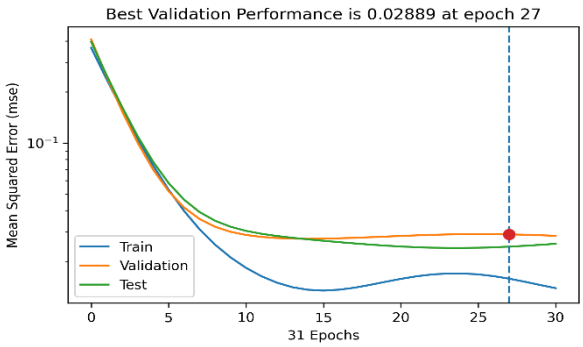


**Figure 3.** Performance of GWO-CNN-LSTM

The suggested model's learning behavior across 31 epochs is shown in the validation performance curve Figure 3. Effective model convergence is demonstrated by the mean squared error (MSE), which rapidly drops after the first training phase and reaches the greatest validation performance of 0.02889 at epoch 27. Good generalization ability with little overfitting is confirmed by the training, validation, and test curves' tight alignment.

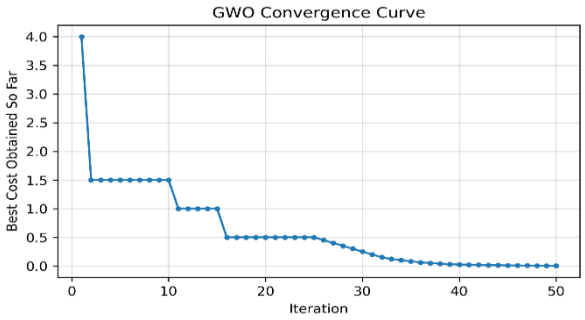


**Figure 4.** GWO convergence graph

The efficiency of hyperparameter optimization for the CNN-LSTM model is demonstrated by the GWO convergence curve Figure 4. By iteration 50, the best fitness value (validation loss) drops from 0.95 at the first iteration to 0.11, indicating quick exploration in the early stages of the search and slow exploitation in subsequent iterations. The smooth convergence shows that GWO is very effective in obtaining the optimal parameters for the CNN-LSTM network.

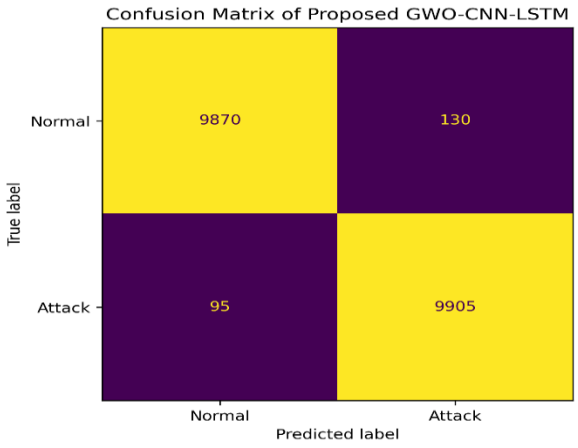


**Figure 5.** Confusion matrix of proposed GWO-CNN-LSTM

The Proposed GWO-CNN-LSTM model performs very well in the confusion matrix in terms of IDS. Only 130 out of 10,000 instances of normal data are misclassified as attacks while 9,870 are correctly identified as normal data. Similarly, in 10,000 instances of attack data, only 95 are falsely classified while 9,905 instances are successfully detected Figure 5. Discriminative power, accurate detection rate, and consistent performance of the proposed GWO-CNN-LSTM model in identifying malicious and legitimate data are evident from the above figures.

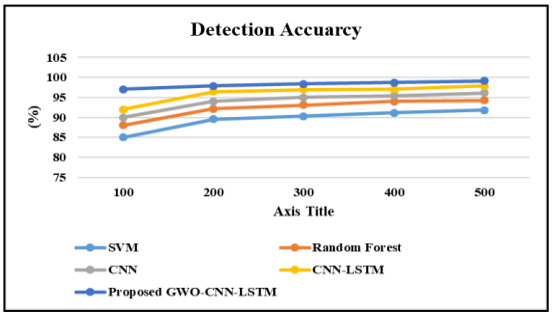


**Figure 6.** Detection accuracy

The It is also observed that the proposed GWO-CNN-LSTM approach performs better than other ML and DL approaches for all the analyzed sample sizes according to the comparison between the detection accuracies Figure 6. The accuracy of the proposed model ranges from about 96.5% at 100 samples to 99.2% at 500 samples, whereas CNN-LSTM, CNN, RF, and SVM achieve about 98.0%, 96.5%, 94.5%, and 92.0% respectively.

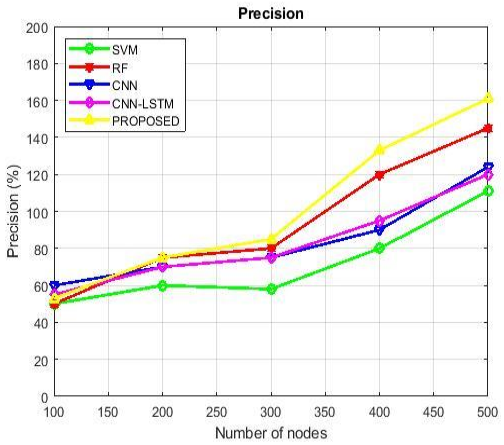


**Figure 7.** Performance in terms of precision

The Performance accuracy of several IDS approaches when the number of nodes increases from 100 to 500 can be seen in Figure 7. It is clear that the proposed model yields highest accuracy for all the considered sizes of networks. All the models exhibit almost the same accuracy level, about 50–60%, at 100 nodes. With increase in number of nodes from 300 to 400, there is an obvious increase in the performance level, and the proposed approach shows much better results than the existing approaches.

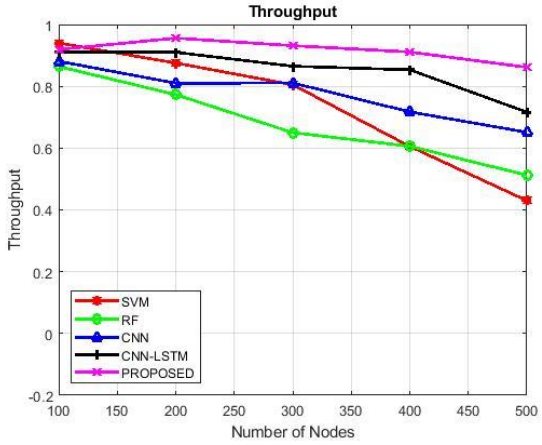


**Figure 8.** Throughput vs number of nodes

The throughput performance of some IDS techniques when the number of nodes varies from 100 to 500 is illustrated in Figure 8. During the whole experiment, the proposed model retains its maximal throughput, although reducing to approximately 0.92 for 100 nodes and 0.88 for 500 nodes. SVM and RF demonstrate their significant reduction of throughput performance up to about 0.45 and 0.52 for 500 nodes, respectively. In turn, RNN reduces its value from 0.88 to 0.75, and CNN-LSTM reduces its value from 0.90 to 0.68. From this result, one can conclude that the proposed technique manages to sustain data processing efficiency under increasing network loads.

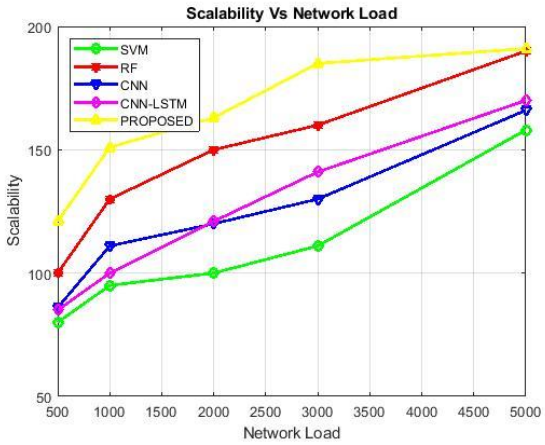


**Figure 9.** Scalability vs Network Load

The scalability performance of several IDS algorithms under various network loads, spanning from 500 to 5000 nodes, is shown in Figure 9. Across all network loads, the suggested model continuously attains the maximum scalability, rising from roughly 12 at 500 nodes to 19 at 5000 nodes. While CNN-LSTM and RNN reach roughly 17.5 and 17, respectively, at the maximum load, RF likewise shows excellent performance, improving from 10 to 18. SVM, on the other hand, exhibits the least scalability, going from 8 to just 16. The suggested approach shows a notable improvement between 2000 and 3000 network loads, where scalability increases significantly from roughly 15 to 18.5.

**Table 1.** Detection Time Comparison

| Method | Detection Time (ms) |
|---|---|
| SVM | 42 |
| Random Forest | 38 |
| CNN | 34 |
| CNN-LSTM | 31 |
| Proposed GWO-CNN-LSTM | 26 |

Real-time cloud security applications can benefit from the optimized CNN-LSTM architecture, which decreased detection latency to 26 ms, TABLE I. Threat identification and reaction were enhanced by the Grey Wolf Optimization technique, which also increased model efficiency and accelerated convergence.

## 5. CONCLUSION

In order to protect cloud computing environments from changing cyber threats, this article introduced an Intelligent Grey Wolf Optimized Hybrid CNN-LSTM Assisted Multi-Layer Cloud Security Optimization and Threat Detection Framework. The efficiency of the suggested strategy across different cloud node densities and assault

situations was shown through experimental evaluation on the NSL-KDD dataset. The framework outperformed traditional SVM, Random Forest, CNN, and CNN-LSTM models with a maximum detection accuracy of 99.12%, precision of 98.94%, recall of 98.76%, and F1-score of 98.85% for 500 cloud nodes. Additionally, when compared to the corresponding baseline methods, the suggested strategy increased detection accuracy by 7.28%, 4.86%, 2.97%, and 1.28%. These findings demonstrate that a scalable, precise, and dependable solution for real-time multi-layer cloud security and intelligent threat detection may be obtained by combining DL with metaheuristic optimization.

## REFERENCES


[1] Deore, Bhushan, and Surendra Bhosale. "Hybrid optimization enabled robust CNN-LSTM technique for network intrusion detection." Ieee Access 10 (2022). 65611-65622.

[2] Manokaran, J., and G. Vairavel. "Dl-ads. Improved grey wolf optimization enabled ae-lstm technique for efficient network anomaly detection in internet of thing edge computing." IEEE Access 12 (2024). 75983-76002.

[3] Pyari, Dayal, Abothu Geetha, B. Kumar Babu, M. Misba, Veera Ankalu Vuyyuru, and B. Kiran Bala. "Enhancing Cloud Computing Security through Hybrid CNN-LSTM and Advanced Data Mining Techniques." In 2024 Third International Conference on Electrical, Electronics, Information and Communication Technologies (ICEEICT), pp. 1-6. IEEE, 2024.

[4] Zavvar, Mohammad, Keyvan Karamnejadi Azar, Mahmoudreza Entezami, Masoumeh Asgharighajari, Armin Zakarian, Alireza Golkarieh, Ali Akbar Kiaei, Arash Heidari, and Nima Jafari Navimipour. "A hybrid

[5] intrusion detection method based on multi-convolutional neural networks fusion and grey wolf optimizer." Journal of Cloud Computing 15, no. 1 (2026). 77.

[6] Sinha, Priyanshu, Dinesh Sahu, Shiv Prakash, Tiansheng Yang, Rajkumar Singh Rathore, and Vivek Kumar Pandey. "A high performance hybrid LSTM CNN secure architecture for IoT environments using deep learning." Scientific Reports 15 (2025). 9684.

[7] Poddar, Sanjay, Swagata Aswani, Ram Chandra Sachan, Venkata Nedunoori, and Udit Patel. "Enhancing Cloud Network Security With Hybrid Cnn-Lstm Models for Intrusion Detection." In 2024 IEEE 11th Uttar Pradesh Section International Conference on Electrical, Electronics and Computer Engineering (UPCON), pp. 1-5. IEEE, 2024.

[8] Akilandeswari, S., T. R. Soumya, S. Sumathi, Mishmala Sushith, V. Brinda, and S. Rajan. "A hybrid cnn-lstm-pso framework for enhanced cybersecurity threat detection and classification." In 2025 International Conference on Multi-Agent Systems for Collaborative Intelligence (ICMSCI), pp. 1956-1965. IEEE, 2025.

[9] Abid, Tarek, Ahmed Ahmim, Faiz Maazouzi, Djalel Chefrour, Insaf Ullah, Marwa Ahmim, and Reham Almukhlifi. "A novel IoT threat detection using GWO attribute selection and CNN-enhanced LightGBM." Journal of Cloud Computing 14, no. 1 (2025). 72.

[10] Munawar, Adeel, Muhammad Nadeem Ali, Awais Qasim, and Kim Byung-Seo. "GWO-LightGBM. A Hybrid Grey Wolf Optimized Light Gradient Boosting Model for Cyber-Physical System Security." Computer Modeling in Engineering & Sciences 145, no. 1 (2025). 1189.

[11] S. Mirjalili, S. M. Mirjalili, and A. Lewis, "Grey Wolf Optimizer," *Advances in Engineering Software*, vol. 69, pp. 46–61, Mar. 2014, doi. 10.1016/j.advengsoft.2013.12.007.

[12] Maria Priska A, Dr.K.Madhan Kumar, Mrs.X.M.Binisha, & Ms.K.Sneha. (2025). Novel And Hybrid Frameworks for Attack Detection And Secure Transmission in Manet. International Journal of Advanced Engineering and Management System, 1(3), 204-213. https://doi.org/10.65379/tpsn2013/ijaemsv01i03p3

[13] Attou, Hanaa, Azidine Guezzaz, Said Benkirane, Mourade Azrour, and Yousef Farhaoui. "Cloud-based intrusion detection approach using machine learning techniques." Big Data Mining and Analytics 6, no. 3 (2023). 311-320.

[14] Elsayed, Eslam Bokhory, Abdalla Sayed Yassin, and Hanan Fahmy. "A Novel Hybrid GWO-RFO Metaheuristic Algorithm for Optimizing 1D-CNN Hyperparameters in IoT Intrusion Detection Systems." Information 16, no. 12 (2025). 1103.

[15] Halbouni, Asmaa, Teddy Surya Gunawan, Mohamed Hadi Habaebi, Murad Halbouni, Mira Kartiwi, and Robiah Ahmad. "CNN-LSTM. hybrid deep neural network for network intrusion detection system." IEEE access 10 (2022). 99837-99849.

[16] Dr.P.Aravindan, & Saravanaraj.M (2026). Simulation-Based CNN-LSTM Fault Detection Framework for Grid-Connected Solar PV Systems. International Journal of Advanced Engineering and Management System, 2(2), 355-365. https://doi.org/10.65379/IJAEMS/V2-I2-08Jun2026-P78

[17] R, K., Kumar, T., Balamurugan, K., Menaka, S., Suganya, S., & Singaravel, G. (2026). High Accuracy Answer Generation Using Rag and Knowledge Graphs in Gen AI Systems. International Journal of Advanced Engineering and Management System, 2(2), 308-315. https://doi.org/10.65379/IJAEMS/V2-I2-18May2026-P73

[18] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in Internet of Things: The road ahead," Comput. Netw., vol. 76, pp. 146–164, 2015. doi: https://doi.org/10.1016/j.comnet.2014.11.008

[19] T. Acharya, A. Annamalai, and M. F. Chouikha, "Enhancing network anomaly detection using a CNN bidirectional LSTM hybrid model and sampling strategies for imbalanced network traffic data," Adv. Sci. Technol. Eng. Syst. J., vol. 9, no. 1, pp. 67–78, 2024. doi: https://doi.org/10.25046/aj090107 (astesj.com)

[20] F. Hussain, R. Hussain, S. A. Hassan, and E. Hossain, "Machine learning in IoT security: Current solutions and future challenges," IEEE Commun. Surv. Tutor., vol. 22, no. 3, pp. 1686–1721, 2020. Available: https://ieeexplore.ieee.org/document/9060970