*Journal of Information & Optimization Sciences*
ISSN 0252-2667 (Print), ISSN 2169-0103 (Online)
Vol. 46 (2025), No. 6, pp. 1995–2004
DOI : 10.47974/JIOS-2028

# HID-AG: Elevating cybersecurity with HybridIDNet and PCA-anomalyguard for intrusion detection excellence

Balamurugan K. *
Sudalaimuthu T. †
*Department of Computer Science and Engineering*
*Hindustan Institute of Technology and Science*
*Hindustan University*
*Padur 603103*
*Chennai*
*India*

Bakkialakshmi VS. §
*Department of Computing Technologies*
*SRM Institute of Science and Technology*
*SRM University*
*Kattankulathur 603203*
*Tamil Nadu*
*India*

**Abstract**

Anomalous patterns in network traffic remain a critical obstacle in modern cybersecurity. Conventional intrusion detection systems (IDS) frequently face limitations in recognizing subtle or adaptive anomalies that signal advanced cyberattacks. To address these challenges, this study presents HID-AG — an IDS specifically developed to enhance anomaly detection capabilities. At its core, HID-AG incorporates HybridIDNet, which synergizes the strengths of CNNs, RNNs, and RF. Within this framework, the CNN module specializes in extracting spatial features, enabling HID-AG to identify anomalies embedded within complex network traffic structures. Employing this HybridIDNet architecture, the proposed approach achieves a notable accuracy of 97.84%, underscoring its effectiveness in

* *ORCID-ID:* **0009-0002-2034-3927**
† *ORCID-ID:* **0000-0003-0371-9371**
§ *ORCID-ID:* **0000-0002-0886-0553**

* *E-mail:* **bigdata.balamurugan@gmail.com (Corresponding Author)**
† *E-mail:* **Sudalaimuthut@gmail.com**
§ *E-mail:* **bakkyam30@gmail.com**

© Taru Publications

confronting intricate cybersecurity threats. Implemented in Python, HID-AG promotes both accessibility and transparency, offering cybersecurity practitioners a practical and adaptable tool for real-world network anomaly detection. Beyond detailing the technical architecture, this paper also delivers a thorough evaluation of HID-AG's performance in addressing anomaly detection tasks.

***Subject Classification:*** *68T07, 68T45, 68M10.*

***Keywords:*** *AnomalyGuard, Convolutional neural network (CNN), Cyber security, Deep learning (DL), HybridIDNet, Machine learning (ML), Random forest classifier (RF), Recurrent neural networks (RNN).*

## 1. Introduction

With the rapid expansion of digital connectivity and data exchange, safeguarding computer systems and networks has become a critical priority. Among the essential tools in the cybersecurity arsenal is Intrusion Detection (ID) as shown in Figure 1 [1] [2]. By employing these techniques, IDS can swiftly detect and respond to a wide spectrum of cyber threats, including viruses, malware, and unauthorized system access [3] [4] [5]. In today's highly interconnected environment, where the consequences of cyberattacks can be extensive and damaging, ID serves as a vital frontline defense and plays a central role in comprehensive cybersecurity strategies [6] [7]. Within this framework, the integration of HybridIDNet (Hybrid Intrusion Detection Network) with PCA-AnomalyGuard (Principal Component Analysis-based Anomaly Detection) represents a powerful approach to enhancing cybersecurity resilience, delivering a dynamic and adaptive barrier against diverse threats posed by cyber adversaries [8] [9]. PCA-AnomalyGuard, in particular, harnesses the analytical capability of Principal Component Analysis (PCA) to identify subtle anomalies in system activity, enabling a proactive stance in detecting behaviors that may signal security breaches [10]. The combined use of HybridIDNet and PCA-AnomalyGuard effectively addresses existing limitations, advancing ID capabilities into a new phase of effectiveness [11]. This hybrid methodology strengthens defenses against known attack vectors while offering the adaptability needed to detect novel or evolving cyber threats [12], [13].

The following sections examine the technical foundations, deployment aspects, and practical implications of HybridIDNet and PCA-AnomalyGuard in real-world cybersecurity contexts [14] [15].

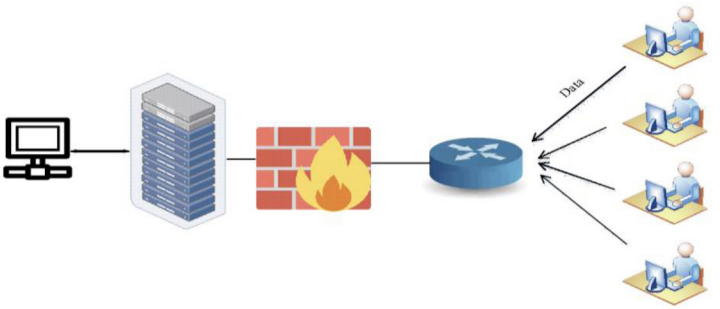



**Figure 1**
**Intrusion Detection System**

## 2. Related Works

Several prior studies have explored anomaly detection in smart grid environments. The work in [16] addressed detection constraints by leveraging both real-time raw network data and the KDD99 dataset to identify abnormalities. Similarly, [17] developed an evaluation framework to systematically and repeatedly test anomaly detection techniques for smart grid infrastructure, ensuring comparability across methods. In [18], an intelligent classification method was introduced to accurately identify diverse attack types targeting smart power grids. A hybrid deep-learning model for detecting denial-of-service attacks was proposed in [19], achieving high detection accuracy; however, the study did not fully address deployment or maintenance challenges in practical grid environments. Finally, [20] demonstrated a robust intrusion detection scheme, yet its adaptability remains questionable due to dependence on specific datasets and preselected features. Unlike these studies, which often focus on specific datasets, fixed feature sets, or single attack types, our approach integrates HybridIDNet with PCA-AnomalyGuard to deliver both high detection accuracy and adaptability to evolving threats. While previous works primarily evaluate detection methods in controlled settings, we emphasize a design that can generalize across varied real-world scenarios, ensuring resilience against both known and emerging anomalies.

## 3. Methodology

This study presents HID-AG, a novel intrusion detection system engineered to tackle key challenges in modern cybersecurity, with a

particular emphasis on anomaly detection. Built upon the powerful HybridIDNet framework, HID-AG leverages the combined capabilities of CNNs, RNNs, and RF. This purposeful integration equips the system to effectively address and manage the complexities of subtle and evolving anomalies in network traffic. The fusion of these distinct neural network models reflects HID-AG's focus on delivering a versatile and adaptive detection mechanism, representing a notable step forward in the field of intrusion detection.

## 4. Dataset

The CIC-DDoS2019 dataset contains a total of 50,063,112 traffic records, of which 50,006,249 correspond to DDoS attack instances and 56,863 represent benign network activity (See Table 1). Each entry in the dataset is described by an average of 86 distinct features. Alongside the raw traffic data, the dataset also includes a reference table categorizing the various attack types, accompanied by concise descriptions for each category. This dataset is particularly valuable for evaluating intrusion detection (ID) models tailored to Smart Grid network environments, as it offers a comprehensive mix of malicious and normal traffic samples. Such curated datasets are crucial for benchmarking deep learning (DL) and machine learning (ML) techniques in both binary and multi-class classification scenarios, enabling a thorough assessment of their capacity to identify and mitigate diverse attack vectors.

**Table 1**

**Dataset Characteristics**

| Types | Training Data | Testing Data | Label |
|---|---|---|---|
| **Benign** | 106,874 | 26,921 | 0 |
| **DDoS** | 997,054 | 314,716 | 1 |
| **Total Data** | **11,03,928** | **341,637** | |

## 5. Proposed Model – HybridIDNet: An Innovative Hybrid Intrusion Detection Model

Intrusion Detection Systems (IDS) are vital for protecting computer networks by detecting and mitigating security threats. HybridIDNet (Hybrid Intrusion Detection Network) is introduced as an advanced solution that integrates Recurrent Neural Networks (RNNs), Convolutional

Neural Networks (CNNs), and the traditional Random Forest (RF) algorithm to create a comprehensive intrusion detection model. This hybrid design captures temporal dependencies, spatial patterns, and fine-grained features within network traffic. RNNs, well-suited for sequential data, model temporal relationships through bidirectional layers that analyze sequences in both forward and backward directions. CNNs, adept at detecting spatial correlations, are implemented as 1D convolutional layers for spatial feature extraction. A fusion layer merges the outputs from the bidirectional RNNs and 1D CNNs, allowing effective utilization of both temporal and spatial insights. The RF component functions as an ensemble classifier, building multiple decision trees and determining predictions via majority voting. Model training begins with parameter initialization, followed by backpropagation, where the loss gradient is calculated and parameters updated using optimization algorithms such as Stochastic Gradient Descent (SGD) or Adam. The RF ensemble is trained concurrently with the deep learning components, ensuring diverse decision boundaries. During detection, HybridIDNet applies the learned parameters to incoming network traffic. The bidirectional RNN layers reveal temporal patterns in activity sequences, while the 1D CNN layers identify spatially localized indicators of intrusions. The fusion layer then consolidates these complementary features into a unified representation, enabling precise and adaptive intrusion detection.

## 6. Novelty of the Work

The novelty of the presented work lies in the holistic and synergistic integration of multiple advanced technologies within the IDS, HID-AG. While many existing systems focus on individual aspects, HID-AG uniquely combines CNNs, RNNs, and RF into a unified architecture called HybridIDNet. This amalgamation empowers HID-AG to confront the intricate challenges posed by anomalies in cybersecurity with a comprehensive approach. Beyond this, HID-AG introduces a ground-breaking feature extraction mechanism named AnomalyGuard, further enhancing its anomaly detection capabilities. AnomalyGuard operates synergistically with CNNs, RNNs, and RF.

## 7. Results and Discussions

The implementation of this project was carried out on an AMD Epyc 7702P system equipped with an NVidia A100 GPU and 16GB of RAM. The

execution environment was set up using Jupyter Notebook, and the programming language utilized for the implementation was Python. Algorithm effectiveness is evaluated using four metrics: Accuracy, Precision, Recall, and F1score. Following the importation of the CIC-DDoS2019 dataset, a meticulous process of data preprocessing was undertaken. This crucial step involved preparing and refining the dataset to ensure its suitability for subsequent analysis and modeling. Figure 2 illustrates the Count of Occurrence in Labels.

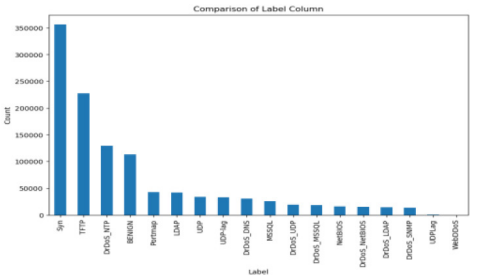



**Figure 2**

**Count of Occurrence in Labels**

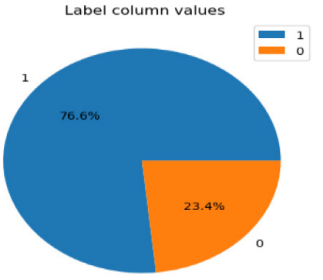



**Figure 3**

**Target Distribution**

The dataset distribution reveals that a significant portion, specifically 76.6%, pertains to DDoS (Distributed Denial of Service) instances, while the remaining 23.4% represents normal or non-malicious data. Figure 3

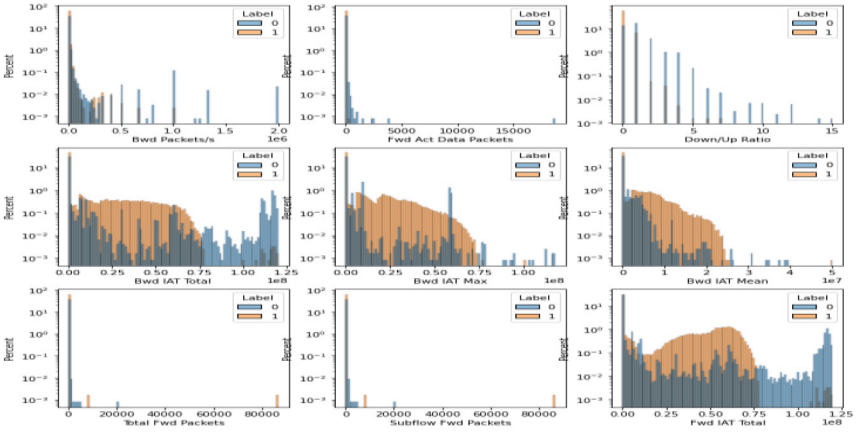



**Figure 4**

**Target Distribution in Various Features**

depicts the Distribution of Targets in the Dataset. Understanding this distribution is essential for developing a predictive model that can effectively capture and distinguish between these two distinct categories, contributing to the overall efficacy of ID and cybersecurity measures. Figure 4 depicts the distribution of targets across different features.

Table 2 presents a comprehensive performance evaluation of various models, showcasing their accuracy, precision, sensitivity, specificity, and F1 Score. Each model, from AlexNet to the Proposed Model, is meticulously assessed, providing a detailed insight into their individual strengths and capabilities.

**Table 2**

**Performance Evaluation of Various Model**

| Model | Accuracy | Precision | Sensitivity | Specificity | F1 Score |
|---|---|---|---|---|---|
| AlexNet | 86.68 | 87.73 | 86.75 | 87.48 | 86.49 |
| MobileNet | 89.08 | 89.12 | 89.78 | 90.62 | 80.58 |
| RNN | 90.37 | 90.42 | 91.69 | 90.45 | 91.07 |
| VGG19 | 92.45 | 93.39 | 92.28 | 92.19 | 92.69 |
| CNN | 93.85 | 94.07 | 94.63 | 93.08 | 93.54 |
| ANN | 94.78 | 94.66 | 94.15 | 94.88 | 94.37 |
| Proposed Model | 97.84 | 96.39 | 97.48 | 96.88 | 97.84 |

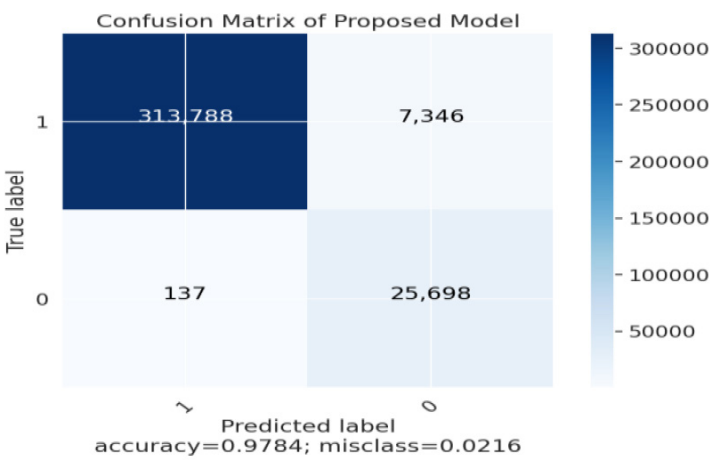



**Figure 5**

**Confusion Matrix of Suggested Model**

The accuracy of the model in predicting both positive and negative cases is a comprehensive assessment of its overall performance. This metric is crucial for evaluating classification algorithms. With a remarkable accuracy of 97.84%, the suggested model surpasses its competitors. This improved precision is evidence of the model's generalizability across different cases and also of its capacity to reduce false positives and negatives (See Figure 5). For real-world applications, the model's 97.84% accuracy means you can trust its predictions with a lot of weight.

## 8. Conclusion and Future Work

In conclusion, this work marks a significant step forward in Intrusion Detection Systems (IDS) by tackling key cybersecurity challenges, particularly those linked to anomaly detection. The core contribution is the development of HID-AG, an advanced IDS that integrates HybridIDNet with AnomalyGuard for enhanced feature extraction. This combination leverages the complementary strengths of CNNs, RNNs, and RF, forming a robust ensemble for identifying anomalies. Within HID-AG, AnomalyGuard plays a critical role in boosting the system's capability to detect and characterize irregularities. By coupling AnomalyGuard's feature extraction with CNN- and RNN-based spatial and temporal modeling, and enhancing interpretability and resilience through RF, HID-AG delivers both high precision and adaptability. Comparative evaluation shows that HID-AG achieves an accuracy of 97.84%, surpassing existing benchmark approaches.

## References

[1] P.R. Kumar, G. B. Mohammad, P. Narsimhulu, D. Narasappa, L. P. Maguluri, S. Singh, and S. Selvarajan, "Computer modeling approaches for blockchain-driven supply chain intelligence: A review on enhancing transparency, security, and efficiency," *Computer Modeling in Engineering & Sciences*, pp. 1–40 (2025).

[2] B Shilpa, P.R.Kumar, and Rajesh Kumar Jha, "LoRa DL: a deep learning model for enhancing the data transmission over LoRa using autoencoder", *The Journal of Supercomputing*, vol. 79, pp. 17079 –17097 (2023).

[3] P.R. Kumar, G. B. Mohammad, and P Dileep, "Real-Time Heart Rate Monitoring System using Least Square Method", *Annals of the*

*Romanian Society for Cell Biology,* vol. 25, Issue. 6, pp. 16302 – 16308 (2021).

[4] M. A. Khan, A. Rehman, K. M. Khan, M. A. Al Ghamdi, and S. H. Almotiri, "Enhance intrusion detection in computer networks based on deep extreme learning machine," *Computers, Materials & Continua*, vol. 66, no. 1 (2021).

[5] J. Parikh, A. Bhargava, S. M. Antony, Y. Puri, U. Maniar, D. Singhal, M. Singh, and M. Sharma, "An edge AI based real-time spatial monitoring system," *Journal of Information and Optimization Sciences,* vol. 46, no. 1, pp. 33–42 (2025)

[6] S. Altamimi and Q. Abu Al-Haija, "Maximizing intrusion detection efficiency for IoT networks using extreme learning machine," *Discover Internet of Things*, vol. 4, no. 1, pp. 5 (2024).

[7] P. William, V. N. R. Inukollu, V. Ramasamy, P. Madan, A. Shrivastava, and A. Srivastava, "Implementation of machine learning classification techniques for intrusion detection system," in *Proc. 2023 4th Int. Conf. Intelligent Engineering and Management (ICIEM)*, pp. 1–7 (May 2023).

[8] Z. S. Alsham, E. Bahçekapılı, and A. Ayaz, "Trends in IoT applications in smart campuses: A topic modeling approach," *COLLNET Journal of Scientometrics and Information Management*, vol. 19, no. 1, pp. 21–40 (2025)

[9] G.B. Mohammad, S. Shitharth, and P. R. Kumar, "Integrated Machine Learning Model for an URL Phishing Detection", *International Journal of Grid and Distributed Computing,* vol. 14, no. 1, pp: 513-529 (2021).

[10] H. Zhang, D. Zhu, Y. Gan, and S. Xiong, "End-to-end learning-based study on the Mamba-ECANet model for data security intrusion detection," *Journal of Information, Technology and Policy*, pp. 1–17 (2024).

[11] M. N. Nikhate, K. L. Bondar, and S. B. Kiwne, "Fixed point theorems for self-mappings in generalized metric spaces," *Journal of Dynamical Systems and Geometric Theories,* vol. 21, no. 2, pp. 121–126 (2023).

[12] B Shilpa, P. R. Kumar and R K. Jha, "Spreading Factor Optimization for Interference Mitigation in Dense Indoor LoRa Networks", *IEEE IAS Global Conference on Emerging Technologies* (GlobConET), pp. 1-5 (2023).

[13] Z. Jin, J. Zhou, B. Li, X. Wu, and C. Duan, "FL-IIDS: A novel federated learning-based incremental intrusion detection system," *Future Generation Computer Systems*, vol. 151, pp. 57–70 (2024).

[14] H. Yu, W. Zhang, C. Kang, and Y. Xue, "A feature selection algorithm for intrusion detection system based on the enhanced heuristic optimizer," *Expert Systems with Applications*, vol. 265, pp. 125860 (2025).

[15] D. Park, S. Kim, H. Kwon, Dongil Shin, and Dongkyoo Shin, "Host-based intrusion detection model using siamese network," *IEEE Access*, vol. 9, pp. 76614–76623 (2021).

[16] S. L. Narayanan, M. Kasiselvanathan, K. B. Gurumoorthy, and V. Kiruthika, "Particle swarm optimization based artificial neural network (PSO-ANN) model for effective k-barrier count intrusion detection system in WSN," *Measurement: Sensors*, vol. 29, pp. 100875 (2023).

[17] M. Sun, Y. Lai, Y. Wang, J. Liu, B. Mao, and H. Gu, "Intrusion detection system based on in-depth understandings of industrial control logic," *IEEE Transactions on Industrial Informatics*, vol. 19, no. 3, pp. 2295–2306 (2022).

[18] A. Deshmukh and K. Ravulakollu, "An efficient CNN-based intrusion detection system for IoT: Use case towards cybersecurity," *Technologies*, vol. 12, no. 10, pp. 203 (2024).

[19] R. Raj, A. Reyaz, P. Kumar, N. N. Gia, and S. E. Zohara, "Protocol translation middleware for scalable and efficient IoT communications," *TARU Journal of Sustainable Technologies and Computing*, vol. 1, no. 2, pp. 53–72 (2019).

[20] R. K. Moje, B. Tiple, S. M. Patil, T. Jadhav, A. P. Munshi, and A. Revekar, "A framework for multi-task learning optimization in deep neural networks: Balancing task priorities for improved performance," *Journal of Information and Optimization Sciences*, vol. 46, no. 4-B, pp. 1141–1151 (2025).

*Received December, 2024*