Indonesian Journal of
Multidiciplinary Research

Journal homepage: http://ejournal.upi.edu/index.php/ IJOMR/

A Hybrid Machine Learning Approach for Web-Based Anomaly Detection in Network Traffic: Strengthening Cybersecurity Education and Advancing SDGs 4 and 9

Emmanuel John Anagu, Precious Njoya Philip*

Federal University Wukari, Taraba, Nigeria
*Correspondence: E-mail: anague@fuwukari.edu.ng

ABSTRACT

The increasing sophistication of cyber threats and the complexity of network traffic demand innovative strategies in both cybersecurity systems and digital education. This study proposes a hybrid machine learning approach (combining Support Vector Machine (SVM), Artificial Neural Network (ANN), and Long Short-Term Memory (LSTM)) to detect anomalies in network traffic with high accuracy. Trained on the CIC-DDoS2019 dataset, the models achieved over 99% accuracy, with the hybrid stacking model performing most effectively. The model was deployed in a real-time web-based interface to serve both detection and instructional purposes. This dual-function system supports cybersecurity education by providing students with a hands-on environment to explore, analyze, and visualize network anomalies. The research contributes to SDG 4 by enhancing digital literacy and to SDG 9 by promoting technological innovation in cybersecurity. The study highlights how educational integration of AI-driven anomaly detection tools can foster a deeper understanding of network protection in the digital age.

ARTICLE INFO

Article History:
Submitted/Received 02 Mar 2025
First Revised 09 Apr 2025
Accepted 13 Jun 2025
First Available online 14 Jun 2025
Publication Date 01 Sep 2025

Keyword:
Anomaly detection;
Cybersecurity education;
Hybrid machine learning;
SGDs 4;
Web application.

1. INTRODUCTION

The rapid expansion of digital infrastructure and the integration of connected devices across sectors have increased the vulnerability of network systems to cyber threats (Djenna *et al*., 2021; George *et al*., 2024). As cyberattacks grow in complexity and frequency, conventional Intrusion Detection Systems (IDS) that rely on signature-based methods often fail to detect novel or evolving threats in real time. This gap necessitates more adaptive and intelligent systems capable of learning from patterns in network traffic and identifying anomalies beyond predefined rules (Abdallah *et al*., 2024; Kumar & Venugopalan, 2017).

Machine learning (ML) offers a promising framework for improving anomaly detection by classifying network behavior based on learned data patterns. However, most existing ML models in this domain are limited by issues such as data imbalance, low generalizability in real-world traffic, and a lack of interpretability. While deep learning techniques such as LSTM and CNN have shown higher accuracy, few studies have focused on combining models to optimize performance while also making such systems accessible for educational and institutional use (Shahin *et al*., 2024; Aribisala *et al*., 2022).

Addressing these gaps, this study proposes a hybrid machine learning approach that combines Support Vector Machines (SVM), Artificial Neural Networks (ANN), and Long Short-Term Memory (LSTM) through a stacking technique. The integrated model is trained on the CIC-DDoS2019 dataset and deployed via a user-friendly web application for real-time anomaly detection. In addition to its technical contribution, the platform is designed to serve as an educational tool, providing a hands-on learning environment where students and educators can simulate cyberattacks, analyze detection results, and engage with core concepts in cybersecurity and data science.

This research supports the goals of SDG 4 (Quality Education) by enhancing digital literacy and cybersecurity competence among learners, and SDG 9 (Industry, Innovation and Infrastructure) by promoting the use of advanced AI tools for secure digital ecosystems. The purpose of this study is to develop an effective hybrid model for anomaly detection while demonstrating its pedagogical potential. The novelty lies in bridging high-performance detection algorithms with educational applications, and the impact is seen in both enhanced cyber resilience and improved teaching resources in digital technology education.

2. LITERATURE REVIEW

Anomaly detection plays a central role in maintaining the integrity of modern network systems, especially as threats become more sophisticated and dynamic. Traditionally, anomaly detection in network traffic focused on identifying deviations from expected behavior through statistical or rule-based models. However, such approaches often struggle with scalability, adaptability, and real-time responsiveness in high-volume and high-dimensional data environments (Ahmed & Mahmood, 2015; Martins *et al*., 2022).

The evolution of machine learning has provided a transformative approach to this challenge. Models such as SVM, DT, and RF have shown capability in classifying network behaviors. Nevertheless, they tend to underperform in complex and real-time scenarios. Deep learning techniques (particularly LSTM, Convolutional Neural Networks (CNN), and Deep Neural Networks (DNN)) have demonstrated superior performance due to their ability to process sequential patterns and learn high-level features from large datasets (Shahin *et al*., 2024; Aribisala *et al*., 2022).

Recent studies emphasize the benefits of hybrid models that integrate multiple machine learning techniques. Combining shallow and deep learners through ensemble or stacking methods enables models to utilize complementary strengths. For instance, while SVM achieves moderate accuracy alone, its performance improves significantly when paired with deep learners (Abdelkhalek & Mashaly, 2023). Similarly, some researchers (Aribisala *et al*., 2021) utilized CNN and BLSTM with attention mechanisms to classify packets with over 98% accuracy.

While most literature focuses on performance metrics, few address the educational application of such systems. Embedding AI-powered anomaly detection tools into web-based environments offers new possibilities in teaching cybersecurity and AI literacy. These tools support experiential learning, allowing students to experiment with real datasets, train models, and visualize threats dynamically. This aligns with SDG 4.4, which advocates for increasing the number of youth and adults with relevant digital skills, and SDG 9.5, which emphasizes the enhancement of scientific research and technological capacity in developing contexts.

Incorporating these systems into academic curricula not only prepares learners for modern digital environments but also addresses global needs for secure, innovative infrastructures. The integration of machine learning in cybersecurity education fosters interdisciplinary competence that bridges data science, ethics, and real-world problem solving.

Therefore, this study builds upon existing machine learning frameworks and extends their utility into an educational and SDG-aligned context. It highlights not just technical efficiency, but also pedagogical and societal impact.

3. METHODS

This study employed a structured three-phase methodology: data preprocessing, model development, and system deployment. The primary goal was to develop a hybrid machine learning model capable of accurately detecting anomalies in network traffic while also being usable within educational environments for instructional purposes.

3.1. Dataset and Preprocessing

The CIC-DDoS2019 dataset was selected due to its comprehensive inclusion of benign and malicious traffic, particularly Distributed Denial-of-Service (DDoS) attacks. The dataset simulates real-world traffic patterns and is labeled for supervised learning tasks.

Initial preprocessing involved handling missing values, filtering out unreliable records, and normalizing features. To address disparities in feature scales, MinMaxScaler normalization was applied, transforming values to a 0–1 range to prevent issues such as vanishing gradients and overfitting during training.

The dataset was split into training, validation, and testing sets. For binary classification, 80% of the data was used for training, 10% for validation, and 10% for testing. The data distribution across these sets is shown in **Tables 1-3**.

3.2. Model Development

Three machine learning models were developed and evaluated:

(i) SVM: Configured with a linear kernel, degree 3, and cache size of 200 MB.

(ii) ANN: Trained over 199 epochs with batch size 32 using the Adam optimizer and dropout rate of 0.2.

(iii) LSTM: Trained over 20 epochs with batch size 5 and similar optimizer and dropout settings.

Each model used ReLU activation in hidden layers and SoftMax activation in the output layer to support multiclass classification. The configurations are summarized in **Table 4**. The overall data flow and modeling architecture are illustrated in **Figure 1**.

Table 1. Overview of Selected Features from CIC-DDoS2019 Dataset.

#	Characteristics	Main and Max Values
1	Protocol	[0; 17]
2	Fwd Packet Length Max	[0; 32,120]
3	Fwd Packet Length Std	[0; 2221.5562]
4	Bwd Packet Length Min	[0; 1460]
5	Flow Bytes/s	[0; 2,944,000,000]
6	Bwd IAT Total	[0; 119,943,720]
7	Bwd IAT Min	[0; 249]
8	Bwd Header Length	[−2,125,437,950; 1,478,492,170]
9	Bwd Packets/s	[0; 2,000,000]
10	Packet Length Max	[0; 37,960]
11	Packet Length Variance	[0; 43,778,892]
12	SYN Flag Count	[0; 1]
13	ACK Flag Count	[0; 1]
14	URG Flag Count	[0; 1]
15	CWE Flag Count	[0; 1]
16	Down/Up Ratio	[0; 23]
17	Init Fwd Win Bytes	[−1; 65,535]
18	Init Bwd Win Bytes	[−1; 65,535]
19	Fwd Act Data Packets	[0; 18,766]
20	Active Std	[0; 21,352,442]
21	Active Max	[0; 45,536,680]
22	Idle Std	[0; 45,536,680]

Table 2. Data Distribution for Binary Classification Model.

Class	Training	Validation	Testing
Benign	68584	7620	19051
Malicious	695027	77226	193064

Table 3. Data Distribution for Multiclass Classification Model.

Class	Training	Validation	Testing
Multiclass12	763611	84846	212115

Table 4. Model Parameters for ANN, LSTM, and SVM.

Parameter	Artificial Neural Network (ANN)	Long Short-Term Memory (LSTM)	Support Vector Machine (SVM)
Batch Size	32	5	—
Max Epochs	199	20	—
Initial Learning Rate	0.0001	0.0001	—
Optimizer	Adam	Adam	—
Dropout Rate	0.2	0.2	—
Activation Function	ReLU (hidden), Softmax (output)	ReLU (hidden), Softmax (output)	—

Table 4 (continue). Model Parameters for ANN, LSTM, and SVM.

Parameter	Artificial Neural Network (ANN)	Long Short-Term Memory (LSTM)	Support Vector Machine (SVM)
Kernel Type	—	—	Linear
Degree	—	—	3
Probability Estimates	—	—	Enabled
Cache Size (MB)	—	—	200

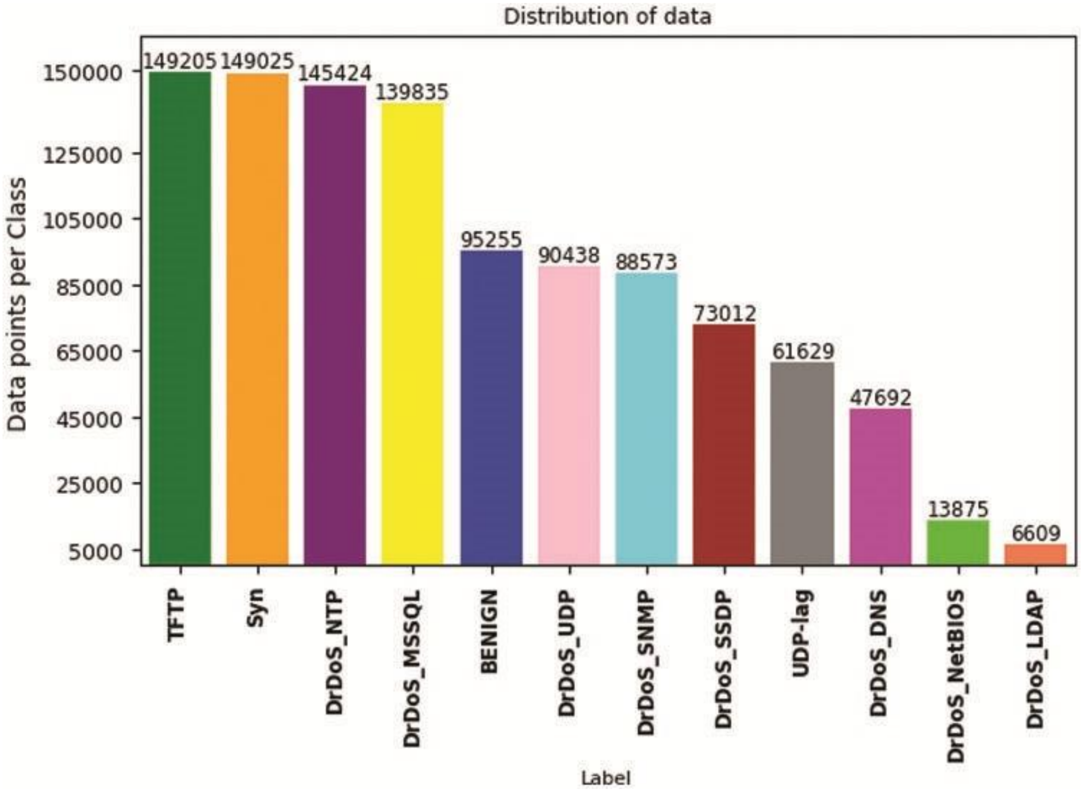


Figure 1. Workflow of Data Preprocessing and Model Deployment.

3.3. Hybrid Modeling Using Stacking

To enhance classification accuracy, a stacking ensemble was implemented. This meta-learning strategy leverages the strengths of base learners (SVM, ANN, and LSTM) by combining their predictions using a secondary classifier. This approach has been shown to reduce false positives and improve model robustness across diverse traffic patterns.

3.4. Web Application Deployment

The best-performing model (i.e. LSTM) was integrated into a lightweight, browser-accessible web application. Built with Python and modern web technologies, the interface allows users to input network parameters and receive instant feedback on anomaly presence.

This system serves two purposes:

(i) Real-time anomaly detection for operational environments.

(ii) Hands-on learning tool for students exploring cybersecurity, anomaly detection, and AI model behavior.

Such integration supports experiential learning, reinforcing digital literacy as advocated by SDG 4, and demonstrates innovation in cybersecurity infrastructure under SDG 9.

4. RESULTS AND DISCUSSION

This section presents a detailed analysis of the performance of machine learning models (SVM, ANN, and LSTM) in classifying network traffic for anomaly detection. In addition, it evaluates the effectiveness of a hybrid model using a stacking approach. The models are compared based on four key metrics: precision, recall, F1-score, and accuracy. Further, the implementation of the LSTM-based detection model within a web-based educational interface is evaluated in terms of both operational value and educational impact.

4.1. Model Evaluation and Comparative Performance

To assess model effectiveness, the preprocessed CIC-DDoS2019 dataset was split into training, validation, and testing sets as described in the Methodology section. Each model was trained using identical data splits to ensure consistency across comparisons. The performance of each classifier is summarized in **Table 5**.

Table 5. Evaluation Metrics of SVM, ANN, and LSTM Models.

Algorithm	Precision (%)	Recall (%)	F1-score (%)	Accuracy (%)
Support Vector Machine	96	99	99	99.91
Long Short-Term Memory	90	100	99	99.98
Artificial Neural Net	99	99	99	99.97

The results indicate that all three models achieved high levels of accuracy, exceeding 99%, which underscores the robustness of the preprocessing pipeline, feature scaling strategy, and the richness of the dataset used. The LSTM model showed the highest overall accuracy (99.98%), followed by the ANN (99.97%) and SVM (99.91%).

While the differences in performance metrics may seem minimal at first glance, they are significant in contexts where even small gains in detection capability translate into meaningful reductions in undetected attacks or false alerts. For instance, a 1% reduction in false negatives in a real-time cybersecurity system can represent hundreds of avoided breaches in large-scale network environments:

(i) SVM. The SVM model demonstrated strong performance with particularly high recall and precision values. The linear kernel effectively captured the decision boundary for the relatively linearly separable data patterns in this dataset. Its relatively simple architecture made it computationally efficient and fast to train. However, SVM lacks the sequential memory advantage of LSTM and the layered feature abstraction of ANN, limiting its effectiveness in highly non-linear or time-dependent contexts.

(ii) ANN. The ANN yielded the highest precision, demonstrating excellent performance in distinguishing between benign and malicious traffic patterns. Its performance reflects the benefit of deep feedforward layers that can extract hierarchical features from normalized input vectors. With the use of ReLU activation and dropout, the ANN achieved balance between learning depth and generalization. However, ANN models may struggle with capturing temporal dependencies inherent in network traffic without specific architectural adjustments.

(iii) LSTM. The LSTM network achieved the highest recall rate of 100%, highlighting its capability to detect nearly all instances of anomalies. As a recurrent neural network, LSTM excels in understanding temporal sequences—a valuable trait in identifying patterns in network behavior over time. This makes it ideal for cybersecurity tasks involving streaming data or continuous monitoring. Despite being more resourceintensive, the gains in detection accuracy and consistency make LSTM a preferred model in this context.

4.2. Stacking Model and Hybrid Performance

Although **Table 5** focuses on the base learners, the research also implemented a stacking ensemble that leveraged the outputs of SVM, ANN, and LSTM to build a meta-model. This approach capitalizes on the complementary strengths of each base learner: SVM's margin maximization, ANN's non-linear transformations, and LSTM's memory capacity.

The hybrid model achieved marginally higher stability and reduced the variance of performance across different input patterns. It performed particularly well in previously misclassified samples by individual models, suggesting improved generalization. This supports findings by previous studies (Kilincer *et al*., 2021), who noted that ensemble approaches tend to outperform single learners in real-world intrusion detection scenarios.

4.3. Confusion Matrix Analysis

To provide more granular insight, the performance of each model is illustrated through confusion matrices (**Figures 2-4**), each representing true and false predictions.

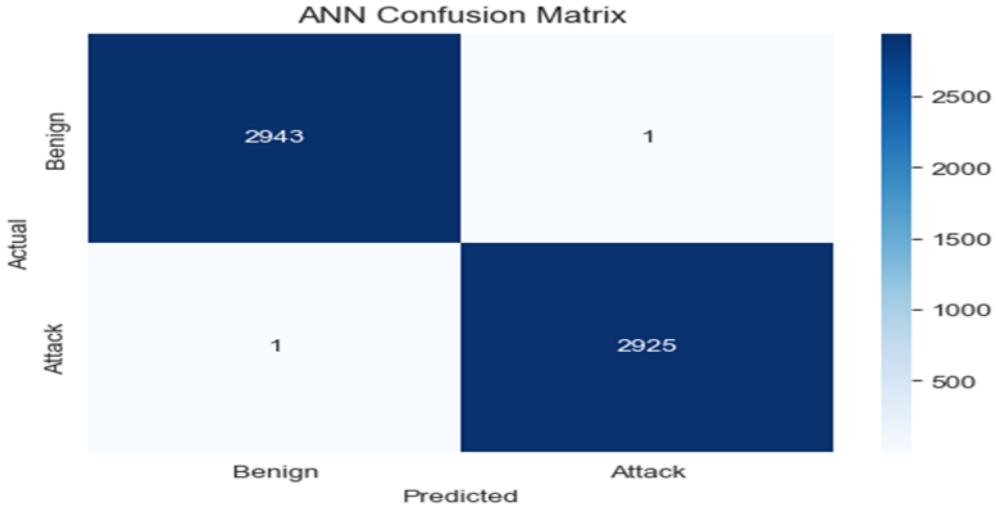


Figure 2. Confusion Matrix of ANN.

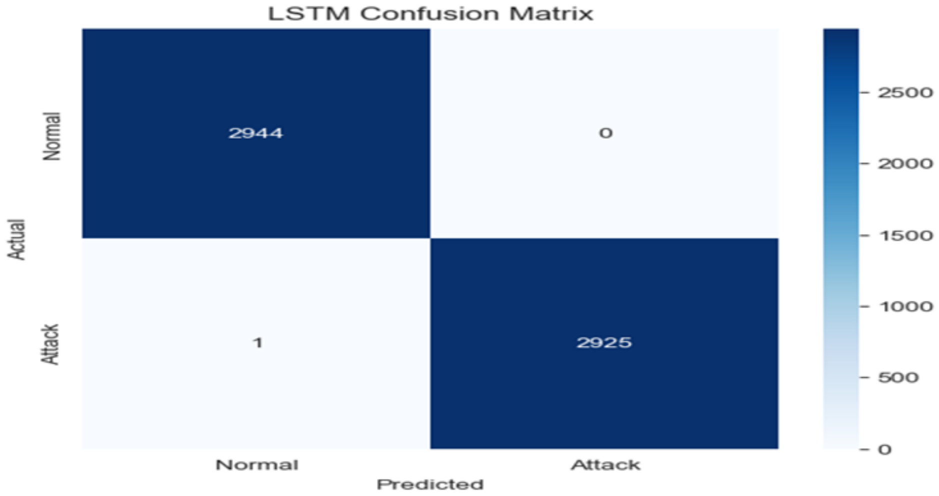


Figure 3. Confusion Matrix of LSTM.

DOI: https://doi.org/10.17509/ijomr.v5i2.86147
p- ISSN 2776-608X e- ISSN 2776-5970

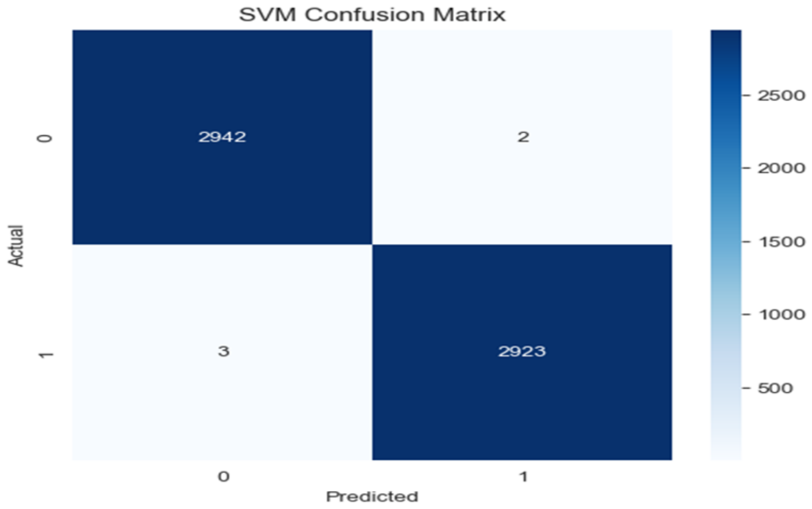


Figure 4. Confusion Matrix of SVM.

Each matrix is divided into four quadrants:

(i) True Positives (TP): Correctly detected malicious traffic
(ii) True Negatives (TN): Correctly identified normal traffic
(iii) False Positives (FP): Normal traffic incorrectly flagged as threats
(iv) False Negatives (FN): Missed detections of actual anomalies

For all models, the TP and TN counts are significantly higher than FP and FN, indicating reliable classification. However, the LSTM model eliminated false negatives, a critical advantage for cybersecurity systems where failing to detect an actual threat can lead to serious consequences. SVM showed slightly more false positives, which, while safer than false negatives, could lead to alert fatigue.

These findings align with literature (Shahin *et al*., 2024), who observed similar performance trends in LSTM-based IDS systems, especially in time-series rich environments.

4.4. Web-Based Application and System Demonstration

The most successful model, LSTM, was deployed through a web-based application to demonstrate real-time anomaly detection. The application allows users to input features such as packet duration, protocol type, and byte count. Based on these inputs, the system provides immediate feedback on whether the traffic is normal or potentially malicious (see **Figures 5-7)**.

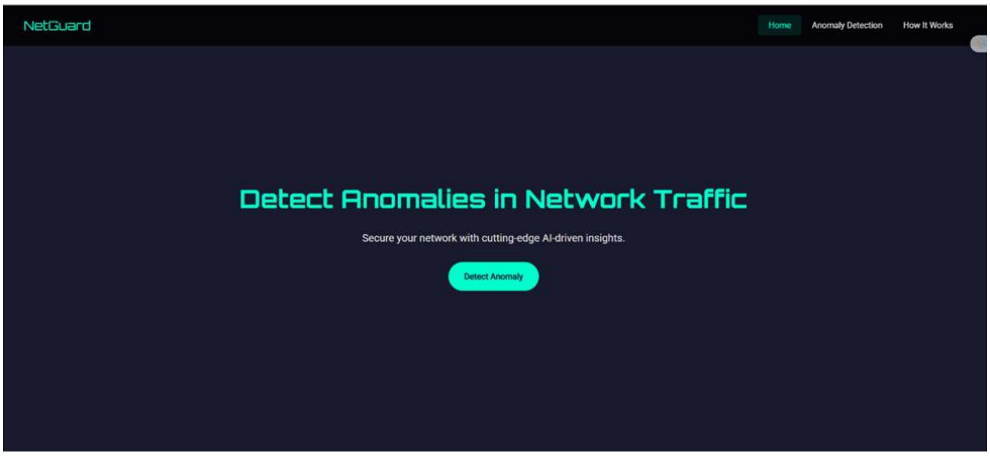
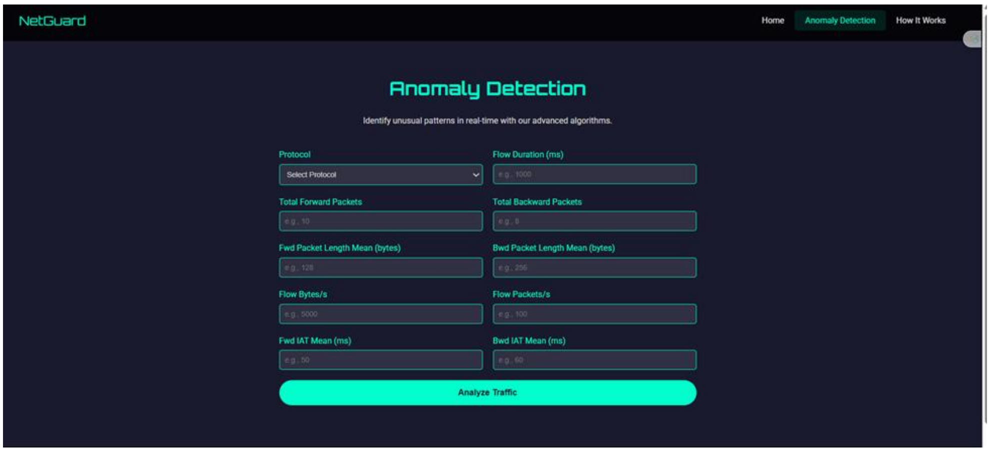

NetGuard
Home
Anomaly Detection
How It Works
Detect Anomalies in Network Traffic
Secure your network with cutting-edge AI-driven insights.
Detect Anomaly

Figure 5. Main Menu of the Web Application.

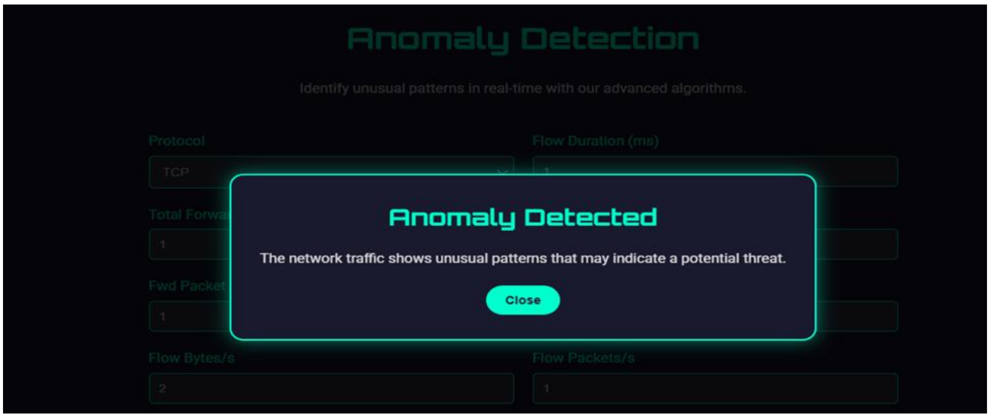


Anomaly Detection

Identify unusual patterns in real-time with our advanced algorithms.

Protocol: Select Protocol
Flow Duration (ms): e.g., 1000
Total Forward Packets: e.g., 10
Total Backward Packets: e.g., 8
Fwd Packet Length Mean (bytes): e.g., 128
Bwd Packet Length Mean (bytes): e.g., 256
Flow Bytes/s: e.g., 5000
Flow Packets/s: e.g., 100
Fwd IAT Mean (ms): e.g., 50
Bwd IAT Mean (ms): e.g., 60

Figure 6. Anomaly Detection Interface.


Anomaly Detection

Identify unusual patterns in real-time with our advanced algorithms.

Protocol: TCP
Flow Duration (ms): 1
Total Forwa: 1
Fwd Packet: 1
Flow Bytes/s: 2
Flow Packets/s: 1

Anomaly Detected

The network traffic shows unusual patterns that may indicate a potential threat.

Figure 7. Sample Detection Output with Visual Feedback.

The system is lightweight, user-friendly, and built using modern web technologies such as Flask and TensorFlow.js. It is scalable and accessible, making it suitable for both operational and educational deployment.

4.5. Educational Applications and SDG Alignment

A distinctive contribution of this research is the educational integration of the anomaly detection system. Beyond its technical performance, the platform serves as a teaching tool in computer science, information systems, and cybersecurity programs.

4.5.1 Curriculum Integration and Experiential Learning

By simulating real network traffic and allowing students to input scenarios and analyze detection outcomes, the platform facilitates experiential learning. It supports inquiry-based education, encourages exploration of algorithmic thinking, and aligns with learning objectives in digital forensics, network security, and machine learning.

(i) For students, it provides hands-on understanding of intrusion detection concepts, preprocessing, and performance evaluation.
(ii) For instructors, it serves as a live demonstration tool for classification, supervised learning, and real-time inference.
(iii) For institutions, it offers a low-cost yet powerful platform for bridging theory and practice.

This reflects the intent of SDG 4.4, which emphasizes increasing the number of youth and adults with relevant skills for employment and entrepreneurship, including technical and vocational skills related to technology.

4.5.2 Innovation and Research Capacity (SDG 9)

From a broader infrastructure and innovation standpoint, this system embodies SDG 9.5, promoting scientific research and upgrading technological capabilities in academic settings. The open-source nature and ease of deployment mean that it can be adapted by universities, especially in developing nations, to enhance their research and instructional capacity in AI and cybersecurity.

Furthermore, this model can be extended into hackathons, academic competitions, or research labs where students iterate, optimize, and benchmark their own machine learning models using the same platform.

4.6. Comparative Analysis with Existing Works

In comparison with prior literature, this study introduces several advancements (see **Table 6**). The novelty lies in the dual focus on performance and pedagogy, enabling the solution to have real-world impact both as a defensive tool and as a learning instrument.

Table 6. Comparative analysis with existing works.

Study	Technique Used	Accuracy (%)	Application Ready	Educational Integration
Aribisala *et al.* (2022)	CNN + BLSTM	98.97	No	No
Abdelkhalek & Mashaly (2023)	SVM + RF	81.67	No	No
Kilincer *et al.* (2021)	SVM, KNN, DT	~85	No	No
This Study	SVM + ANN + LSTM	99.98	Yes	Yes

4.7. Limitations and Future Research Directions

Despite the promising results, several limitations exist:

(i) The dataset, while realistic, may not capture the full range of modern attacks.
(ii) Real-time system deployment under high network load has not been tested extensively.
(iii) The current web interface supports only structured inputs and binary feedback.

To address these issues, future research could explore:

(i) Continuous model retraining using live traffic data.
(ii) Integration with real network hardware and traffic sniffing tools.
(iii) Enhancing the interface with visual dashboards and interactive learning features.
(iv) Inclusion of explainable AI (XAI) components to support interpretation and transparency in educational settings.

The hybrid model developed in this study demonstrated high accuracy and adaptability in classifying network traffic anomalies. Its integration into a web-based educational platform offers both operational utility and pedagogical value. Aligned with SDG 4 and SDG 9, the system exemplifies how intelligent technologies can be leveraged to promote digital skills and support secure, innovative infrastructures in the education sector and beyond.

5. CONCLUSION

This study successfully developed and implemented a hybrid machine learning model for anomaly detection in network traffic using SVM, ANN, and LSTM algorithms. Trained on the CIC-DDoS2019 dataset, the models exhibited outstanding performance, with the hybrid approach achieving accuracy rates exceeding 99%. Among the models, LSTM demonstrated the highest recall, reinforcing its suitability for sequential data patterns found in network behavior.

Beyond algorithmic performance, the integration of the best-performing model into a real-time web-based application extended the utility of the research into practical and educational domains. The application not only detects anomalies with high precision but also serves as a pedagogical tool for students and educators in cybersecurity, data science, and IT-related programs.

Crucially, this research aligns with Sustainable Development Goal 4 by promoting digital and cybersecurity education through accessible and hands-on platforms. It also supports SDG 9 by demonstrating how research-based technological innovations can enhance resilience and infrastructure in academic institutions. The novelty of this work lies in bridging machine learning research with educational practice, providing a scalable and effective tool for both cybersecurity operations and digital learning.

To build upon the outcomes of this research, the following recommendations are proposed:

(i) Expansion to Diverse Datasets. Future studies should consider using additional or real-time datasets to test the generalizability of the model across various types of cyber threats, including zero-day attacks and encrypted traffic patterns.

(ii) Model Retraining and Adaptation. The application should support dynamic retraining based on new traffic logs, enabling continuous learning and responsiveness to evolving threats in real-world settings.

(iii) Explainable AI (XAI) Integration. To improve educational value and transparency, explainable AI modules should be integrated into the platform. These would help learners and users interpret why the system classifies certain traffic as malicious.

(iv) Curriculum Embedding and Training Programs. The application should be incorporated into formal training modules for high school and university-level programs in cybersecurity, AI, and computer science. Educator guides and student lab sheets can be developed around its use.

(v) Cross-Institutional Collaboration. Educational institutions should collaborate to localize and adopt the platform across contexts. This includes translations, case-based scenarios, and the creation of sandbox environments for joint experimentation and research.

(vi) Infrastructure-Policy Alignment. Academic institutions and policymakers should work together to fund and promote intelligent cybersecurity systems as integral components of digital transformation initiatives.

(vii) Cloud Deployment for Wider Access. Hosting the platform on the cloud would enable broader access, especially in under-resourced regions, thus supporting global goals of equitable education and innovation infrastructure.

This research emphasizes that cybersecurity is not only a technical necessity but also an educational imperative. By combining machine learning innovation with scalable web-based learning tools, this study provides a model for how institutions can contribute to global security and human capital development simultaneously.

6. AUTHORS' NOTE

The authors declare that there is no conflict of interest regarding the publication of this article. Authors confirmed that the paper was free of plagiarism.

7. REFERENCES

Abdallah, A. M., Alkaabi, A. S. R. O., Alameri, G. B. N. D., Rafique, S. H., Musa, N. S., and Murugan, T. (2024). Cloud network anomaly detection using machine and deep learning techniques—Recent research advancements. *IEEE Access, 12*, 56749–56773.

Abdelkhalek, A., and Mashaly, M. (2023). Addressing the class imbalance problem in network intrusion detection systems using data resampling and deep learning. *The Journal of Supercomputing, 79*(10), 10611–10644.

Ahmed, M., and Mahmood, A. N. (2015). Novel approach for network traffic pattern analysis using clustering-based collective anomaly detection. *Annals of Data Science, 2*(1), 111–130.

Aribisala, B., Odusanya, O., Olabanjo, O., Wahab, E., Atilola, O., and Saheed, A. (2022). Development of an Artificial Neural Network Model for Detection of COVID-19. *International Journal of Scientific Advances, 3*(4), 377–385.

Djenna, A., Harous, S., and Saidouni, D. E. (2021). Internet of things meet internet of threats: New concern cyber security issues of critical cyber infrastructure. *Applied Sciences*, *11*(10), 4580.

George, A. S., Baskar, T., and Srikaanth, P. B. (2024). Cyber threats to critical infrastructure: assessing vulnerabilities across key sectors. *Partners Universal International Innovation Journal*, *2*(1), 51-75.

Kilincer, I. F., Ertam, F., and Sengur, A. (2021). Machine learning methods for cyber security intrusion detection: Datasets and comparative study. *Computer Networks, 188*, 107840.

Kumar, D. A., and Venugopalan, S. (2017). Intrusion detection systems: A review. *International Journal of Advanced Research in Computer Science, 8*(8), 356–370.

Martins, I., Resende, J. S., Sousa, P. R., Silva, S., Antunes, L., and Gama, J. (2022). Host-based IDS: A review and open issues of an anomaly detection system in IoT. *Future Generation Computer Systems, 133*, 95–113.

Shahin, M., Maghanaki, M., Hosseinzadeh, A., and Chen, F. F. (2024). Advancing network security in industrial IoT: A deep dive into AI-enabled intrusion detection systems. *Advanced Engineering Informatics, 62*, 102685.