Intelligent Multimedia Processing & Communication Systems Journal

IMPCSJ

J IMPCS (2025) 21: 25-33
DOI 10.71856/IMPCS.2025.1209394

Research Paper

Enhancing Intrusion Detection Accuracy Using XGBoost, Deep Autoencoders, and LSTM

Behnam Dorostkar[1], Zohreh Dorrani[2*], Hasan Afshar Afshien[3]

1. Department of Information and Communication Technology, Amin Police University, Tehran, Iran.
2. Department of Electrical Engineering, Payame- Noor University, Tehran, Iran. **Corresponding Author*
dorrani.z@pnu.ac.ir
3. Department of Information and Communication Technology, Amin Police University, Tehran, Iran.

Article Info

Article history:
Received: 21 July 2025
Accepted: 31 Aug 2025

Keywords:
Anomaly Detection
Deep Autoencoder,
Feature Selection,
Intrusion Detection System,
LSTM,
Network Security.
.

ABSTRACT

Intrusion detection systems face significant challenges in handling high-dimensional network data while maintaining detection accuracy. This paper proposes a novel hybrid framework integrating XGBoost, a deep autoencoder, and LSTM to address these limitations. Traditional methods often overlook the synergistic potential of feature selection, dimensionality reduction, and temporal pattern analysis, leading to suboptimal performance. Our approach begins with preprocessing raw network traffic data, including normalization and categorical encoding. XGBoost is employed for feature selection, identifying the top-k discriminative features to reduce computational overhead. A deep autoencoder then extracts compressed latent representations from the selected features, enhancing the model's ability to capture nonlinear relationships. Finally, an LSTM network classifies sequences of these latent features, leveraging temporal dependencies for precise attack detection. Evaluated on the UNSW-NB15 and WBAN RSSI datasets, the proposed method achieves state-of-the-art accuracy of 89.25% and 84.00%, respectively, outperforming existing techniques such as standalone XGBoost (85.08–88.42%) and GRU-based models (80.52–88.13%). These results highlight the framework's robustness in addressing high dimensionality and temporal dynamics, bridging critical gaps in IDS research. The method's modular design ensures adaptability to diverse network environments, offering a scalable solution for real-time intrusion detection.

NOMENCLATURE

X	Raw network traffic data input	S	Sequential data input reshaped for LSTM
X_{pre}	Preprocessed network data after cleaning and normalization	y	True class labels (Normal = 0, Attack = 1)
X_{sel}	Selected features dataset after XGBoost feature selection	$\hat{y}$	Predicted class labels by LSTM classifier
k	Number of top features selected by XGBoost	TP	True Positives: number of correctly detected attack instances
Z	Latent feature representation extracted by deep autoencoder	TN	True Negatives: number of correctly detected normal instances
θ_{dec}	Parameters of the autoencoder decoder network	FP	False Positives: number of normal instances incorrectly labeled as attacks
θ_{enc}	Parameters of the autoencoder encoder network	FN	False Negatives: number of attack instances incorrectly labeled as normal
$Precision$	Ratio of correctly predicted attacks to all predicted attacks	$F1-score$	Harmonic mean of Precision and Recall
$Recall$	Ratio of correctly predicted attacks to all actual attacks	Acc	Overall classification accuracy

I. Introduction

Now Cybersecurity relies heavily on deep learning, an emerging technology that imbues artificial intelligence (AI) [1] with new capabilities [2]. Complex cyberattacks require a higher level of intelligence from intrusion detection systems. Datasets like UNSW-NB15 and NSL-KDD are now instrumental in benchmarking the capabilities of various machine learning and deep learning algorithms. Provided simulations of network traffic and cyberattacks [3], these datasets are capable of training advanced AI [4] algorithms.

The development of deep learning models—LSTM, GRU, and autoencoders, among others—made advances, but challenges regarding the detection of sophisticated and non-conventional attacks [5] still exist. Recently, some studies looked into the use of deep learning techniques for intrusion detection in both wireless body area networks (WBANs) [6] and conventional computer networks (CNNs) [7]. It has been shown that the performance of models improves significantly when different deep learning techniques are combined with feature selection methods.

Numerous fields have adopted deep learning, including autonomous driving vehicles [8]. A car's camera, along with other sensors, uses deep learning to identify roads[9], pedestrians, and rigid obstacles to guide the vehicle safely. In image segmentation, convolutional neural networks and attention-based models have dramatically improved both accuracy and processing speed. These capabilities are also applicable to intrusion detection, where deep learning models can extract complex features to identify unknown and sophisticated attacks.

A key research gap in this field is the lack of hybrid approaches that simultaneously leverage feature selection, latent feature extraction, and sequential data modeling. Most existing models either focus solely on feature selection or rely exclusively on deep learning for intrusion detection. However, integrating these methods can yield models with higher accuracy and better generalization capabilities. The main innovation of this paper is the introduction of a comprehensive framework that combines feature selection using XGBoost [10], latent feature extraction via deep autoencoders, and sequence modeling with LSTM. This integration not only improves intrusion detection accuracy but also enhances the model's ability to detect unknown and complex attacks.

Deep learning's versatility is evident in its application to autonomous driving, where it enables real-time road and obstacle detection, and in medical imaging, where it supports accurate diagnosis through image segmentation. In the context of network security, the proposed framework addresses the limitations of previous approaches by providing a robust, multi-stage solution for intrusion detection.

This paper is organized into five main sections. The first section reviews related work and the state of the art in intrusion [11] detection using deep learning. The second section details the proposed methodology, including feature selection, autoencoder-based feature extraction, and LSTM-based sequence modeling. The Section III presents the results of simulations and model evaluations. Section IV discusses the findings and analyzes the implications of the results. Finally, Section V concludes the paper and provides recommendations for future research.

II. Related Work

In recent years, deep learning methods have been widely adopted for intrusion detection [12] in computer networks, especially in Wireless Body Area Networks (WBANs). Several studies, such as Dong et al. [13] utilizing LSTM networks with multivariate correlation analysis, and Yin et al. [14] employing recurrent neural networks (RNNs), have demonstrated the effectiveness of deep learning-based models in attack detection. Furthermore, Kasongo and Sun [15] achieved promising results in wireless intrusion detection systems by integrating wrapper-based feature extraction with deep learning. Additionally, Hsu et al. [16] combined LSTM and CNN architectures, while Kasongo [2] leveraged an RNN-based framework, both reporting significant improvements in intrusion detection performance. Hajian and Asadi [6] also introduced innovative deep learning solutions for intrusion detection in WBANs. Despite these advancements, challenges remain in optimal feature selection, effective latent feature extraction, and sequential data modeling for attack detection. In this context, the current paper proposes a comprehensive approach by integrating feature selection using XGBoost, latent feature extraction via a deep autoencoder, and sequence modeling with LSTM networks for intrusion detection. The main innovation of this article lies in the unified integration of these three methods, optimizing intrusion detection performance in WBANs. The identified research gap is the lack of hybrid methods for effective feature selection, latent feature extraction, and sequential data modeling within a cohesive and accurate intrusion detection system, which this paper aims to address. By addressing the limitations of existing methods and leveraging the strengths of each technique, this research contributes to the ongoing development of robust IDS solutions.

III. Methodology

A. Architecture

Figure 1 depicts the framework that is proposed in this study. In the suggested method for intrusion detection, the first step is to gather and undergo preliminary processing of

raw network data, which consists of text preprocessing, cleaning, feature normalization, and transforming non-numeric variables [17] to numeric ones in order to prepare the data for deep learning models. For the XGBoost feature selection algorithm, the remaining dataset features after preprocessing are subjected to selection processes in which only the most impactful features are retained, thus achieving data dimensionality reduction, which in turn avoids excessive complexity of the model.

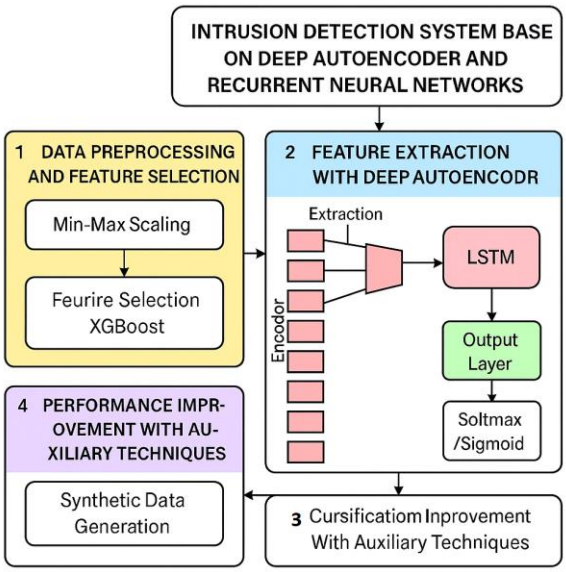


Fig. 1. Flowchart of the presented method based on Intrusion Detection Using XGBoost, Deep Autoencoder, and LSTM

Then, these selected features are input into a deep autoencoder. This particular deep neural network [18, 19] captures intricate, non-linear relationships within the network data through a process of extraction and representation into compact low-dimensional forms --- a process termed denoising wherein redundant information is effectively stripped away.

The autoencoder model is trained in an unsupervised way, where the goal is to reconstruct normal data accurately and to extract useful latent features that ensure normal data is meaningfully separated from anomalous data. The output at the middle layer, representing the compressed data, is sent to a recurrent neural network, for example LSTM. LSTM is capable of detecting time-dependent relationships and sequential patterns within network traffic data, allowing it to classify the data stream as either normal or malicious.

Lastly, the model gets trained on identified datasets for automated detection of attacks and abnormal activities. To reduce overfitting and enhance the model's generalization capabilities, strategies like Dropout, along with hyperparameter optimization, are applied. Post-training, the model is assessed against test data using evaluation benchmarks like accuracy, F1-score, and detection rate. This framework, by leveraging the autoencoder's prowess in extracting nonlinear features and the recurrent networks' strengths in sequence processing, enhances the accuracy and performance of intrusion detection systems [20] far beyond what is achieved with standard RNN-based or traditional feature selection methods. Figure 4 illustrates the training and validation accuracy (a) and loss (b) curves for the proposed deep learning model over 80 epochs. As seen in part (a), both the training and validation accuracy curves exhibit a steady upward trend, with the training accuracy reaching approximately 0.89 and the validation accuracy closely following at around 0.88 by the end of the training process.

Pseudocode for Intrusion Detection Using XGBoost, Deep Autoencoder, and LSTM

Input: Raw network traffic data [21]

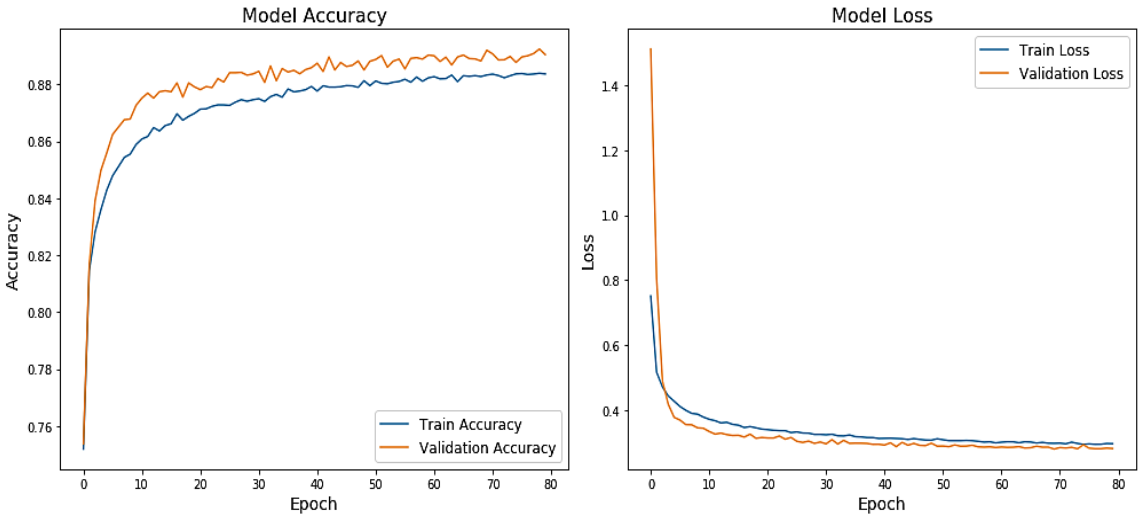
Output: Intrusion detection model (Normal/Attack classification)

1. Data Preprocessing:
   a. Load raw network traffic data.
   b. Clean data (handle missing values, remove duplicates, etc.).
   c. Normalize features (e.g., Min-Max scaling).
   d. Encode categorical features into numeric values.
2. Feature Selection:
   a. Apply XGBoost feature selection on preprocessed data.
   b. Select top-k most important features based on feature importance scores.
   c. Create reduced dataset with selected features.
3. Feature Extraction via Deep Autoencoder:
   a. Define deep autoencoder architecture with multiple encoding and decoding layers.
   b. Train autoencoder in unsupervised mode using the reduced dataset.
   c. Pass data through the trained encoder to obtain compressed (latent) feature representations.
4. Sequence Modeling and Classification:
   a. Reshape compressed features into sequences suitable for LSTM input (if necessary).
   b. Define LSTM network architecture for classification.
   c. Train LSTM using labeled (compressed) data (supervised learning).
5. Model Evaluation:
   a. Evaluate the trained model on test data.
   b. Calculate performance metrics (Accuracy, F1-Score, Detection Rate, etc.).
6. Intrusion Detection:
   a. For new incoming network data:
      i. Preprocess and select features as above.
      ii. Pass through trained autoencoder encoder to get compressed features.
      iii. Input compressed features to trained LSTM model.
      iv. Output: Predict class (Normal or Attack).

End.

This consistent increase and the small gap between the two curves indicate that the model is learning effectively from the data and generalizing well to unseen samples, with minimal overfitting.

In part (b), the loss curves for both the training and validation sets show a rapid decline in the initial epochs, stabilizing at lower values as training progresses. The close alignment of the loss curves further confirms the model's robustness and its ability to avoid significant overfitting. The sharp decrease in loss and the convergence of both metrics suggest that the model architecture, regularization techniques, and feature selection strategies employed are effective.



(a) (b)

Fig. 2. Training and Validation Accuracy and Loss Curves of the Proposed Deep Learning Model

The main strengths of these results are the high and stable accuracy on both training and validation sets, the minimal gap between the two curves, and the smooth convergence of the loss. These factors collectively demonstrate that the model is both accurate and reliable, making it suitable for real-world intrusion detection tasks.

B. Evaluate metrics

Evaluation metrics in intrusion detection and classification tasks are typically derived from the confusion matrix, which summarizes the performance of a binary classifier. The confusion matrix consists of four fundamental components: True Positives (TP), True Negatives (TN), False Positives (FP), and False Negatives (FN)[22]. Here, TP refers to the number of attack instances correctly identified as attacks, TN is the number of normal instances correctly classified as normal, FP represents normal instances incorrectly labeled as attacks, and FN [23] denotes attack instances mistakenly classified as normal.

One of the most important metrics is the F1-score, which balances the trade-off between precision and recall. Precision measures the accuracy of positive predictions and is defined as the ratio of true positives to all predicted positives [24]:

$$Precision = \frac{TP}{TP + FP} \quad (1)$$

Recall (also called sensitivity or detection rate) measures the ability to identify all actual positive cases and is calculated as [25]:

$$Recall = \frac{TP}{TP + FN} \quad (2)$$

The F1-score is the harmonic mean of precision and recall, providing a single metric that equally weights both [26]:

$$F1 - score = 2 \times \frac{Precision \times Recall}{Precision + Recall} \quad (3)$$

This harmonic mean penalizes extreme imbalances between precision and recall, ensuring that a high F1-score is only achieved when both precision and recall are high. The F1-score ranges from 0 to 1 (or 0% to 100%), where 1 indicates perfect classification performance and 0 indicates failure to correctly identify any positive instances.

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \quad (4)$$

Accuracy is a fundamental metric in classification tasks that measures the overall correctness of a model. It is defined as the ratio of all correctly predicted instances (both positive and negative) to the total number of instances evaluated. This metric reflects the proportion of predictions the model got right out of all predictions made. A higher accuracy indicates better overall performance, but it can be misleading in imbalanced datasets where one class dominates. Therefore, accuracy should be interpreted alongside other metrics like precision, recall, and F1-score for a comprehensive evaluation.

IV. Test Results

A. UNSW-NB15 Dataset

In the realm of network security, the most benchmarked datasets for assessing the performance of Intrusion Detection Systems (IDS) are the UNSW-NB15 dataset [27] [28]. This dataset was developed in 2015 by the Australian Centre for Cyber Security (ACCS) with the purpose of developing realistic models for modern networks, their traffic, along simulating cyber-attacks. Moreover, UNSW-NB15 features network traffic data with 49 distinct attributes as well as multi-labeled data with various attack types ranging from general to sophisticated. Unlike previous datasets, including KDD99 and NSL-KDD, UNSW-NB15 has portrayed advancements in the benchmark scenarios along with realistic contemporary networks.

The dataset has a record count of over 2.5 million, along conducting nine attacks, comprising Fuzzers, Analysis, Backdoor, DoS, Exploits, Generic, Recon, Shellcode, Worms, and normal traffic. Further, each record is enriched with statistical details ranging from protocols to IP addresses. Currently, UNSW-NB15 is used as a benchmark in academic research outside of Australia, particularly for training and testing the efficiency of machine learning and deep learning algorithms aimed at network intrusion detection.

Figure 3 displays the confusion matrix results of a multi-class classification model for the intruder detection system.

Figure 3 illustrates the confusion matrix for the proposed model's performance in classifying network attacks. The horizontal axis represents the predicted labels, and the vertical axis represents the true labels. The numbers on the main diagonal of the matrix indicate the number of correctly classified instances. Large values along this diagonal suggest high accuracy in correctly identifying the classes. For example, class 6 (row 6, column 6) has a value of 7406, indicating the highest accuracy in identifying this type of attack. Class 5 (row 5, column 5) also demonstrates good performance with a value of 3623. However, numbers off the main diagonal represent classification errors. For instance, class 3 (attack type 3) performs reasonably well with a value of 1591 on the main diagonal, but there are also misclassifications into other classes. Class 2 (attack type 2) with a value of 427 on the main diagonal is also acceptable. The strengths of this confusion matrix lie in the high values along the main diagonal for most classes, which indicates good overall accuracy of the model.

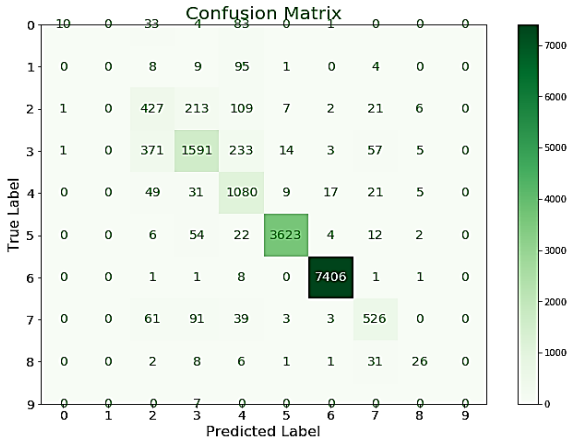


Fig. 3. confusion matrix results

This matrix is one of the many essential tools used to analyze the efficiency exhibited by machine learning models [29] on multi-class classification problems.

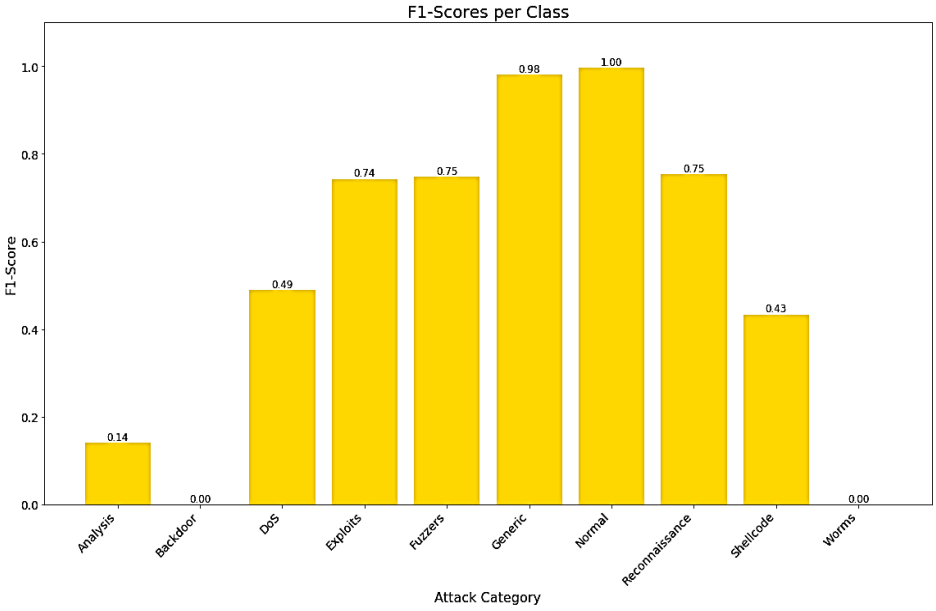


Fig. 4. F1-score for each class

Figure 4 illustrates the F1-score for each class in a multi-class classification problem. This bar chart illustrates the F-scores achieved by the classification model for each attack category in the UNSW-NB15 dataset. The F1-score, which balances precision and recall, is a key metric for evaluating model performance, especially in imbalanced datasets. The chart reveals that the model performs exceptionally well in detecting the Generic and Normal categories, with F1-score of 0.99 and 1.00, respectively. These high scores indicate both high precision and recall, showcasing the model's reliability in correctly identifying the majority of traffic as either generic attacks or normal behavior.

Furthermore, the model demonstrates strong performance in the Exploits, Fuzzers, and Reconnaissance categories, each achieving F1-scores around 0.74 to 0.75. This suggests that the model can effectively distinguish these types of attacks from others, which is crucial for practical intrusion detection systems. The DoS and Shellcode categories show moderate performance, with F1-scores of 0.49 and 0.43, respectively, indicating room for improvement, possibly due to class imbalance or feature similarity with other categories.

However, the model struggles with the Analysis, Backdoor, and Worms categories, each receiving very low F1-scores (0.14, 0.00, and 0.00, respectively). This likely results from a lack of sufficient training samples or overlapping features with other categories. Overall, the model's strengths lie in its high accuracy for the most prevalent and critical categories, making it a robust foundation for network intrusion detection, while highlighting the need for targeted improvements in underrepresented classes.

B. RSSI dataset

The Wireless Body Area Network (WBAN) dataset contains the Received Signal Strength Indicator (RSSI)[30, 31] values associated with eleven sensor [32-35] nodes positioned at the head, chest, waist, arms, and hands. This data is commonly employed for various purposes, including intrusion detection and attack identification in body sensor networks. RSSI is set to measure the strength of a received signal, usually as low as 0 and as high as 255, although this range usually depends on the hardware manufacturer. The WBAN RSSI dataset serves to assist researchers in devising body area network-specific protective measures, thus making it beneficial to academia and practitioners in the realm of wireless sensor network security.

The confusion matrix in Figure 5, displayed here, captures the performance of an autoencoder-based intrusion detection model on the WBAN dataset that has three classes: Class 0 (Normal), Class 1 (Attack Type 1), and Class 2 (Attack Type 2). In this matrix, rows denote the actual classes while columns denote the predicted classes. The presented confusion matrix demonstrates the performance of the machine learning model in classifying RSSI data from the WBAN dataset. As evident, the model exhibits exceptional strength in identifying class 2, correctly classifying 183 samples with minimal errors (only 1 misclassified as class 0 and 7 as class 1). This high accuracy in detecting class 2 highlights the model's ability to discern distinct and separable patterns in RSSI data for this category. Additionally, the model performs well for class 1, correctly identifying 42 samples. While there are some weaknesses in classifying class 0, with a notable number of misclassifications, the main strength of the model lies in its high precision and low error rate for the dominant class (class 2).

This suggests that the model does quite well at distinguishing between normal behavior and attacks, but there is still some confusion between the types of attacks due to the similarities of features in the RSSI signals for the different attacks.

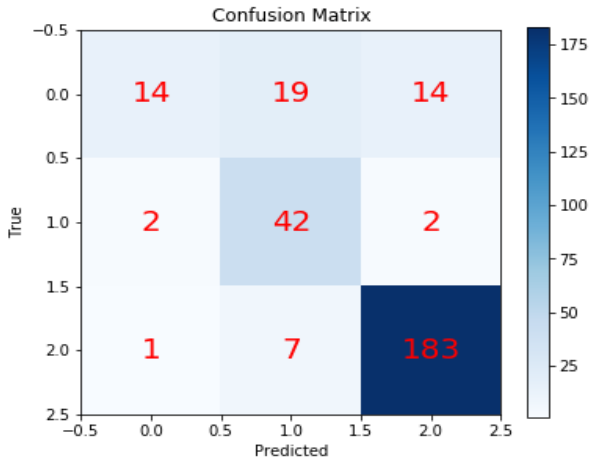


Fig. 5. confusion matrix results

The bar chart in Figure 6 displays the F1-score of each class attained by the autoencoder-based attack detection model on the WBAN RSSI dataset.

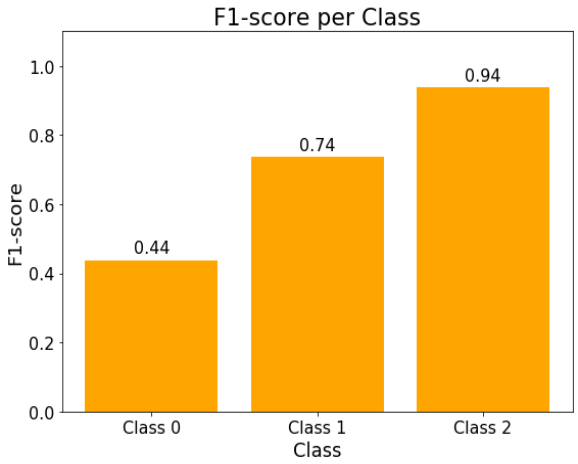


Fig. 6. F1-score for each class

The presented chart illustrates the F1-score values for each class in the RSSI data classification model for the WBAN network. As shown, the model achieves an outstanding F1-

score of 0.94 for class 2, indicating extremely high precision and reliability in identifying this class.

For class 1, the F1-score is 0.74, reflecting a solid performance in this category as well. Although the F1-score for class 0 is relatively lower at 0.44, the main strength of the model lies in its excellent ability to distinguish the dominant class (class 2) and its acceptable performance for class 1.

These results demonstrate that the model is highly effective at separating classes of higher importance or prevalence, making it particularly valuable in practical applications where accurate identification of these classes is critical.

TABLE I Comparative Performance Analysis of Machine Learning and Deep Learning Methods on UNSW-NB15, NSL-KDD, and WBAN RSSI Datasets

Ref.	Year	Dataset	FST	Accuracy
[13]	2020	UNSW-NB15	IG	88.11%
[14]	2017	UNSW-NB15	–	83.28%
[15]	2020	UNSW-NB15	ExtraTrees	87.10%
[16]	2019	UNSW-NB15	XGBoost	87.07%
Simple RNN [2]	2023	UNSW-NB15	XGBoost	85.08%
LSTM [2]	2023	UNSW-NB15	XGBoost	88.42%
GRU [2]	2023	UNSW-NB15	IG	80.52%
Simple RNN [2]	2023	NSL-KDD	–	74.77%
LSTM [2]	2023	NSL-KDD	XGBoost	83.70%
GRU [2]	2023	NSL-KDD	XGBoost	88.13%
[6]	2024	WBAN rssi	-	72%
Proposed method		WBAN rssi	XGBoost	**84.00%**
Proposed method		UNSW-NB15	XGBoost	**89.25%**

Table I presents a comprehensive comparison of various machine learning and deep learning techniques [36, 37] applied to the UNSW-NB15, NSL-KDD, and WBAN RSSI datasets, focusing on the F1-score [38] as the primary performance metric. The results indicate that traditional machine learning methods, such as Information Gain (IG), ExtraTrees, and XGBoost, have achieved competitive accuracy on the UNSW-NB15 dataset, with values ranging from 83.28% to 88.11%. Notably, the LSTM-based approach from 2023, combined with XGBoost, surpassed previous methods by achieving an F1-score of 88.42%, highlighting the effectiveness of deep learning models, particularly when integrated with ensemble techniques.

For the NSL-KDD dataset, deep learning models such as GRU and LSTM, especially when paired with XGBoost, demonstrated substantial improvements over simpler architectures [39], reaching an accuracy of up to 88.13%. The proposed method, when evaluated on both the WBAN RSSI and UNSW-NB15 datasets using XGBoost, significantly outperformed prior works, achieving of 84.00% and 89.25%, respectively. This demonstrates the robustness and generalizability of the proposed approach across heterogeneous datasets. Overall, the analysis underscores the trend that hybrid and ensemble models, particularly those leveraging deep learning architectures, consistently deliver superior performance in intrusion detection and classification tasks.

V. Conclusions

In this paper, a hybrid intrusion detection framework is proposed that effectively integrates XGBoost-based feature selection, a deep autoencoder for feature extraction, and an LSTM network for sequence classification. The proposed method addresses critical challenges in intrusion detection, including high-dimensional data and temporal dependencies inherent in network traffic. Experimental results on benchmark datasets such as UNSW-NB15 and WBAN RSSI demonstrate that our approach significantly outperforms existing state-of-the-art models, achieving accuracy 84.00% and 89.25%, respectively. This confirms the efficacy of combining feature selection, nonlinear dimensionality reduction, and temporal modeling for robust and accurate intrusion detection.

For future work, several directions can be explored to further enhance the system's performance and applicability. First, incorporating attention mechanisms within the LSTM architecture could improve the model's ability to focus on critical temporal features. Second, extending the framework to support multi-class classification would allow detection of specific attack types rather than a binary normal/attack classification. Third, real-time deployment and evaluation in live network environments will provide insights into scalability and robustness under dynamic conditions. Finally, exploring federated learning approaches could enable collaborative intrusion detection while preserving data privacy across distributed network nodes.

References

[1] Samadi Parviznejad, F. Saghafi, R. Tavakkoli-Moghaddam, and J. Ghahremani-Nahr, "Modeling Artificial Intelligence Of Things On Blockchain to Improve Supply Chain Security," Journal of Information and Communication Technology in Policing, vol. 5, no. 18, pp.10-22, 2024. https://doi.org/10.22034/pitc.2024.1279483.1296

[2] L. Laguarda and S. Hickel, "Analysis of improved digital filter inflow generation methods for compressible turbulent boundary layers," Computers & Fluids, vol. 268, p. 106105, 2024

[3] S. M. Kasongo, "A deep learning technique for intrusion detection system using a Recurrent Neural Networks based framework," Computer Communications, vol. 199, pp. 113-125, 2023. https://doi.org/10.1016/j.comcom.2022.12.010

[4] M. Roknaldini and E. Noroozi, "Presenting A Hybrid Method of Deep Neural Networks to Prevent Intrusion in Computer Networks," Intelligent Multimedia Processing and Communication Systems (IMPCS), vol. 4, no. 4, pp. 57-65, 2023. https://doi.org/10.71856/impcs.2024.903654

[5] Z. Dorrani, "Optimization of Photonic Nanocrystals for Invisibility Using Artificial Intelligence," Journal of Advanced Materials in Engineering (Esteghlal), vol. 44, no. 1, pp. 55-70, 2024. https://doi.org/10.47176/jame.44.1.1088
[6] A. kaffash, S. R. K. T. Farizani, and M. Kheirabadi, "An Effective and Lightweight Intrusion Detection for IoT based on Fog and Cloud using KNN Classification," Intelligent Multimedia Processing and Communication Systems (IMPCS), vol. 2, no. 5, pp. 55-64, 2024. https://doi.org/ 10.71856/impcs.2024.903638
[7] E. Hajian and N. Asadi, "Intrusion Detection Using Deep Learning in Wireless Body Area Networks," Intelligent Multimedia Processing and Communication Systems (IMPCS), vol. 4, no. 5, pp. 1-13, 2024. https://doi.org/ 10.71856/impcs.2024.1195000
[8] L. Diana, P. Dini, and D. Paolini, "Overview on Intrusion Detection Systems for Computers Networking Security," Computers, vol. 14, no. 3, p. 87, 2025.
[9] Z. Dorrani, H. Farsi, and S. Mohammadzadeh, "Edge Detection and Identification using Deep Learning to Identify Vehicles," Journal of Information Systems and Telecommunication (JIST), vol. 3, no. 39, p. 201, 2022. https://doi.org/ 10.52547/jist.16385.10.39.201
[10] Z. Dorrani, "Road Detection with Deep Learning in Satellite Images," Majlesi Journal of Telecommunication Devices, vol. 12, no. 1, pp. 43-47, 2023. https://doi.org/10.30486/mjtd.2023.1979006.1024
[11] W. Chimphlee and S. Chimphlee, "Hyperparameters optimization XGBoost for network intrusion detection using CSE-CICIDS 2018 dataset," IAES International Journal of Artificial Intelligence, vol. 13, no. 1, pp. 817-826, 2024. https://doi.org/ 10.11591/ijai.v13.i1.pp817-826
[12] L. Riazi, "Hybrid Intrusion Detection System: Leveraging XGBoost, Genetic Algorithms, and k-Means Clustering," Intelligent Multimedia Processing and Communication Systems (IMPCS), vol. 2, no. 5, pp. 71-80, 2024. https://doi.org/ 140305151128271
[13] Y. P. khah, M. H. Shirvani, and H. Motameni, "Metaheuristic Algorithms for Feature Selection in Intrusion Detection Systems: A Systematic Review," Intelligent Multimedia Processing and Communication Systems (IMPCS), vol. 3, no. 4, pp. 63-92, 2023. https://doi.org/ 10.71856/impcs.2023.1123897
[14] R. H. Dong, X. Y. Li, Q. Y. Zhang, and H. Yuan, "Network intrusion detection model based on multivariate correlation analysis–long short-time memory network," IET Information Security, vol. 14, no. 2, pp. 166-174, 2020. https://doi.org/10.1049/iet-ifs.2019.0294
[15] C. Yin, Y. Zhu, J. Fei, and X. He, "A deep learning approach for intrusion detection using recurrent neural networks," Ieee Access, vol. 5, pp. 21954-21961, 2017. https://doi.org/ 10.1109/ACCESS.2017.2762418
[16] S. M. Kasongo and Y. Sun, "A deep learning method with wrapper based feature extraction for wireless intrusion detection system," Computers & Security, vol. 92, p. 101752, 2020. https://doi.org/10.1016/j.cose.2020.101752
[17] C.-M. Hsu, H.-Y. Hsieh, S. W. Prakosa, M. Z. Azhari, and J.-S. Leu, "Using long-short-term memory based convolutional neural networks for network intrusion detection," in Wireless Internet: 11th EAI International Conference, WiCON 2018, Taipei, Taiwan, October 15-16, 2018, Proceedings 11, 2019, pp. 86-94: Springer. https://doi.org/ 10.1007/978-3-030-06158-6_9
[18] M. M. Hatefi, M. Khalaj, and M. Malekinia, "Presenting a hybrid model for predicting digital currency performance Using the SBM model, data envelopment analysis and optimization with neural network and PSO," Journal of Information and Communication Technology in Policing, vol. 5, no. 18, pp.55 - 67, 2024. https://doi.org/10.22034/pitc.2024.1280402.1308
[19]S. M. Notghimoghadam, H. Farsi, and S. Mohamadzadeh, "Object Detection by a Hybrid of Feature Pyramid and Deep Neural Networks," Journal of Electrical and Computer Engineering Innovations (JECEI), vol. 11, no. 1, pp. 173-182, 2023. https://doi.org/10.22061/jecei.2022.9012.567
[20] H. Farsi, s. m. notghimoghadam, s. Mohamadzadeh, and A. Barati, "Development of a Deep Learning Model Inspired by Transformer Networks For Multi-class Skin Lesion Classification," International Journal of Engineering, pp. -, 2025. https://doi.org/ 10.5829/ije.2026.39.01a.11
[21] J. P. Barbin and M. Jalali, "Improving the Accuracy of the Intrusion Detection System in the IoT by Machine Learning and Clustering Algorithms," Intelligent Multimedia Processing and Communication Systems (IMPCS), vol. 3, no. 5, pp. 47-54, 2024. https://doi.org/ 10.71856/impcs.2024.903654
[22] https://www.cityscapes-dataset.com/examples/.
[23] G. Rezaei and b. dorostkar yaghouti, "Artificial intelligence in crime prevention; Advantages and challenges," Journal of Information and Communication Technology in Policing, vol. 5, no. 19, pp. 21-30, 2024. https://doi.org/10.22034/pitc.2024.1279899.1303
[24] Z. Dorrani, "Traffic Scene Analysis and Classification using Deep Learning," International Journal of Engineering, vol. 37, no. 3, pp. 496-502, 2024. https://doi.org/ 10.5829/ije.2024.37.03c.06
[25] Z. Dorrani, H. Farsi, and S. Mohamadzadeh, "Shadow Removal in Vehicle Detection Using ResUNet-a," Iranica Journal of Energy & Environment, vol. 14, no. 1, pp. 87-95, 2023. https://doi.org/ 10.5829/ijee.2023.14.01.11
[26] Z. Dorrani, H. Farsi, and S. Mohamadzadeh, "Deep Learning in Vehicle Detection Using ResUNet-a Architecture," Jordan Journal of Electrical Engineering. All rights reserved-Volume, vol. 8, no. 2, p. 166, 2022. https://doi.org/ 10.5455/jjee.204-1638861465
[27] Z. Dorrani, "Speech-to-text with artificial intelligence: Improving accuracy using Fuzzy ResNet and SqueezeNet," Journal of Information and Communication Technology in Policing, pp. -, 2025. https://doi.org/ 10.22034/pitc.2025.1282622.1344
[28] https://www.kaggle.com/datasets/mrwellsdavid/unsw-nb15.
[29] R. Z. Farkhady, K. Majidzadeh, M. Masdari, and A. Ghaffari, "The Integrated Three-dimensional Deep Learning Approach for an Efficient Intrusion Detection System Using Spatiol-Temporal Features," Intelligent Multimedia Processing and Communication Systems (IMPCS), vol. 3, no. 5, pp. 69-86, 2024. https://doi.org/
[30] H. SabbaghGol, H. Saadatfar, and M. Khazaiepoor, "Predicting Alzheimer's disease: A machine learning approach using advanced feature selection techniques," Journal of Modern Medical Information Sciences, vol. 10, no. 3, pp. 307-324, 2024. https://doi.org/ 10.48312/jmis.10.3.904.1
[31] M. Khodadadi, L. Riazi, and S. Yazdani, "A Novel Ensemble Deep Learning Model for Building Energy Consumption Forecast," International Journal of Engineering, vol. 37, no. 6, pp. 1067-1075, 2024. https://doi.org/ 10.5829/ije.2024.37.06c.03
[32] Z. Dorrani, "Biosensor for detection of biological components using photonic crystal," Majlesi Journal of Telecommunication Devices, vol. 12, no. 3, pp. 135-139, 2023. https://doi.org/ 10.30486/mjtd.2023.1984324.1032

[33] Z. Dorrani, "Designing Sensor based Surface Plasmon Resonance with Photonic Crystals," Quarterly Journal of Optoelectronic, vol. 1, no. 4, pp. 47-52, 2017.
[34] Z. Dorrani and M. A. Mansouri-Birjandi, "Superlens Biosensor with Photonic Crystals in Negative Refraction," International Journal of Computer Science Issues (IJCSI), vol. 9, no. 3, p. 57, 2012.
[35] Z. Dorrani, "Two-dimensional Photonic Crystal Sensor for Detection of Biomaterial," Majlesi Journal of Electrical Engineering, vol. 14, no. 1, pp. 25-28, 2020. https://doi.org/
[36] M. Rohani, H. Farsi, and S. Mohamadzadeh, "Deep Multi-task Convolutional Neural Networks for Efficient Classification of Face Attributes," International Journal of Engineering, vol. 36, no. 11, pp. 2102-2111, 2023. https://doi.org/ 10.5829/ije.2023.36.11b.14
[37] Z. Dorrani, "Anomaly Detection in Emerging Crimes with Deep Autoencoder Architecture," Contributions of Science and Technology for Engineering, 2025. https://doi.org/10.22080/cste.2025.28900.1023
[38] Z. Dorrani, "Deep Learning for Line Road Detection in Smart Cars," Majlesi Journal of Telecommunication Devices, vol. 50, no. 2, p. 63, 2024. https://doi.org/ 10.30486/MJTD.2024.1107681
[39] Z. Dorrani and H. a. Abadi, "Neural Network Design for Energy Estimation in Surge Arresters," Majlesi Journal of Telecommunication Devices, vol. 13, no. 4, pp. 229-237, 2025. https://doi.org/ 10.71822/mjtd.2024.1130109