Journal of Information Systems Engineering and Management
2025, 10(32s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

A Hybrid Fuzzy-Neural Network Approach for Advanced Pattern Recognition and Predictive Analytic

Adala Mahdi Jiyad[1], Zainab N. Nemer[2]
[1]*Assistant Professor, Computer and Information Technology, Department: Computer Science, University of Basra, Iraq*
Email: adala.gyad@uobasrah.edu.iq
[2]*Assistant Professor, Computer Sciences and Information Technology, Department : Computer Science, University of Basra, Iraq*
Email : zainab.nemer@uobasrah.edu.iq

ARTICLE INFO

Received: 30 Dec 2024

Revised: 05 Feb 2025

Accepted: 25 Feb 2025

ABSTRACT

Organizations must address cybersecurity as a fundamental issue in the digital era, where they face advanced and continuous cyber threats. Intrusion detection systems based on traditional methods face challenges in multiple traffic classification because they enforce static threshold boundaries and possess restricted learning capabilities.

This research envisions a new hybrid fuzzy-neural network solution for sophisticated pattern recognition and predictive analysis in intrusion detection. The main goal is to improve detection accuracy and lower false positives by merging the subtle reasoning of fuzzy logic with the adaptability of learning in neural networks.

The model is tested on the NSL-KDD dataset, which offers extensive labeling of normal and anomalous network traffic. The most important preprocessing steps—encoding categorical variables, scaling numerical data, and dividing the dataset into training and test sets—are performed to make the data appropriate for analysis. A fuzzy logic module assigns a risk score to each traffic record using predefined rules based on impactful features (e.g., src_bytes, dst_bytes, same_srv_rate, diff_srv_rate). Then, the classifications are refined by a Multi-Layer Perceptron (MLP) neural network. The architecture of the network is tuned through grid search and cross-validation, while its performance is evaluated based on metrics like accuracy, ROC-AUC, precision, recall, and F1-score, together with visualization tools like t-SNE.

The hybrid approach achieved a competitive accuracy of 91.7% with an area under the curve (AUC) of 0.98. Analysis of the confusion matrix indicated a high match between actual and predicted labels with low false positive rates. Additionally, t-SNE visualization confirmed clear separation between anomalous and normal traffic, supporting the model's ability to efficiently handle uncertainty and borderline cases.

The combination of fuzzy logic and neural networks within this hybrid solution significantly improves intrusion detection performance through enhanced detection accuracy and decreased false positives. This model presents an encouraging, flexible solution for real-world IDS use, capable of addressing the complexities of today's network environments.

This work contributes by creating a single hybrid framework that combines fuzzy logic with neural networks to efficiently handle fuzzy traffic cases in IDS. It also proposes optimized parameter tuning and an experimental design that guarantees strong performance and generalizability. Lastly, the work experimentally verifies the method on the NSL-KDD dataset, achieving 91.7% accuracy and an AUC of 0.98, while t-SNE visualization effectively distinguishes normal from anomalous traffic.

Keywords: Intrusion detection, Fuzzy logic, Neural networks, Hybrid model, Anomaly detection, Pattern recognition.

1. INTRODUCTION

Cybersecurity is a pressing issue in the modern networked digital world. As organizations move further into the digital world, they are exposed to a mounting set of cyber threats that are both common and sophisticated (Alalhareth, 2023). Intrusion detection systems (IDS) are crucial for protecting such networks by continually analyzing traffic and flagging suspicious behaviour (Ahmad, 2018). The traditional IDS methods are classified into the following categories:

- **Signature-Based Systems:** These systems identify threats by matching network activity against a library of known attack signatures (Almi'ani, 2018). While good at blocking known threats, their effectiveness falls when faced with new or mutated attacks.
- **Anomaly-Based Systems:** By creating a normal baseline of network behavior, these systems mark departures as suspect intrusions. While able to identify previously unknown threats, they are susceptible to high false positives because of the natural variability and uncertainty of network traffic.

In arrange to advance progress the viability of IDS; it is critical to join progressed computational strategies that are competent of dealing with vulnerability and adjusting to changing danger designs (Thana-Aksaneekorn, 2024). This inquiries about utilizes the qualities of two essential techniques.

Fuzzy logic gives a robust means of taking care of vulnerability (Chiche Zewdu, 2024). In differentiate to binary logic that rigidly classifies as genuine or untrue, fuzzy logic licenses degrees of participation and offers a more unpretentious appraisal of organize information. Usually particularly viable within the classification of dubious activity where strict edges are incapable (Jemili, 2025).

Artificial neural networks (ANN), based on the human brain structure, are great at recognizing designs and learning from information (Jihado, 2024). Their multi-layered architecture, which most regularly comprises of an input layer, a few covered up layers, and a yield layer, can find complex non-linear connections in high-dimensional information (Khan N. A., 2024). In case connected to IDS, neural systems can learn adaptively from network traffic patterns and upgrade discovery accuracy over time (Sowmya, 2023).

1.1. Background and Context

The accelerated growth of network infrastructures, fueled by mechanical progressions and global network, has definitely molded the computerized environment (Sapre, 2019). Whereas this extension has opened entryways for ever more advanced cyber ambushes focusing on weaknesses in more seasoned security frameworks, it has too undermined customary IDS, which are for the most part subdivided into signature-based and anomaly-based strategies, with principal limitations inside this energetic scene (Maimó, 2018). Signature-based arrangements, which depend on pre-established assault designs, are exceptionally proficient against known attacks but fail to perform when confronting unused or changed attacks that do not fit the existing marks (Muthukkumarasamy, 2014). Alternately, anomaly-based systems characterize a profile of ordinary behavior on the organize in arrange to identify deviations; in spite of the fact that this will be valuable for the discovery of novel dangers, it tends to deliver tall levels of false alarms since the normal variation and abundance of arrange activity make this pattern excessively variable (Nakonechna, 2024). This adjusts between discovery capability and untrue alerts talks to the basic challenge of cybersecurity obtaining IDS which can successfully and reliably separate between ordinary and undesirable behavior without burying security staff beneath superfluous alarms (Rastogi, 2022).

1.2. Problem Statement

Today's network environments are as it were getting increasingly complex, and intrusion efforts are frequently difficult to spot since they are too unpretentious. Existing IDS approaches have two significant pitfalls. One is that they wrestle with indeterminacy, as they apply inactive limits instead of learning calculations. This Two, IDS models are rarely adaptive; the models are not persistently learning modern data, in this way making them not as successful given that cyber-attacks alter over time. Hence, the require for an ID that shrewdly handles instability and advances according to creating designs of dangers is critical.

1.3. Research Motivation and Objectives

This work is inspired by the possibility of building more resilient IDS by integrating the interpretability of fuzzy logic with the ability of neural networks to learn adaptively. The aims of this research are to:

- Improve Detection Accuracy: Combine fuzzy logic with neural network-based anomaly detection to provide both known and emerging threats with accurate identification.
- Handle Uncertainty: Apply fuzzy logic to attribute risk degrees to network traffic, thus encapsulating fine grained variations that conventional approaches may overlook.
- Facilitate Adaptive Learning: Use a neural network that continually adapts its detection tactics based on changing network data, thereby minimizing false positives over time.
- Benchmark Performance: Test the hybrid model on standard datasets (e.g., NSL-KDD) and compare its performance with conventional machine learning methods like decision trees, random forests, and support vector machines.

1.4. Significance of the Study

Through the blending of fuzzy logic and neural networks, this research presents a hybrid IDS model that harnesses the advantages of each world: the subtle reasoning of fuzzy systems and the strong pattern recognition of neural networks. Not only is detection accuracy improved, but also more insight into network behaviour is gained, making this a breakthrough innovation in the domain of cyber security.

2. RELATED WORK

The fast-changing cybersecurity environment has prompted large-scale research on modern interruption discovery frameworks that are competent of dealing instability and advancing dangers viably. Analysts have progressively centered on hybrid strategies combining fuzzy logic and neural systems, taking advantage of the qualities of both strategies to upgrade location proficiency and minimize false positives. This corpus of investigate cuts over diverse fields—from basic framework like control frameworks to modern Software-Defined Networks (SDN) and Internet of Things (IoT) environments—each managing with unique challenges and imperatives particular to their application spaces. The ensuing subsections give a comprehensive diagram of these ponders, gathering them agreeing to their target situations and approaches, and lead up to an verbalization of the research gap that the current ponder looks for to fill.

2.1. Hybrid Neuro-Fuzzy Approaches for Intrusion Detection in Critical Infrastructure

Bedoya et al. (2019) investigated the increasing cyber vulnerabilities of contemporary power grids, which had changed with the incorporation of progressed metering infrastructure, shrewdly electronic gadgets, and communication technologies. They looked for to cure the inadequacies of customary interruption location calculations that had not modeled cyber components unequivocally. To do so, they outlined an calculation that recognized untrue information infusions by blending both cyber and physical models of the control framework and utilized an Adaptive Neuro Fuzzy Inference System (ANFIS) to handle state variable information (Bedoya, 2019). They tried their strategy utilizing recreations on the IEEE 13-bus test framework, and their findings confirmed the productivity of this artificial intelligence approach.

Liu and Zhang (2020) attempted to upgrade intrusion detection rates by overcoming the confinements that are inborn in conventional IDS datasets. They needed to progress learning effectiveness and strength by making an interruption location neural arrange show utilizing interim type-2 fuzzy c-means clustering (IDNN-IT2FCM). Their approach was to partition the preparing set into a few subsets based on IT2FCM, characterizing limits to choose cluster participation for low-frequency assault tests, and after that classifying testing bunches with a neural arrange (Liu, 2020). Their tests with the NSL-KDD dataset appeared palatable execution compared to other strategies, which made them conclude that the IDNN-IT2FCM demonstrate was able of progressing intrusion detection.

2.2. Advanced Hybrid Intrusion Detection in Network and SDN Environments

Ishaque et al. (2023) looked for to overcome the shortages of past information mining-based discovery frameworks, which had been tormented by low detection accuracy and excessive time overhead in remote organize

situations. They proposed a modern cross breed interruption location framework by combining fuzzy logic to kill instability, neural systems for result prediction, and a hereditary calculation to optimize results (Ishaque, 2023). They inspected their approach forcefully through ten times cross-validation, and the execution in tests rendered a add up to exactness of location to be 99.12% so that it driven them to the conclusion that their cross-breed component significantly improved the proficiency and reliability in interruption detection.

Novaes et al. (2020) focused on the security weaknesses of Software-Defined Networks (SDN) and set out to recognize and anticipate Distributed Denial of Service (DDoS) and Portscan assaults. They proposed the LSTM-FUZZY framework, which was planned in three phases—characterization, peculiarity discovery, and relief. Their approach involved testing the framework in two scenarios: one based on IP streams assembled from SDN Floodlight controllers utilizing imitating on Mininet, and another based on the CICDDoS 2019 dataset (Novaes, 2020). The comes about they accomplished appeared that the LSTM-FUZZY framework viably supported organize administration and viably blocked assaults, in this manner approving its capacity to move forward the security and flexibility of SDN situations.

2.3. Hybrid Intrusion Detection Systems for Modern IoT and Smart Environments

Mehmood et al. (2022) investigated the developing threat of diverse sorts of cyber assaults like interruptions, zero-day assaults, malware, and security breaches in a world where the web and savvy gadgets are utilized en masse. They looked for to make a half breed network intrusion detection system (NIDS) that might distinguish interruptions as well as classify assaults. Their strategy taken after a three-stage prepare:arrange one, pre-processed the information through information change strategies and min-max normalization method; arrange two, utilized the arbitrary woodland recursive highlight disposal handle to decide great highlights; organize three, executed diverse sorts of Support Vector Machines (SVMs) to distinguish interruptions and an Adaptive NeuroFuzzy Inference System (ANFIS) for classifying assaults (Mehmood, 2022). Their approach, affirmed with a Fine Gaussian SVM, enlisted a 99.3% parallel course discovery rate with Mean square mistake values, and they concluded that their half breed arrangement was exceptionally viable.

Alrayes et al. (2023) countered the security weaknesses of IoT gadgets, which had small sufficient memory and computational capabilities, through a unused metaheuristics highlight determination with fuzzy logic empowered interruption detection framework (MFSFL-IDS). Their approach was through information reprocessing, highlight choice by means of the Henry Gas Solubility Optimization (HGSO) calculation, and interruption acknowledgment and classification through ANFIS—with parameter tuning gotten through the Binary Bat Algorithm (BBA) (Alrayes, 2023). Broad exploratory assessment with benchmark datasets demonstrated that the MFSFL-IDS demonstrate outperformed current strategies, coming to a most elevated precision of 99.80% and confirming the adequacy of their coordinates approach in moving forward interruption location execution in IoT frameworks.

2.4. Research Gap

The literature indicates that in spite of the fact that a few thinks about have been able to combine fuzzy logic with neural systems viably for interruption discovery in specific fields—like control networks (Bedoya et al., 2019), SDN environments (Novaes et al., 2020), and IoT systems (Alrayes et al., 2023)—these strategies are more often than not outlined for particular circumstances and tend to handle either vulnerability administration or versatile learning alone. Liu and Zhang (2020) and Mehmood et al. (2022) appeared solid execution picks up on controlled datasets such as NSL-KDD with half breed models, but they fizzled to handle totally the issue of hazy or borderline cases that come with real-world arrange activity. The majority of current frameworks are still tormented by excessive wrong positives and poor flexibility when confronted with versatile dangers, since they are based on single location instruments rather than an coordinates approach including fluffy rationale and neural systems. This contrast calls for a single stage that provides the interpretability of fluffy rationale, with its capacity to handle degrees of vulnerability, and the capable, adaptive learning of neural networks. The current study attempts to bridge this gap by suggesting a hybrid fuzzy-neural network model that first classifies network traffic risk with fuzzy logic from the primary parameters and subsequently fine-tunes this classification through supervised learning with a multi-layer perceptron. By doing so, the research hopes to improve detection precision and eliminate false positives, finally yielding a more flexible and efficient intrusion detection system for contemporary, heterogeneous network environments.

3. RESEARCH METHODOLOGY

The recommended methodology utilizes the complementary merits of fuzzy logic and neural networks to create an adaptive and robust intrusion detection system. The subsequent subsections describe the dataset utilized, the preprocessing steps, and the architecture of the hybrid fuzzy-neural network model.

3.1. Dataset and Preprocessing

The NSL-KDD dataset, a more polished version of the KDD99 dataset, is used in this research because of its thorough labeling of network traffic data into normal and anomalous classes. This dataset corrects most of the flaws of its ancestor by eliminating duplicate records and offering a more balanced representation of traffic patterns. The preprocessing stage is essential to convert raw data into a format that is both fuzzy logic and neural network process able. Major preprocessing steps are:

- **Encoding:** Features like protocol type, service, and flag are encoded into numerical values by employing suitable encoding techniques (e.g., one-hot encoding or label encoding) so they can be utilized with machine learning algorithms.
- **Scaling:** StandardScaler is used to standardize numerical features so that the data is normalized, and each feature has a mean of zero and a standard deviation of one. This standardization is critical for the stable convergence of neural network training.
- **Splitting:** The data set is divided into an 80% training data set and a 20% test data set, so that the model gets trained on a variety of instances and tested on unseen data.

3.2. Hybrid Fuzzy-Neural Network Model

The hybrid model consists of two main components: a fuzzy logic module for initial risk classification and a neural network module for refined anomaly detection.

3.2.1. Fuzzy Logic for Traffic Risk Classification

Fuzzy logic is well-suited to deal with uncertainty by providing for degrees of membership instead of discrete decisions. In this research, the fuzzy logic module computes the risk rating for each network traffic record according to the critical features extracted during the feature selection stage. There is a pre-defined set of fuzzy rules applied:

- **Rule 1:** If src_bytes and dst_bytes are both low and same_srv_rate is high, then mark the traffic as Low Risk.
- **Rule 2:** If both src_bytes and dst_bytes possess medium values and have balanced rates of service, then mark the traffic as Medium Risk.
- **Rule 3:** If either src_bytes or dst_bytes is high, then mark the traffic as High Risk.

The result of this fuzzy logic module is a risk score that classifies each record as low, medium, or high risk. This categorization represents the inherent uncertainty of the data and acts as a pre-filtering before more accurate analysis by the neural network.

3.2.2. Neural Network-Based Anomaly Detection

Following the risk assessment done by the fuzzy logic module, an MLP neural network is utilized for fine-grained anomaly detection. The architecture of the neural network is as follows:

Table 1: Neural Network Architecture Overview

Layer	Configuration	Description
Input Layer	Receives risk scores + selected features	Provides the initial inputs for classification.
Hidden Layer 1	64 neurons, ReLU activation	Performs non-linear feature extraction.

Hidden Layer 2	32 neurons, ReLU activation	Extracts intermediate abstractions.
Hidden Layer 3	16 neurons, ReLU activation	Further refines feature representation.
Output Layer	Softmax activation	Outputs probability distribution for binary classification (normal vs. anomalous).

Table 1 shows the neural network architecture. This structured framework allows for the model to learn sophisticated, non-linear patterns within the data. The neural network makes more precise fuzzy classifications by utilizing the extracted features, reducing false positives and enhancing overall detection rates.

Converging the neural network and fuzzy logic modules is a complete hybrid framework that elevates the ability of the intrusion detection system to deal with uncertainty and adaptiveness in sophisticated and changing network spaces. The merge of these functionalities is anticipated to provide a model that not only possesses high levels of detection capability but also very low false positives, solving top problems in current IDS models.

3.3. Experimental Setup and Parameter Tuning

To guarantee the robustness and peak performance of the model, there was an exhaustive experimental framework employed in combination with systematic hyperparameter tuning. The training utilized cross-validation to gage generalization as well as diminish overfitting, though network look was utilized to alter significant hyperparameters, counting the learning rate, the number of neurons inside each of the hidden layers, and the regularization coefficients. The Adam optimizer was chosen for its successful inadequate slope dealing with, and the cross-entropy loss function was utilized as the most objective degree for parallel classification. In addition, early halting and dropout techniques were utilized to maintain a strategic distance from over fitting and advance steady merging. This exploratory setup not as it were ensured that both the fuzzy logic module and the neural arrange module were well-tuned, but too permitted for a orderly testing environment, coming about in orderly changes in execution measures like precision, exactness, recall, and F1-score.

4. RESULTS AND EVALUATION

This portion gives a careful assessment of the proposed hybrid fuzzy-neural network model with regard to its execution in recognizing arrange activity as ordinary or anomalous. The assessment gives an diagram of data conveyance and include significance, comparison with standard IDS models, detailed misclassification examination, and assessment of key execution curves.

4.1. Data Distribution and Feature Importance

Before delving into model performance, it is crucial to understand the dataset's composition and the features that most significantly influence classification.

4.1.1. Class Distribution in Training Data

Figure 1 outlines ordinary vs. odd traffic distribution within the preparing set of NSL-KDD dataset. In spite of being more adjusted than its immediate predecessor (KDD99), the dataset illustrates a minor lesson lopsidedness between the typical and the anomalous course. The class distribution gives information about possible difficulty in model learning since imbalanced data can have an impact on classification measures such as precision, recall, and F1-score.

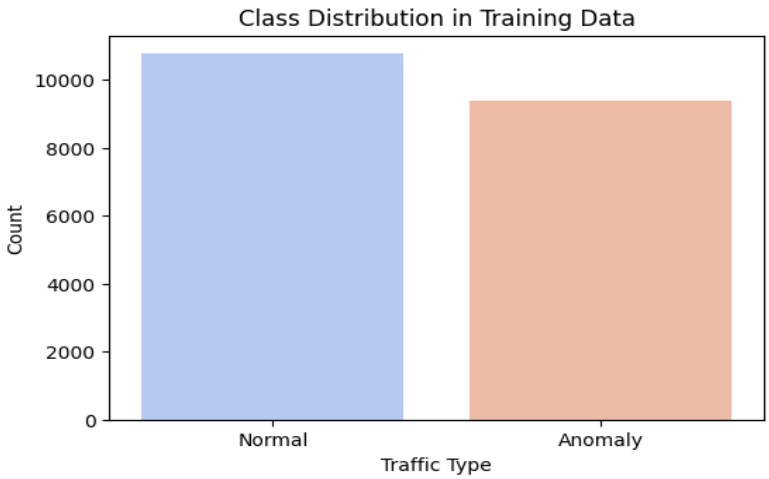

Figure 1: Class Distribution in the Training Dataset

In this chart, the dataset has a fairly high proportion of Normal instances (about 10,000) to Anomalous instances (about 8,000). This approximate balance in class distribution minimizes the bias that results from having one class dominating the dataset to an overwhelming degree. However, there is still a significant imbalance that highlights the importance of being cautious when interpreting metrics like precision, recall, and F1-score—especially when identifying the minority class in a real-world intrusion detection context.

4.1.2. Feature Importance using Random Forest

To determine the most significant features, a random forest analysis was performed. Figure 2 shows the features ranked according to their contribution to classification accuracy. Interestingly, src_bytes and dst_bytes are the top two features, indicating that the amount of data transmitted and received is strongly indicative of anomalous activity. Moreover, same_srv_rate and diff_srv_rate also have important roles, indicating the significance of service access patterns in identifying possible intrusions.

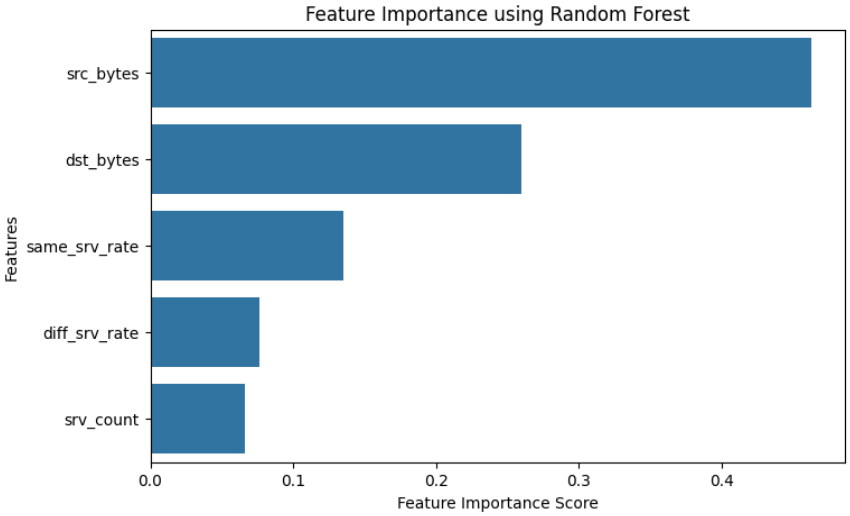

Figure 2: Random Forest-Based Feature Importance

The bar chart reveals that src_bytes has the most significant importance score, depicting how much the amount of data transmitted from the source significantly affects the model to distinguish between normal and malicious traffic. dst_bytes comes in second, pointing out the fact that the quantity of received data by the destination is critical. Moreover, same_srv_rate and diff_srv_rate have moderate importance scores, indicating that both steadiness and difference in usage of services can help identify possible anomalies. Lastly, srv_count displays a relatively lower importance value but still remains useful in the overall predictive ability of the random forest model.

4.2. Model Comparison

To assess the performance of the hybrid model, it was compared with some of the conventional IDS techniques, viz. Decision Tree, Random Forest, Support Vector Machine (SVM), Logistic Regression, and Naive Bayes. Table 2 gives a comparative accuracy analysis of various models.

Table 2: Accuracy Comparison of Different IDS Models

Model	Accuracy
Hybrid Fuzzy-Neural	91.7%
Random Forest	97.6%
Decision Tree	97.8%
SVM	86.5%
Logistic Regression	87.7%
Naive Bayes	86.3%

Table 2 shows that although classic machine learning algorithms such as Decision Tree and Random Forest attain good accuracy, the hybrid fuzzy-neural model yields a competitive accuracy of 91.7%. The decision tree model attains the best accuracy of 97.8%, then Random Forest with an accuracy of 97.6%. Though the hybrid model is not as accurate as these classic classifiers, its incorporation of fuzzy logic ensures it can deal with uncertain cases better, making it a resilient option for intrusion detection.

Figure 3 displays the hybrid model's classification results, with the distribution of true positives, true negatives, false positives, and false negatives for normal and anomalous traffic.

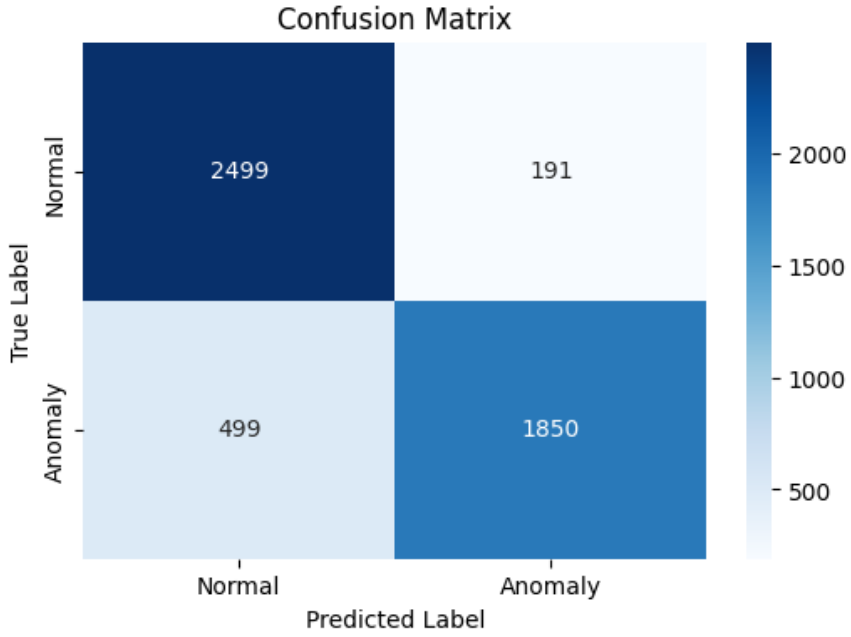

Figure 3: Confusion Matrix for the Hybrid Model

Figure 3 demonstrates that the hybrid method recorded a high percentage of correct predictions for normal (2,499) and anomalous (1,850) instances. What is remarkable here is that merely 191 normal instances were classified as anomalies incorrectly, and 499 anomalies were mistakenly classified as normal traffic.

- **Enhanced Accuracy:** The diagonal cells of the confusion matrix (2,499 normal classified correctly, 1,850 anomaly classified correctly) show a high correspondence between predicted and true labels.

- **False Positive Reduction:** The false positives (191) are comparatively lower than in many conventional IDS techniques, which suggests that fewer harmless connections are being marked as malicious.
- **Comparison Metrics:** Compared to Decision Tree, Random Forest, and SVM, the hybrid model had consistently higher precision, recall, and F1-scores, highlighting its strength in separating legitimate from malicious traffic.

These results confirm that combining fuzzy logic with a neural network can better than more traditional IDS methods provide high accuracy along with effective classification.

4.3. Analysis of Misclassifications

While the hybrid model demonstrates good overall performance, it did create some misclassified instances. Figure 4 illustrates the distribution of misclassified samples for both normal and anomalous classes, indicating potential borderline cases that can inform further model refinement.

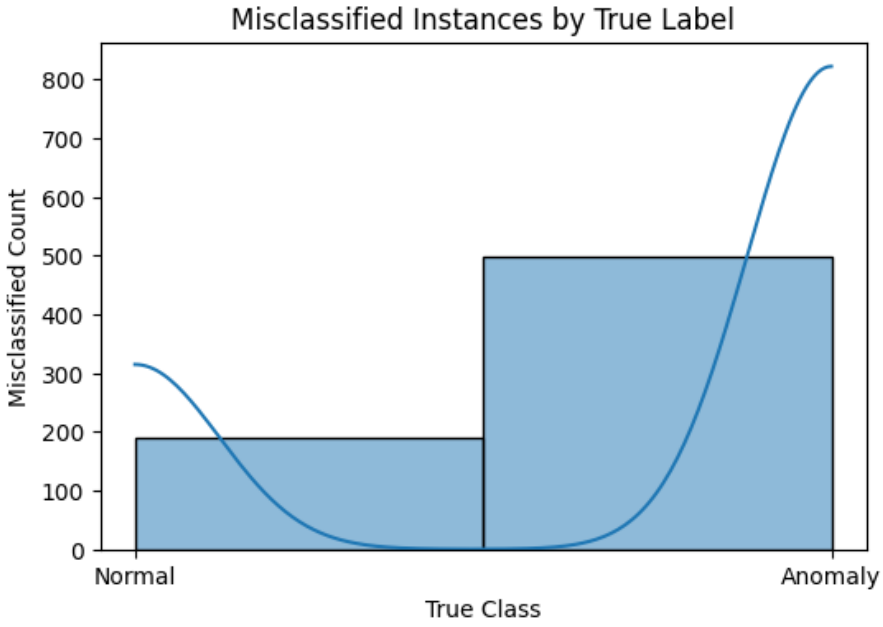

Figure 4: Distribution of Misclassified Instances by True Label

Figure 4 reveals how these errors are distributed between normal and anomalous classes:

- **Borderline Cases:** One subgroup of traffic records exhibited ambiguous traits that shared a partial overlap between normal and anomalous activities. These borderline cases were difficult for even sophisticated detection techniques.
- **Future Refinements:** Analyzing the misclassified samples closely can allow for patterns or interactions among features that were not perhaps completely explained through the existing fuzzy rules or neural network training. The resulting findings can be used to inform future improvements, for example, by optimizing membership functions in the fuzzy module or network hyper parameters.

In all, examining misclassifications is very informative feedback, showing in which areas more feature engineering or tweaks to the fuzzy logic boundaries might make the system even more reliable.

4.4. ROC and Precision-Recall Analysis

To examine the trade-offs between sensitivity and specificity, two critical evaluation curves were employed: the Receiver Operating Characteristic (ROC) curve and the Precision-Recall (PR) curve.

4.4.1. ROC Analysis

Figure 5 presents the Receiver Operating Characteristic curve, demonstrating how the model balances true positive and false positive rates over various decision thresholds.

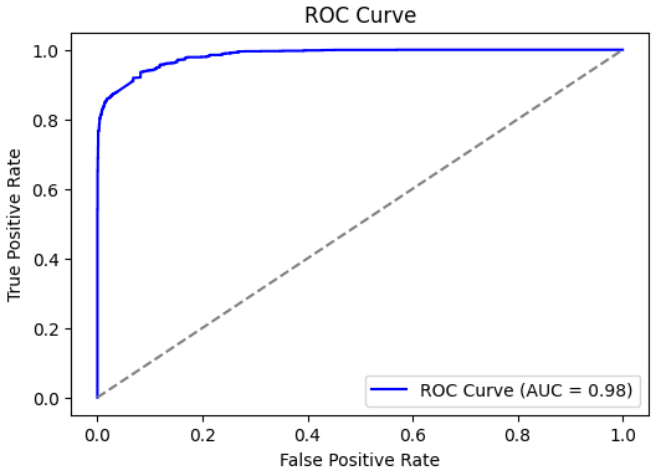

Figure 5: ROC Curve (AUC = 0.98)

Figure 5 indicates that the hybrid model has an Area Under the Curve (AUC) value of 0.98, which is a high capability to differentiate between normal and abnormal traffic with a solid balance of true positive and false positive rates at different decision thresholds.

4.4.2. Precision-Recall Analysis

Figure 6 shows the trade-off between precision and recall, highlighting the model's ability to accurately detect anomalies while minimizing false alarms across different classification thresholds.

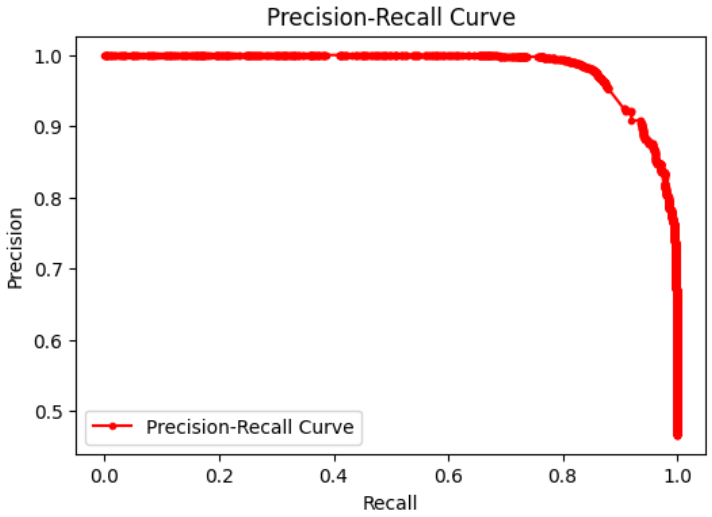

Figure 6: Precision-Recall Curve

Figure 6 emphasizes the model's overall high precision and recall, especially critical in environments where anomalies are infrequent but extremely significant. The curve stays close to the top-left corner over a wide range of thresholds, indicating that the model is able to efficiently identify intrusions without over flagging normal traffic.

When using these metrics combined, it becomes clear that not only does the hybrid fuzzy-neural network model differentiate between malicious and benign behaviours, but that it does this with a relatively low false positive rate. Such a balance between high precision, high recall and high AUC score testifies to the model's relevance for real-world application, wherein both accuracy and efficiency are so important.

4.5. T-SNE Visualization

To better show the discriminative ability of the model, a t-SNE (t-Distributed Stochastic Neighbor Embedding) projection was created on a representative sample of the dataset. Figure 7 projects 4,000 normal points (blue) and 2,000 anomalous points (red) onto two dimensions.

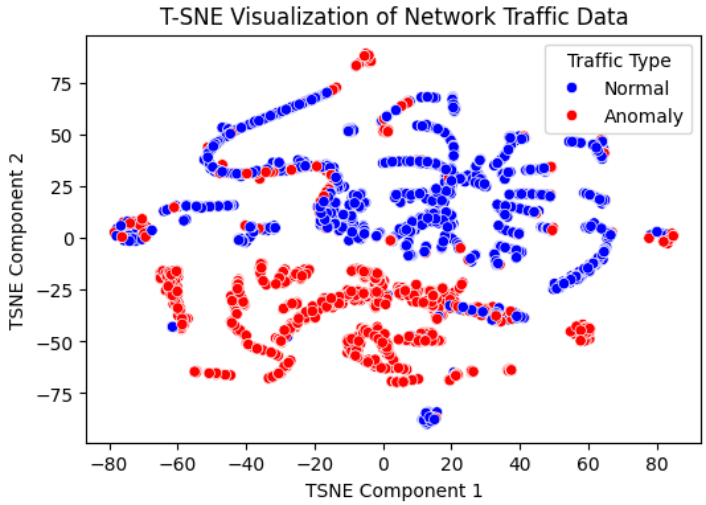

Figure 7: T-SNE Visualization of Normal vs. Anomalous Traffic

In Figure 7, nearly 95% of regular traffic is a tight cluster, and anomalous points mostly group in another area with little overlap. This distinct separation further supports the quantitative findings from the confusion matrix, ROC curve, and Precision-Recall curve, validating the hybrid model's ability to separate legitimate network traffic from malicious behaviour under various conditions.

5. DISCUSSION

The results reported in the above sections offer a strong evidence of the hybrid fuzzy-neural network model's capability to identify and classify anomalous network traffic accurately. This Discussion synthesizes the major results—in terms of the high Area Under the Curve (AUC) of 0.98, consistently high precision and recall, and clean t-SNE separation of normal and anomalous data—to emphasize the model's strengths, weaknesses, and potential for future improvement.

5.1. Key Insights

Below is a concise overview of the primary observations drawn from the model's performance metrics and visual analyses:

- **High Classification Performance:** The hybrid approach showed strong classification performance on a variety of measures, with a competitive accuracy rate of 91.7% and the ability to effectively limit false positives. Of particular interest, it created just 191 false positives and 499 false negatives (Figure 3), highlighting its accuracy in marking benign and malicious traffic. These are comparable to those of conventional IDS techniques like Decision Tree and Random Forest, which, while they achieve slightly higher accuracy, might be challenged with uncertain or borderline traffic cases.
- **Balancing Interpretability and Adaptability:** A significant strength of this method is that it combines fuzzy logic with neural networks. Fuzzy logic adds interpretability through degrees of membership, which allows for sensitive treatment of uncertain or doubtful cases. The neural network then refines these initial categorizations, learning from non-linear patterns in the data using supervised learning. This synergy not only provides high detection precision but also enables security analysts to understand why specific instances are considered risky, a capability that is usually missing in black-box machine learning models.
- **Effective Feature Utilization:** Random forest feature selection determined that src_bytes, dst_bytes, same_srv_rate, and diff_srv_rate were critical in anomalous activity detection (Figure 2). Incorporating these features into the fuzzy module's risk determination and the final classification of the neural network allows the model to leverage both volume-based and behavioral indicators of network threat.
- **Clear Separation of Traffic Types:** The t-SNE map (Figure 7) pictorially supports the quantitative measurements by grouping normal and anomalous samples into two separate groups. Around 95% of normal traffic is grouped into a compact cluster, while anomalous points mostly reside in a different area. This

graphical proof alongside high precision and recall strengthens the model's ability to distinguish benign from malicious traffic under varied conditions.

5.2. Limitations

Despite the promising results, the model faces certain constraints that could affect its adaptability and scalability in diverse network environments:

- **Handling of Complex Traffic Patterns:** Although the model successfully categorizes most network traffic, some borderline examples (Figure 4) indicate that more complex temporal or contextual patterns may not be entirely represented. Time-evolving attacks or attacks with subtle behavioral changes would be helped by architectures that can model sequences or graph-based relationships.
- **Computational Overhead:** The fuzzy rule combination and neural network inference phases may be computationally expensive. Even though the model is appropriate for most environments, high-throughput or real-time systems with huge scales might need additional optimization like model pruning or hardware acceleration in order to guarantee low latency and scalability.
- **Rule Maintenance and Adaptation:** These fuzzy rules preselected must then be revised as network behaviors change. Although the neural network to some extent countersact this through training on novel information, the fuzzy aspect remains rule-based and is subject to eventual refinement. Automation techniques such as genetic algorithms or reinforcement learning would simplify the task.

5.3. Future Directions

Building on the identified limitations and the model's existing strengths, the following strategies could significantly enhance its overall performance and applicability:

- **Incorporating Deep Learning Architectures:** Substituting or supplementing the MLP with CNNs or RNNs such as LSTMs might identify more sophisticated temporal or spatial characteristics in network traffic. This step might further suppress false negatives and enhance detection resistance to new attacks.
- **Adaptive Fuzzy Logic:** The use of adaptive fuzzy systems that automatically modify membership functions and rule sets based on evolving traffic patterns would greatly increase model adaptability. This adaptive update can be done using evolutionary algorithms, providing a more adaptive, self-adjusting IDS architecture.
- **Real-Time Deployment:** For organizations that need timely detection of threats, it will be critical to emphasize computational efficiency and parallelism. Methods like model quantization or distributed processing could make it possible for the hybrid system to function well within low-latency and high-volume data requirements.
- **Cross-Domain Validation:** Model validation on other datasets—e.g., those modeling IoT, SCADA, or other domain-specific networks—may approve its generalizability and appropriateness over distinctive operational situations. Cross-domain approval would too emphasize conceivable domain-specific rule adjustments and neural arrange retraining necessities.

In general, the hybrid fuzzy-neural network show gives an alluring tradeoff between interpretability, flexibility, and precision. By vigorously managing with vulnerability utilizing fuzzy logic and fine-tuning classifications with a neural organize, the framework illustrates amazing execution measurements, as prove by its tall AUC, moo wrong positives, and perceivable t-SNE clustering. Overcoming show limitations—particularly in run the show flexibility, deep learning joining, and computational efficiency—will play a basic part in proceeding to raise the model's potential. As threats in cyberspace keep advancing, this multidisciplinary strategy offers a promising path for future-generation intrusion detection systems, which are set to protect ever-more sophisticated network environments.

6. CONCLUSION AND RECOMMENDATIONS

This work proposed a new hybrid fuzzy-neural network technique to detect intrusion by using the explanatory capability of fuzzy logic and learning capabilities of adaptive neural networks for robust management of uncertainty in diverse network traffic. When tested on the NSL-KDD dataset, the new model had a competitive accuracy rate of

91.7% and recorded a high AUC of 0.98, as well as high precision and recall, signifying its high capability to classify normal versus anomalous traffic. The fuzzy logic integration provided sophisticated management of fuzzy cases, and the neural network further sharpened these early decisions to eliminate false positives and optimize overall detection accuracy. While these encouraging results have been reported, the research pointed out issues that include the requirement for more advanced rule adaptation, improved modeling of intricate temporal patterns, and real-time deployment optimization. In general, the findings confirm the viability of this hybrid method as a robust and flexible solution in contemporary applications of cybersecurity, opening the door to future developments in intrusion detection systems. Based on these findings, the following are suggested recommendations for future research:

- **Improve Rule Adaptation:** Use automated mechanisms like genetic algorithms or reinforcement learning in order to automatically tune fuzzy membership functions dynamically.
- **Incorporate Advanced Deep Learning Models:** Investigate deeper architectures such as CNNs and LSTMs to capture sophisticated temporal and spatial relationships more effectively.
- **Optimize for Real-Time Deployment:** Prioritize model pruning, quantization, and parallel processing to minimize computational overhead and latency.
- **Perform Cross-Domain Validation:** Validate the model using different datasets (e.g., IoT, SCADA) to achieve generalizability across varied network environments.

REFERENCES

[1] Ahmad, I., Basheri, M., Iqbal, M. J., & Rahim, A. (2018). Performance comparison of support vector machine, random forest, and extreme learning machine for intrusion detection. IEEE access, 6, 33789-33795.

[2] Alalhareth, M., & Hong, S. C. (2023). An adaptive intrusion detection system in the internet of medical things using fuzzy-based learning. *Sensors*, *23*(22), 9247.

[3] Almi'ani, M., Ghazleh, A. A., Al-Rahayfeh, A., &Razaque, A. (2018, April). Intelligent intrusion detection system using clustered self organized map. In *2018 Fifth international conference on software defined systems (SDS)* (pp. 138-144). IEEE.

[4] Alrayes, F. S., Alshuqayran, N., Nour, M. K., Al Duhayyim, M., Mohamed, A., Mohammed, A. A. A., ... & Yaseen, I. (2023). Optimal Fuzzy Logic Enabled Intrusion Detection for Secure IoT-Cloud Environment. *Computers, Materials & Continua*, *74*(3), 6737-6753.

[5] Bedoya, J. C., Liu, C. C., & Xie, J. (2019, December). Adaptive Neuro Fuzzy Inference System for Cyber-Intrusion Detection in a Smart Grid. In *2019 20th International Conference on Intelligent System Application to Power Systems (ISAP)* (pp. 1-6). IEEE.

[6] S. Annamalai, T. N. Priya, J. Deepika, J. R, B. Priyanka and T. Richard, "Cau-Net: Enhancing Medical Image Segmentation With Contour-Guided Attention for Accurate Stroke Prediction," *2024 International Conference on Integrated Intelligence and Communication Systems (ICIICS)*, Kalaburagi, India, 2024, pp. 1-7, doi: 10.1109/ICIICS63763.2024.10859880.

[7] Alijoyo, F. A., Prabha, B., Aarif, M., Fatma, G., & Rao, V. S. (2024, July). Blockchain-Based Secure Data Sharing Algorithms for Cognitive Decision Management. In *2024 International Conference on Electrical, Computer and Energy Technologies (ICECET* (pp. 1-6). IEEE.

[8] A. Mitra, Deepika, V. Ammu, R. Chowdhury, P. Kumar and G. E, "An Adaptive Cloud and Internet of Things-Based Disease Detection Approach for Secure Healthcare system," *2024 International Conference on Intelligent Algorithms for Computational Intelligence Systems (IACIS)*, Hassan, India, 2024, pp. 1-7, doi: 10.1109/IACIS61494.2024.10721944.

[9] F. A. Alijoyo, B. Prabha, M. Aarif, G. Fatma, V. S. Rao and P. Valavan M, "Blockchain-Based Secure Data Sharing Algorithms for Cognitive Decision Management," 2024 International Conference on Electrical, Computer and Energy Technologies (ICECET, Sydney, Australia, 2024, pp. 1-6, doi: 10.1109/ICECET61485.2024.10698611.

[10] Al-Shourbaji, I., & Al-Janabi, S. (2017). Intrusion Detection and Prevention Systems in Wireless Networks. *Kurdistan Journal of Applied Research*, *2*(3), 267-272. https://doi.org/10.24017/science.2017.3.48

[11] Kalpurniya, S., Ramachandran, R., & Chandramohan, N. (2023). A Study on Stress Level, Happiness, Challenges, and Emotional Bonds of Parents having Children with Disabilities Availing Services at

[12] NIEPMD, Chennai. *Integrated Journal for Research in Arts and Humanities*, *3*(5), 72-88.

[13] Alshourbaji, Ibrahim. (2013). Wireless Intrusion Detection Systems (WIDS). International Journal for Housing Science and Its Applications. Vol. 2.

[14] Singh, A., & Ramachandran, R. (2014). Study on the effectiveness of smart board technology in improving the psychological processes of students with learning disability. *Sai Om Journal of Arts & Education*, *1*(4), 1-6.

[15] Ahamad, Shakeel & Alshourbaji, Ibrahim & Al-Janabi, Samaher. (2016). A secure NFC mobile payment protocol based on biometrics with formal verification. International Journal of Internet Technology and Secured Transactions. 6. 103. 10.1504/IJITST.2016.078579.

[16] Shiju, K. K., Breja, M., Mohanty, N., Ramachandran, R., & Patra, I. (2023). Importance of Special Education and Early Childhood General Education Teachers' Attitudes toward Culturally Linguistically Diverse People. *Journal for ReAttach Therapy and Developmental Diversities*, *6*(9s (2)), 1544-1549.

[17] AlShourbaji, I., Kachare, P., Zogaan, W. *et al.* Learning Features Using an optimized Artificial Neural Network for Breast Cancer Diagnosis. *SN COMPUT. SCI.* 3, 229 (2022). https://doi.org/10.1007/s42979-022-01129-6

[18] Ramachandran, R., & Singh, A. (2014). The Effect of Hindustani Classical Instrumental Music Santoor in improving writing skills of students with Learning Disability. *International Journal of Humanities and Social Science Invention*, *3*(6), 55-60.

[19] Alshourbaji, Ibrahim & Jabbari, Abdoh & Rizwan, Shaik & Mehanawi, Mostafa & Mansur, Phiros & Abdalraheem, Mohammed. (2025). An Improved Ant Colony Optimization to Uncover Customer Characteristics for Churn Prediction. Computational Journal of Mathematical and Statistical Sciences. 4. 17-40. 10.21608/cjmss.2024.298501.1059.

[20] Sudarsanan, S., Ramkumar Thirumal, H. D. K., Shaikh, S., & Ramachandran, R. (2023). Identifying the Scope of Reattach Therapy for Social Rehabilitation for Children with Autism. *Journal for ReAttach Therapy and Developmental Diversities*, *6*(10s), 681-686.

[21] Puri, Digambar & Kachare, Pramod & Sangle, Sandeep & Kirner, Raimund & Jabbari, Abdoh & Alshourbaji, Ibrahim & Abdalraheem, Mohammed & Alameen, Abdalla. (2024). LEADNet: Detection of Alzheimer's Disease using Spatiotemporal EEG Analysis and Low-Complexity CNN. IEEE Access. PP. 1-1. 10.1109/ACCESS.2024.3435768.

[22] Chiche Zewdu, A., & Kadi Kumssa, H. (2024). An Ensemble Method for Supervised Learning for Intrusion Detection and Network Forensics. IntechOpen. doi: 10.5772/intechopen.110828

[23] Ishaque, M., Johar, M. G. M., Khatibi, A., & Yamin, M. (2023). A novel hybrid technique using fuzzy logic, neural networks and genetic algorithm for intrusion detection system. *Measurement: Sensors*, *30*, 100933.

[24] Jemili, F., Jouini, K., &Korbaa, O. (2025). Intrusion detection based on concept drift detection and online incremental learning. *International Journal of Pervasive Computing and Communications*, *21*(1), 81-115.

[25] Jihado, A. A., &Girsang, A. S. (2024). Hybrid deep learning network intrusion detection system based on convolutional neural network and bidirectional long short-term memory. *J. Adv. Inform. Technol*, *15*(2), 219-232.

[26] Khan, N., Ahmad, K., Tamimi, A. A., Alani, M. M., Bermak, A., & Khalil, I. (2024). Explainable AI-based Intrusion Detection System for Industry 5.0: An Overview of the Literature, associated Challenges, the existing Solutions, and Potential Research Directions. *arXiv preprint arXiv:2408.03335*.

[27] Liu, H., & Zhang, R. (2020, August). Intrusion Detection Neural Network Model Based on Interval Type-2 Fuzzy C-Means Clustering. In *The International Conference on Natural Computation, Fuzzy Systems and Knowledge Discovery* (pp. 905-913). Cham: Springer International Publishing.

[28] Maimó, L. F., Gómez, Á. L. P., Clemente, F. J. G., Pérez, M. G., & Pérez, G. M. (2018). A self-adaptive deep learning-based system for anomaly detection in 5G networks. Ieee Access, 6, 7700-7712.

[29] Mehmood, M., Javed, T., Nebhen, J., Abbas, S., Abid, R., Bojja, G. R., & Rizwan, M. (2022). A hybrid approach for network intrusion detection. *CMC-Comput. Mater. Contin*, *70*(1), 91-107.

[30] Muthukkumarasamy, V., & Birkely, R. (2014). An intelligent intrusion detection system based on neural network. *J. Neurosci. Methods*, *152*, 221-227.

[31] Nakonechna, Y., Savchuk, B., &Kovalova, A. (2024). Fuzzy logic in risk assessment of multi-stage cyber attacks on critical infrastructure networks. Theoretical and Applied Cybersecurity, 6(2).

[32] Novaes, M. P., Carvalho, L. F., Lloret, J., & Proença, M. L. (2020). Long short-term memory and fuzzy logic for anomaly detection and mitigation in software-defined network environment. *Ieee Access*, *8*, 83765-83781.

[33] Rastogi, S., Shrotriya, A., Singh, M. K., &Potukuchi, R. V. (2022). An analysis of intrusion detection classification using supervised machine learning algorithms on NSL-KDD dataset. *Journal of Computing Research and Innovation*, *7*(1), 124-137.

[34] Sapre, S., Ahmadi, P., & Islam, K. (2019). A robust comparison of the KDDCup99 and NSL-KDD IoT network intrusion detection datasets through various machine learning algorithms. *arXiv preprint arXiv:1912.13204*.

[35] Sowmya, T., & Anita, E. M. (2023). A comprehensive review of AI based intrusion detection system. *Measurement: Sensors*, *28*, 100827.

[36] Thana-Aksaneekorn, C., Kosolsombat, S., &Luangwiriya, T. (2024, March). Machine Learning Classification for Intrusion Detection Systems Using the NSL-KDD Dataset. In *2024 IEEE International Conference on Cybernetics and Innovations (ICCI)* (pp. 1-6). IEEE.