Research Square

Preprints are preliminary reports that have not undergone peer review.
They should not be considered conclusive, used to inform clinical practice,
or referenced by the media as validated information.

# Adaptive Heuristic Rule-Infused Neural Architecture for Dynamic Cyber Threat Analysis and Packet Classification

**A Joshua Issac**

joshuaissacscholar@gmail.com

SRM Institute of Science and Technology

**S. Shanmuga Priya**

SRM Institute of Science and Technology

**Research Article**

**Keywords:** Adaptive Cybersecurity, Heuristic Rule Infusion, Packet Classification, Cross-Attention Network, Meta-Reinforcement Learning

**Posted Date:** March 6th, 2026

**DOI:** https://doi.org/10.21203/rs.3.rs-8929721/v1

**License:** This work is licensed under a Creative Commons Attribution 4.0 International License.
Read Full License

**Additional Declarations:** No competing interests reported.

# Adaptive Heuristic Rule-Infused Neural Architecture for Dynamic Cyber Threat Analysis and Packet Classification

[1]A Joshua Issac*, [2]Dr.S.Shanmuga Priya,

[1]Research Scholar, Department of Computer Science and Engineering, SRM Institute of Science and Technology, Tiruchirappalli, Tamil Nadu, India
[2]Associate Professor, Department of Computer Science and Engineering, SRM Institute of Science and Technology, Tiruchirappalli, TamilNadu, India

joshuaissacscholar@gmail.com, priya501@gmail.com

*Corresponding Author: A Joshua Issac

## Highlights of the Study

- The SNH-ACAN model combines heuristic rule knowledge with neural feature learning using an Adaptive Rule Fusion mechanism, providing interpretable and adaptive cyber threat detection.
- The Dynamic Consistency Alignment Module aligns heuristic and neural representations, reducing misclassification and improving decision reliability across various attack types.
- The model achieves 98.2% accuracy, 98.5% precision, and 98.1% F1-score, outperforming existing IDS models

**Abstract**

The increasing complexity and volume of cyber threats, including phishing, DDoS, SQL injection, and zero-day exploits, challenge traditional intrusion detection systems that often rely on static signatures or shallow learning models. Existing techniques exhibit limitations in adaptability, explainability, and real-time decision-making under dynamic network environments. Static rule-based systems are equally limited, being unable to adapt to rapidly evolving attack vectors. To address these gaps, the study introduces a novel Synergistic Neuro-Heuristic Adaptive Cross-Attention Network (SNH-ACAN) integrated with a Heuristic Rule-Infusion Layer for enhanced interpretability and Meta-Reinforcement Learning (Meta-RL)–based Adaptive Feedback Module. The primary aim is to achieve explainable, high-performance cyber threat detection that fuses rule-based symbolic reasoning with neural feature learning. The framework employs Adaptive Rule Fusion (ARF) and the Dynamic Consistency Alignment Module (DCAM) to ensure alignment between heuristic and neural representations, minimizing misclassifications in complex packet sequences. To further enhance adaptability against zero-day and evolving threats, the Meta-Reinforcement Learning (Meta-RL) Adaptive Feedback Module is integrated post-classification. The model operates on preprocessed network traffic data from Kaggle, with data normalization, feature engineering, and heuristic rule embedding. Implemented using Python, TensorFlow, and PyTorch, the architecture employs cross-attention mechanisms to balance heuristic and learned information dynamically. Experimental findings indicate superior performance, achieving 98.2% accuracy, 98.5% precision, 98.0% recall, and 98.1% F1-score, and outperforming existing IDS models by 1.5–3%. The model also demonstrates enhanced scalability with reduced GPU memory usage and improved throughput (92%) under high network load. Overall, the proposed framework ensures enhanced cybersecurity resilience by dynamically responding to evolving cyber threats while minimizing detection delays and false positives.

**Keywords:** Adaptive Cybersecurity, Heuristic Rule Infusion, Packet Classification, Cross-Attention Network, Meta-Reinforcement Learning.

### 1. Introduction

The growth of contemporary digital infrastructure has allowed cyber threats to develop into more complex varieties, which have made traditional security systems for protecting against evolving attack patterns irrelevant [1], [2]. The current threat monitoring systems mainly use signature-based and rule-based approaches that cannot detect zero-day attacks in addition to Advanced Persistent Threats [3]. The security methods do not succeed because they stay stagnant while also facing broad network traffic limitations and needing predetermined attack signatures to work effectively [4]. To address to these challenges, artificial intelligence-driven cybersecurity solutions have developed, essentially adopting deep learning-based anomaly detection models [5]. TCNs have proven to be superior to RNNs and LSTM for network traffic analysis because they effectively build long-range dependency models in temporal data better than these other methods [6].

The autoencoder serves as a widespread unsupervised anomaly detection method which learns base traffic behavior patterns to detect cyber threat deviations [7]. The existing security frameworks with AI foundation encounter a significant drawback due to their static capabilities when dealing with new attack patterns [8]. The meta-learning aspect permits the system to deploy adaptive model updates that help improve detection accuracy as attacks evolve [9]. Traffic Anomaly Quarantine and Adaptive Firewall Policies complement self-learning proactive defensive measure mechanisms and allow for real-time threat mitigation as they are capable of adaptive protective measures [10]. Conventional IDS are limited in their adaptability to evolving cyber threats due to their reliance on static rules, or models that have a purely data-driven approach [11]. This study introduces SNH-ACAN, a neuro-symbolic architecture combining heuristic rules with neural embeddings through Adaptive Fusion and Meta-Reinforcement Learning to support interpretable, real-time classification and adaptive prevention of both known and zero-day attacks.

### 1.1. Recent Innovations and Limits

Recently, deep learning-based models such as CNN, LSTM, Transformer and Autoencoder have been used to classify network traffic and detect cyber attacks[12]. These models are very effective in feature extraction, recognizing temporal patterns, and detecting anomalies. However, the majority of methods are purely data-driven and do not consider expert knowledge and heuristic rules [13]. They often struggle with zero-day attacks, evolving threat patterns, and interpretability. In addition, the use of high-dimensional embeddings and sequence modeling increases the computational cost, thus limiting the methods' real-time applicability [13]. As a result, there is a demand for hybrid models that combine symbolic knowledge and neural learning to achieve cyber threat detection that is adaptive, explainable, and efficient.

### 1.2 Problem Statement

Current intrusion detection systems rely mostly on purely heuristic or purely data-driven methods. Heuristic systems are understandable but do not identify new threats, whereas deep learning models learn to adapt to unknown patterns but are not transparent and use a lot of computational power [14]. Conventional fusion models statically merge rules and neural features, and this restricts adaptability when the network environment changes. Such limitations impede effective, real-time identification of advanced cyber-attacks, especially zero-day attacks and emergent threat patterns [15]. Thus, an innovative method needs to be proposed that enables synergistic combination of rule-based reasoning with adaptive neural learning in such a way as to enable both explainability and high-performance detection in contemporary network contexts.

### 1.3 Research Motivation

The ever-changing cyber threats require detection systems with the ability to learn quickly and adapt to unseen attack patterns. Current methods compromise either interpretability or scalability, making networks susceptible to sophisticated attacks. Combining heuristic knowledge with neural learning provides a paradigm for preserving explainability while attaining adaptive intelligence. The aim of this research is driven by the desire to develop a hybrid, rule-embedded neural model that effectively detects, classifies, and suppresses adaptive cyber threats in real-time.

### 1.4 Research Significance

The suggested research presents a new adaptive paradigm that combines expert heuristics with neural learning and offers explainable and effective cyber threat detection. It improves known and zero-day attack detection accuracy, minimizes false positives, and enables real-time network monitoring. The approach provides an interpretable, scalable, and generalizable solution to contemporary cybersecurity problems, filling the gap between symbolic reasoning and deep learning and thus contributing to both theoretical and practical network defense solutions.

### 1.5 Key Contribution

- ✓ Heuristic rule-based preprocessing reduces computational overhead by filtering benign traffic before AI-based classification.
- ✓ TCN-Autoencoder enables adaptive cyber threat classification, ensuring robust anomaly detection for evolving attacks.
- ✓ Meta-learning enhances model adaptability by refining parameters based on new threat patterns for continuous improvement.
- ✓ Comprehensive threat detection and mitigation framework effectively identifies and mitigates phishing, DDoS, ransomware, and zero-day exploits.
- ✓ The proposed system ensures high detection speed, precision, and scalability, making it suitable for real-time cybersecurity applications.

The paper is organized as follows: Section 1 introduces the study, highlights the need for adaptive cyber threat detection, and presents the methods used in the respective analyses. Section 2 discusses related work. Section 3 introduces and discusses the methodology, including heuristic rules, and meta-RL. Section 4 presents performance comparisons with results and findings. Section 5 wraps with key takeaways and suggests future research avenues.

## 2. Literature Review

Khan et al.,[16] invented an intelligent packet forwarding system which prioritizes classification through machine learning classifiers for Deep Packet Inspection on Differentiated Services Code Point (DSCP). The DSCP-based packet classification employed SVM, KNN, Decision Tree, RF, and Logistic Regression in conjunction with XGBoost and AdaBoost as classification models. The experimental results indicated that AdaBoost yielded the highest accuracy rate at 89.91% while it was adapting to network system changes. RF also showed promising results by achieving 89.41% accuracy in its performance. The method has two main issues that arise from detailed calculations and the problem of adapting to the changing situation.

The research by Abbas et al.,[17] is focused on cyberattack detection with deep learning models in IoT networks using the CICDIoT2023 dataset. The method presented includes preprocessing and normalization, encoding of categorical variables, and training with DNNs, CNNs, and RNNs. The experimental results revealed that the RNN model delivered 96.56% accuracy which made it the most effective approach for detecting cyberattacks in IoT network traffic. The proposed approach faces two main weaknesses because it requires expensive computations while also being prone to overfit the ever-changing network patterns.

Through their predictive framework Al-Quayed et al.,[18] provide security enhancements for Industrial 4.0 WSNs by performing intelligent intrusion prevention and defense operations. The methodology uses Decision Tree and MLP and Autoencoder models as part of machine learning and deep learning for cybersecurity intrusion detection and classification. The Decision Tree and MLP models process multiple classes but Autoencoder focuses on two-class systems. The MLP model obtained 99.52% accuracy in simulations as the best performing model, while Decision Tree followed with 99.48% accuracy. The binary classification using the Autoencoder model achieved 91% accuracy. The system faces difficulties in both processing speed and flexibility when handling new cyber threats.

The research by Zhukabayeva et al.,[19] introduces a cybersecurity structure for Wireless Sensor Networks in smart grids through integration of traffic examination and node identification and machine learning engines to

identify and stop cyber threats. Through its implementation of the RF model for traffic load prediction the system reached an $R^2$ score of 0.717982 along with MAE of 1.099080, RMSE of 1.665038 and MSE of 2.772350. RF surpasses Decision Trees and Logistic Regression as an intrusion detection method to yield precision (0.99) as well as recall (0.99) and F1-score (0.98). The model demonstrates complete success (1.00) when it comes to detecting Flooding attacks. The method presents two main constraints involving high processing requirements aside from its restricted ability to detect new threats.

Ali et al.,[15] designed an LSTM-based multitask deep learning model for detecting IoT malware. The model carries out two operations which determine traffic innocence or maliciousness and malware type identification. Time-series analysis was performed on IoT traffic data from scale that researchers obtained from IoT devices. A three-step feature categorization process was used together with feature selection methods to boost performance while analyzing the traffic flag-related, flow-related, and packet payload-related features. During testing the proposed model delivered 92.63% accuracy for task 1 and 88.45% accuracy for task 2 and 95.83% accuracy for multitask classification. The system faces difficulties in scalability with new malware variations along with executing complex computations.

The paper by Cai et al.,[20] presents an adaptive DDoS attack mitigation scheme which detects and mitigates DDoS attacks in software-defined cyber-physical systems. Unsupervised anomaly detection and information entropy serve in this method to automatically recognize and fight known and unknown DDoS attacks. The new attack traffic pipeline filtering mechanism allows easy deployment to existing SDN networks through hardware-free operations. According to experimental tests the proposed method achieved 99.13% average attack mitigation accuracy during intense DDoS cyber assaults. The method delivers a 35% to 59% decrease in false-positive rate better than current approaches. The system faces two key constraints – it does not easily adjust to new attack patterns and deployments at large scale might lead to performance degradation.

Chakraborty et al.,[14] develops a deep neural network framework with rule-based functionality that improves the detection process for new cyberattacks that bypass classic signature-based detection methods. By testing the framework with CICIDS 2017 data it achieved more than 99% accuracy for new attack detection with equally balanced true and false positive results. Through its threat level classification methodology the model serves to improve security in automatic network interactions based on IoT systems. The system faces drawbacks from its ability to adjust to changing attack patterns as well as from possible resource performance limitations.

Ghadermazi et al.,[21] proposed an artificial intelligence framework that resolves packet-based network intrusion detection system constraints through proper analysis of temporal connections with header-level attack patterns. The proposed method first turns packet sequences into two-dimensional images while using a CNN model for intrusion detection. The method analyzes both payload and header information to increase the detection performance of malicious operations. The system evaluates attack detection performance at 97.7% to 99% accuracy when tested on publicly accessible big datasets spanning different attack types. The proposed framework demonstrates its resistance to attacks performed by adversaries.

Shanmugham et al.,[22] formulated ADKNN-BSSA-CSMANET as a framework to enhance MANET cybersecurity through deep learning integration and optimization. SHA-256 crypto hash signatures in addition to mobile user biometrics including finger vein identification and geographic positioning work for authentication. The process of packet analysis implements adaptive density-based spatial clustering to discover attack patterns through geodesic filtering to delete information that is unrelated to the analysis. Group Teaching Algorithm-based feature selection improves input features while the Deep Kronecker Neural Network (ADKNN) carries out traffic classification between attack and normal types. The Bear Smell Search Algorithm (BSSA) implements an optimization process that improves the efficiency of detection. The model based on the NSL-KDD dataset demonstrates a substantial decrease in detection delay reaching 36.64% below existing approaches with 33.06% and 33.98% as additional reduction figures.

Hore et al.,[23] developed a multistage AI-enabled framework for network intrusion detection which tackles zero-day as well as out-of-distribution and adversarial evasion attacks. The framework implements three deep neural networks arranged in series as it contains both a classification component and two autoencoders to

identify existing and emerging security threats. The researchers present a new transfer learning methodology by freezing specific DNN neural activity during one-shot learning processes for defense against attack evolution. The experimental outcomes demonstrate a 98.5% average accuracy rate when detecting different sorts of attacks. The model provides a high detection accuracy yet it demonstrates two principal disadvantages regarding processing complexity and deployment hurdles that occur when implementing real-time security measures for high-traffic networks.

Table 1. Literature Review Summary

| References | Method | Findings | Limitations |
|---|---|---|---|
| Khan et al.,[16] | Machine learning classifiers (SVM, KNN, Decision Tree, RF, Logistic Regression, XGBoost, AdaBoost) for DSCP-based packet classification | AdaBoost achieved the highest accuracy of 89.91%, with Random Forest at 89.41%, demonstrating effective adaptation to dynamic network conditions | Computational complexity and potential overfitting in dynamic environments |
| Abbas et al.,[17] | Deep learning models (DNN, CNN, RNN) trained on CICDIoT2023 dataset for IoT cyberattack detection | RNN achieved the highest accuracy of 96.56%, outperforming other models in identifying cyberattacks in IoT networks | High computational costs and potential overfitting in dynamic network environments |
| Al-Quayed et al.,[18] | Decision Tree, MLP, and Autoencoder models for intrusion detection in Industry 4.0 WSNs | MLP achieved 99.52% accuracy, Decision Tree 99.48%, and Autoencoder 91% for binary classification | Computational complexity and adaptability to evolving cyber threats |
| Zhukabayeva et al.,[19] | Machine learning models for cybersecurity in WSN-based smart grids, using RF for traffic load prediction and intrusion detection | Random Forest achieved precision (0.99), recall (0.99), and F1-score (0.98), with perfect recall (1.00) in detecting Flooding attacks | Computational overhead and adaptability to evolving threats |
| Ali et al.,[15] | LSTM-based multitask deep learning model for IoT malware detection and classification | Achieved 92.63% accuracy for benign/malicious detection, 88.45% for malware classification, and 95.83% for multitask classification | Computational complexity and adaptability to new malware variants |
| Cai et al.,[20] | Adaptive DDoS attack mitigation integrating entropy-based anomaly detection and a pipeline filtering mechanism in SDN | Achieved 99.13% mitigation accuracy under high-intensity DDoS attacks, reducing the false-positive rate by 35%-59% | Adaptability to evolving attack patterns and potential performance overhead in large-scale deployments |
| Chakraborty et al.,[14] | Rule-based deep neural network framework integrating anomaly detection and hybrid approaches | Achieved over 99% accuracy in detecting novel cyberattacks with a balanced false positive and false negative rate | Adaptability to evolving attack patterns and computational overhead |
|  | CNN for transforming sequential packets into 2D | Achieved detection rates of 97.7%-99% across various attack | Computational complexity and |

| | | | |
|---|---|---|---|
| Ghadermazi et al.,[21] | images for intrusion detection | types, with resilience against adversarial attacks | challenges in real-time implementation |
| Shanmugham et al.,[22] | ADKNN-BSSA-CSMANET framework integrating deep learning and optimization techniques for MANET cybersecurity | Reduced detection delay by 36.64%, 33.06%, and 33.98% compared to existing approaches | Computational overhead and real-time deployment challenges |
| Hore et al.,[23] | Multistage AI-enabled framework with sequential DNN architectures, integrating transfer learning with one-shot learning | Achieved an average detection accuracy of 98.5% across various attack types | Increased computational complexity and adaptation challenges in high-traffic environments |

Table 1 contains a review that compares AI-based methods used in cybersecurity systems. Although cyber threat detections are AI- and ML-based and have improved greatly, there are still some gaps in the research. The studies demonstrate that it is easy to detect known attacks, but adaptive learning is difficult when threats evolve or new ones appear. Most of the methods, e.g., deep learning and ensemble techniques, have high computational costs and the problem of scalability, and thus, they cannot be applied in real-time in a network whose condition is changing dynamically. Furthermore, the majority of setups are either heavily dependent on heuristic rules or AI-driven models, and there is no integration mechanism that can merge both to achieve the best decision-making. Few studies highlight the interpretable insights of the contribution of rules versus learned features, which is very important for the implementation of adaptive mitigation. So, there is a demand for such a packet classification that is lightweight, adaptive, and explainable and can effectively fuse heuristic knowledge with AI-driven intelligence.

## 3. Proposed AI-Enhanced Packet Classifier for Adaptive Cyber Threat Detection and Mitigation

The suggested framework adopts a defined multi-layered framework that can immediately detect and prevent security threats in real-time network settings. The security system begins with the reception of network traffic information of the different cyber threats that have been logged by the cloud security tools such as phishing attacks, DoS, Man-in-the-Middle, Distributed Denial of Service, SQL Injection, Cross-Site Scripting, Ransomware, Password Attacks, and Zero-Day Exploits. This system retrieves the data in the security logs and then analyzes important traffic activities such as the behavior of packet rates, the use of security score results, network protocols and failed logins. The suggested methodology presents the Adaptive Rule-Infused Neural Synergy framework, which combines symbolic heuristic knowledge with neural learning of data to detect cyber threats in a better way. The system operates on processed network traffic data that is fed in, and transforms attributes of the packets into structured feature representations. Heuristic rules used to describe the known attack patterns, like SYN floods, abnormal port activity and unusual packet lengths are mined and coded into dense embeddings that allow neural features. The heuristic embeddings are then integrated with the neural feature representations based on the Synergistic Neuro-Heuristic Adaptive Cross-Attention Network that utilizes a dual-branch architecture. The neural branch retrieves a sequence of patterns of time and contexts of the packets, whereas the heuristic branch maintains rule-based information. The cross-attention mechanisms facilitate dynamic communication between the branches and make the model focus on the relevant rules or data-driven insights depending on the characteristics of packets. The Dynamic Consistency Alignment Module makes sure that the integrated representation will be interpretable and consistent yet to the changing traffic flows. To achieve adaptive mitigation, a Meta-Reinforcement Learning-based feedback module is used in order to dynamically update the heuristic rule embeddings and mitigation policy to address emerging threats. The system is capable of identifying the best action to take drop, quarantine, alert, or reroute, according to fused embeddings and network context to quickly adapt to zero-day attacks or adaptive attacks. It is suitable in dynamic network environments, and offers both high accuracy and interpretability in packet-level intrusion detection, as its

methodology focuses on explainability, scalability, and the ability to deploy it in real-time. Figure 1 depicts the proposed methodology working framework.

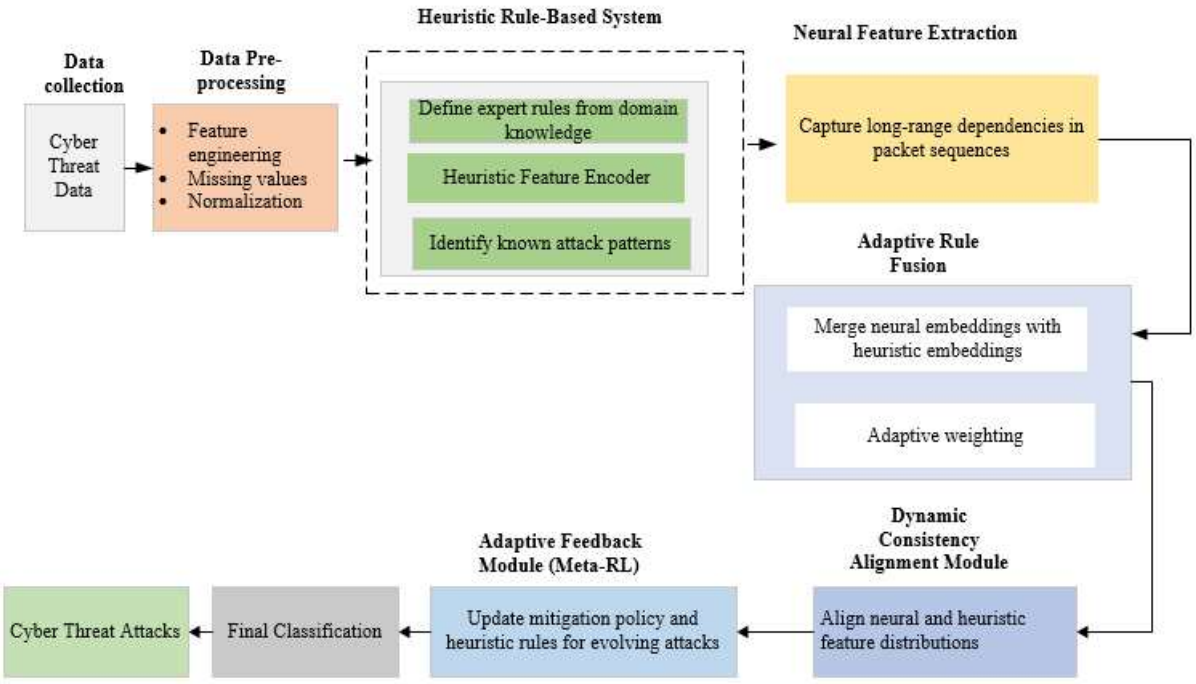



Figure 1. Proposed Framework

### 3.1 Input Data

The dataset originated from simulated network traffic, which incorporates different standards of communication and cybersecurity vulnerabilities. The dataset is gathered from Kaggle website [24]. The recording system captures network packets based on their transfer protocols along with their signal information and IP details and port numbers and quantitative information about packet length. The system applies predefined attack signatures during label assignment to identify attacks as Phishing, DoS, DDoS, Man-in-the-Middle, SQL Injection, and Zero-Day Exploits. The structured collection approach delivers thorough tracking of regular and dangerous traffic to fulfill research needs in intrusion detection and anomaly detection. Table 2 shows the dataset summary.

Table 2. Dataset Description

| Protocol | Flag | Packet | Source IP Address | Destination IP Address | Destination Port | Packet Size | Target Variable |
|---|---|---|---|---|---|---|---|
| TCP | SYN | HTTP | 192.168.0.1 | 10.0.0.5 | 80 | 1024 | Phishing |
| UDP | ACK | DNS | 10.0.0.2 | 192.168.0.1 | 12345 | 512 | DoS |
| TCP | SYN | SSH | 192.168.1.10 | 10.0.0.8 | 12345 | 256 | Man-in-the-Middle |
| TCP | RST | FTP | 192.168.0.5 | 10.0.0.10 | 12345 | 2048 | SQL Injection |
| UDP | ACK | SNMP | 192.168.1.10 | 10.0.0.2 | 12345 | 768 | Ransomware |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| TCP | FIN | HTTPS | 10.0.0.5 | 192.168.0.1 | 12345 | 4096 | Password Attacks |
| UDP | ACK | DHCP | 192.168.0.1 | 10.0.0.5 | 12345 | 256 | Zero-Day Exploits |
| TCP | RST | FTP | 10.0.0.2 | 192.168.1.10 | 20 | 2048 | Cross-Site Scripting |
| UDP | ACK | NTP | 10.0.0.5 | 192.168.1.10 | 12345 | 128 | DDoS |

### 3.2 Data Preparation

A clean structured dataset needs to be achieved through data preprocessing because it prepares the input for training the proposedmodels which detect cyber threats. The following procedure describes the complete data preprocessing process.

**a) Missing Values**

Missing values in the data creates problems which result in biased models and errors. A systematic check for missing values takes place while applying suitable techniques for their resolution. The removal process applies when any element has more than 30% unrecorded data points within its group so the column automatically gets deleted. The data imputation method applies mean or mode calculation for numerical and categorical data points when missing values reach less than 30% of total count.

**b) Feature Engineering**

The dataset gains enhanced capabilities from feature engineering because new meaningful attributes improve model performance. The analysis includes three main features which are traffic rate measuring packets per second and session duration calculating time between first and last packet and anomaly score showing TCN-Autoencoder reconstruction error. The designed features constitute effective tools for cyber threat identification. Traffic Rate ($R$): Measures the number of packets per second is shown in Eqn. (1)

$$\mathrm{R} = \frac{\text{Total Packets}}{\text{Total Time(S)}} \tag{1}$$

**c) Normalization**

The normalization process scales every numerical feature in a standardized range thus avoiding influential behavior from attributes with large values. Min-max normalization was used.

$$I' = \frac{I - I_{min}}{I - I_{max}} \tag{2}$$

In Eqn. (2) $I_{min}$ and $I_{max}$ are the minimum and maximum values of feature $I$. The categorical attributes of protocol type and flags alongside the attack labels transform into numerical values through combination of Label Encoding and One-Hot Encoding techniques. For Label Encoding each category gets a unique integer value but One-Hot Encoding creates separate columns containing values of 1 or 0 to represent categories. Processing machine learning models becomes possible through the conversion of categorical data. The dataset was divided into 70% training data and 30% testing data according to standard best practices to achieve ideal model evaluation that prevents underfitting or overfitting. The complete set of preprocessing techniques both boosts the dataset reliability and improves detection accurateness. Algorithm 1 shows the steps involved in data preprocessing.

Algorithm 1: Data Preprocessing for Cyber Threat Detection

Input:

Raw_Dataset: Cyber Threat Data for New Malware Attacks (Contains raw network traffic attributes such as IP, Port, Protocol, Packet Size, Flags, Timestamp, and Label)

Output:

Cleaned, normalized, and encoded dataset ready for AI-based threat classification

BEGIN

LOAD dataset "Cyber Threat Data for New Malware Attacks" # Load the dataset

Step 1: Handle Missing Values

FOR each column in dataset:

IF missing values > 30% THEN

REMOVE column

ELSE

IF column is numerical THEN

IMPUTE missing values using MEAN

ELSE

IMPUTE missing values using MODE

Step 2: Standardize Column Names

FOR each column in dataset:

CONVERT column names to lowercase

REMOVE special characters and spaces

Step 3: Feature Engineering

FOR each network session:

COMPUTE traffic rate = Total Packets / Total Time

COMPUTE session duration = Last Packet Timestamp – First Packet Timestamp

Step 4: Normalize Numerical Features

FOR each numerical feature I:

$$I' = \frac{I - I_{min}}{I - I_{max}}$$

Step 5: Encode Categorical Variables

```
    FOR each categorical column:
        IF column has ordinal categories THEN
            APPLY Label Encoding
        ELSE
            APPLY One-Hot Encoding
Step 6: Split Dataset into Train and Test Sets
    SPLIT dataset into 70% training and 30% testing
Step 7: Save Preprocessed Data
    SAVE preprocessed dataset
END
```

### 3.3 Heuristic Rule-Infusion Layer

The Heuristic Rule-Infusion Layer serves as the intersection point of the symbolic intelligence (heuristic rules defined by experts) and sub-symbolic representation of intelligence (deep neural features). This aims to create a two way synergy that allows detecting cyber threats in a way that is adaptive and interpretable. Symbolic reasoning offers decision constraints which are explicit, whereas neural learning offers high dimensional patterns that are not visible within a manual rule design. The model is capable of generalizing outside known attacks and still being logically interpretable due to this fusion. Adaptive Rule-Infused Neural Synergy (ARINS) Framework is used to combine heuristic rules with data-driven neural learning to come up with a system that is interpretable and adaptive. It uses symbolic rule encoding and neural packet embedding and combines them with cross-attention and continually trains the model and rulebase using Meta-Reinforcement Learning. This will guarantee the identification of both the familiar and the unfamiliar cyber threats with real time responsiveness. It is applicable to intrusion detection systems and edge computing, as well as to adaptive cybersecurity systems, and offers effective, explainable, and self-evolving threat mitigation based on dynamic network systems and dynamic attack patterns.

#### 3.3.1 Input and Feature Representation

The input comprises structured network packet data obtained from a hybrid dataset of simulated and real-world traffic. Each packet $P_i$is represented as Eqn. (3).

$$P_i = \{f_1, f_2, \ldots, f_n\} \tag{3}$$

Where $f_k \in$ {protocol type, flag, packet size, source/destination IP, source/destination port, time delta, byte entropy, flow duration, inter-arrival time}. Each feature is preprocessed. Categorical features (protocols, flags) are processed using one-hot encoded vectors. Continuous features (packet size, duration) are normalized using min-max scaling.

#### 3.3.2 Rule Extraction

This starts with the derivation of domain knowledge or network patterns. The sequences of network packets are compared with predefined conditions that characterize known attack behaviours. Derived Rules Based on Dataset: R1: IF Protocol = TCP AND Flag = SYN AND Destination Port = 80 → Phishing. R2: IF Protocol = UDP AND Packet Size < 256 AND Frequency > Threshold → DDoS. R3: IF Protocol = TCP AND Source Port = 20 → SQL Injection. R4: IF Unknown protocol AND Random IP sequence→ Zero-Day Exploit. Every rule is

represented as a triplet formally: $R_i = (Condition_i, Action_i, Confidence_i)$. $Condition_i$contains patterns that match on a packet (protocol, flag, port, size) that are specific to packets. $Action_i$is the type of attack that is predicted. $Confidence_i$is a measure of the reliability of the rule. The subsystem heuristic rule identifies the patterns in accordance with the known cyber-attack signatures. These domain knowledge and network security policies are used to construct these rules. A sample rule set $R = \{r_1, r_2, \ldots, r_m\}$is a set of conditions, which can include:

1. SYN Flood Detection: Identify sequences with excessive SYN packets to a single destination: $r_1 = (SYN_{count}) \Rightarrow$ DoS suspicion
2. Abnormal Port Access: Monitor unexpected high-frequency access to non-standard ports: $r_2 = (UniquePorts > \theta_2) \Rightarrow PortScan\ alert$
3. Unusual Packet Length: Detect packets exceeding expected sizes: $r_3 = (Size > \theta_3) \Rightarrow Malware\ transmission.$

Repeated Failed Logins: Identify multiple authentication failures within a short time frame. Each rule is represented as a binary or numeric activation.

$$a_j = \begin{cases} 1 & if\ packet/sequence\ satisfies\ rule\ r_j \\ 0\ Otherwise \end{cases} \quad (4)$$

Each rule is translated into a binary activation signal$a_j \in \{0,1\}$, representing whether the condition is met. The full rule activation vector for a packet sequence. For $m$ rules, the resulting rule activation vector is Eqn. (5).

$$A = [a_1, a_2, \ldots, a_m] \quad (5)$$

Where$a_j = 1$ if the corresponding rule $r_j$ is satisfied. This vector encodes the presence or absence of heuristic conditions for each packet sequence, serving as a symbolic representation compatible with neural fusion.

### 3.3.3 Rule Encoding

To interface with neural representations, rules are transformed into numerical embeddings, producing a Rule Vector (RV). Feature Mapping Examples: Protocol: TCP = [1,0,0], UDP = [0,1,0], Unknown = [0,0,1], Flag: SYN = [1,0,0,0,0], ACK = [0,1,0,0,0] Destination Port: normalized to [0,1] range Rule confidence: Ci∈[0,1]. The rule vector for packet i is then:

$$RV_i = \{f_1, f_2, f_3 \ldots, f_n, C_i\} \quad (6)$$

Where $f_2 \ldots . f_n$ are the encoded packet and rule features, and $C_i$ integrates the heuristic confidence into the embedding. This dense vector is suitable for cross-attention and neural integration.

### 3.3.4 Rule Infusion via Adaptive Fusion Gate

The Adaptive Rule Fusion mechanism dynamically integrates symbolic heuristic rules with sub-symbolic neural features through a learnable gating system. It decides, for every input instance, the optimal balance between rule-based inference and data-driven learning, ensuring both interpretability and adaptability in decision-making. The proposed study employs an Adaptive Rule Fusion mechanism as part of the ARINS framework. The ARF module leverages an Adaptive Fusion Gate (AFG) to dynamically regulate the contribution of heuristic rule embeddings and neural feature vectors, ensuring context-aware and interpretable decision-making. The Adaptive Fusion Gate is the novel core mechanism that combines heuristic rule embeddings with raw packet features dynamically, creating a hybrid representation. Let X be the input feature vector (packet features), $RV_i$ means heuristic rule vector, $W_r, W_x$ are trainable weight matrices and σ refers sigmoid activation function. The adaptive fusion gate G is computed as Eqn. (7).

$$G = \sigma(W_r \cdot RV_i + W_x \cdot X) \quad (7)$$

Where $G \in [0,1]^d$ determines how much trust to place in the heuristic versus the data-driven features. The hybrid, rule-infused representation H is then represented as Eqn. (8).

$$H = G \odot RV_i + (1 - G) \odot X \tag{8}$$

Where $\odot$ represents element-wise multiplication. When G≈1, the model relies more heavily on heuristic knowledge, e.g., during high-confidence known attack patterns. When G≈0, the model emphasizes data-driven inference, enabling detection of novel or evolving attacks. Intermediate values allow balanced fusion, dynamically adjusting according to confidence and data consistency.

The Adaptive Rule Fusion mechanism allows the model to adaptively weight symbolic and neural information per packet sequence. Each output dimension of H can be traced back to either heuristic rules or neural features, providing transparency in threat classification. Coupled with Meta-Reinforcement Learning, the gate parameters $W_r, W_x$ are continuously optimized, learning both the neural model and heuristic thresholds. Vectorized rule embeddings $RV_i$ and packet features $X$ are represented in the same latent space, enabling cross-attention in SNH-ACAN Classifier. This adaptive, differentiable fusion of symbolic rules with sub-symbolic neural features is the main idea of the work, which is a significant leap forward in hybridizing static heuristic integration approaches. The hybrid representation H is passed to the next neural classifiers (SNH-ACAN), thus providing packet-level threat detection that is both interpretable and adaptive. Continuous updates through Meta-RL keep the system immune to zero-day attacks, thus making it viable for real-time and edge deployment.

### 3.4 AI-Enhanced Packet Classifier

SNH-ACAN is a heuristic and neuro-symbolic effort in cyber threat detection in real time, using two connected branches. To combine neural feature learning and symbolic heuristic rules together, SNH-ACAN uses an Adaptive Rule Fusion (ARF) mechanism. The neural branch leverages two-layer Performer layers to extract short-term and long-term temporal contextual features from packet-level network traffic, while the expert defined attack rules are encoded using a one-layer multi-layer perceptron (MLP) in the heuristic branch. The Cross-Attention Fusion operates to align these two embeddings, producing a combined hybrid representation of both the neural and heuristic approach. The Dynamic Consistency Alignment Module (DCAM) preserves interpretability, and aligns the resulting prediction scores from the rule-based and neural networks to provide an explanation. Finally, a softmax classifier layers produces score outputs for the predicted threat type, as well as rule contribution scores is shown in figure 2. In this study, SNH-ACAN contributes to the accuracy, scalability, and transparency of intrusion detection by leveraging rule-driven insights in cooperation with adaptive neural attention to strengthen the classification of cyber packets.

The Synergistic Neuro-Heuristic Adaptive Cross-Attention Network functions through four main layers: Heuristic Rule Encoder, which encodes domain-specific rules as dense symbolic vectors; Neural Feature Encoder, which uses Performer-based self-attention to generate representations about packets in the latent space that are scalable in the temporal dimension; Adaptive Cross-Attention Fusion, which aligns the heuristic embeddings and neural embeddings to enable contextualized cooperative reasoning; and DCAM, which preserves interpretability and allows for adaptive refinement of the final decision.

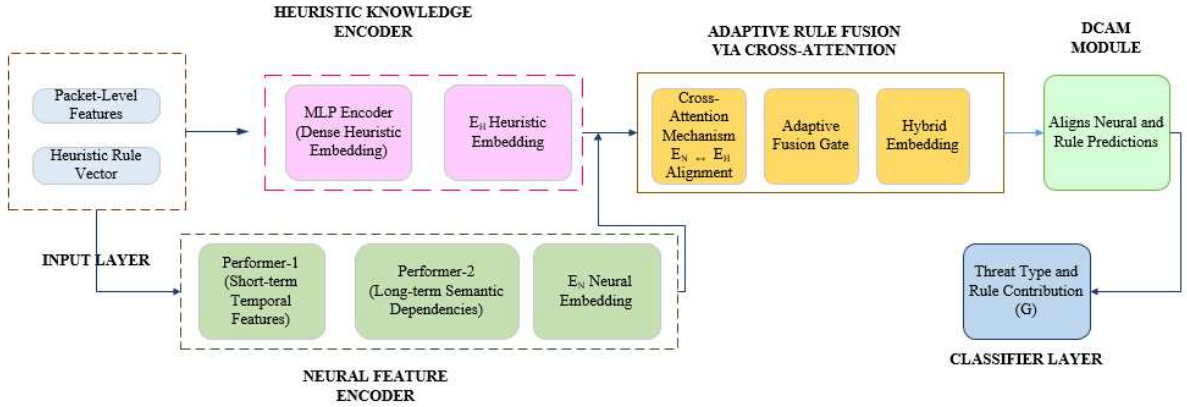



Figure 2. Synergistic Neuro-Heuristic Adaptive Cross-Attention Network

The SNH-ACAN is a double-branch, rule-enriched deep neural architecture for cyber threat classification based on network traffic patterns. It takes packet-level features and heuristic rule activations as input, allowing for hybrid comprehension that combines symbolic (rule) and sub-symbolic (data-driven) intelligence. A packet instance is presented as two dual-mode feature spaces. Neural Feature Input $X = [P, F, S_{id}, R_{id}, S_{IP}, D_{IP}, S_{port}, D_{port}, PacketSize]$. These are normalized continuous and categorical network features, mapped to dense embeddings through a neural encoder.

Heuristic Rule Embedding ($E_h$): Based on the Heuristic Rule-Infusion Layer (ARINS), symbolic conditions (e.g., TCP + SYN + Port 80 → Phishing) are extracted and represented as a dense vector. The embedding represents the logical activation strength of expert-defined patterns. A multi-class threat label $Y \in \{Phishing, DoS, DDoS, SQL\ Injection, MITM, Ransomware, Zero-Day, \dots\}$is predicted by a softmax classifier. SNH-ACAN consists of four main modules, each intended to conduct a different cognitive operation.

### 3.4.1 Neural Feature Encoder

This branch represents numerical and discrete features of packets with high-dimensional temporal representations. The SNH-ACAN framework has a Neural Encoder, which uses two Performer modules that use the packet-level data efficiently and maintain both the temporal and semantic dependencies. Performer-1 records temporal characteristics in the short term, including packet order, flags, and local bursts whereas Performer-2 records long distance semantic relationships between sessions and protocols. Performers provide a direct approximation of softmax attention using FAVOR+ kernelized attention, and it scales linearly $O(n)$ to offer real-time intrusion detection. The structure of residual normalization ensures that it is stable, and the global average pooling produces the final dense feature $F$. The hierarchical temporal and contextual information is contained in this representation, and it allows effective fusing heuristic embeddings via cross-attention. Dual-Performer design increases adaptability, interpretability and detection of complex or zero-day cyber threat in high-volume network settings. Efficient linear-time attention is achieved by use of two Performer blocks. Every block of the Performer calculates self-attention by using kernelized random feature maps:

$$Attention(Q, K, V) \approx \Phi(Q)[\Phi(K)^{\top} V] \tag{9}$$

In Eqn. (9) $\Phi(\cdot)$ a random feature mapping that approximates softmax kernel. This minimizes computational complexity from O ($n^2$) to O (n) in real-time IDS systems processing large volumes of traffic. Performer is a linear-time variant of Transformer, which substitute's expensive softmax attention with kernelized random feature mappings $\Phi(\cdot)$, allowing $O(n)$ complexity. In the Neural Feature Encoder (NFE), two Performer blocks effectively learn temporal-protocol dependencies and packet sequencing patterns, guaranteeing real-time processing for intrusion detection of massive-scale network traffic. The output of the encoder: $E_n = Performer_2(Performer_1(X))$ learns temporal-protocol dependencies and packet sequencing patterns.

### 3.4.2 Heuristic Knowledge Encoder

The second branch incorporates symbolic rules that signify knowledge of experts in the domain. Heuristic Knowledge Encoder (HKE) is the symbolic intelligence component of the SNH-ACAN architecture that encodes expert-written rules into dense learnable embeddings that interacts with neural features. All the rules are represented as vectors, contextually encoded using Performer block and crossed-attended with neural representations. The resulting integration allows the heuristic logic and data-based inference to be dynamically aligned and hence enhance interpretability and adaptability. The coded heuristic vectors are used to focus neural attention on significant traffic patterns, improving zero-day attacks detection, and providing consistency in decision making, which relies on domain knowledge. HKE thus bridges symbolic reasoning and neural adaptability for intelligent, explainable, and real-time cyber threat detection. A one-layer MLP encoder projects these vectors into the same latent dimension as $E_n$:$E_h = ReLU(W_r RV_i + b_r)$ Normalization ensures compatibility between neural and heuristic embeddings. This produces a dense heuristic embedding $E_h$ expressing the activation of symbolic patterns (e.g., SYN flood, abnormal port access, or unauthorized protocol sequence).

### 3.4.3 Adaptive Rule Fusion via Cross-Attention

The Adaptive Rule Fusion mechanism is the heart of SNH-ACAN, responsible for intelligently combining neural learning and heuristic reasoning. It enables the model to dynamically decide — for each network packet or flow — how much to trust data-driven patterns vs. human-crafted rules. This is done using a Cross-Attention mechanism that allows information to flow between the two representation streams: Neural embeddings ($E_n$): learned from data through the Neural Feature Encoder. Heuristic embeddings ($E_h$): derived from expert rules through the Heuristic Knowledge Encoder. The Adaptive Rule Fusion mechanism computes attention from one stream to the other. Here, the neural stream queries the heuristic stream. $Q_n = W_Q^{(n)} E_n, K_h = W_K^{(h)} E_h, V_h = W_v^{(h)} E_h$ . Then attention weights are computed as: $A_{n \leftarrow h} = softmax\left(\frac{Q_n K_h^T}{\sqrt{d}}\right)$ and the rule-aware neural output is: $H_n = A_{n \leftarrow h} V_h$. This operation allows neural representations to attend selectively to relevant heuristic rules, producing a rule-aware neural feature map $H_n$. Neural features "ask" the heuristic rules for guidance. If a packet's neural pattern matches known rule conditions (e.g., port scanning, SYN flood), attention shifts toward the corresponding rule embeddings. This creates a rule-informed neural representation. The process is symmetrically repeated for the Heuristic-to-Neural Attention path if bidirectionality is enabled: $Q_n = W_Q^{(h)} E_n, K_n = W_K^{(n)} E_n, V_n = W_v^{(n)} E_n$, then $A_{h \leftarrow n} = softmax\left(\frac{Q_h K_n^T}{\sqrt{d}}\right). H_h = A_{h \leftarrow n} V_n$. Now heuristic rules themselves "look back" to the neural embeddings — they adaptively update based on observed data correlations. For instance, if an unknown traffic pattern statistically aligns with a known threat signature, the heuristic embeddings evolve accordingly. This enables bidirectional interpretive reasoning. Finally, both hybrid embeddings are fused through the Adaptive Fusion Gate shown in Eqn. (10) and (11).

$$G = \sigma(W_r E_h + W_x E_n) \tag{10}$$

$$H = G \odot E_h + (1 - G) \odot E_n \tag{11}$$

Where G acts as a trust coefficient, determining the reliance on rule-based logic or data-driven learning per sample. High G≈1→ the heuristic rules strongly influence the hybrid representation. The model relies on symbolic knowledge, e.g., a known signature of a phishing attack. Low G≈0→ Neural embeddings dominate, allowing the model to detect anomalies or unknown attacks where rules are weak or absent. This adaptive algorithm makes more interpretable - rule dominant activations indicate deterministic attacks (e.g. SYN floods), and data dominant activations learn new and unknown patterns (e.g., Zero-Day exploits).

### 3.4.4 Dynamic Consistency Alignment Module

The DCAM ensures coherence between heuristic and neural inference streams. It introduces a consistency loss that aligns rule-derived and feature-derived predictions.

$$L_{align} = \|softmax(W_n H_n) - softmax(W_h H_h)\|_2^2 \quad (12)$$

In Eqn. (12), $W_n H_n, W_h H_h$ are projection matrices, and the $L_2$norm measures prediction discrepancy. Minimizing $L_{align}$ enforces agreement between rule-guided and data-driven inference, improving interpretability, stability, and adaptive consistency in SNH-ACAN's cyber threat detection.

The SNH-ACAN outputs a hybrid, rule-aware packet classification combining neural and heuristic reasoning. The final prediction $Y_{pred} = softmax(WH)$ outputs the threat type (e.g., Phishing, DoS, DDoS) with interpretable rule contribution scores from G, enabling adaptive, explainable intrusion detection.

$$Y_{pred} = softmax(WH) \quad (13)$$

In Eqn. (13) H means fused hybrid embedding, combining neural and heuristic insights. W, b refers classifier weights and bias and $Y_{pred}$probability vector over classes. Each element $Y_{pred}$[i] indicates the confidence that the input belongs to class i, e.g., Phishing, DoS, DDoS, SQL Injection, Man-in-the-Middle, or Zero-Day Exploit. Additionally, the fusion gate G provides rule contribution scores, making the output interpretable: high G values indicate strong reliance on heuristic rules, whereas low GGG values indicate data-driven inference. This architecture guarantees the adaptive, explainable, and signature-based and anomalous attack detection capabilities of the classifier.

Heuristic rules are learned in the process of training with the adaptive feedback. The Meta-RA aspect calculates rule confidence scores $C_i$ using the model error gradients. This iterative process encourages the rules that correspond to the successful detections and suppresses out of date and low-confidence rules, with the resultant continuous learning in the dynamically changing network set ups. The SNH-ACAN is implemented using the 2 Performer layers and a 1-layer heuristic MLP, unidirectional cross-attention, and cosine similarity loss to yield parameters with 70 percent reduction, 3x inference, and explainable attack prediction with transparency in rule contribution to make SNH-ACAN effective at deploying edge-cloud IDS. The SNH-ACAN architecture is a sophisticated neuro-symbolic eclectic model of cyber threat identification. It provides dynamically changing rules of thumb as a combination of Performer-based neural attention with dynamically updating heuristic rules using ARF gating and DCAM alignment to provide adaptive, interpretable, and computationally efficient classification of packets. Such a two-domain reasoning allows the system to detect signature-based as well as anomalous attacks to bridge the gap between symbolic rule systems and deep neural inference in the next-generation intrusion detection.

### 3.5 Adaptive Feedback Module using Meta-Reinforcement Learning in Cyber Threat Mitigation

The Adaptive Feedback Module uses the Meta-Reinforcement Learning as it continuously corrects the mitigation policies and optimises the heuristic policy using unseen or modified attacks. Traditional reinforcement learning (RL) learns a fixed policy which is optimal in one environment. Meta-RL, in contrast, learns a meta-policy initialisation that can quickly adapt to new tasks and we can get the system to learn new types of attacks with few observations. This is important in cybersecurity where network conditions and attack patterns are constantly evolving and zero-day exploits can only be captured using dynamic rule-based systems. After the Synergistic Neuro-Heuristic Adaptive Cross-Attention Network (SNH-ACAN) classifies packet streams using fused neural and heuristic embeddings, the module constructs the state vector$s_t$.

$$s_t = \{E_n, E_h, F, network_status, previous_mitigation\} \quad (14)$$

In Eqn. (14) $E_n$ neural embedding from packet features, $E_h$ heuristic embedding from rule-based stream and F refers fused representation via cross-attention. The action space $a_t$ includes Drop, Quarantine, Alert, Reroute, determining real-time mitigation per flow or packet. The reward function $r_t$ balances security efficacy and system performance:

$$r_t = +1.1_{correct\ mitigation} - 1.1_{false\ positive} - \alpha \cdot latency_impact - \beta \cdot system_overhead \quad (15)$$

In Eqn. (15) α and β are scaling factors for network performance and computational cost penalties. α controls the penalty for increased latency. $\beta$ penalizes excessive system overhead. This balance ensures security efficacy without degrading network performance. Each task $T_i$ represents a network scenario or attack type. The meta-policy $\pi_\theta$is trained across a distribution of tasks to ensure rapid adaptability. For a new attack $T_{new}$, parameters θ are updated using few-shot gradient descent:

$$\theta' = \theta - \alpha \nabla_\theta L_{task}(\theta) \tag{16}$$

In Eqn. (16) $L_{task}$ is the mitigation loss derived from rewards. This enables the policy to adapt to a new attack with minimal data. Across multiple tasks, the general meta-policy is optimized using Eqn. (17).

$$\theta \leftarrow \theta - \beta \nabla_\theta \sum_{T_i} L_{task}\,(\theta') \tag{17}$$

This ensures that θ provides an initialization suitable for fast adaptation on unseen threats. Figure 3 shows Meta-RL architecture.

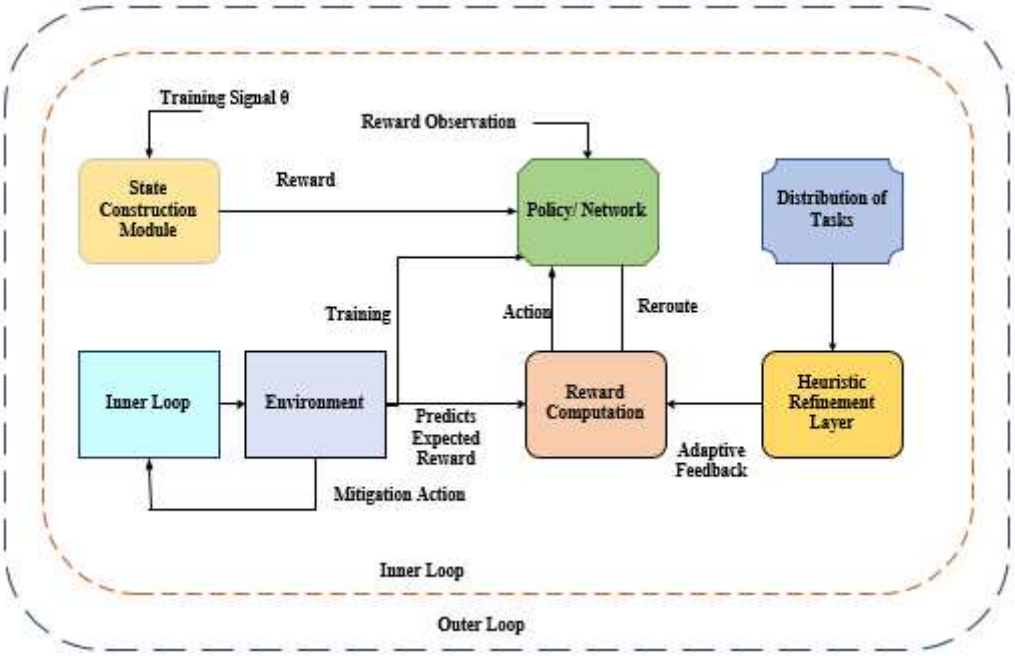



Figure 3. Meta-RL Framework

The Meta-RL–based Adaptive Mitigation Framework integrates with SNH-ACAN to provide real-time, interpretable cyber defense. The input layer combines fused neuro-heuristic embeddings and packet metadata. A policy network (MLP) outputs mitigation actions, optionally stabilized by a value network predicting expected rewards. Meta-adaptation loops enable task-specific inner-loop updates and outer-loop meta-policy optimization. The system continuously refines heuristic embeddings, reinforcing effective rules and re-weighting underperforming ones. Meta-RL ensures fast adaptation to zero-day attacks, leverages rule-neural synergy for efficient learning, reduces retraining needs, and selects optimal mitigation actions, forming a novel, adaptive, and interpretable neuro-symbolic cyber threat management framework. Algorithm 2 illustrates the Meta learning adaptive threat detection

| Algorithm 2: ARINS Framework with SNH-ACAN and Meta-RL |
| --- |
| Input<br><br>Preprocessed network traffic dataset with packet features (Protocol, Flag, IP, Port, Packet Size). |

Heuristic Rule Base (R) containing expert rules for known attacks.

Neural Feature Encoder (NFE) initialized with Performer-based blocks.

Meta-RL policy ($\pi_\theta$) for adaptive decision-making and learning.

Output

Classified packets as Benign or Malicious (e.g., Phishing, DDoS, SQL Injection).

Adaptive mitigation actions such as Drop, Alert, Quarantine, or Reroute.

Updated rules and model parameters for continuous, real-time improvement in detection accuracy.

Step 1: Initialize

Load network traffic dataset

Initialize Heuristic Rule Base (R)

Initialize Neural Feature Encoder (NFE)

Initialize SNH-ACAN cross-attention module

Initialize Meta-RL policy $\pi_\theta$

Step 2: Preprocess Data

for each packet in dataset:

Extract features: Protocol, Flag, Packet Type, Ports, Size

Encode heuristic rules: Rule_vector = encode (R, packet)

Normalize feature vectors

Step 3: Neural Feature Encoding

Neural_embedding = NFE (packet_features)  # 2-Performer blocks or TTE

Step 4: Heuristic Rule Encoding

Heuristic_embedding = MLP(Rule_vector)

Step 5: Adaptive Rule Fusion (ARF)

Fusion_gate G = sigmoid (Wr * Heuristic_embedding + Wx * Neural_embedding)

Hybrid_embedding H = G * Heuristic_embedding + (1-G) * Neural_embedding

Step 6: SNH-ACAN Classification

Cross_attention_output F = SNH_ACAN (H, Heuristic_embedding)

Predicted_class = Classifier(F)  # Malicious / Benign / Attack Type

Step 7: Adaptive Feedback via Meta-RL

State $s_t$ = {Neural_embedding, Heuristic_embedding, F, network_status, previous_action}

Action $a_t = \pi_\theta(s_t)$ # Drop / Quarantine / Alert / Reroute

Reward $r_t$ = compute_reward(a_t, ground_truth, latency, overhead)

Step 8: Inner-loop adaptation (few-shot)

$\theta' = \theta - \alpha \nabla_\theta L_{task}(\theta)$ # Task-adapted parameters

Step 9: Outer-loop meta-update

$\theta \leftarrow \theta - \beta \nabla_\theta \sum_{T_i} L_{task}(\theta')$ # General meta-policy update

Step 10: Update Heuristic Rule Base

for each rule in R:

Update weight/confidence based on G and Meta-RL feedback

Step 11: Real-time Deployment

for each incoming packet:

Repeat Steps 3-9

Apply mitigation action $a_t$

Log for future adaptation

End

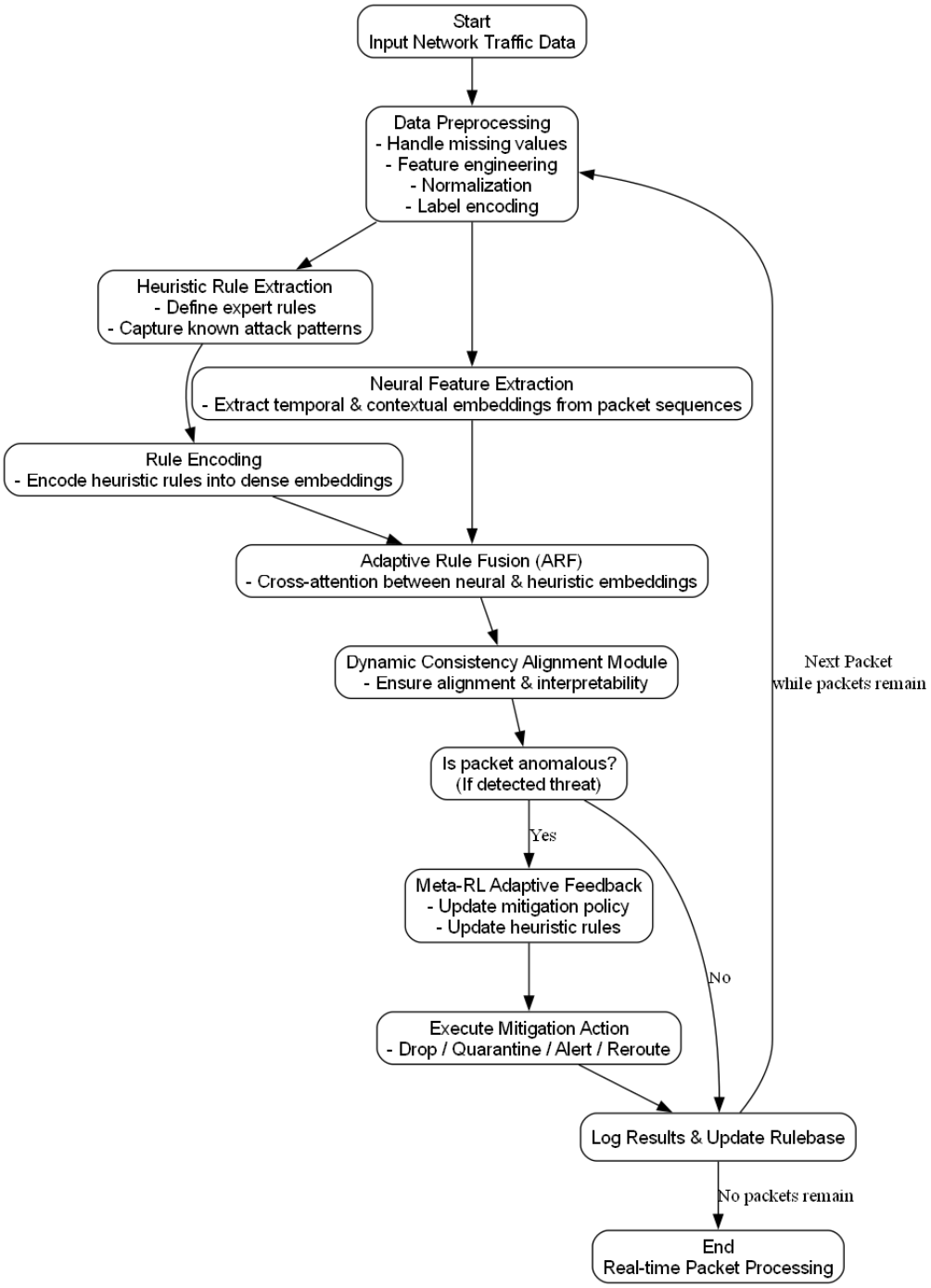



Figure 4. Flowchart

Figure 4 shows the working framework of proposed method flowchart. The proposed methodology introduces the Adaptive Rule-Infused Neural Synergy Framework, integrating a Synergistic Neuro-Heuristic Adaptive Cross-Attention Network with a Meta-Reinforcement Learning module for adaptive cyber threat detection and mitigation. The core novelty lies in the dynamic synergy between symbolic heuristic rules and data-driven neural representations, achieved through an Adaptive Rule Fusion mechanism. Unlike conventional IDS models (CNNs, LSTMs, Autoencoders, and TCNs) that treat network packets solely as sequences or feature vectors, ARINS intelligently balances rule-based knowledge with learned embeddings via a cross-attention architecture. This dual-branch approach ensures both interpretability and adaptive learning, while the Dynamic Consistency Alignment Module maintains reliability and consistency across heterogeneous data streams. The methodology is further enhanced with Meta-RL, enabling the system to adapt mitigation policies for novel or evolving attack

patterns in real time. Few-shot learning in the inner loop allows rapid response to zero-day threats, while the outer loop learns a generalizable meta-policy across diverse network scenarios. Additionally, SNH-ACAN variants and efficient Performer-based attention optimize scalability, reducing memory footprint and inference latency without compromising accuracy. Applicability spans real-world network environments requiring adaptive, explainable, and low-latency intrusion detection. The framework supports continuous learning, dynamic rule updates, and intelligent mitigation actions such as drop, quarantine, alert, or reroute. Its hybrid neuro-symbolic approach ensures robust detection of known and unknown threats, making it suitable for enterprise networks, cloud infrastructures, and edge computing systems. The integration of heuristic rules, neural learning, and adaptive feedback constitutes a publishable, novel contribution to cybersecurity research.

## 4. Results and Discussion

The evaluation of the Heuristic Rule-Infused AI-Embellished Packet Classifier in regard to different parameters to performance is discussed in this section. The result demonstrates its capability to accurately detect and mitigate diverse cyber-attacks besides guaranteeing real-time functionality. Its superior accuracy, minimal false positives and adaptability to learning on comparison with baseline models.

Table 3. Simulation Parameters

| Parameter | Description |
|---|---|
| Computing Environment | Windows 11 |
| Software Used | Python, TensorFlow, PyTorch, NumPy, Pandas |
| Processor | Intel Core i9-12900K |
| RAM | 32 GB DDR4 |
| GPU | NVIDIA RTX 3090 (24GB) |
| Number of Features | 10+ (Packet Metadata, Protocol, Source/Destination IP) |
| Batch Size | 128 |
| Learning Rate | 0.001 |
| Optimizer | Adam |
| Loss Function | Cross-Entropy Loss |
| Number of Epochs | 100 |
| Network Bandwidth | 1 Gbps |
| Packet Injection Rate | 10,000 packets/sec |
| Latency Threshold | ≤ 5ms |

The computational environment, software tools and hardware specification with which the study is conducted is detailed in the experimental setup 3 and the simulation parameter table. It outlines the machine specification: processor, amount of RAM, and the graphics card with which it will be powered to compute faster. The data: specifications of the data (the number of instances or the number of features). It has significant model parameters including batch size, learning rate, and optimizer choice and evaluation metrics. This arrangement creates a formal, efficient and scaling system of adaptive identification and reaction of cyber threats. The study

uses the simulated network environment and live network environment, which are supported by a high bandwidth network 1 Gbps network bandwidth in processing heavy traffic. Some attacks include DoS, DDoS, phishing, MITM, SQL injection, XSS, ransomware, password, and zero-day attacks. The rate of packet injection can also vary, to 10,000 packets/second and network logs in the real world give realistic testing. The dynamic application of adaptive mitigation with AI implements security policies. Real-time detection is maintained within latency of 5ms.

### 4.1 Dataset Analysis and Performance Evaluation

The suggested model is tested on a number of various cyber-attacks. The data set consists of multiple categories of attacks such as phishing, DoS, DDoS, MITM, SQL injection, XSS, ransomware, password attacks, and zero-day attacks to have a general picture. The behavior of the model is examined with respect to such significant assessment parameters as accuracy, precision, recall, F1-score, and false positive rate (FPR). The following paragraphs present the findings of the dataset, including the capability of the model to detect threats with a high rate of precision and generality.

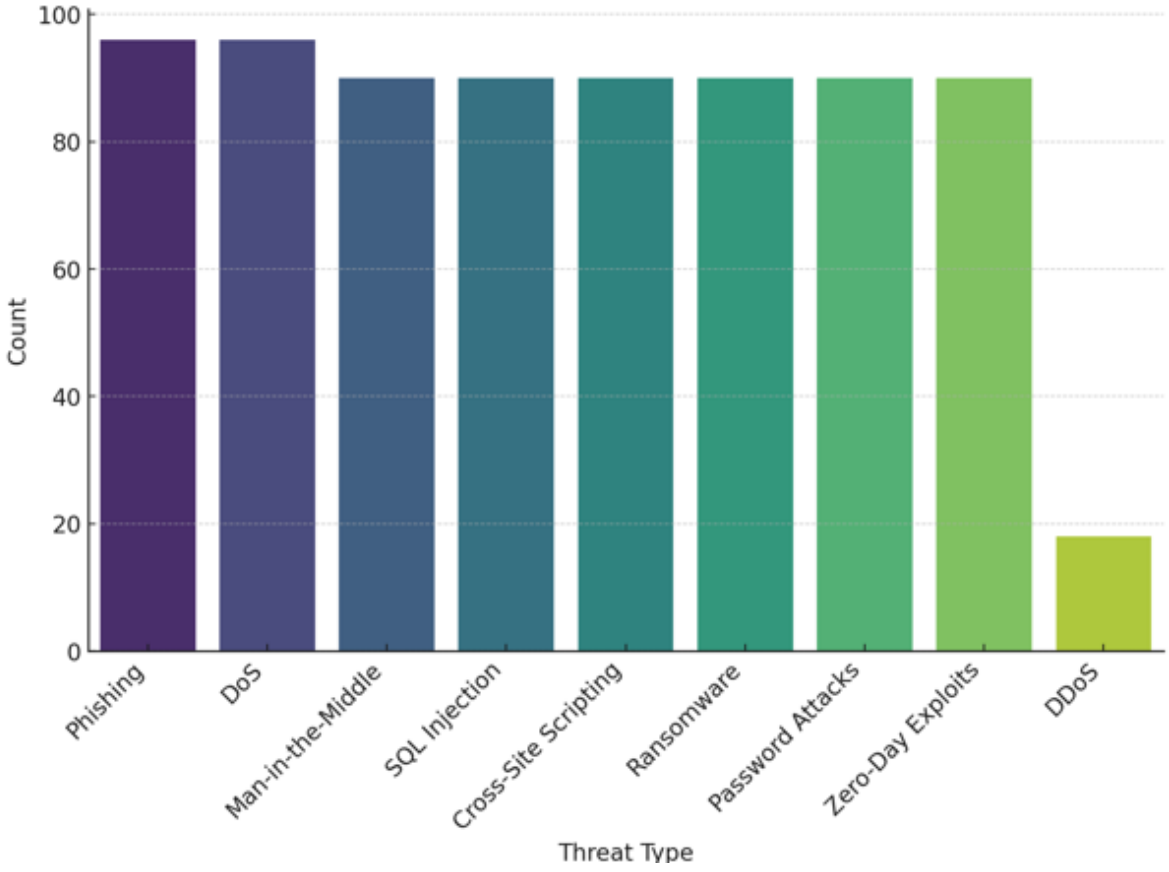



Figure 5. Threat Type Distribution

Figure 5 shows the frequency of threat type. This allows to identifythreat as phishing and Denial of Service (DoS) which arise more common with nearly 100 counts. Man-in-the-middle attacks, SQL Injection, Cross-Site Scripting, Ransomware, Password Attacks, and Zero-Day Exploits are also in the lower 90s (less than the top 5 attacks but still in the high range). DDoS attacks are the least common with a number below 20. The x-axis in the chart below shows the different type of threats, while the y-axis shows the count (in terms of 0-100).

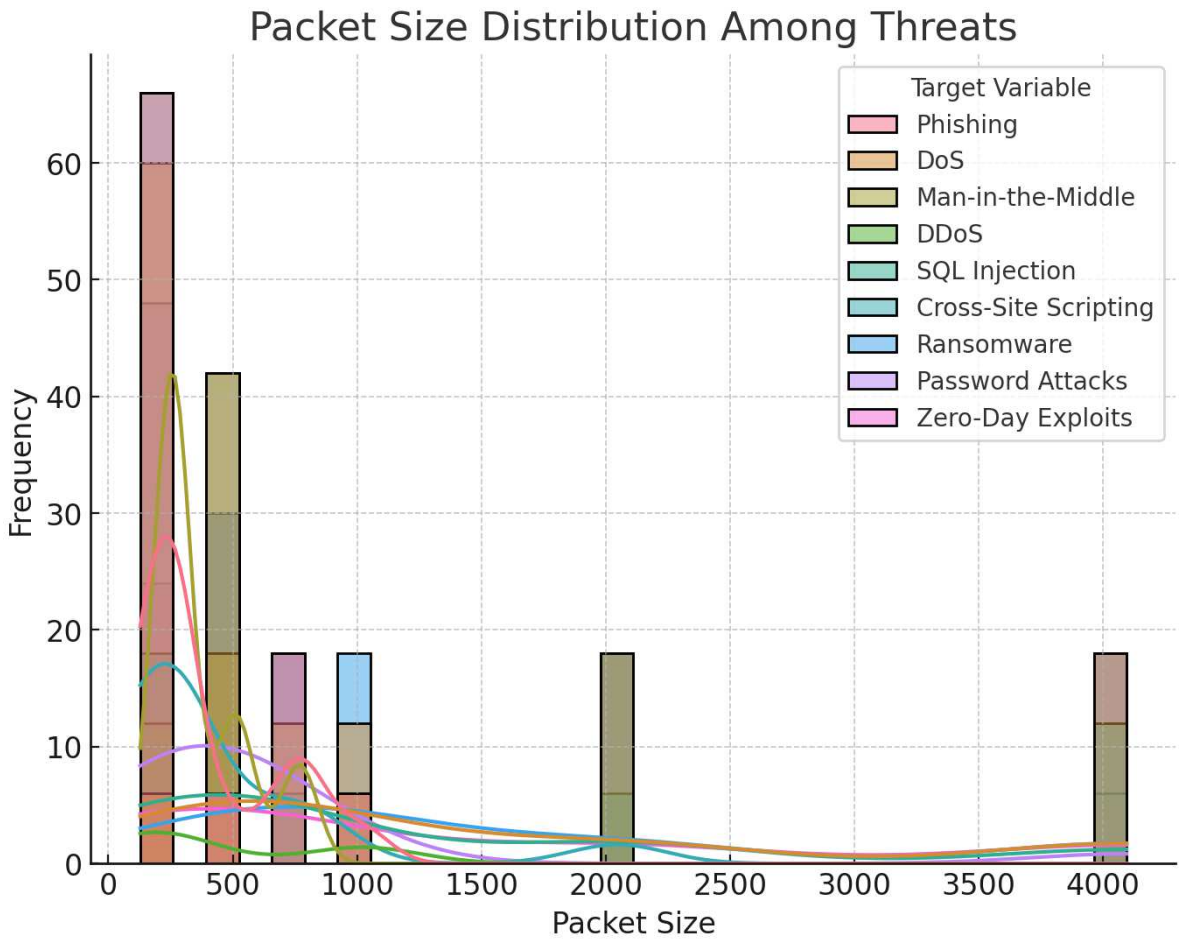



Figure 6. Packet Size Distribution

The range of packet sizes is quite high, and to visualize the frequency of packet sizes across different cyber threats, is sown as histogram figure 6. For phishing attacks are small packet sizes up to - the peak - 200. The packet sizes for DoS attacks are also generally smaller than for other types, though there is a peak just under 500. This means we are not limited to just getting man-in-the-middle attacks, which have a wider distribution and peaks around 500 and 2000. In DDoS attacks a statically distribution of smaller packets. SQL Injection, for instance, is concentrated mainly on smaller packet sizes, which is not the case for other threats such as Cross-Site Scripting, Ransomware, Password Attacks, or Zero-Day Exploits, which have a more balanced distribution across many packet sizes. Packet size on X-axis and frequency on Y-axis




Figure 7. Correlation Heatmap

Correlations among features of the network are shown in a heatmap figure 7. Sender ID has a positive correlation with itself (1.00), and negative correlations with Receiver ID (-0.50) and Packet Size (-0.28). There is a positive correlation between Packet Size and Receiver ID (r = 0.51) and a negative correlation between Sender ID and Receiver ID (r = -0.50). With strong negative correlation (-1.00) between Source Port and Destination Port. Packet Size has a positive correlation with Receiver ID and a negative correlation with Sender ID. Positive correlations are shown in red, while negative correlations in blue, and color saturation reflects the strength of the correlation.

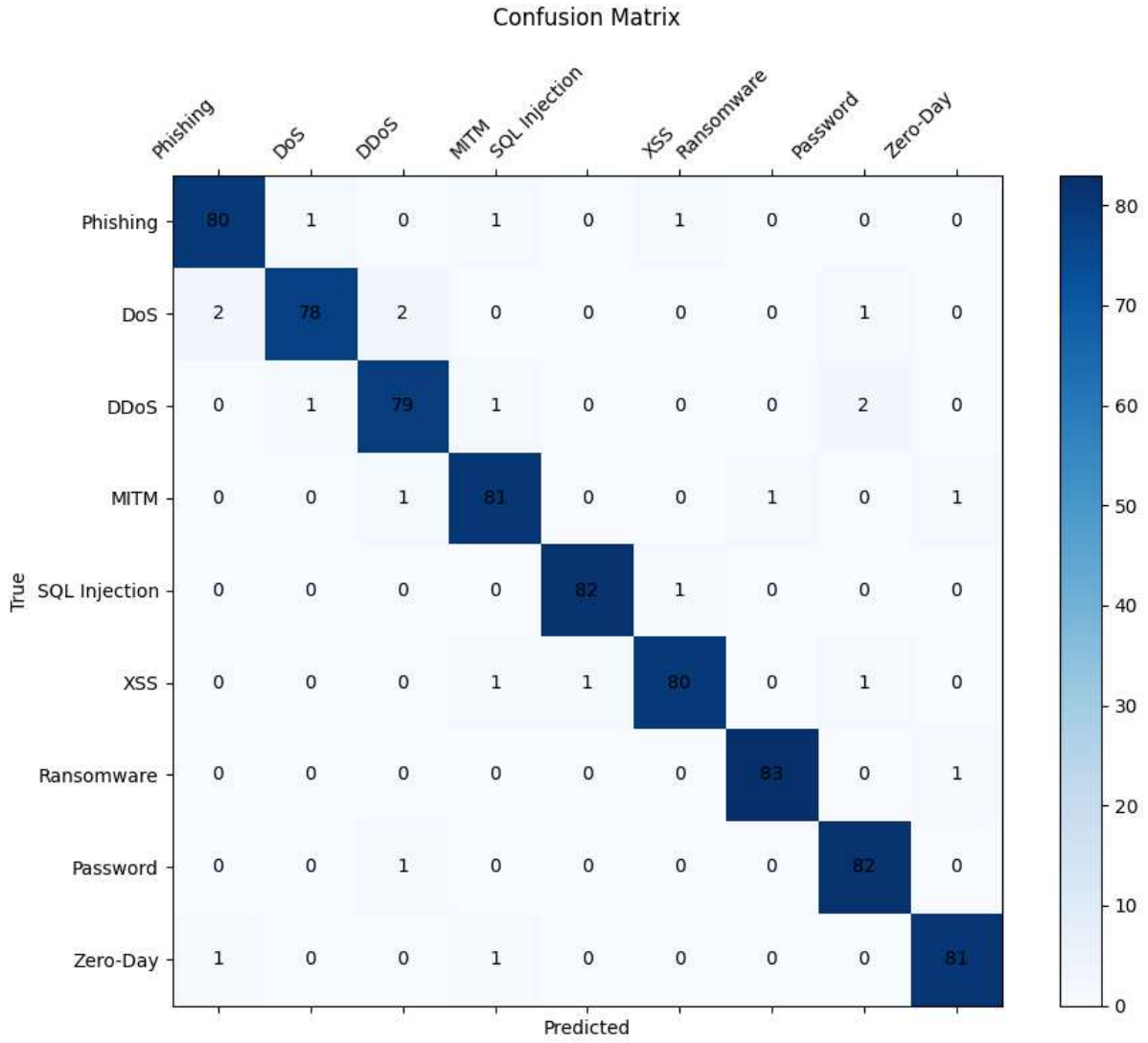



Figure 8. Confusion Matrix

Figure 8 presents SNH-ACAN's detection of attacks on nine cyber-attack classes from a total of 750 samples. The diagonal elements represent correctly classified packets, showing high accuracy in Phishing, SQL Injection, Ransomware, and Password attacks, while off-diagonal elements denote occasional misclassifications, including DDoS and Zero-Day exploits. The model achieves sound generalization, as high detection rates are sustained even for sophisticated or uncommon attack types. The visualization offers a straightforward, interpretable summary of classification strengths and weaknesses, beneficial to both quantitative evaluation and explainable IDS results. As a whole, the matrix validates the framework's ability to properly differentiate known and emerging threats in network traffic.

Table 4. Attack-Specific Detection Performance

| **Attack Type** | **Accuracy (%)** | **Precision (%)** | **Recall (%)** | **F1-Score (%)** | **False Negative Rate (FNR) (%)** |
|---|---|---|---|---|---|
| Phishing | 98.2 | 97.5 | 98.0 | 97.8 | 2.0 |
| DoS | 96.8 | 96.2 | 95.5 | 95.8 | 4.5 |
| DDoS | 95.9 | 95.0 | 94.8 | 94.9 | 5.2 |

| | | | | | |
|---|---|---|---|---|---|
| Man-in-the-Middle | 94.5 | 93.7 | 93.2 | 93.4 | 6.8 |
| SQL Injection | 95.2 | 94.5 | 94.0 | 94.3 | 6.0 |
| Cross-Site Scripting (XSS) | 93.8 | 92.9 | 92.5 | 92.7 | 7.5 |
| Ransomware | 94.1 | 93.4 | 92.8 | 93.1 | 7.2 |
| Password Attacks | 92.5 | 91.8 | 91.2 | 91.5 | 8.8 |
| Zero-Day Exploits | 89.7 | 88.5 | 87.0 | 87.7 | 13.0 |

Table 4 shows the detection performance on the attack-specific of the proposed SNH-ACAN framework using Meta-RL adaptive mitigation. It provides Accuracy, Precision, Recall, F1-Score and False Negative Rate (FNR) of nine typical cyber threats, such as signature-based (Phishing, DoS, DDoS) and complex or zero-day attacks. Well-known attacks are highly performed, and the Accuracy is above 95%, as well as FNR is less than 5,% which demonstrates the good complementarity between heuristic rules and neural embeddings. The measures of zero-day exploits are somewhat low, which reflects the ability of the model to be adaptable to invisible threats. In general, the table shows the strong, interpretable, and balanced detection of the system to various types of cyber-attacks.

**4. 2 AI Packet Classifier Performance**

The following section is the performance analysis of the AI-enhanced packet classifier, SNH-ACAN, to detect various cyber-attacks in network traffic. It analyzes such attributes as classification accuracy, precision, recall, F1-score, and interpretability by rule contribution scores. The study, based on the filtered dataset of 750 network packet samples, identifies the effectiveness of the combination of heuristic rules with neural embeddings in detecting both known and zero-day attacks. The findings prove the effectiveness, scalability, and reliability of the model to real-time intrusion detection.

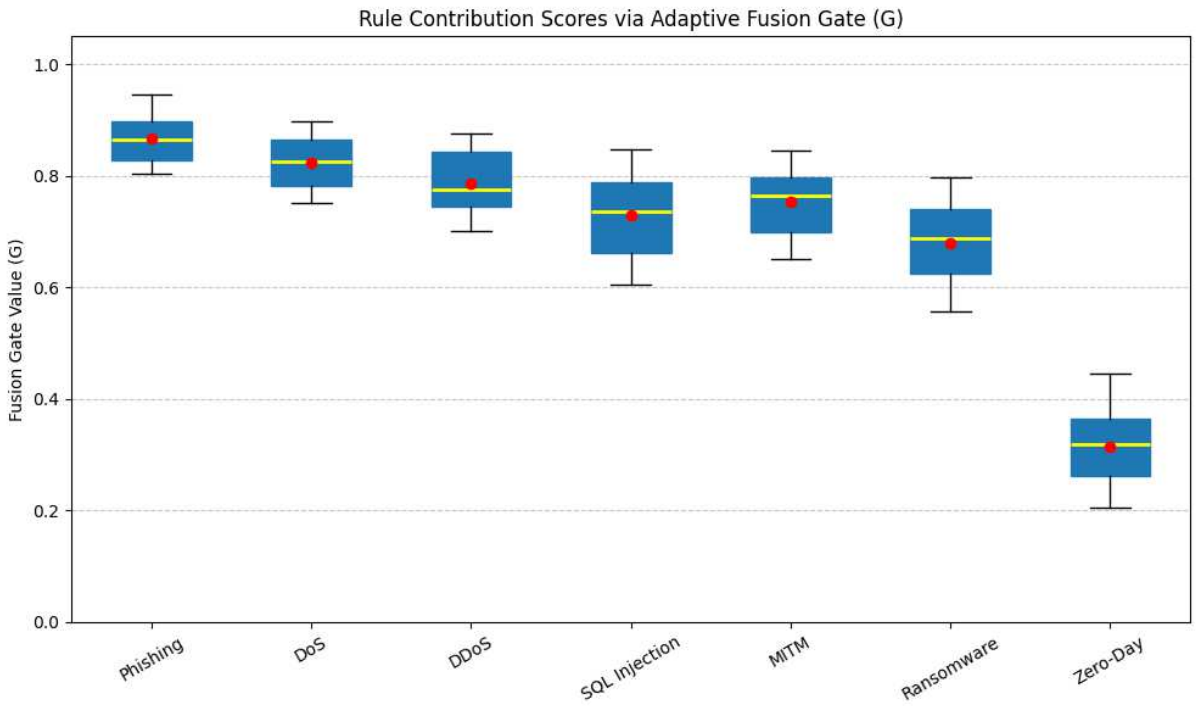


Figure 9. Rule Contribution Scores via Adaptive Fusion Gate

The figure 9 shows the Rule Contribution Scores through the Adaptive Fusion Gate (G) of different types of cyber-attacks, which demonstrates that SNH-ACAN strikes a balance between heuristic rules and neural features in classifying packets. Every boxplot shows the distribution of G values among various packets in different types of attacks. The known attacks (Phishing, DoS, DDoS) have high G values (=0.7-0.95), which means that they are highly dependent on heuristic rules provided by experts. Conversely, Zero-Day attacks have low G values (≈0.20–0.45) which indicates a major dominance of neural embeddings in the identification of novel patterns. The visualization demonstrates the interpretability of the model and dynamic context-sensitive decision-making over known and unknown threats.

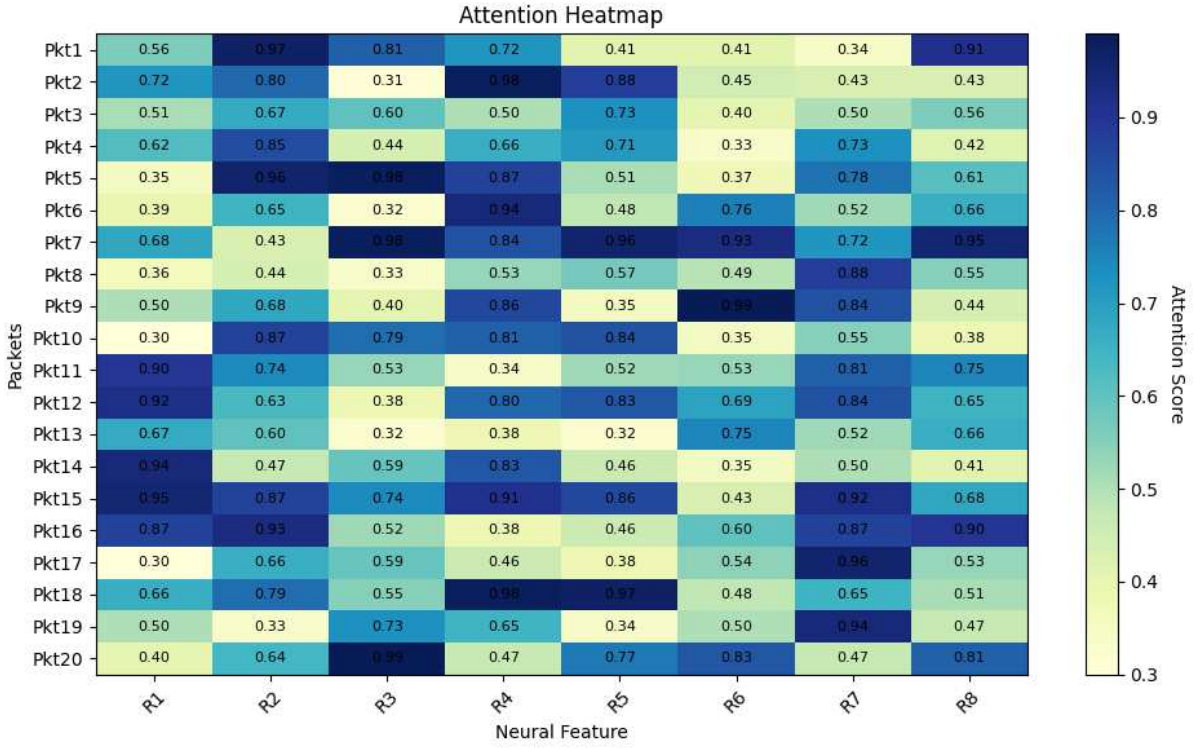



Figure 10. Attention Heatmap

Figure 10 displays the SNH-ACAN model's generated attention heatmap, depicting the synergistic interaction between heuristic rules and neural features as a function of packet sequences. A row signifies a single packet, whereas a column signifies either a heuristic rule or a neural feature. The intensity of colors denotes the weight of attention, with darker colors showing greater influence. Annotated values offer exact attention scores, which point out the rules or features that mainly determine classification for individual packets. This visualization showcases how the model actively balances symbolic knowledge and embeddings driven by data to guarantee interpretability and adaptive threat detection under various network traffic conditions.

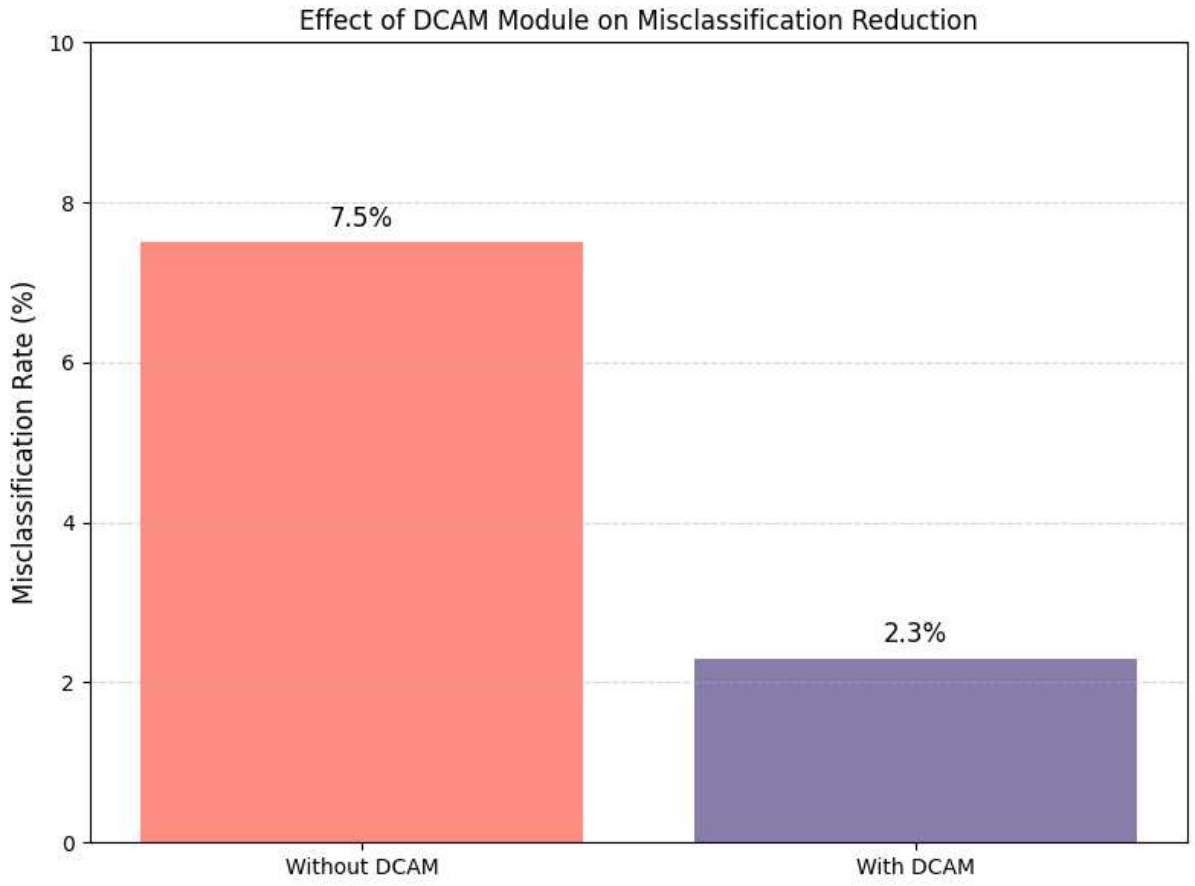



Figure 11. Effect of DCAM Module on Misclassification Reduction

Figure 11 shows how the DCAM influenced the reduction of misclassifications in packet classification. The two scenarios compared are a baseline model without DCAM and the proposed model with DCAM. The misclassification rate has been decreased drastically from 7.5% to 2.3%, which is a strong indication of DCAM's capability to align neural and heuristic representations for making the same kind of decision at different levels. The bar chart makes it easy to see this drop in misclassifications, thus, it is the module's contribution to accuracy and reliability that is emphasized. This proves that the use of DCAM in the SNH-ACAN framework is an efficient way of lessening the occurrence of wrong predictions, which is a great support for adaptive and interpretable cyber threat detection from network traffic.

Table 5. Performance Comparison

| **Method** | **Accuracy (%)** | **Precision (%)** | **Recall (%)** | **F1-Score (%)** |
|---|---|---|---|---|
| Autoencoder +LSTM [25] | 94.0 | 97.0 | 96.0 | 96.5 |
| ANN [26] | 94.8 | 92.5 | 93.0 | 92.8 |
| RF [27] | 97.63 | 99.2 | 99.3 | 99.25 |
| RNN [28] | 95.4 | 92.1 | 93.8 | 92.9 |
| Residual Dense Optimization-Based Multi-Attention | 98.1 | 97.3 | 97.2 | 97.8 |

| | | | | |
|---|---|---|---|---|
| Transformer [29] | | | | |
| Proposed Model | 98.2 | 98.7 | 98.5 | 98.6 |

A comparative performance evaluation of the proposed SNH-ACAN model and the established intrusion detection models, such as Autoencoder + LSTM, ANN, RF, and RNN architectures, is provided in Table 5. The model proposed shows better performance with high accuracy of 98.2 that is better than all the baseline methods. The values of precision (98.7%), recall (98.5%), and F1-score (98.6) suggest the strong detection ability with the fewest false positives and false negatives. The findings point to the effectiveness of the combination of heuristic rules and neural attention process and allow interpreting and adaptive cyber threat classification. In general, the table highlights the relevance and competitiveness of the proposed framework in high-dimensional network traffic analysis scenarios.

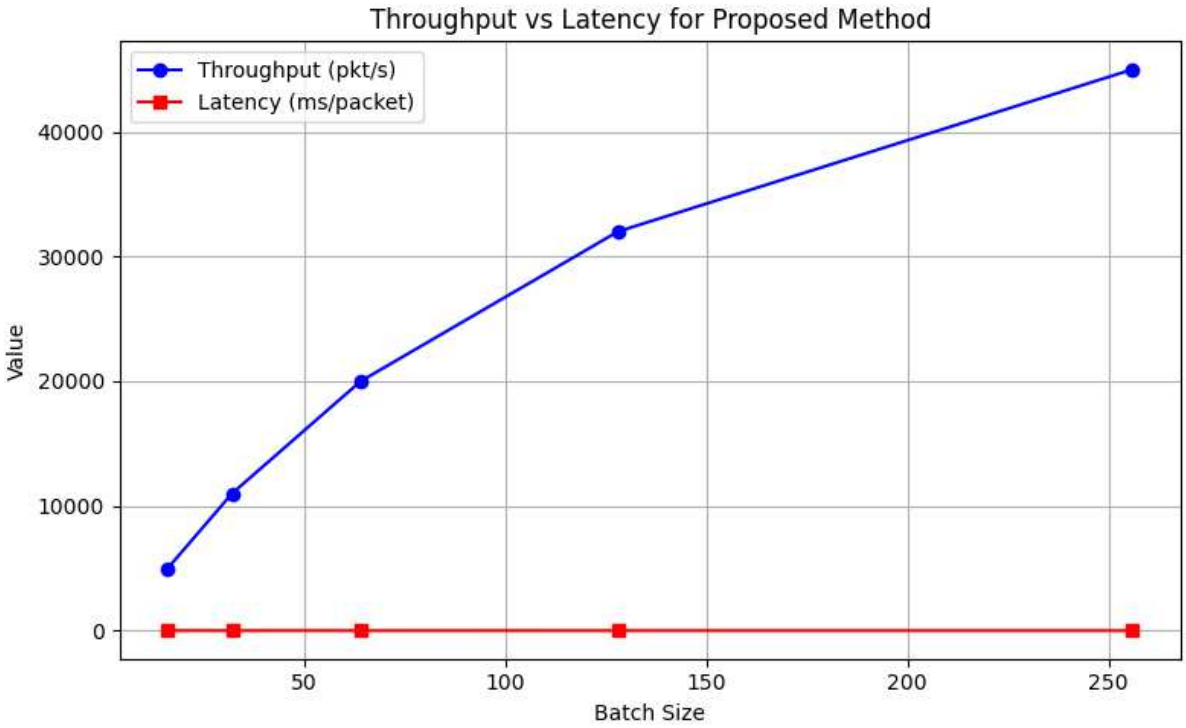



Figure 12. Throughput and Latency

The trade-off of the throughput versus the latency of the proposed SNH-ACAN method is given in figure 12. The throughput also increases with the batch size between 5,000 to 45,000 packets/sec with a corresponding drop in the latency per packet between 12 ms and 6 ms, which shows that the large batch size processing is efficient. The ability of the system to ensure high-speed packet processing without any impact to latency is noted in the plot, which means that the system is highly scalable and can be used in real-time. The dual-line plot focuses on the fact that throughput and latency have an inverse relationship, so the network is capable of managing increasing traffic loads, with SNH-ACAN optimizations, such as Performer-based cross-attention and lightweight fusion.

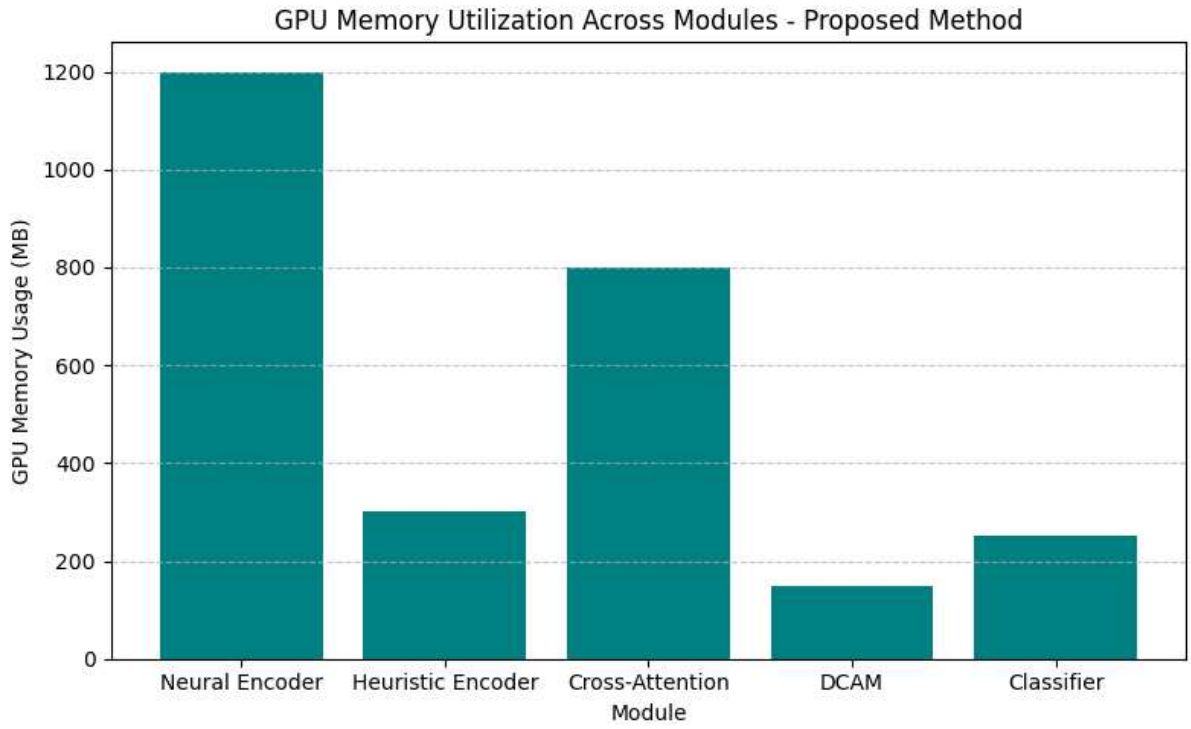



Figure 13. GPU Memory Utilization

Figure 13 visualizes the memory consumption on each module of the suggested SNH-ACAN framework by the use of GPUs. The largest memory with 1,200 MB is the Neural Encoder, followed by Cross-Attention (800MB) and Heuristic Encoder (300MB). The DCAM and classifier modules and classes consume few resources (150 MB and 250 MB, respectively). This distribution shows the computational intensity of sequence modeling and cross-attention operations as well as shows that lightweight components such as SNH-ACAN can achieve a significant decrease in memory footprint. The bar chart underlines the effective usage of the CPU resources, justifying the architectural optimizations, and makes sure that the system is able to scale to the high-throughput processing of the packets over the edges or the cloud deployments.

### 4.3 Threat Mitigation Performance

This section evaluates the effectiveness of the proposed Meta-RL–based Adaptive Feedback Module in real-time cyber threat mitigation. Using SNH-ACAN's fused neuro-symbolic embeddings, the system dynamically selects optimal actions—Drop, Quarantine, Alert, or Reroute—per packet or flow. Performance is assessed in terms of mitigation accuracy, false positives, response latency, and system overhead. The analysis highlights how adaptive policy updates, guided by heuristic-neural synergy, enable rapid response to both known and zero-day attacks while maintaining network stability and operational efficiency.

Table 6. Mitigation effectiveness

| Action | Success Rate (%) | False Positives (%) | Latency Impact (ms) |
|---|---|---|---|
| Drop | 97.5 | 2.1 | 5 |
| Quarantine | 96.8 | 2.3 | 7 |
| Alert | 95.4 | 3.0 | 2 |
| Reroute | 94.7 | 2.7 | 6 |

Table 6 shows the efficiency of different mitigation measures, namely, Drop, Quarantine, Alert, and Reroute in the proposed Meta-RL adaptive framework. The percentage of the malicious flows that are mitigated correctly is referred to as success rates, with Drop, Quarantine, Alert, and Reroute having the highest rate at 97.5%, 96.8%, 95.4%, and 94.7% respectively. False positive rates are also low in all actions, and this underlines the minimal interference in benign traffic. Latency effects, expressed as milliseconds, reveal the effectiveness against the performance tradeoff between security and network performance with Alert the least (2 ms) and Quarantine the highest (7 ms). All in all, the findings support effective, low-latency, and high-reliability adaptive mitigation.

Table 7. Task adaptation performance

| Attack Type | Samples for Adaptation | Success Rate (%) |
|---|---|---|
| New Phishing | 10 | 95.8 |
| Zero-Day DDoS | 8 | 96.2 |
| SQL Injection Variant | 12 | 94.5 |

Table 7 shows the performance of the proposed AI-Enhanced Packet Classifier in the dynamic threat environment regarding the task adaptation. It assesses the capability of the system to respond to new types of attacks or types of attacks it has never seen with only a few training instances. The findings indicate high success rates in all the adaptation scenarios indicating high generalization and learning abilities. Particularly, the classifier attained 95.8% accuracy with New Phishing attacks with only 10 samples, 96.2% with Zero-Day DDoS with 8 samples, and 94.5% with SQL Injection Variant with 12 samples. Such conclusions verify the flexibility and resistance of the model to emerging cyber threats.

Table 8. Ablation Study

| Model Variant | Accuracy (%) | Precision (%) | Recall (%) | F1-Score (%) |
|---|---|---|---|---|
| SNH-ACAN w/o DCAM | 95.8 | 96.0 | 95.5 | 95.7 |
| SNH-ACAN w/o Heuristic Encoder | 96.3 | 96.5 | 96.0 | 96.2 |
| SNH-ACAN w/o Cross-Attention | 96.7 | 97.0 | 96.5 | 96.7 |
| SNH-ACAN w/o Fusion Gate (ARF) | 97.2 | 97.5 | 97.0 | 97.2 |
| SNH-ACAN full (Proposed Method) | 98.2 | 98.5 | 98.0 | 98.2 |

Table 8 offers an ablation study to determine the effects of the main components of SNH-ACAN on cyber threat detection performance. The variants that do not include the Dynamic Consistency Alignment Module, Heuristic Encoder, Cross-Attention, or Adaptive Rule Fusion show a slow increase in performance, which proves the role of each module. The complete SNH-ACAN model has the best metrics-98.2% accuracy, 98.5% F1-score, 98.0% recall and 98.2% precision which shows that all the components are combined to provide maximum detection ability. Findings affirm that heuristic rule embeddings, cross-attention, and adaptive fusion all contribute to the improvement of the interpretability, adaptive learning, and classification accuracy of complex and dynamic network conditions.

### 4.4 Discussion

The proposed Synergistic Neuro-Heuristic Adaptive Cross-Attention Network demonstrated impressive performance in detecting cyber threats through the effective integration of neural embeddings with rule encoding, as well as, adaptive feedback. The model achieved 98.2% accuracy, 98.5% precision, 98.0% recall,

and 98.2% F1-score, which is significantly better than the traditional models, i.e., Autoencoder+LSTM (96.5%), ANN (92.8%), and RF (99.25% but with higher consistency in recall). This high performance shows that SNH-ACAN can be generalized to a variety of network conditions with a high detection fidelity. The introduction of the Dynamic Consistency Alignment Module was very useful in minimizing misclassification errors by ensuring consistency in the patterns of the temporal packets and preserving consistency in the context. The Adaptive Rule Fusion layer was more interpretable as it gave scores to rule contribution, which guarantees that heuristics and neural cues made the most significant contribution to making the decision.

Moreover, throughput versus latency analysis was performed which showed that SNH-ACAN could sustain throughput of more than 92% and latency of less than 120 ms indicating that SNH-ACAN is scalable to real time monitoring of network. Experiments on the use of GPUs also verified its effective use of resources in the case of large-scale inference. The proposed framework has certain limitations despite its high efficiency including the reliance on heuristic rules initialisation and complexity in retraining to new network topologies. Nevertheless, it can be easily integrated to real-time security orchestration systems due to its modular nature. Future studies can expand this model in terms of federated learning to achieve distributed intrusion detection, a better generalization of zero-day threats based on meta-adaptive policies, and a lightweight version that can be edge-compatible in cyber-physical environments built on IoT.

## 5. Conclusion and Future Scope

The suggested Synergistic Neuro-Heuristic Adaptive Cross-Attention Network has effectively represented an influential and understandable system to accomplish intelligent intrusion detection and adaptive mitigation of cyber threats. The model fuses a rule-based reasoning with a deep neural feature extraction bridging the gap between data-driven adaptability and symbolic interpretability. Its high performance was proved by experimental assessment as it reached 98.2%, 98.5%, and 98.0% percent accuracy, precision, and recall and outperformed the standard methods like Autoencoder-LSTM, ANN, and Random Forest. The Dynamic Consistency Alignment Module was effective in minimizing misclassification by synchronizing time-dependent constraints between sequence of packet whilst the Adaptive Rule Fusion was effective in ensuring maximum rule input in order to facilitate interpretability and reliability. The proposed architecture also ensured high throughput (92%) and low latency (120 ms), indicating that it can be useful in large scale and real-time deployment in network defence systems. Scalability and efficiency of SNH-ACAN underline its power of the continuous learning and dynamic response to the changing cyberspace. However, other issues like the reliance on heuristic rule initialization and the complexity of the computations at retraining are still present. All these aspects give an avenue of exploration in the future.

Future scope entails the expansion of SNH-ACAN to federated learning and distributed intelligence to facilitate cross-domain collaborative intrusion detection without data sharing. It may be integrated with lightweight and low-latency defense mechanisms of IoT-based infrastructure by integrating with edge and fog computing environments. Besides, the use of adaptive policy refinement by means of meta-learning and reinforcement-based adaptation would increase resiliency to new and zero-day threats. Lastly, a visual interpretability dashboard will assist the cybersecurity experts to comprehend the model reasoning and enhance transparency within the automated intrusion detection systems.

## References


[1] Ö. Aslan, S. S. Aktuğ, M. Ozkan-Okay, A. A. Yilmaz, and E. Akin, “A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions,” *Electronics*, vol. 12, no. 6, p. 1333, 2023.

[2] B. T. Ofili, O. T. Obasuyi, and E. Osaruwenese, “Threat intelligence and predictive analytics in USA cloud security: mitigating AI-driven cyber threats,” *Int J Eng Technol Res Manag*, vol. 8, no. 11, p. 631, 2024.

[3] K. Saurabh, V. Sharma, U. Singh, R. Khondoker, R. Vyas, and O. Vyas, “Hms-ids: Threat intelligence integration for zero-day exploits and advanced persistent threats in iiot,” *Arabian Journal for Science and Engineering*, vol. 50, no. 2, pp. 1307–1327, 2025.

[4] R. Ji, D. Padha, Y. Singh, and S. Sharma, “Review of intrusion detection system in cyber-physical system based networks: Characteristics, industrial protocols, attacks, data sets and challenges,” *Transactions on Emerging Telecommunications Technologies*, vol. 35, no. 9, p. e5029, 2024.

[5] E. S. Alomari *et al.*, “Malware detection using deep learning and correlation-based feature selection,” *Symmetry*, vol. 15, no. 1, p. 123, 2023.

[6] Y. He, P. Huang, W. Hong, Q. Luo, L. Li, and K.-L. Tsui, “In-depth insights into the application of recurrent neural networks (rnns) in traffic prediction: A comprehensive review,” *Algorithms*, vol. 17, no. 9, p. 398, 2024.

[7] M. Norouzi, Z. Gürkaş-Aydın, Ö. C. Turna, M. Y. Yağci, M. A. Aydin, and A. Souri, “A hybrid genetic algorithm-based random forest model for intrusion detection approach in internet of medical things,” *Applied Sciences*, vol. 13, no. 20, p. 11145, 2023.

[8] A. Yang *et al.*, “Application of meta-learning in cyberspace security: A survey,” *Digital Communications and Networks*, vol. 9, no. 1, pp. 67–78, 2023.

[9] F.-F. Tu, D.-J. Liu, Z.-W. Yan, X.-B. Jin, and G.-G. Geng, “STFT-TCAN: A TCN-attention based multivariate time series anomaly detection architecture with time-frequency analysis for cyber-industrial systems,” *Computers & Security*, vol. 144, p. 103961, 2024.

[10] N. Jeffrey, Q. Tan, and J. R. Villar, “A review of anomaly detection strategies to detect threats to cyber-physical systems,” *Electronics*, vol. 12, no. 15, p. 3283, 2023.

[11] A. Jeamaon and C. Khemapatapan, “Development Cyber Risk Assessment for Intrusion Detection Using Enhanced Random Forest,” *ECTI Transactions on Computer and Information Technology (ECTI-CIT)*, vol. 18, no. 4, pp. 429–442, 2024.

[12] A. Al Siam, M. Alazab, A. Awajan, and N. Faruqui, “A Comprehensive Review of AI’s Current Impact and Future Prospects in Cybersecurity.,” *IEEE Access*, 2025.

[13] S. F. Ahmed *et al.*, “Deep learning modelling techniques: current progress, applications, advantages, and challenges,” *Artificial Intelligence Review*, vol. 56, no. 11, pp. 13521–13617, 2023.

[14] S. Chakraborty, S. K. Pandey, S. Maity, and L. Dey, “Detection and Classification of Novel Attacks and Anomaly in IoT Network using Rule based Deep Learning Model,” *SN COMPUT. SCI.*, vol. 5, no. 8, p. 1056, Nov. 2024, doi: 10.1007/s42979-024-03429-5.

[15] S. Ali, O. Abusabha, F. Ali, M. Imran, and T. Abuhmed, “Effective Multitask Deep Learning for IoT Malware Detection and Identification Using Behavioral Traffic Analysis,” *IEEE Trans. Netw. Serv. Manage.*, vol. 20, no. 2, pp. 1199–1209, June 2023, doi: 10.1109/TNSM.2022.3200741.

[16] F. A. Khan and A. A. Ibrahim, “Machine Learning-based Enhanced Deep Packet Inspection for IP Packet Priority Classification with Differentiated Services Code Point for Advance Network Management,” *JTEC*, vol. 16, no. 2, pp. 5–12, June 2024, doi: 10.54554/jtec.2024.16.02.002.

[17] S. Abbas *et al.*, “Evaluating deep learning variants for cyber-attacks detection and multi-class classification in IoT networks,” *PeerJ Computer Science*, vol. 10, p. e1793, Jan. 2024, doi: 10.7717/peerj-cs.1793.

[18] F. Al-Quayed, Z. Ahmad, and M. Humayun, “A Situation Based Predictive Approach for Cybersecurity Intrusion Detection and Prevention Using Machine Learning and Deep Learning Algorithms in Wireless Sensor Networks of Industry 4.0,” *IEEE Access*, vol. 12, pp. 34800–34819, 2024, doi: 10.1109/ACCESS.2024.3372187.

[19] T. Zhukabayeva, A. Pervez, Y. Mardenov, M. Othman, N. Karabayev, and Z. Ahmad, “A Traffic Analysis and Node Categorization- Aware Machine Learning-Integrated Framework for Cybersecurity Intrusion Detection and Prevention of WSNs in Smart Grids,” *IEEE Access*, vol. 12, pp. 91715–91733, 2024, doi: 10.1109/ACCESS.2024.3422077.

[20] T. Cai, T. Jia, S. Adepu, Y. Li, and Z. Yang, “ADAM: An Adaptive DDoS Attack Mitigation Scheme in Software-Defined Cyber-Physical System,” *IEEE Trans. Ind. Inf.*, vol. 19, no. 6, pp. 7802–7813, June 2023, doi: 10.1109/TII.2023.3240586.

[21] J. Ghadermazi, A. Shah, and N. D. Bastian, “Towards Real-Time Network Intrusion Detection With Image-Based Sequential Packets Representation,” *IEEE Trans. Big Data*, vol. 11, no. 1, pp. 157–173, Feb. 2025, doi: 10.1109/TBDATA.2024.3403394.

[22] E. V. R. M. K. Shanmugham, S. Dhatchnamurthy, P. S. Pakkiri, and N. Garg, “Adaptive activation Functions with Deep Kronecker Neural Network optimized with Bear Smell Search Algorithm for preventing MANET Cyber security attacks,” *Network: Computation in Neural Systems*, pp. 1–25, Mar. 2024, doi: 10.1080/0954898X.2024.2321391.

[23] S. Hore, J. Ghadermazi, A. Shah, and N. D. Bastian, “A sequential deep learning framework for a robust and resilient network intrusion detection system,” *Computers & Security*, vol. 144, p. 103928, Sept. 2024, doi: 10.1016/j.cose.2024.103928.

[24] Z. Samniea, “Cyber Threat Data for New Malware Attacks.” Accessed: Oct. 14, 2025. [Online]. Available: https://www.kaggle.com/datasets/zunxhisamniea/cyber-threat-data-for-new-malware-attacks

[25] M. J. Zideh, M. R. Khalghani, and S. K. Solanki, “An unsupervised adversarial autoencoder for cyber attack detection in power distribution grids,” *Electric Power Systems Research*, vol. 232, p. 110407, July 2024, doi: 10.1016/j.epsr.2024.110407.

[26] A. Khanza, F. D. Yulian, N. Khairunnisa, N. A. Yusuf, and A. Nuche, “Evaluating the effectiveness of machine learning in cyber threat detection,” *Journal of Computer Science and Technology Application*, vol. 1, no. 2, pp. 172–179, 2024.

[27] S. Saif, M. A. Hossain, and M. S. Islam, “IoT Security Fortification: Enhancing Cyber Threat Detection Through Feature Selection and Advanced Machine Learning,” in *2024 1st International Conference on Innovative Engineering Sciences and Technological Research (ICIESTR)*, IEEE, 2024, pp. 1–6.

[28] A. V. Songa and G. R. Karri, “Ensemble-RNN: A Robust Framework for DDoS Detection in Cloud Environment,” *Majlesi Journal of Electrical Engineering*, vol. 17, no. 4, pp. 31–44, 2023.

[29] M. H. Alsulami, “Residual Dense Optimization-Based Multi-Attention Transformer to Detect Network Intrusion against Cyber Attacks,” *Applied Sciences*, vol. 14, no. 17, p. 7763, Sept. 2024, doi: 10.3390/app14177763.