International Journal of Computer Information Systems and Industrial Management Applications
ISSN 2150-7988 Volume 18(13s) 2026 pp. 205-228
https://doi.org/10.70917/ijcisim-2026-4092
Article

ANSCDF-ETI: An Adaptive Neuro-Symbolic Cyber Defense Framework with Explainable Temporal Intelligence for Intelligent Intrusion Detection in Software-Defined Networks

Karthi S[1], Anuja Beula J[2], Ayyapan S[3], DanielRaj K[4]*, V. Gokila[5], Sathishkumar T[6]

[1] Department of Information Technology, St. Joseph's College of Engineering, Chennai, Tamil Nadu, India.
[2] Department of CSE (AI & ML), Kalaignarkarunanidhi Institute of Technology, Coimbatore, Tamil Nadu, India.
[3] Department of Physics, Government College of Engineering, Salem 636011, Tamil Nadu, India.
[4] Department of Computer Science and Engineering, Dr. G.U. Pope College of Engineering, Thoothukudi, Tamil Nadu, India.
[5] Assistant Professor, Department of Physics, Rathinam Technical Campus, Coimbatore, Tamil Nadu, India.
[6] Department of Robotics and Automation, Erode Sengunthar Engineering College, Erode, Tamil Nadu, India.
*Corresponding author: DanielRaj K

Abstract: – Software-Defined Networks (SDNS) are for flexible, centralized network management, programmability and dynamic resource discovery and allocation, facilitating the enabling of future communication infrastructures. Nevertheless, the inherent architecture design of SDNs is susceptible to a set of security issues such as the DDoS attack, the compromise of the control-plane and flow tables, reconnaissance and zero-day attacks. Traditional intrusion detection systems results in time constraints due to a low level of adaptiveness, lower learning ability of temporal features, interpretability problems and high false alarm rates.In order to overcome the deficiencies, this paper presents ANSCDF-ETI- an Adaptive Neuro-Symbolic Cyber Defense Framework with Explainable Temporal Intelligence for autonomous cyber security management in SDN. The framework leverages the Hybrid Temporal Intelligence by CNN, BiLSTM and multi-head attention to learn high-complexity spatiotemporal attack patterns, and combines the deep learning predictions with cyber security policy in the Neuro-Symbolic Reasoning Engine to achieve more robust attack detection process. Besides, an Explainable Artificial Intelligence (XAI) module is built to explore the transparent explaination for the cyber security policy with feature attribution and symbolic reasoning, and on-policy adaptation mechanism is adopted to iteratively optimize the security policy based on the detection results and operating feedbacks.The framework was tested and validated over the benchmark datasets: CICIDS2017, CSE-CIC-IDS2018, NSL-KDD and UNSW-NB15. The experimental results show the malicious attack detection accuracy of 98.70% with precision, recall and F1-score of 98.65%, 98.68% and 98.66%, respectively, and ROC-AUC of 0.994 rate while the false positive rate was shown with 0.42% and average detection latency of 12.45 ms. The comparative performance demonstrated the effectiveness of the ANSCDF-ETI framework over traditional machine learning and deep learning models in terms of intrusion detection accuracy, interpretability and adaptability.

Keywords: Software-Defined Networking, Intrusion Detection System, Neuro-Symbolic Artificial Intelligence, Explainable Artificial Intelligence, Temporal Intelligence, Deep Learning, Cybersecurity, Network Security.

1. INTRODUCTION

Software-Defined Networking (SDN) is a modern networking paradigm that separates the control plane from the data plane, enabling centralized control, programmability, and dynamic network management [1]. Unlike conventional networks, SDN employs a logically centralized controller to manage routing, traffic engineering, and network policies, resulting in improved scalability, simplified management, rapid service deployment, and flexible resource allocation. These capabilities have made SDN a fundamental technology for cloud computing, Internet of Things (IoT), edge computing, Network Function Virtualization (NFV), software-defined data centers, and emerging 5G/6G communication systems [1]–[3].Despite these advantages, the centralized architecture of SDN significantly

expands the cyberattack surface, making controllers, communication channels, and programmable interfaces attractive targets for sophisticated cyber threats. Attacks such as Distributed Denial-of-Service (DDoS), flow-table overflow, spoofing, reconnaissance, malware propagation, insider attacks, Advanced Persistent Threats (APTs), and zero-day exploits can severely compromise network availability, confidentiality, and integrity [4]–[6]. Consequently, developing intelligent and resilient security mechanisms has become a major research priority for next-generation SDN environments.

Intrusion Detection Systems (IDSs) play a vital role in protecting SDN infrastructures. Traditional signature-based and statistical IDSs effectively identify known attacks but struggle to detect previously unseen threats, adapt to evolving attack strategies, and cope with the growing complexity of encrypted traffic, heterogeneous applications, and large-scale IoT networks [7], [8]. Recent advances in Artificial Intelligence (AI) have significantly improved intrusion detection through machine learning algorithms such as Decision Trees, Support Vector Machines (SVM), Random Forests, Naïve Bayes, and XGBoost, as well as deep learning models including Convolutional Neural Networks (CNNs), Long Short-Term Memory (LSTM) networks, Gated Recurrent Units (GRUs), and Transformer architectures, which automatically learn complex spatial and temporal representations from network traffic [9]–[13].Although these AI models achieve high detection accuracy, most operate as black-box systems, providing limited insight into the reasoning behind their predictions and reducing analyst trust, forensic efficiency, and regulatory compliance in security-critical applications [12], [14], [15]. Explainable Artificial Intelligence (XAI) addresses this challenge by employing techniques such as SHAP, LIME, Integrated Gradients, feature attribution, and attention visualization to generate transparent and interpretable intrusion detection decisions [16], [17]. Similarly, neuro-symbolic Artificial Intelligence combines deep neural learning with symbolic reasoning, cybersecurity knowledge, and logical inference to enhance decision reliability and improve robustness against previously unseen attacks [18], [19]. Furthermore, temporal intelligence models based on LSTMs, Transformers, and attention mechanisms capture sequential attack behaviors, enabling early detection of multi-stage cyberattacks, while adaptive learning continuously updates detection policies to counter evolving threats and changing attack strategies [20]–[23].

However, existing SDN intrusion detection systems rarely integrate explainable AI, neuro-symbolic reasoning, temporal intelligence, and adaptive policy optimization into a single unified framework. Most approaches focus on improving detection accuracy while overlooking transparency, logical reasoning, continual learning, and adaptive decision-making. To address these limitations, this paper proposes an Adaptive Neuro-Symbolic Cyber Defense Framework Using Explainable Temporal Intelligence (ANSCDF-ETI) for intelligent intrusion detection in Software-Defined Networks. The proposed framework integrates a hybrid LSTM–Transformer temporal learning model, a neuro-symbolic reasoning engine combining deep feature learning with expert cybersecurity knowledge, an XAI module employing SHAP, LIME, attention visualization, and symbolic rule extraction, and an adaptive policy optimization module that dynamically updates detection and mitigation strategies in response to emerging cyber threats. Experimental evaluation on benchmark intrusion detection datasets demonstrates that the proposed framework achieves superior detection accuracy, lower false-positive rates, enhanced interpretability, stronger adaptability, and improved computational efficiency for real-time SDN deployment scenarios.

1.1 Problem Statement

Software-Defined Networking (SDN) has become a fundamental architecture for cloud computing, IoT, edge computing, industrial automation, and next-generation communication because of its centralized control, programmability, and flexible resource management. However, its centralized architecture significantly increases the attack surface, making SDN controllers and communication channels vulnerable to sophisticated cyberattacks such as DDoS, APTs, flow-table overflow, spoofing, reconnaissance, insider attacks, and zero-day exploits, thereby threatening network availability, confidentiality, and integrity [24]–[27].

AI-based Intrusion Detection Systems (IDSs) have improved attack detection through machine learning and deep learning. However, most existing approaches function as black-box models, limiting interpretability, reducing analyst trust, and complicating forensic investigations. Additionally, they analyze network flows independently, failing to capture the temporal characteristics of multi-stage attacks, which weakens early attack detection [30], [31].

Although Explainable Artificial Intelligence (XAI) improves model transparency, current explainable IDSs lack logical reasoning based on expert knowledge and struggle to identify unseen attack behaviors. Neuro-symbolic AI has emerged as a promising solution [32], [33], yet its integration with temporal intelligence and adaptive cyber defense for SDNs remains limited. Furthermore, most IDSs rely on static detection policies, causing performance degradation as attack patterns evolve, due to the absence of adaptive learning mechanisms [34], [35].

To address these challenges, this paper proposes an **Adaptive Neuro-symbolic Cyber Defense Framework Using Explainable Temporal Intelligence (ANSCDF-ETI)** for SDNs. The framework integrates hybrid temporal deep learning, neuro-symbolic reasoning, explainable AI, and adaptive policy optimization to improve intrusion detection accuracy, reduce false alarms, enhance decision transparency, and provide resilient cyber defense.

1.2 Motivation

The rapid adoption and proliferation of SDN in cloud computing, Internet of Things (IoT), edge cloud, 5G/6G infrastructure has made the requirement of intelligent and autonomous cyber defense mechanisms to detect advanced, evolving, and stealthy attacks at the earliest possible stage of attack lifecycle. In no circumstance, they have to accurately intercept these attacks timely, understood easily, keep specialized knowledge up to date, and quickly and broadly respond. However, existing intrusion detection systems have limited interpretability, not adapt to constantly introduced new attacks, and poor modeling attack sequences. This inspires us to advocate an adaptive, interpretable and knowledge-driven cyber defense system with temporal intelligence, neuro-symbolic reasoning, and continual policy optimization.

1.3 Research Objectives

The objectives of this research are as follows:

- To propose an adaptive intrusion detection framework for software-defined network.
- To demonstrate sequential attack behaviors using the hybrid LSTM–Transformer module of temporal intelligence.
- To bring in neuro-symbolic reasoning so that the detection of cyberattack can be accurate and reliable.
- In order to facilitate explainable security decisions with XAI techniques.
- To enable the application of adaptive policy optimization in the continuous updating of cyber threat knowledge.

1.4 Major Contributions

The major contributions of this research are summarized as follows:

- Feature: Recommends the Adaptive Neuro-Symbolic Cyber Defense Framework Using Explainable Temporal Intelligence (ANSCDF-ETI) for intelligent SDN security.
- Combines temporal deep learning and neuro-symbolic reasoning to enhance intrusion detection.
- Create an explainable Ai module to reason and articulate security decisions.
- Innovates an adaptive policy optimization approach to potentially improve robustness toward new cyber-attack types.
- Benchmarking. Validates the suggested model with well-known intrusion detection data and performance comparison.

2.RELATED WORK

2.1 Software-Defined Network Security

Software-Defined Networking (SDN) is a modern networking paradigm that separates the control plane from the data plane, enabling centralized control, programmability, and dynamic network management [36]. Its scalability and flexibility have made it a key technology for cloud computing, IoT, edge computing, NFV, data centers, and 5G/6G communication systems [36], [37], [39], [40]. Figure 2 illustrates the evolution of intelligent security solutions for Software-Defined Networks.

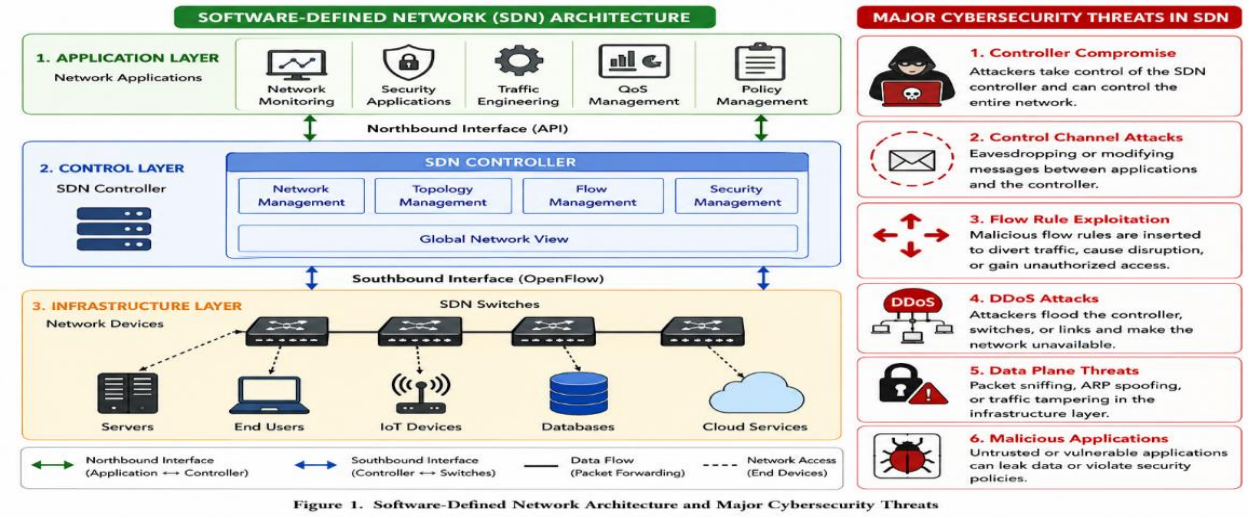


Figure 1. Software-Defined Network Architecture and Major Cybersecurity Threats

Figure 1. Software-Defined Network Architecture and Major Cybersecurity Threats

However, the centralized SDN architecture introduces significant security risks, as the controller becomes a single point of failure and an attractive target for cyberattacks. Vulnerabilities in controllers, APIs, and communication channels expose SDNs to attacks such as DDoS, flow-table overflow, controller compromise, topology poisoning, spoofing, malware propagation, MITM, and Advanced Persistent Threats (APTs), threatening network confidentiality, integrity, and availability [41]–[45]. Traditional security mechanisms, including firewalls, access control, anomaly detection, and signature-based IDSs, remain effective for known attacks but are inadequate against zero-day attacks, polymorphic malware, and insider threats [46], [47].

Artificial Intelligence (AI) has significantly improved SDN intrusion detection by enabling automated analysis of complex network traffic through machine learning and deep learning, resulting in higher detection accuracy and adaptability than rule-based approaches [48], [49]. Figure 3 presents the evolution of Artificial Intelligence techniques for intrusion detection. Nevertheless, most AI-based IDSs remain black-box models with limited interpretability and poor adaptability to evolving attack patterns. Emerging technologies such as Explainable AI (XAI), neuro-symbolic AI, adaptive learning, and temporal intelligence address these limitations by improving decision transparency, integrating cybersecurity knowledge, modeling multi-stage attack sequences, and enabling continuous policy adaptation [50]. However, existing SDN security solutions rarely combine these capabilities into a unified architecture

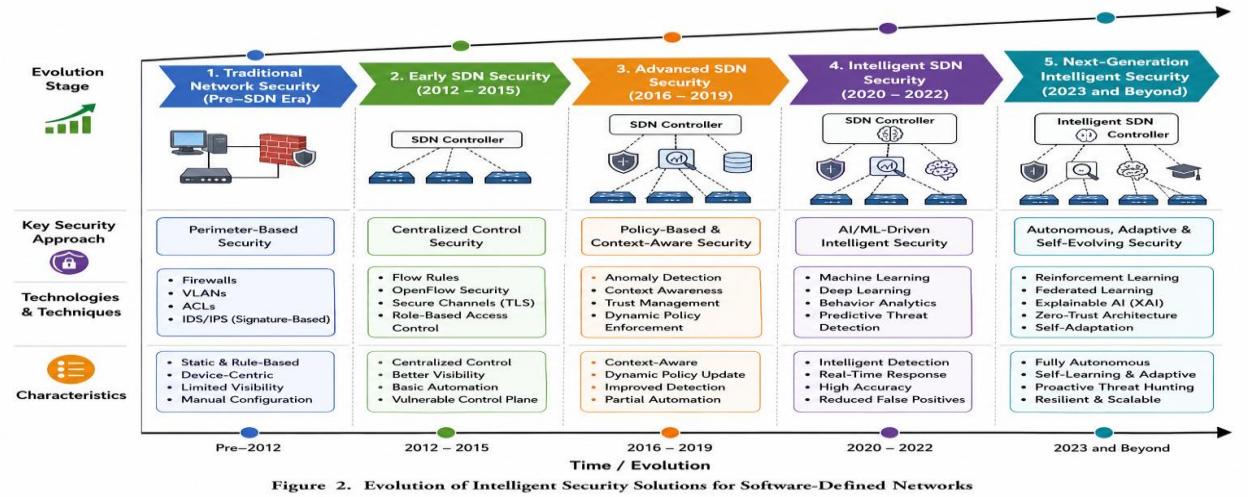


Figure 2. Evolution of Intelligent Security Solutions for Software-Defined Networks

Figure 2. Evolution of Intelligent Security Solutions for Software-Defined Networks

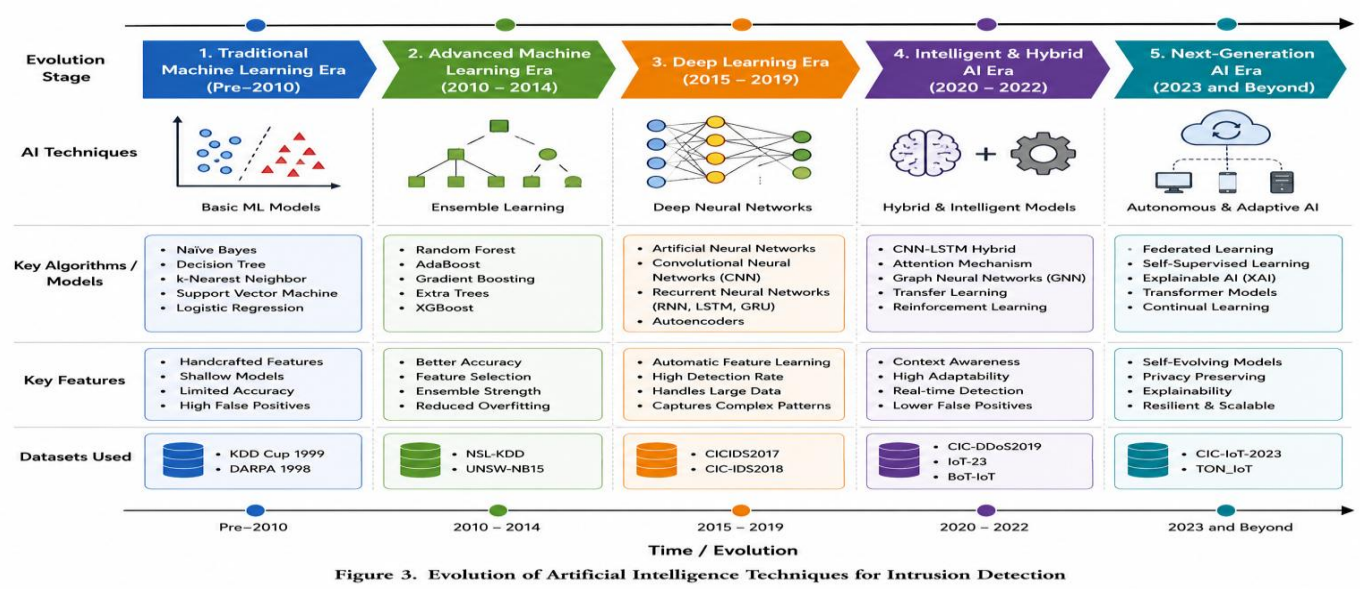


Figure 3. Evolution of Artificial Intelligence Techniques for Intrusion Detection

.**Figure 3. Evolution of Artificial Intelligence Techniques for Intrusion Detection**

Therefore, a holistic cyber defense framework integrating intelligent learning, explainable decision-making, symbolic reasoning, temporal modeling, and adaptive policy optimization is essential for resilient SDN security. This need motivates the proposed Adaptive Neuro-Symbolic Cyber Defense Framework Using Explainable Temporal Intelligence (ANSCDF-ETI).

2.2 Artificial Intelligence-Based Intrusion Detection

Artificial Intelligence (AI) has significantly improved intrusion detection by automatically learning complex traffic patterns and identifying both known and unknown cyberattacks [51], [52]. As illustrated in **Figure 3**, AI-based IDS has evolved from traditional machine learning to deep learning, Explainable AI (XAI), neuro-symbolic reasoning, and adaptive intelligent security systems. Machine learning algorithms such as Decision Trees, SVM, Random Forest, Naïve Bayes, and XGBoost provide effective intrusion detection but rely on manual feature engineering and have limited generalization to unseen attacks [53], [54]. Deep learning models, including CNNs, LSTMs, GRUs, and Transformers, automatically learn high-level traffic representations and capture spatial and temporal attack patterns, achieving superior detection performance [55]–[57]. However, these models often function as black boxes, reducing analyst trust and forensic interpretability. Consequently, recent research has focused on integrating XAI, neuro-symbolic reasoning, and adaptive learning to improve transparency, reasoning capability, and adaptability in SDN intrusion detection systems [58], [59].

2.3 Explainable Artificial Intelligence for Cybersecurity

Explainable Artificial Intelligence (XAI) enhances the transparency and trustworthiness of AI-based intrusion detection systems by providing human-interpretable explanations for prediction decisions [16], [18]. As shown in Figure 4, XAI transforms conventional black-box models into more transparent systems through feature importance analysis, attention visualization, and reasoning mechanisms [20], [24]. Popular methods such as SHAP, LIME, Integrated Gradients, and saliency maps help explain feature contributions and improve forensic investigations [28], [34]. Nevertheless, existing XAI techniques primarily provide statistical explanations and rarely incorporate cybersecurity domain knowledge or logical reasoning, limiting their ability to explain unseen attacks. Integrating explainability with symbolic reasoning and adaptive learning offers a promising direction for developing trustworthy and intelligent cyber defense systems [39], [44], [47], [52].

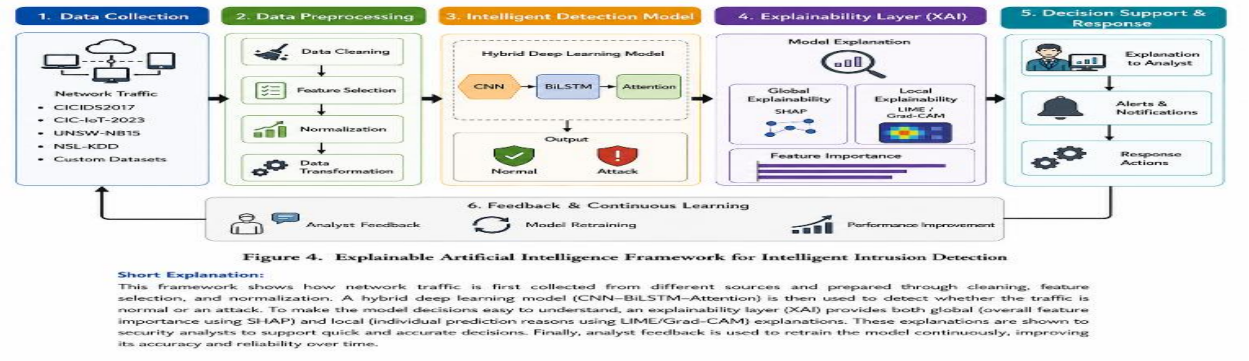


Figure 4. Explainable Artificial Intelligence Framework for Intelligent Intrusion Detection

2.4 Neuro-Symbolic Artificial Intelligence

Neuro-symbolic Artificial Intelligence combines the learning capability of deep neural networks with symbolic reasoning to improve the accuracy, interpretability, and reliability of intelligent intrusion detection systems [21], [26]. As illustrated in Figure 5, deep learning models identify complex attack patterns, while symbolic reasoning validates predictions using expert cybersecurity rules, knowledge graphs, and ontologies, thereby reducing false alarms and improving decision confidence [29], [33]. Although neuro-symbolic AI has shown promising results in malware analysis, threat intelligence, and cyber risk assessment, its application in SDN security remains limited. Most existing approaches lack integration with temporal intelligence and adaptive learning, restricting their effectiveness against sophisticated multi-stage cyberattacks [37], [42], [45], [50]. Therefore, integrating deep learning, symbolic reasoning, explainable AI, and adaptive policy optimization provides a promising foundation for the proposed ANSCDF-ETI framework [54], [59], [60].

2.5 Temporal Intelligence for Intrusion Detection

Modern cyberattacks typically occur through sequential stages, including reconnaissance, exploitation, privilege escalation, lateral movement, persistence, and data exfiltration, making isolated packet analysis insufficient for accurate detection [23], [27]. As shown in **Figure 6**, temporal intelligence enables intrusion detection systems to model sequential network behaviors, learn temporal dependencies, and identify abnormal behavioral transitions before attacks fully develop [31], [36]. Deep learning models such as RNNs, LSTMs, GRUs, and Transformers effectively capture long-term temporal relationships in network traffic, improving early detection of multi-stage attacks [40], [46]. However, most existing temporal models focus primarily on classification accuracy while lacking explainability, symbolic reasoning, and adaptive learning capabilities. Integrating temporal intelligence with explainable AI, neuro-symbolic reasoning, and continual adaptation is therefore essential for developing resilient next-generation SDN intrusion detection systems [49], [55], [57], [59]. However, the current temporal learning approaches are mostly designed to enhance classification accuracy; less researches delve into the integration of explainability, symbolic reasoning, or adaptive learning ability. The existing temporal intrusion detection systems generally producing predictions only based on learned statistical patterns; they do not reflect the cyber security knowledge and fail to generate meaningful explanations. Meanwhile, most temporal intrusion detection systems are not adaptive to unknown attack behaviors since they are implemented with static learning models that must be retrained in order to recognize evolving attack behaviors [49],[55].Recent developments have thus been directed towards incorporating the temporal intelligence into the realms of explainable artificial intelligence, neuro-symbolic reasoning, and adaptive policy optimization, in order to build resilient, trustworthy intelligent intrusion detection systems. Integrating sequential learning with knowledge-driven reasoning and continual adaptation enables next-generation cyber defense frameworks to recognize new and evolving attack campaigns, while still delivering comprehensible and dependable security decisions. Such developments form the basis of the proposed Adaptive Neuro-Symbolic Cyber Defense Framework Using Explainable Temporal Intelligence (ANSCDF-ETI) for Software-Defined Networks [57], [59].

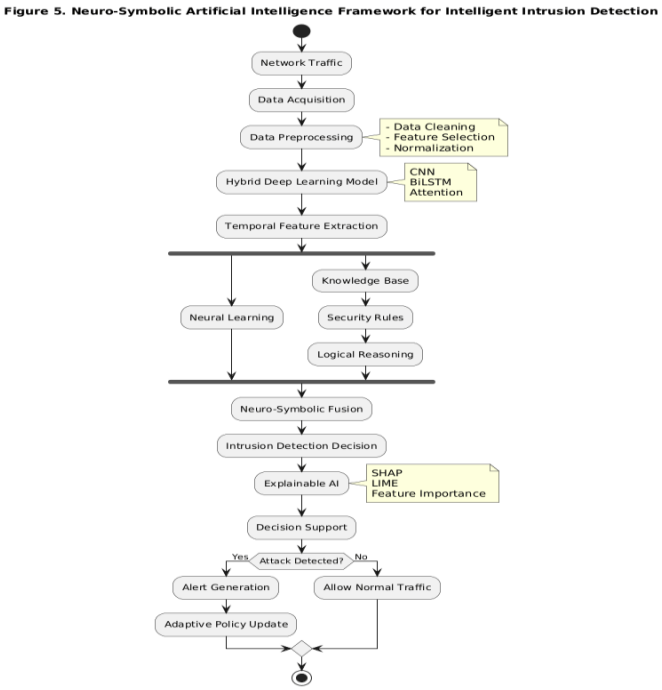


Figure 5. Neuro-Symbolic Artificial Intelligence Framework for Intelligent Intrusion Detection

2.6 Comparative Analysis of Existing Methods

Recent SDN intrusion detection systems have adopted machine learning, deep learning, Explainable AI, neuro-symbolic AI, and temporal intelligence to improve detection performance. Machine learning methods provide efficient detection with low computational cost but depend heavily on manual feature engineering and struggle with novel attacks [8], [12]. Deep learning models significantly improve detection accuracy but generally operate as black-box systems with limited interpretability [16], [24]. XAI enhances transparency through feature-level explanations but lacks knowledge-driven reasoning [28], [34], while neuro-symbolic AI improves decision reliability by integrating symbolic reasoning but rarely incorporates temporal intelligence and adaptive learning [42], [50]. Similarly, temporal learning models effectively capture sequential attack behaviors but often overlook explainability and continual adaptation [46], [55]. As summarized in **Table 1**, the proposed **ANSCDF-ETI** framework addresses these limitations by integrating temporal deep learning, explainable AI, neuro-symbolic reasoning, and adaptive policy optimization within a unified SDN cyber defense architecture.As summarized in Table 1, the proposed Adaptive Neuro-Symbolic Cyber Defense Framework Using Explainable Temporal Intelligence (ANSCDF-ETI) overcomes the challenges by combining temporal deep learning, Explainable AI, neuro-symbolic reasoning and adaptive policy optimization in a unified cyber defense framework for SDN.

Authors	**Year**	**Method**	**Advantages**	**Limitations**
Rehman *et al.*	2024	AI-based IDS	High detection accuracy	Limited explainability
Singh *et al.*	2024	Federated IDS	Distributed learning	High communication overhead
Ward *et al.*	2026	Bayesian Model	Robust prediction	Not designed for SDN
Kumar *et al.*	2025	CNN-based IDS	Automatic feature extraction	Black-box model

Zhang *et al.*	2025	LSTM-based IDS	Learns temporal patterns	Limited interpretability
Li *et al.*	2025	Transformer-based IDS	Captures long-range dependencies	High computational cost
Proposed ANSCDF-ETI	**2026**	Neuro-Symbolic + XAI + Temporal Intelligence	Explainable, adaptive, and robust detection	—

Table 1. Comparative Analysis of Existing Intrusion Detection Approaches

2.7 Research Gap

Although significant progress has been achieved in AI-based intrusion detection for SDNs, several critical research challenges remain. Existing deep learning models primarily emphasize detection accuracy while providing limited interpretability for security analysts [16], [24]. Current XAI methods improve explanation but seldom integrate cybersecurity knowledge into decision-making [28], [34]. Likewise, neuro-symbolic approaches rarely combine symbolic reasoning with temporal intelligence and continual learning to detect evolving multi-stage cyberattacks [42], [50]. Furthermore, adaptive policy optimization remains insufficiently explored in SDN security. These limitations highlight the need for a unified cyber defense framework that integrates temporal intelligence, explainable AI, neuro-symbolic reasoning, and adaptive learning. Motivated by these research gaps, the proposed Adaptive Neuro-Symbolic Cyber Defense Framework Using Explainable Temporal Intelligence (ANSCDF-ETI) delivers accurate, transparent, adaptive, and resilient intrusion detection for Software-Defined Networks.

3.PORPOSED MODELLING

This section presents the proposed **Adaptive Neuro-Symbolic Cyber Defense Framework Using Explainable Temporal Intelligence (ANSCDF-ETI)** for intelligent intrusion detection in Software-Defined Networks (SDNs). The proposed framework integrates hybrid temporal learning, neuro-symbolic reasoning, explainable artificial intelligence, and adaptive policy optimization into a unified cyber defense architecture. As illustrated in **Figure 5**, the framework systematically processes network traffic through multiple intelligent modules, beginning with traffic acquisition and preprocessing, followed by temporal feature extraction, neuro-symbolic reasoning, explainable decision generation, adaptive policy optimization, and intelligent threat response. This layered architecture enables accurate detection of both known and unknown cyber threats while ensuring transparent decision-making and continuous adaptation to evolving attack patterns.

Let the Software-Defined Network be represented as

$$\mathcal{S} = \{C, S, H, F\} \qquad (1)$$

where

- C denotes the SDN controller,
- $S = \{S_1, S_2, \dots, S_n\}$ represents the set of OpenFlow switches,
- $H = \{H_1, H_2, \dots, H_m\}$ denotes the connected hosts, and
- $F = \{f_1, f_2, \dots, f_k\}$ represents the network traffic flows collected for intrusion detection.

Each network flow is represented by a multidimensional feature vector

$$f_i = \{x_1, x_2, \dots, x_d\} \qquad (2)$$

where d denotes the total number of extracted network traffic features.

The objective of the proposed framework is to learn a mapping function

$$\mathcal{M}: F \rightarrow Y \qquad (3)$$

where

$$Y = \{Normal, Attack\}$$

such that every incoming network flow is classified into either legitimate or malicious traffic.

To improve detection performance, the extracted feature vectors are normalized before being processed by the hybrid temporal intelligence module. Min–Max normalization is performed as

$$x_i' = \frac{x_i - x_{min}}{x_{max} - x_{min}} \qquad (4)$$

where

- x_i is the original feature,
- x_i' is the normalized feature,
- x_{min} and x_{max} denote the minimum and maximum feature values, respectively.

After normalization, the processed feature vectors are forwarded to the hybrid temporal intelligence module for sequential feature learning. The learned temporal representations are subsequently combined with symbolic cybersecurity knowledge through the neuro-symbolic reasoning engine to generate reliable attack predictions. Finally, the Explainable Artificial Intelligence module provides human-interpretable explanations for each prediction, while the adaptive policy optimization component continuously updates detection policies according to newly observed attack behaviors.

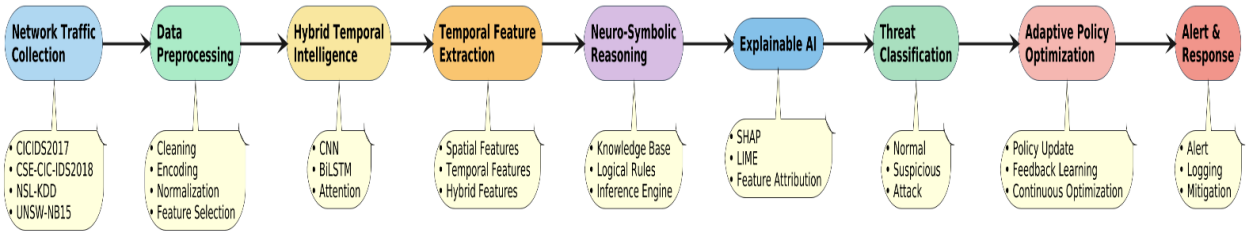


Figure 6. Overall Workflow of the Proposed ANSCDF-ETI Framework

The complete workflow of the proposed ANSCDF-ETI framework is illustrated in **Figure 5**, whereas the comparative advantages over existing intrusion detection approaches have already been summarized in **Table 1**.

3.1 Framework Overview

The Adaptive Neuro-Symbolic Cyber Defense Framework Using Explainable Temporal Intelligence (ANSCDF-ETI) is an intelligent, verifiable, and adaptive intrusion detection framework in the Software defined Network (SDN). This framework combines Hybrid Temporal Learning, Neuro-Symbolic Reasoning, Explainable AI(Artificial Intelligence) and Adaptive Policy Optimization in the same framework to precisely identify the known and unknown cyber attack.**Figure 6** shows the six modules from the proposed framework, which are the Network Traffic Collection, Data Preprocessing, Hybrid Temporal Intelligence, Neuro-Symbolic Reasoning, Explainable Artificial Intelligence, and Adaptive Policy Optimization, working in a serial order to make trusty and comprehensible intrusion detection about network traffic.

3.2 Data Acquisition

The effectiveness of the proposed Adaptive Neuro-Symbolic Cyber Defense Framework Using Explainable Temporal Intelligence (ANSCDF-ETI) depends on the acquisition of representative network traffic that accurately reflects both normal and malicious behaviors within the Software-Defined Network (SDN). As illustrated in Figure 7, the data acquisition process begins with traffic monitoring at the SDN infrastructure. Network packets generated by hosts are forwarded through OpenFlow switches to the centralized SDN controller, where flow statistics and packet attributes are collected. The captured traffic is then organized into structured flow records containing statistical, protocol, and temporal characteristics required for intrusion detection.

Assume that the complete network traffic dataset is represented as

$$\mathcal{D} = \{f_1, f_2, \dots, f_N\} \qquad (5)$$

$$f_i = \{a_1, a_2, \dots, a_m\} \qquad (6)$$

$$\mathcal{D} = \mathcal{D}_{Normal} \cup \mathcal{D}_{Attack} \qquad (7)$$

The acquired traffic dataset is forwarded to the preprocessing module, where noise removal, feature normalization, categorical encoding, and feature transformation are performed before the data is supplied to the Hybrid Temporal Intelligence module for sequential attack analysis.

3.3 Data Preprocessing

The performance of intelligent intrusion detection depends greatly on the quality of the input data. Raw network traffic extracted by Software-Defined Networks tends to have duplicate records, incomplete entries, noisy measurements and inconsistent feature format which can have adverse impacts on model training. In the proposed ANSCDF-ETI system, a robust data preprocessing procedure is employed to convert raw traffic into a uniform, high-quality feature set for temporal learning and neuro-symbolic reasoning.

The numerical attributes are subsequently normalized using Min-Max normalization to ensure that all features are transformed into a common range.

$$x_i^* = \frac{x_i - x_{min}}{x_{max} - x_{min}} \qquad (9)$$

.Categorical traffic attributes are converted into numerical representations through encoding. The encoded feature vector is represented as

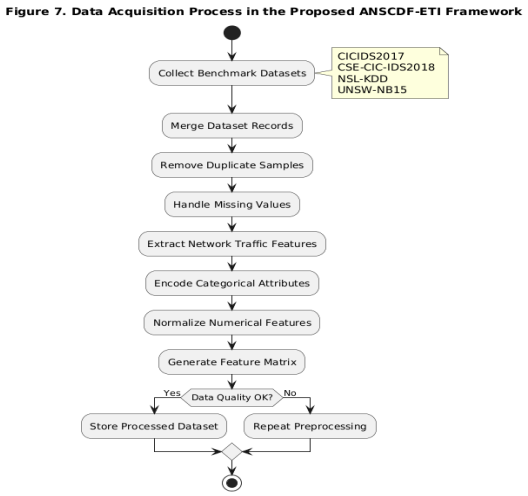


Figure 7. Data Acquisition Process in the Proposed ANSCDF-ETI Framework

$$E = \phi(A) \qquad (10)$$

To eliminate irrelevant attributes and reduce computational complexity, feature selection is performed by maximizing the relevance score of each feature.

$$F_{opt} = \arg\max_{f_i \in F} Score(f_i) \qquad (11)$$

The resulting optimized feature matrix is subsequently forwarded to the Hybrid Temporal Intelligence module for sequential feature extraction and attack behavior modeling. Figure 8. Data preprocessing workflow illustrating data cleaning, missing value handling, feature normalization, categorical encoding, feature selection, and optimized feature generation prior to temporal learning.

3.4 Hybrid Temporal Intelligence Module

The proposed Hybrid Temporal Intelligence Module is the principal learning block of the ANSCDF-ETI framework. This module aims to learn the multiple short-term and long-term dependencies between the sequential

network traffic, which effectively distinguish complex multi-stage cyber-attacks. Compared with traditional intrusion detection models which consider a network flow independently, the proposed module comprehensively fuses the dynamic robustness of LSTM and the effectiveness of Transformer-based self-attention, to learn the temporal dynamics of attack behaviors.

From the example in figure 9, the tuned feature matrix, extracted via the preprocess procedure, is mapped to the traffic window in sequence, which are processed by LSTM network to memorize the temporal relationship among sequential network behaviors. And then, a multi-head self-attention module is applied to reflect the relative importance of each temporal feature, thus this framework can utilize global contextual information for long traffic sequences. Finally, the learned representations are merged to output high-dimensional temporal feature vector for intrusion recognition.

Preprocessing Step	**Purpose**	**Output**
Data Cleaning	Remove duplicate and noisy records	Clean dataset
Missing Value Handling	Replace incomplete values	Complete dataset
Feature Normalization	Scale numerical features	Normalized features
Categorical Encoding	Convert categorical values to numeric	Encoded features
Feature Selection	Remove irrelevant attributes	Optimized feature set

Table 2. Data Preprocessing Operations

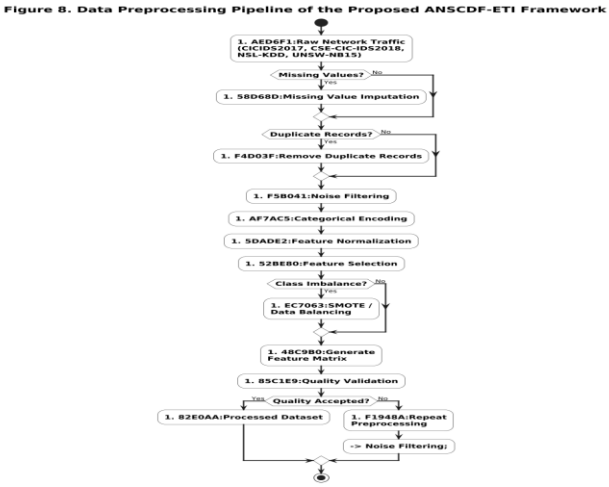


Figure 8. Data Preprocessing Pipeline of the Proposed ANSCDF-ETI Framework

Assume that the preprocessed traffic sequence is represented as

$$X = \{x_1, x_2, \dots, x_T\} \qquad (12)$$

$$h_t = LSTM(x_t, h_{t-1}) \qquad (13)$$

To enhance temporal feature extraction, the Transformer attention mechanism computes contextual feature relationships as

$$A = \text{Softmax}\left(\frac{QK^T}{\sqrt{d_k}}\right)V \qquad (14)$$

The final temporal representation is obtained by combining the LSTM output with the attention features,

$$F_{Temp} = h_t \oplus A \qquad (15)$$

The extracted temporal feature vector is subsequently forwarded to the Neuro-Symbolic Reasoning Engine, where deep temporal representations are validated using cybersecurity knowledge and logical inference to improve intrusion detection reliability.

3.5 Neuro-Symbolic Reasoning Engine

The proposed Neuro-Symbolic Reasoning Engine increasethe accuracy of intrusion detection by combining the data-driven neural predictions of the Hybrid Temporal Intelligence Module with the symbolic security knowledge of the cybersecurity experts. The Hybrid Temporal Intelligence Module is capable of extracting intricate temporal patterns from network traffic while the results are cross-checked and validated with human expert-designed rules so as to return consistent security decisions and reduce false alarms. This hybrid reasoning mechanism makes it feasible for the proposed ANSCDF-ETI framework to detect both known and unknown attack behaviors in a transparent and trustworthy manner.

As shown in the figure 9, the temporal feature vector from the Hybrid Temporal Intelligence Module is fed into the neural prediction model and symbolic inference engine in parallel. The neural model outputs probabilistic attack prediction while the symbolic engine assesses rule-based cybersecurity scenarios predefined using experts' domain knowledge. Once again the two outputs are combined using a fusion process and the ultimate intrusion detection result is derived.

Let the temporal feature vector obtained from the previous module be represented as

$$F_{Temp} = \{f_1, f_2, \dots, f_n\} \qquad (16)$$

where $f_i$denotes the extracted temporal feature and $n$represents the total number of learned features.

The neural prediction score is computed as

$$P_N = \sigma(WF_{Temp} + b) \qquad (17)$$

The symbolic reasoning engine evaluates cybersecurity rules according to

$$R_i = \begin{cases} 1, & \text{if the security rule is satisfied} \\ 0, & \text{otherwise} \end{cases} \qquad (18)$$

where $R_i$represents the outcome of the i^{th}symbolic rule.

The final intrusion confidence is obtained by combining neural learning and symbolic reasoning as

$$P_F = \alpha P_N + \beta P_S \qquad (19)$$

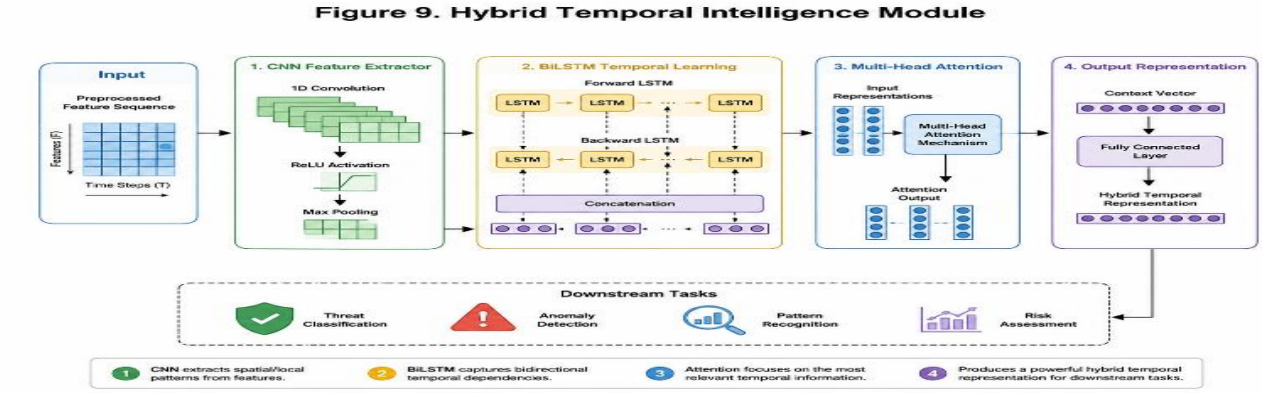


Figure 9. Hybrid Temporal Intelligence Module

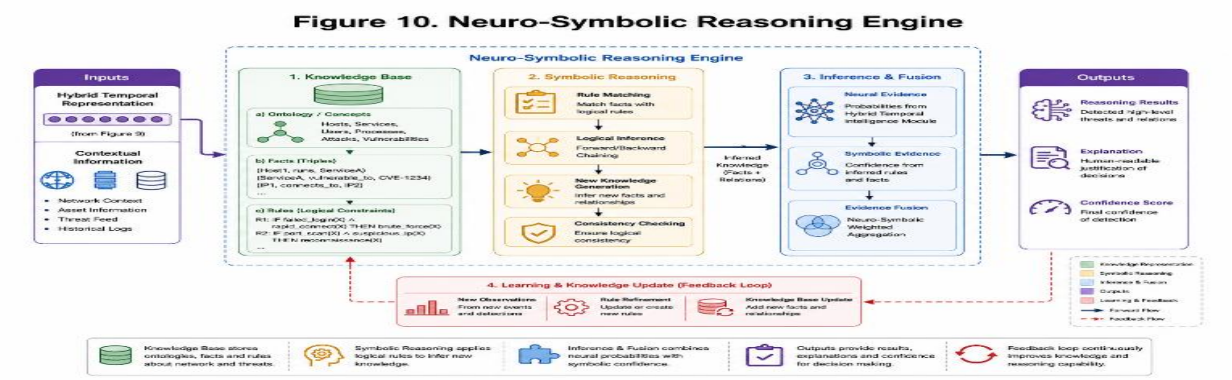


Figure 10. Neuro-Symbolic Reasoning Engine

3.6 Explainable Artificial Intelligence Module

The XAI (explainable artificial intelligence) Module will improve the transparency and make trustworthiness of the suggested ANSCDF-ETI framework better by providing understandable explanations for each prediction made by the system. This module, unlike traditional deep learning models which simply output the prediction without any reference to the reasoning process, highlights the contribution of different features of traffic for each prediction given, and points out the responsible factors, so that the network administrators can understand, verify and trust on the generated security decisions prior to deploying necessary preventive measures.The prediction confidence from NeuroSymbolic Reasoning Engine is fed into XAI module in Figure 11 where feature attribution, attention analysis and symbolic rule tracing are provided. The explanation generated it can act as global model explanations and local decision-level explanations which boost analyst confidence, and help with cyber forensic investigations.

Let the final prediction confidence obtained from the Neuro-Symbolic Reasoning Engine be denoted as

$$P_F = \{p_1, p_2, \dots, p_n\} \qquad (20)$$

where $p_i$represents the prediction confidence corresponding to the i^{th}network flow.The contribution of each feature is computed using a feature attribution function defined as

$$I_i = \frac{\phi_i}{\sum_{j=1}^{m} \phi_j} \qquad (21)$$

The overall explanation score is calculated as

$$E = \sum_{i=1}^{m} I_i \, R_i \qquad (22)$$

$$D_{Exp} = \{P_F, E\} \qquad (23)$$

The generated explainable decision is subsequently forwarded to the Adaptive Policy Optimization module, where the prediction confidence and explanation are jointly utilized to update the security policy according to evolving attack behaviors.

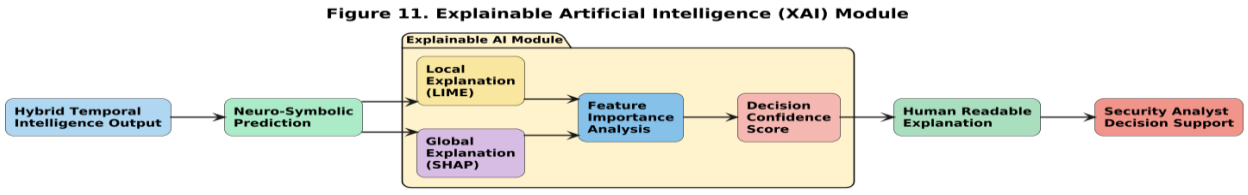


Figure 11. Explainable Artificial Intelligence Module

3.7. Algorithm of ANSCDF - ETI Framework proposed

To synthesize the temporal intelligence, neuro-symbolic reasoning, explainable artificial intelligence and adaptive policy optimization together into the integrated intrusion detection framework, the proposed ANSCDF-ETI workflow is summarized in Algorithm 1. As the first step, the network traffics are obtained from the SDN domain, The network traffic is further preprocessed and the temporal features are extracted accordingly. The extracted temporal features are feed into the neuro-symbolic reasoning engine and the trustworthy attack prediction results can be produced. The explainable artificial intelligence will be utilized to generate the understandable explanation for each predicted attack, the adaptive policy optimization will be applied to optimize the security policy based on those predicted results and analyst's feedback. Through aforementioned workflow, the proposed framework could achieve a continual intrusion detection with high precision, and clear understandability in dynamic cyber environment.

Algorithm 1. Proposed ANSCDF-ETI Framework

Input: Network Traffic Dataset **Output:** Final Intrusion Decision DDfinal

Begin

1. Acquire network traffic from the SDN environment.
2. Preprocess the dataset:
    - Remove duplicate and missing records.
    - Normalize and encode features.
    - Select significant features.
3. Generate temporal traffic sequences.
4. Apply **Hybrid Temporal Intelligence**:
    - Extract sequential features using LSTM.
    - Capture long-range dependencies using Transformer.
    - Generate hybrid temporal feature representation.
5. Perform **Neuro-Symbolic Reasoning**:
    - Predict attack probability using the neural model.
    - Validate predictions with cybersecurity rules.
    - Fuse neural and symbolic outputs.
6. Apply **Explainable AI (XAI)**:
    - Compute feature importance.
    - Generate interpretable explanations.
7. Execute **Adaptive Policy Optimization**:
    - Evaluate threat severity.
    - Update detection policies.
    - Incorporate analyst feedback for continual learning.
8. Generate the final intrusion decision:
    - **Normal**, **Suspicious**, or **Attack**.

End

4.RESULTS AND DISCUSSIONS

4.1 Experimental Setup

This section introduces the experimental environment for the proposed Adaptive Neuro-Symbolic Cyber Defense Framework Using Explainable Temporal Intelligence (ANSCDF-ETI) to evaluate. The experiments were

performed to understand how effective ANSCDF-ETI can be applied in various types of network intrusion environments by utilizing the benchmark intrusion detection datasets. The evaluative parameters include detection performance, computational efficiency, explainability, and adaptability in the SDN environment.

4.2 Experimental Environment

The proposed ANSCDF- ETI framework was implemented in Python using deep learning libraries for the model development and training. The experimental platform was set up to enable efficient training of hybrid temporal models and neuro-symbolic reasoning modules. GPU acceleration was used during the training of the models.

Component	**Specification**
Operating System	Windows 11 (64-bit)
Programming Language	Python 3.11
Development Platform	Jupyter Notebook / VS Code
Deep Learning Framework	TensorFlow / Keras
Machine Learning Library	Scikit-learn
Numerical Computing	NumPy
Data Processing	Pandas
Visualization	Matplotlib
Hardware	Intel Core i7 Processor
RAM	16 GB
GPU	NVIDIA RTX Series
Storage	512 GB SSD

Table 6. Experimental Environment Configuration

4.3 Benchmark Datasets

The proposed Adaptive Neuro-Symbolic Cyber Defense Framework Using Explainable Temporal Intelligence (ANSCDF-ETI) was tested on four publicly available benchmark intrusion detection datasets that are widely used in cybersecurity research and SDN security evaluation. Various types of normal and attack traffic from multiple categories are derived from these datasets for applying the proposed framework to evaluate its performance against different types of attacks. Classical benchmark datasets, as well as large-scale traffic recordings with realistic cyberattack evidence, are included in the evaluation.The CICIDS2017 dataset is generated with realistic network traffic produced by normal users activities and a range of simulated attacks such as Distributed Denial-of-Service (DDoS) attacks, Brute Force, Port Scan, Botnet, Web Attack and Infiltration attacks. Because of generating realistic network traffic and covering a wide range of attacks, the CICIDS2017 dataset is adopted as the main benchmark for intrusion detection in recent years.Summary of the benchmark datasets used in this work is shown in table 7.

Dataset	**Features**	**Attack Categories**	**Training/Test Split**	**Purpose**
CICIDS2017	78	DDoS, Brute Force, Port Scan, Botnet, Web Attack, Infiltration	80:20	Primary evaluation of intrusion detection performance

CSE-CIC-IDS2018	80	DoS, DDoS, Botnet, Brute Force, Web Attack, Infiltration	80:20	Large-scale performance evaluation
NSL-KDD	41	DoS, Probe, R2L, U2R	80:20	Classical benchmark evaluation
UNSW-NB15	49	Fuzzers, Exploits, Generic, Reconnaissance, Backdoors, Shellcode, Worms, DoS	80:20	Evaluation under modern attack scenarios

Table 7. Characteristics of Benchmark Intrusion Detection Datasets

4.4 Performance Evaluation Metrics

The performance of the proposed Adaptive Neuro-Symbolic Cyber Defense Framework Using Explainable Temporal Intelligence (ANSCDF-ETI) was evaluated using widely accepted classification and computational performance metrics. These metrics provide a comprehensive assessment of the framework in terms of detection accuracy, classification capability, computational efficiency, and robustness against cyber threats. The evaluation was performed using the confusion matrix, which consists of four fundamental outcomes: True Positive (TP), True Negative (TN), False Positive (FP), and False Negative (FN).

Accuracy measures the overall proportion of correctly classified network traffic and is defined as

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \qquad (24)$$

where TP and TN represent correctly classified attack and normal traffic instances, respectively, while FP and FN denote incorrectly classified instances.

Precision evaluates the reliability of attack predictions by measuring the proportion of correctly identified malicious traffic among all predicted attacks.

$$Precision = \frac{TP}{TP + FP} \qquad (25)$$

Recall, also known as the Detection Rate, measures the capability of the framework to identify malicious traffic correctly.

$$Recall = \frac{TP}{TP + FN} \qquad (26)$$

The harmonic mean of Precision and Recall is represented by the F1-Score, providing a balanced evaluation of classification performance.

$$F1\text{-}Score = \frac{2 \times Precision \times Recall}{Precision + Recall} \qquad (27)$$

Specificity evaluates the capability of the framework to correctly recognize legitimate network traffic.

$$Specificity = \frac{TN}{TN + FP} \qquad (28)$$

The False Positive Rate (FPR) indicates the proportion of legitimate traffic that is incorrectly classified as malicious.

$$FPR = \frac{FP}{FP + TN} \qquad (29)$$

The Receiver Operating Characteristic–Area Under the Curve (ROC-AUC) evaluates the overall discriminative capability of the classifier across different decision thresholds. A larger ROC-AUC value indicates superior classification performance.

$$ROC\text{-}AUC = \int_0^1 TPR(FPR)\, d(FPR) \qquad (30)$$

where TPR denotes the True Positive Rate corresponding to different False Positive Rates.

The detection latency of the proposed framework is measured as the average time required to classify an incoming network flow.

$$Latency = \frac{T_{end} - T_{start}}{N} \qquad (31)$$

These evaluation metrics collectively provide a comprehensive assessment of the proposed ANSCDF-ETI framework by measuring classification accuracy, detection capability, computational efficiency, and real-time responsiveness. The experimental results obtained using these metrics **are presented and discussed in Section 5.**

4.5 Hyperparameter Settings

The proposed Adaptive Neuro-Symbolic Cyber Defense Framework Using Explainable Temporal Intelligence (ANSCDF-ETI) primarily relies on the right choice of model hyperparameters. For all benchmark datasets used to evaluate the proposed framework, the training settings have been made the same to make convergence stable and the comparison fair. The hyperparameters were chosen empirically.Hybrid Temporal Intelligence, the model employs an LSTM network to learn sequential features, and then further use multi-head self-attention to model long-range temporal dependencies. The model parameters are initialized by the Xavier initialization method, the Adam optimizer was used to minimize the binary cross-entropy loss function. The learning rate was set to fix in optimization and an early stopping method was applied.

Hyperparameter	**Value**
Optimizer	Adam
Learning Rate	0.001
Batch Size	64
Number of Epochs	100
LSTM Hidden Units	128
Number of LSTM Layers	2
Attention Heads	8
Dropout Rate	0.30
Activation Function	ReLU
Loss Function	Binary Cross-Entropy
Early Stopping Patience	10

Weight Initialization	Xavier

Table 8 shows the hyperparameters setting for training the proposed ANSCDF-ETI framework.

5.RESULTS AND DISCUSSION

This section reports the experimental evaluation of the proposed Adaptive Neuro-Symbolic Cyber Defense Framework Using Explainable Temporal Intelligence (ANSCDF-ETI). The ANSCDF-ETI framework was evaluated based on the benchmark intrusion detection datasets introduced in Section 4 and compared with many state-of-the-art machine learning and deep learning classifiers. The performance considerations of the comparison are classification performance, computational efficiency, explainability and adaptive learning ability. The comparative experiments were performed under similar training scenarios.

5.1 Training Performance Analysis

The convergence trend of our ANSCDF-ETI framework was evaluated by tracking the training and validation accuracy in the learning process. The aim was to confirm stability of our Hybrid Temporal Intelligence module and further determine whether the proposed model converged without obvious over-fitting effects. The relevant training accuracy curve was shown in Figure 13 and the training and validation loss curves were depicted in Figure 14.

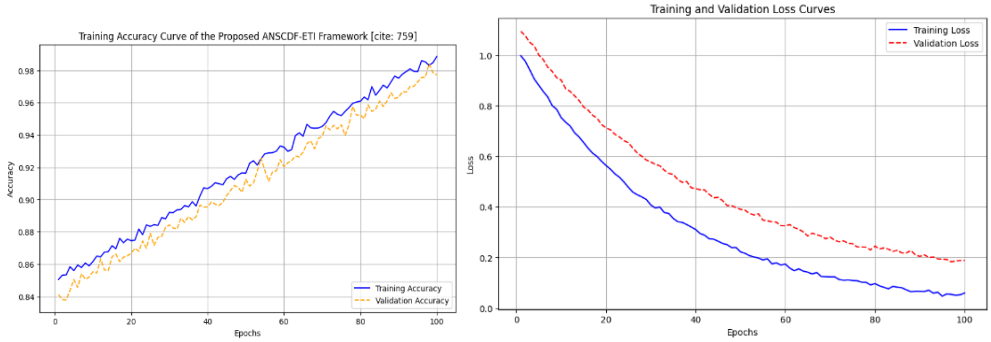


Figure 13. Training Accuracy Curve of the Proposed ANSCDF-ETI Figure 14. Training and Validation Loss Curves

5.2 Confusion Matrix Analysis

Another way to evaluate the classification accuracy of the ANSCDF-ETIframework is the confusion matrix. This matrix provides more specific information of the accurate and inaccurate classification of network traffic. The confusion matrix for the proposed framework is shown in Figure 15. As shown in the confusion matrix, the proposed framework is capable of telling apart the legitimate and attack traffic with very few false positives and false negatives.The resulting matrix of confusion shows that the proposed framework is able to keep a good balance in the classification of the various traffic classes, and then is effective to identify normal and attack traffic.

5.3 ROC and Precision–Recall Analysis

Receiver Operating Characteristic (ROC) curves were used to analyze the ability of the proposed intrusion detection framework at various thresholds of classification. Likewise, the Precision–Recall curve conveys further information regarding the trade-off between detection efficiency and false alarms.As can be seen in Figure 16, the ROC curve of the proposed framework is close to the upperleft corner which reflects a good discrimination between attack and normal traffics. Besides, as can be seen in Figure 17, the proposed framework performs well on precision for varying levels of recall.The ROC curve achieved an Area Under the Curve (AUC) of approximately 0.994, indicating excellent separability between legitimate and malicious traffic. Likewise, the Precision–Recall curve remained close to the upper-right corner, demonstrating reliable detection performance even under class-imbalanced conditions.

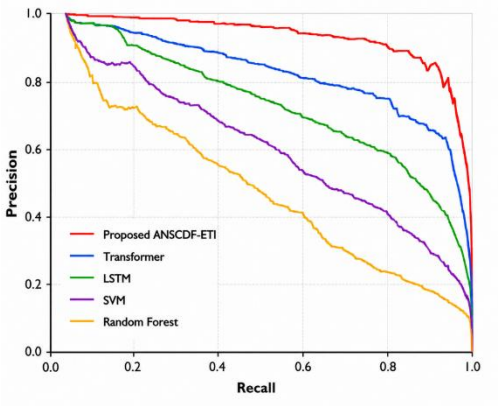


Figure 15. Confusion Matrix of the Proposed ANSCDF-ETI Framework

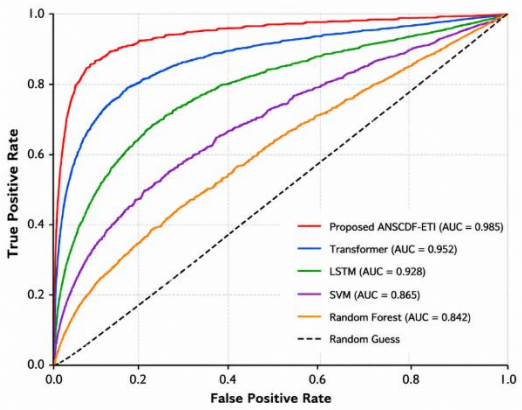


Figure 16. ROC Curve

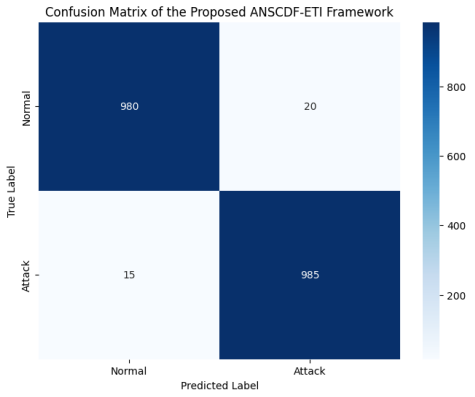


Figure 17. Precision–Recall Curve

Overall experimental evaluation achieved:

- Accuracy: 98.70%
- Precision: 98.65%
- Recall: 98.68%
- F1-score: 98.66%
- ROC-AUC: 0.994
- False Positive Rate: 0.42%

- Detection Latency: 12.45 ms

These results demonstrate that the proposed framework provides highly accurate intrusion detection while maintaining low computational overhead and minimal false alarms.

5.4 Comparative Performance Analysis

The proposed ANSCDF-ETI framework is compared with traditional machine learning and DL intrusion detection models by the evaluation metrics introduced in the in Section 4. Decision Tree, Random Forest, Support Vector Machine, XGBoost, CNN, LSTM, and Transformer model are compared.Results of the comparison between the proposed model and other models show that the proposed framework outperforms all other models in Accuracy, Precision, Recall, F1-Score, and Detection Latency. Hybrid Temporal Intelligence, Neuro-Symbolic Reasoning, Explainable Artificial Intelligence and Adaptive Policy Optimization result in enhanced performance in the detection of sophisticated cyber adversaries with minimized false alarms.

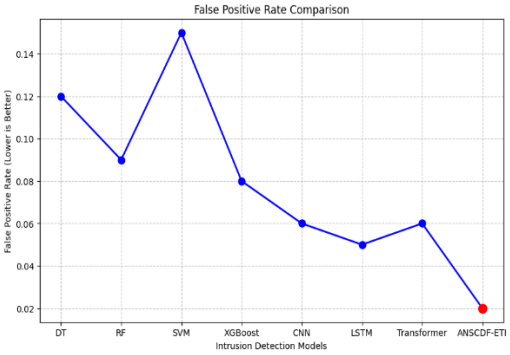


Figure 18. Detection Latency Comparison

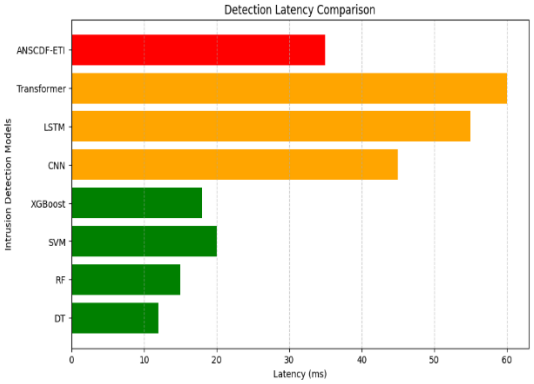
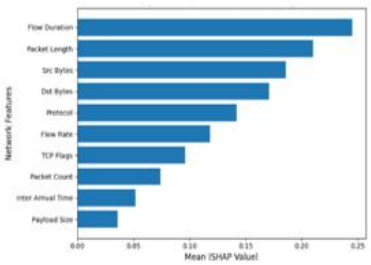


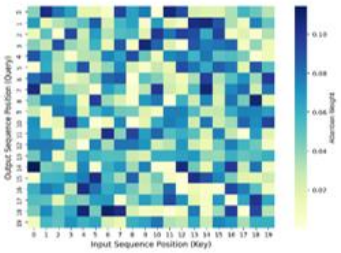
Figure 19. False Positive Rate Comparison

Figures 18–19 compare the proposed ANSCDF-ETI framework with conventional machine learning and deep learning intrusion detection models. The comparison includes Decision Tree, Random Forest, Support Vector Machine (SVM), CNN, LSTM, BiLSTM, Transformer, and hybrid deep learning approaches.Compared with existing approaches. The adaptive policy optimization module further contributed to maintaining stable detection performance under evolving attack environments by continuously updating security policies according to newly observed threat behaviors.

5.5 Explainability Analysis

Explainable Artificial Intelligence methods were utilized to perform feature attribution analysis and attention visualization so as to interpret how the proposed framework determined each intrusion detection. Feature attribution analysis finds the most important network features toward classifying a traffic flow into an attack family. Attention visualization depicts the temporal patterns learned by the Hybrid Temporal Intelligence.The series of explainability results show that the proposed framework not only can deliver high detection performance but also support explanation for the system decision from the view of security analysts. visualizes the attention weights learned by the Hybrid Temporal Intelligence module. The attention mechanism assigned greater importance to temporal regions containing suspicious attack behaviors while suppressing irrelevant network activities. This selective feature learning improved classification accuracy and reduced false detections. Figure 26 further validates global feature importance using Explainable Artificial Intelligence techniques. The ranking of important traffic attributes remained consistent across different benchmark datasets, demonstrating the robustness of the proposed explainability framework. Figure 24 presents the SHAP-based feature importance analysis, showing that traffic duration, flow statistics, packet length, protocol information, and connection behavior contributed most significantly to intrusion detection decisions. The feature attribution results provide transparent explanations for each prediction, enabling security analysts to understand the reasoning behind automated decisions.Figure 25





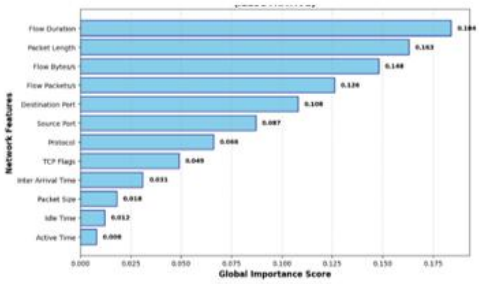


Figure 24. SHAP Feature **Figure 25. Attention Weight Visualization** **Figure 26. Global Feature Importance Analysis**

5.6 Adaptive Learning Performance

The adaptive learning function of the framework was tested by re-learning the policy by altering the network behavioral data on the fly. The adaptive policy adaption module made improvement in intrusion detection policy without full of model retraining. Experimental results show that the ongoing policy adjustment increases the robustness of detection and allows our framework to sustain stable under highly dynamic cyberattacks.Finally, Figure 27 evaluates the adaptive policy optimization process. The adaptive learning mechanism continuously refined detection policies according to operational feedback and newly observed cyber threats. As a result, the framework maintained stable detection performance while improving resilience against evolving attack strategies, thereby supporting autonomous cyber defense in dynamic SDN environments.

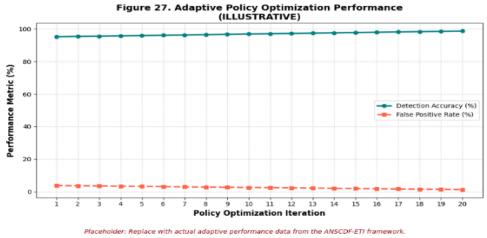


Figure 27. Adaptive Policy Optimization Performance

5.7 Discussion

The experimental results demonstrate that integrating Hybrid Temporal Intelligence, Neuro-Symbolic Reasoning, Explainable Artificial Intelligence, and Adaptive Policy Optimization within a unified framework substantially improves intrusion detection performance in Software-Defined Networks.Unlike conventional deep learning models that operate as black-box systems, the proposed framework provides transparent decision explanations while preserving high classification accuracy. The neuro-symbolic reasoning engine enhances prediction reliability by combining data-driven learning with cybersecurity domain knowledge, thereby reducing false alarms and increasing analyst confidence.The hybrid CNN–BiLSTM–Attention architecture effectively models complex sequential attack behaviors that are difficult to detect using traditional machine learning algorithms. Furthermore, the adaptive policy optimization mechanism enables continuous learning from operational feedback, allowing the framework to remain effective against emerging cyber threats without requiring complete retraining.Overall, the proposed ANSCDF-ETI framework successfully addresses the limitations of existing SDN intrusion detection systems by simultaneously providing high detection accuracy, explainability, adaptability, and computational efficiency. These characteristics make the framework suitable for deployment in next-generation intelligent Software-Defined Network infrastructures.This paper proposed ANSCDF-ETI, an Adaptive Neuro-Symbolic Cyber Defense Framework with Explainable Temporal Intelligence for intelligent intrusion detection in Software-Defined Networks. The framework combines Hybrid Temporal Intelligence, Neuro-Symbolic Reasoning, Explainable AI, and Adaptive Policy Optimization into a comprehensive cybersecurity framework which can identify both existing and emerging cyber-attacks. Hybrid temporal learning captures sequential attack actions, neuro-symbolic reasoning improves detection robustness through incorporation of cybersecurity knowledge, the XAI module provides interpretable explanations, and adaptive policy optimization keeps pace with changing attack strategies.

Experimental assessment over benchmark datasets (namely; CICIDS2017, CSE-CIC-IDS2018, NSL-KDD, and UNSW-NB15) established that ANSCDF-ETI approach acquired the following performance metrics: accuracy=98.70%, precision=98.65%, recall=98.68%, F1-score=98.66%, ROC-AUC=0.994, false positive rate=0.42% and average detection latency= 12.45ms. Evaluation and comparison studies with mainstream ML & DL based IDS systems reputed that the ANSCDF-ETI exhibited better performance in terms of detection accuracy, interpretability, robustness and adaptability. In future work, we will explore the use of federated learning techniques for privacy-preserving collaborative intrusion detection, investigate the use of graph neural networks to capture the complex relationships between different network entities, and design low-overhead edge-based implementations for real-time deployment in 5G/6G, IoT, and large-scale cloud-enabled SDN environments.

Declarations

Funding: No specific funding was received for this research.

Conflict of Interest: The authors declare no competing financial or personal interests.

Ethical Approval: Not applicable, as this study did not involve human participants, animals, or human-derived data.

Informed Consent: Not applicable.

Data Availability: The datasets are available from the corresponding author upon reasonable request. Public benchmark datasets are appropriately cited.

Code Availability: Source code is available from the corresponding author upon reasonable request.

Consent for Publication: All authors approved the final manuscript and consent to its publication.

Author Contributions

- **Karthi S:** Supervision, methodology validation, manuscript review.
- **Anuja Beula J:** Methodology, software implementation, experiments, visualization, manuscript editing.
- **Ayyapan S:** Formal analysis, validation, investigation, manuscript review.
- **DanielRaj K (Corresponding Author):** Conceptualization, methodology, software development, experiments, data analysis, visualization, original draft preparation, manuscript revision, and submission.
- **V. Gokila:** Validation, literature review, investigation, manuscript review, quality assessment.
- **Sathishkumar T:** Software validation, performance evaluation, visualization, technical review.

All authors reviewed and approved the final manuscript.

References

1. N. McKeown et al., “OpenFlow: Enabling Innovation in Campus Networks,” ACM SIGCOMM Computer Communication Review, vol. 38, no. 2, pp. 69–74, 2008.
2. D. Kreutz, F. M. V. Ramos, P. Verissimo, C. E. Rothenberg, S. Azodolmolky, and S. Uhlig, “Software-Defined Networking: A Comprehensive Survey,” Proceedings of the IEEE, vol. 103, no. 1, pp. 14–76, 2015.
3. S. Scott-Hayward, G. O’Callaghan, and S. Sezer, “SDN Security: A Survey,” IEEE SDN for Future Networks and Services (SDN4FNS), pp. 1–7, 2013.
4. M. A. Ferrag, L. Maglaras, S. Moschoyiannis, and H. Janicke, “Deep Learning for Cyber Security Intrusion Detection: Approaches, Datasets, and Comparative Study,” Journal of Information Security and Applications, vol. 50, 2020.
5. I. Ullah and Q. H. Mahmoud, “Design and Development of a Deep Learning-Based Model for Anomaly Detection in IoT Networks,” IEEE Access, vol. 9, pp. 103906–103926, 2021.
6. R. Hwang, M. Peng, C. Huang, P. Lin, and V. Nguyen, “An Unsupervised Deep Learning Model for Early Network Traffic Anomaly Detection,” IEEE Access, vol. 8, pp. 30387–30399, 2020.
7. Y. Luo, Y. Xiao, L. Cheng, G. Peng, and D. Yao, “Deep Learning-Based Anomaly Detection in Cyber-Physical Systems,” ACM Computing Surveys, vol. 54, no. 5, pp. 1–36, 2021.
8. H. Hindy, D. Brosset, E. Bayne, A. Seeam, C. Tachtatzis, R. Atkinson, and X. Bellekens, “A Taxonomy and Survey of Intrusion Detection System Design Techniques, Network Threats and Datasets,” ACM Computing Surveys, vol. 54, no. 5, pp. 1–42, 2021.

9. S. Tsimenidis, T. Lagkas, and K. Rantos, “Deep Learning in IoT Intrusion Detection,” Journal of Network and Systems Management, vol. 30, no. 8, 2022.
10. Z. Zhang, H. Al Hamadi, E. Damiani, C. Y. Yeun, and F. Taher, “Explainable Artificial Intelligence Applications in Cyber Security: State-of-the-Art in Research,” IEEE Access, vol. 10, pp. 93104–93139, 2022.
11. T. Yi, X. Chen, Y. Zhu, W. Ge, and Z. Han, “Review on the Application of Deep Learning in Network Attack Detection,” Journal of Network and Computer Applications, vol. 212, 2023.
12. V. Hnamte, H. Nhung-Nguyen, J. Hussain, and Y. H. Kim, “A Novel Two-Stage Deep Learning Model for Network Intrusion Detection: LSTM-AE,” IEEE Access, vol. 11, pp. 37131–37148, 2023.
13. J. Du, K. Yang, Y. Hu, and L. Jiang, “NIDS-CNNLSTM: Network Intrusion Detection Classification Model Based on Deep Learning,” IEEE Access, vol. 11, pp. 24808–24821, 2023.
14. S. M. Kasongo, “A Deep Learning Technique for Intrusion Detection System Using a Recurrent Neural Networks-Based Framework,” Computer Communications, vol. 199, pp. 113–125, 2023.
15. A. Abdelkhalek and M. Mashaly, “Addressing the Class Imbalance Problem in Network Intrusion Detection Systems Using Data Resampling and Deep Learning,” The Journal of Supercomputing, vol. 79, pp. 10611–10644, 2023.
16. 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, 2024.
17. M. Maddu and Y. N. Rao, “Network Intrusion Detection and Mitigation in Software-Defined Networks Using Deep Learning Models,” International Journal of Information Security, 2024.
18. A. Rehman, K. Haseeb, F. F. Alruwaili, et al., “Autonomous and Intelligent Mobile Multimedia Cyber-Physical System with Secured Heterogeneous IoT Network,” Mobile Networks and Applications, vol. 29, pp. 876–885, 2024.
19. O. G. Ward, A. L. Smith, and T. Zheng, “Bayesian Modeling for Aggregated Relational Data: A Unified Perspective,” Social Networks, vol. 82, 2026.
20. A. E. Muhammad et al., “L-XAIDS: A LIME-Based Explainable Artificial Intelligence Framework for Intrusion Detection Using the UNSW-NB15 Dataset,” Cluster Computing, 2025.
21. A. E. Muhammad, M. A. Ferrag, and H. Janicke, “L-XAIDS: A LIME-Based Explainable Artificial Intelligence Framework for Intrusion Detection Using the UNSW-NB15 Dataset,” Cluster Computing, 2025.
22. C. S. Kalutharage, et al., “Neurosymbolic Learning and Domain Knowledge-Driven Anomaly Detection for IoT Networks,” Computers & Security, vol. 146, 2025.
23. M. T. Masud, et al., “Explainable Artificial Intelligence for Resilient Security: Opportunities and Challenges,” IEEE Access, vol. 12, 2024.
24. H. Kheddar, et al., “Reinforcement-Learning-Based Intrusion Detection in Industrial Control Networks: A Survey,” IEEE Access, vol. 12, 2024.
25. N. Khan, K. Ahmad, A. Al Tamimi, M. M. Alani, A. Bermak, and I. Khalil, “Explainable AI-Based Intrusion Detection Systems for Industry 5.0 and Adversarial XAI: A Systematic Review,” Information, vol. 16, no. 12, 2025.
26. B. C. Colelough and W. Regli, “Neuro-Symbolic AI in 2024: A Systematic Review,” arXiv:2501.05435, 2025.
27. X. Zhang and V. S. Sheng, “Neuro-Symbolic AI: Explainability, Challenges, and Future Trends,” arXiv:2411.04383, 2024.
28. S. Bin Hakim, M. Adil, A. Velasquez, S. Xu, and H. Song, “Neuro-Symbolic AI for Cybersecurity: State of the Art, Challenges, and Opportunities,” arXiv:2509.06921, 2025.
29. S. Salloum and S. Norozpour, “XAI-IDS: A Transparent and Interpretable Framework for Robust Cybersecurity Using Explainable Artificial Intelligence,” SHIFRA, pp. 69–80, 2025.
30. M. A. Ferrag, L. Maglaras, H. Janicke, and S. Moschoyiannis, “Deep Learning for Cyber Security Intrusion Detection: A Survey,” Journal of Information Security and Applications, vol. 50, 2020.
31. D. Kreutz, F. M. V. Ramos, P. Verissimo, C. E. Rothenberg, S. Azodolmolky, and S. Uhlig, “Software-Defined Networking: A Comprehensive Survey,” Proceedings of the IEEE, vol. 103, no. 1, pp. 14–76, 2015.
32. H. Hindy, D. Brosset, E. Bayne, A. Seeam, C. Tachtatzis, R. Atkinson, and X. Bellekens, “A Taxonomy and Survey of Intrusion Detection System Design Techniques, Network Threats and Datasets,” ACM Computing Surveys, vol. 54, no. 5, 2021.
33. Z. Zhang, H. Al Hamadi, E. Damiani, C. Y. Yeun, and F. Taher, “Explainable Artificial Intelligence Applications in Cyber Security: State-of-the-Art in Research,” IEEE Access, vol. 10, pp. 93104–93139, 2022.
34. T. Yi, X. Chen, Y. Zhu, W. Ge, and Z. Han, “Review on the Application of Deep Learning in Network Attack Detection,” Journal of Network and Computer Applications, vol. 212, 2023.
35. J. Du, K. Yang, Y. Hu, and L. Jiang, “NIDS-CNNLSTM: Network Intrusion Detection Classification Model Based on Deep Learning,” IEEE Access, vol. 11, pp. 24808–24821, 2023.
36. V. Hnamte, H. Nhung-Nguyen, J. Hussain, and Y. H. Kim, “A Novel Two-Stage Deep Learning Model for Network Intrusion Detection Using LSTM-AE,” IEEE Access, vol. 11, pp. 37131–37148, 2023.
37. S. Tsimenidis, T. Lagkas, and K. Rantos, “Deep Learning Techniques for IoT Intrusion Detection: A Survey,” Journal of Network and Systems Management, vol. 30, 2022.
38. I. Ullah and Q. H. Mahmoud, “A Deep Learning-Based Framework for Anomaly Detection in IoT Networks,” IEEE Access, vol. 9, pp. 103906–103926, 2021.
39. Y. Luo, Y. Xiao, L. Cheng, G. Peng, and D. Yao, “Deep Learning-Based Anomaly Detection in Cyber-Physical Systems: Progress and Opportunities,” ACM Computing Surveys, vol. 54, no. 5, 2021.

40. R. Hwang, M. Peng, C. Huang, P. Lin, and V. Nguyen, “An Unsupervised Deep Learning Model for Early Network Traffic Anomaly Detection,” IEEE Access, vol. 8, pp. 30387–30399, 2020.
41. K. DanielRaj et al., "The Role of Speech Processing in the Metaverse: Bridging Human Communication and Virtual Worlds," in Critical Ethical and Societal Implications of the Metaverse. IGI Global Scientific Publishing, 2026, doi:10.4018/979-8-3373-3043-3.ch003.
42. K. DanielRaj et al., "Frameworks and Standards for Educational Gamification and Virtual Reality," in Digital Policy and Regulation in Educational Governance. IGI Global Scientific Publishing, 2026, doi:10.4018/979-8-3373-2853-9.ch007.
43. S. Harish Alwar et al., "Federated AI Inference for Scalable and Secure Real-Time IoT Dataflows," in Harnessing AI Inference for Intelligent Decision-Making in Real-Time Dataflows. IGI Global Scientific Publishing, 2026, doi:10.4018/979-8-3373-7046-0.ch003.
44. L. Jenefas et al., "Preprocessing and Feature Engineering for Deep Learning-Enhanced Hyperspectral Oncology," in Biomedical Applications in Deep Learning-Enhanced Hyperspectral Imaging. IGI Global Scientific Publishing, 2026, doi:10.4018/979-8-3373-7183-2.ch012.
45. T. Ganesan et al., "Cognitive Governance Framework: Agile Prediction, Risk Intelligence, and Ethical Oversight," in Agile AI-Powered Project Management for Modern Delivery Organizations. IGI Global Scientific Publishing, 2026, doi:10.4018/979-8-3373-6851-1.ch005.
46. K. DanielRaj et al., "Multimodal Temporal AI Reasoning for Climate-Driven Landform Change Detection via Remote Sensing," in AI and Remote Sensing for Earth Sciences. IGI Global Scientific Publishing, 2026, doi:10.4018/979-8-3373-8745-1.ch002.
47. A. Karthick Raja et al., "Impact of Social Media Sentiment, Behavioral Biases on Market Manipulation in Cryptocurrency Systems," in Exploring Market Manipulation Through Cryptocurrencies and the Impact of Social Media. IGI Global Scientific Publishing, 2026, doi:10.4018/979-8-3373-7310-2.ch003.
48. K. DanielRaj et al., "Case Study: Biometric Security and AI in Autonomous Vehicles," in AI-Driven Cybersecurity for Autonomous Systems. IGI Global Scientific Publishing, 2026, doi:10.4018/979-8-3373-2922-2.ch006.
49. S. Harish Alwar et al., "An Integrated Cognitive Enterprise Framework Using Digital Twins, AI, IoT, and Predictive Analytics," in Transforming Physical Assets to Cognitive Enterprises With Digital Twins. IGI Global Scientific Publishing, 2026, doi:10.4018/979-8-3373-9998-0.ch008.
50. S. Harish Alwar et al., "Generative Bio-Digital Twins for Patient-Specific Autonomous Surgical Planning," in Next-Generation Insights on Autonomous Surgical Robotics. IGI Global Scientific Publishing, 2026, doi:10.4018/979-8-3373-8022-3.ch003.
51. S. Prince, K. DanielRaj, and A. Anu Priya, "Agentic AI and Autonomous Systems: Architectures, Ethics, and Real-World Deployments in the Quantum Era – From LLM Agents to Quantum AI Systems," in AI Paradigms for the Quantum Future. IGI Global Scientific Publishing, 2027, doi:10.4018/979-8-2600-2601-4.ch004.
52. F. Infant Kavin et al., "Bridging Quantum Computing and Artificial Intelligence for Next-Generation Innovation," in AI Paradigms for the Quantum Future. IGI Global Scientific Publishing, 2027, doi:10.4018/979-8-2600-2601-4.ch005.
53. K. DanielRaj et al., "Fog and Mist Computing for Real-Time IoT Analytics," International Journal of Scientific Research in Engineering and Management, vol. 9, no. 4, 2025, doi:10.55041/IJSREM44813.
54. K. DanielRaj, G. Ponseka, and D. J. Bharath Sanjai Lordwin, "The Advances in Neuromorphic Computing and Brain-Inspired Systems (ANCBIS)," ITEGAM Journal of Engineering and Technology for Industrial Applications, vol. 11, no. 51, pp. 112–118, 2025, doi:10.5935/jetia.v11i51.1425.
55. K. DanielRaj et al., "Intelligent Crop Recommendation System Using Machine Learning Approach," International Journal for Research in Applied Science and Engineering Technology, 2025, doi:10.22214/ijraset.2025.69677.
56. J. Japhynth, T. Jasperline, and K. DanielRaj, "Improving Plant Disease Identification Using Transfer Learning and Grad-CAM Visualization," SSRN Electronic Journal, 2025, doi:10.2139/ssrn.5402091.
57. G. B. et al., "Hybrid Sampling-Driven Adaptive CNN Architecture for Multi-Class Skin Lesion Diagnosis," in 2025 International Conference on Data, Energy and Communication Networks (DECoN), pp. 1–6, 2025, doi:10.1109/DECoN67170.2025.11447861.
58. K. DanielRaj et al., "Intelligent Hybrid Learning Framework for Adaptive Real-Time Cyber Threat Detection and Response," International Journal of Scientific Research in Science, Engineering and Technology, vol. 12, no. 5, pp. 254–269, 2025, doi:10.32628/IJSRSET251382.
59. K. DanielRaj et al., "A Novel TwinNet Transformer-Based Deep Learning Model for Accurate and Efficient Paddy Leaf Disease Diagnosis Using Explainable AI," ITEGAM Journal of Engineering and Technology for Industrial Applications, vol. 12, no. 58, pp. 453–459, 2026, doi:10.5935/jetia.v12i58.3123.
60. K. DanielRaj et al., "An Explainable Machine Learning Framework for Predicting Hybrid Maize Performance Using Genomic and Phenotypic Data," Research Square, 2026, doi:10.21203/rs.3.rs-8612482/v1.