applied sciences

MDPI

Article

An AI-Driven LSTM–Fuzzy Framework for Adaptive DDoS Detection in Cyber–Physical Systems (CPSs)

Hakan Aydin

Department of Computer Engineering, Faculty of Engineering and Natural Sciences, İstanbul Topkapı University, Istanbul 34310, Turkey; hakanaydin@topkapi.edu.tr

Abstract

Cyber–Physical Systems (CPSs) are increasingly vulnerable to Distributed Denial-of-Service (DDoS) attacks, which can disrupt critical operations and compromise system safety. Although deep learning (DL) techniques are widely adopted for cyberattack detection, conventional DL-based classifiers often struggle to handle the uncertainty and ambiguity inherent in network traffic data. To address this limitation, this paper proposes an AI-driven hybrid framework, termed LSTM–Fuzzy–CPS, for adaptive DDoS detection in CPS environments. Unlike prior LSTM–Fuzzy approaches that are primarily restricted to SDN settings, the proposed framework is adapted for CPS environments and introduces continuous risk scoring, reduced false positives for safety-critical operation, and proportional mitigation mechanisms. The framework consists of a detection module and a conceptual mitigation module. The detection module, named LSTM–Fuzzy–Detector, integrates an LSTM network with a Mamdani-type fuzzy inference system that maps LSTM outputs into a continuous risk score using triangular membership functions (Low, Medium, High) and centroid defuzzification. The mitigation module is designed as a rule-based conceptual framework that translates risk levels into adaptive response actions; however, its experimental implementation is left for future work. The proposed detector is evaluated on the CICIoT2023 dataset and achieves an accuracy of 99.83% with a false-positive rate of 0.12%, demonstrating strong robustness against complex and evolving attack patterns. These results indicate that the proposed framework provides an effective, interpretable, and scalable solution for intelligent threat detection in CPS environments.

Keywords: Cyber–Physical Systems (CPS); DDoS detection; LSTM; fuzzy logic; cyber resilience

Check for updates

Academic Editor: Christos Bouras

Received: 21 April 2026
Revised: 21 May 2026
Accepted: 24 May 2026
Published: 16 June 2026

Copyright: © 2026 by the author. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license.

1. Introduction

Cyber–Physical Systems (CPSs) integrate computational intelligence with physical processes across critical domains such as industrial automation, energy systems, transportation, and healthcare [1]. While this tight integration enhances efficiency and automation, it also introduces significant security vulnerabilities at the interface of cyber and physical components [2]. Unlike traditional IT systems, attacks on CPSs may directly affect physical processes due to their tight coupling with sensing and actuation mechanisms. This can result in equipment damage, operational disruptions, or safety-critical failures [3]. Although the confidentiality, integrity, and availability (CIA) triad remains a cornerstone of cybersecurity [4], availability is particularly critical in CPSs, where service disruption can lead to severe real-world consequences.

Among emerging threats, Distributed Denial-of-Service (DDoS) attacks represent a major risk to CPS environments [5]. By overwhelming network resources with excessive traffic, such attacks can delay or block communication between sensors, controllers, and actuators, thereby degrading system performance or causing operational failure [6]. The scale and intensity of DDoS attacks have increased significantly in recent years, with reported peak traffic exceeding 31.4 Tbps in 2025, highlighting the growing capability of large-scale coordinated attacks targeting networked systems. This trend is illustrated in Figure 1 [7].

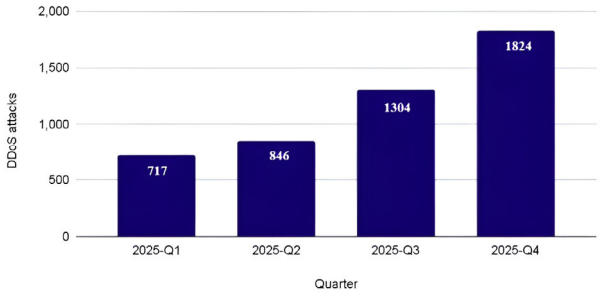


Figure 1. Growth of large-scale DDoS attack volumes between 2020 and 2025 [7].

To address these challenges, machine learning and deep learning approaches have been widely adopted for intrusion detection in CPS and IoT systems [8]. In particular, Long Short-Term Memory (LSTM) networks are effective in capturing temporal dependencies in network traffic [9]. However, existing LSTM-based intrusion detection systems typically rely on binary classification or fixed decision thresholds, which may struggle to handle the uncertainty, ambiguity, and gradual evolution of traffic patterns in CPS environments [10]. Recent studies further demonstrate the effectiveness of deep learning approaches in IoT intrusion detection systems, particularly in improving detection accuracy for complex and high-dimensional network traffic [11].

To overcome these limitations, this paper proposes an AI-driven hybrid framework, LSTM–Fuzzy–CPS, for adaptive DDoS detection and resilience enhancement in CPS environments. The proposed framework integrates an LSTM-based model with a fuzzy inference system to enable uncertainty-aware risk assessment and multi-level traffic classification. Unlike conventional binary approaches, the fuzzy layer models traffic behavior using graded risk levels (e.g., benign, suspicious, malicious), enabling more flexible and interpretable decision-making.

In addition to detection, the framework incorporates an adaptive mitigation mechanism that translates fuzzy risk levels into dynamic response actions, such as traffic regulation, prioritization, and anomaly isolation. This integration of detection and response supports cyber resilience by enabling CPSs to maintain operational continuity under attack conditions. Unlike prior LSTM–Fuzzy works (e.g., Novaes et al.'s [12], which focused on SDN environments), this paper makes three CPS-focused contributions: (1) the adaptation of LSTM–Fuzzy to CPS traffic with explicit consideration of real-time, safety-critical false positive avoidance; (2) a continuous risk score instead of binary output, critical for avoiding harmful false positives in physical systems; (3) a proportional mitigation framework mapping fuzzy risk levels to graded responses.

The main contributions of this study are summarized as follows:

- A hybrid LSTM–Fuzzy framework (LSTM–Fuzzy–CPS) for uncertainty-aware DDoS detection in CPS environments;
- A novel detection model (LSTM–Fuzzy–Detector) that captures ambiguous and evolving traffic patterns while reducing false positives;

- The fuzzy layer replaces binary classification with a continuous risk score using membership functions (Low, Medium, High) and rule-based inference;
- An adaptive mitigation mechanism incorporating a rule-based "safe list" strategy for dynamic response;
- A comprehensive evaluation on the CICIoT2023 dataset, including accuracy and computational performance analysis.

The remainder of this paper is organized as follows. Section 2 reviews related work. Section 3 presents the materials and methods. Section 4 describes the proposed methodology. Section 5 reports experimental results. Section 6 provides discussion, and Section 7 concludes the paper.

2. Materials and Methods

This study utilizes the CICIoT2023 dataset, which is publicly available through the Canadian Institute for Cybersecurity (CIC) repository [13]. To address class imbalance, a stratified subsample with approximately 40% benign and 60% attack traffic was used. All experiments were conducted in a standard cloud-based computing environment. Preprocessing involved the removal of missing values and duplicate records. A set of network flow features was selected, including packet rate, inter-arrival time, flow duration, source/destination IP addresses and ports, bandwidth consumption, and protocol type. All features were normalized, and sequential samples were generated using a sliding window approach. The dataset was partitioned into training, validation, and test sets via stratified sampling. To ensure transparency, the reduced-sample dataset consisted of 52,000 network flows, with 40% being benign traffic and 60% being attack traffic. All 33 DDoS attack categories from the original CICIoT2023 dataset were retained. Features included packet rate, inter-arrival time, flow duration, bandwidth consumption, protocol type, entropy-based IP and port features, packet length statistics, and TCP flag counts. Source and destination IP addresses are included as input features for contextual information. However, the fuzzy inference engine does not directly operate on IP addresses; instead, it uses three abstract traffic attributes (traffic intensity, temporal irregularity, bandwidth consumption) derived from LSTM hidden states. The model is designed to prioritize behavioral patterns over endpoint identifiers, but we acknowledge that IP information may indirectly influence the learned LSTM representations. An IP-independent evaluation is planned for future work to verify generalization. Sequential samples were generated using a sliding window approach with a window size of 10 time steps. During preprocessing, duplicate records were removed, and feature normalization was performed using only statistics from the training set to prevent data leakage.

The proposed hybrid model integrates an LSTM network with a Mamdani-type fuzzy inference system. The LSTM architecture consists of multiple hidden layers with dropout regularization. The network was trained using a standard optimizer with binary cross-entropy loss, and early stopping was applied to prevent overfitting. The LSTM output is fed into the fuzzy inference system, which employs triangular membership functions (Low, Medium, High) and centroid defuzzification to produce a continuous risk score. Hyperparameters were optimized via grid search, and the best-performing configuration was selected based on validation performance. The dataset was split into training (70%), validation (15%), and test (15%) sets using stratified sampling. Grid search optimization of the fuzzy inference engine parameters was performed using validation set accuracy as the primary metric.

3. Related Work on Deep Learning and Fuzzy Logic-Based IDS

CPS are increasingly exposed to cyber threats due to the tight integration of computational and physical processes [1]. Among these threats, DDoS attacks are particularly critical as they can disrupt real-time communication between sensors, actuators, and controllers [14]. Recent studies have widely explored deep learning approaches for intrusion detection. LSTM-based and hybrid architectures have shown strong performance in modeling temporal dependencies in network traffic.

For example, Kodyš et al. [15] proposed a deep learning-based intrusion detection approach for IoT environments using convolutional neural networks, demonstrating that deep architectures significantly improve detection capability for complex and high-dimensional network traffic patterns. Similarly, Javaid et al. [16] introduced a deep learning-based intrusion detection framework showing that neural network-based models can significantly enhance detection performance compared to traditional machine learning approaches, particularly in high-dimensional network traffic environments. A recent benchmark study by Afraji et al. [17] further confirmed that hybrid deep learning architectures such as CNN–LSTM–GRU achieve state-of-the-art performance (above 99% accuracy) on IoT intrusion detection datasets, demonstrating the superiority of hybrid models in capturing both spatial and temporal dependencies in network traffic.

Despite these promising results, most LSTM-based intrusion detection systems rely on binary classification or fixed thresholds, which limit their ability to model uncertain or evolving traffic patterns in CPS environments. In parallel, fuzzy logic has been widely adopted to address uncertainty in control and decision systems by enabling graded reasoning rather than hard class boundaries. However, its integration with deep learning models for CPS-specific intrusion detection remains limited. Fuzzy-based approaches assign membership degrees to multiple classes, enabling more flexible and interpretable decision-making under uncertainty. In this context, Novaes et al. [12] proposed an LSTM–Fuzzy model for anomaly detection in SDN environments, demonstrating strong performance on the CICDDoS2019 dataset. However, their approach does not explicitly address CPS-specific safety constraints.

Table 1 summarizes representative deep learning and LSTM-based intrusion detection studies, highlighting their reported performance and computational metrics where available.

The comparative analysis highlights several research gaps. First, existing LSTM-based intrusion detection systems typically rely on binary classification or fixed thresholds, which limit their ability to model ambiguous and evolving traffic patterns in CPS environments. Second, although fuzzy logic has proven effective in handling uncertainty in control systems [27], its integration with deep learning for CPS-oriented DDoS detection remains underexplored. Third, despite high reported accuracies on the CICIoT2023 dataset, most studies do not incorporate fuzzy-based risk modeling for graded decision-making. Finally, computational efficiency metrics such as training and inference time are often omitted, even though they are critical for real-time CPS deployment.

In contrast, the proposed approach employs fuzzy membership functions (Low, Medium, High) to transform LSTM outputs into a continuous risk score instead of a binary prediction. To address the identified limitations, we introduce the LSTM–FUZZY–CPS framework, which integrates deep temporal feature learning with fuzzy uncertainty modeling and supports both detection and risk-aware interpretation for CPS environments.

The studies by Jony and Arnob [24], Gueriani et al. [25], and Lilhore et al. [26] also utilized the CICIoT2023 dataset with LSTM-based architectures. However, unlike the proposed method, none of these approaches integrates fuzzy logic with LSTM for uncertainty-aware DDoS detection. Comparative results show that the proposed LSTM–Fuzzy–Detector

(99.83% accuracy) outperforms these prior LSTM-based methods (98.75%, 98.42%, and 96.21%, respectively) on the same dataset. Overall, the results confirm that the proposed fuzzy-enhanced LSTM model improves detection performance while additionally enabling continuous risk scoring and enhanced interpretability.

Table 1. Studies utilizing deep learning and LSTM-based methods for intrusion detection on CICIoT2023 and related datasets.

Reference	Method	Dataset	Accuracy
Kodyš et al. [15]	Deep Learning IDS (CNN)	IoT Environments	N/A
Javaid et al. [16]	Deep Learning IDS Framework	Network Traffic	N/A
Afraji et al. [17]	CNN-LSTM-GRU	IoT Intrusion Datasets	>99
Al-Ghamdi and Alansari [18]	CNN-RNN Comparative Model	CICIoT2023	94.8–97.5
Alashjaee [19]	Attention-based CNN-LSTM Hybrid IDS	NSL-KDD, Bot-IoT	94.8–97.5
Hoummady and Jaafar [20]	Stacked LSTM	CICIoT2023	99.3
Hizal et al. [21]	Two-Stage LSTM/DNN/CNN	CICIoT2023	>95
Ain et al. [22]	CNN-LSTM-Autoencoder	CICIoT2023	96.78
Khanday et al. [23]	1D-CNN	CICIoT2023	99.87
Novaes et al. [12]	LSTM–FUZZY	CICDDoS2019, Mininet	>96
Jony and Arnob [24]	LSTM	CICIoT2023	98.75%
Gueriani et al. [25]	CNN-LSTM	CICIoT2023	98.42%
Lilhore et al. [26]	LSTM-CNN	CICIoT2023	96.21%
This study	LSTM–FUZZY–CPS (LSTM–Fuzzy–Detector)	CICIoT2023	99.83

4. DDoS Attack Landscape and CPS Security Challenges

CPS integrates computation, communication, and control across critical domains such as power grids, industrial automation, healthcare, and transportation [1]. Unlike traditional IT systems, where cyberattacks mainly affect data and services, attacks on CPS can directly manipulate physical processes, potentially causing equipment damage, operational disruption, or safety-critical failures [28]. Among various cyber threats, DDoS attacks represent a major risk to CPS due to their ability to disrupt communication between distributed components [14]. Attackers typically use botnets to generate high-volume traffic that exhausts network resources, preventing normal system operation. Recent studies indicate that adaptive and intelligent DDoS attacks, which adjust their behavior based on system responses, may cause more severe impacts than traditional brute-force approaches [29,30].

Several structural and operational characteristics increase CPS vulnerability to DDoS attacks. Attackers take advantage of these weaknesses to infiltrate the Industrial Control System (ICS) environment, including specific components such as Supervisory Control and Data Acquisition (SCADA), Programmable Logic Controller (PLC), Distributed Control System (DCS), Remote Terminal Unit (RTU), Human–Machine Interface (HMI), and Master

Terminal Unit (MTU) [31]. The impact of DDoS attacks extends beyond network degradation. In smart grid systems, delayed or blocked control signals may lead to instability and cascading outages [32]. In healthcare applications, compromised networked medical devices can pose direct risks to patient safety [33]. DDoS attacks cause extended service outages and revenue loss to organizations that rely heavily on digital infrastructure [34].

Given these challenges, robust and adaptive intrusion detection mechanisms are essential for CPS security. Although machine learning-based approaches have demonstrated high detection performance, often exceeding 99% accuracy in controlled environments, many existing models rely on binary classification or static thresholds [35]. This limits their ability to handle ambiguous and evolving attack behaviors. These limitations motivate the need for adaptive, uncertainty-aware detection frameworks, such as the LSTM–Fuzzy logic approach proposed in this study.

5. The Proposed LSTM–Fuzzy–CPS System

5.1. The Proposed LSTM–Fuzzy–CPS System Architecture

This section presents the proposed LSTM–Fuzzy–CPS framework, a hybrid detection and mitigation system designed for CPS. Unlike conventional IT networks, CPS integrates computational processes with physical components such as sensors, actuators, and controllers, where communication delays or disruptions may directly impact physical operations. In this context, DDoS attacks can severely degrade system reliability by generating excessive malicious traffic. In addition, ambiguous or borderline traffic patterns often lead to misclassification in traditional intrusion detection systems, increasing the risk of false alarms and unnecessary control actions. To address these limitations, the proposed framework combines LSTM networks for temporal feature learning with fuzzy logic for uncertainty handling. The overall system consists of two main components: a detection module (LSTM–Fuzzy–Detector) and a mitigation module (Defense Engine). The LSTM component captures sequential traffic dependencies, while the fuzzy inference layer provides graded risk assessment under uncertain or evolving traffic conditions.

Figure 2 illustrates the overall architecture of the proposed system.

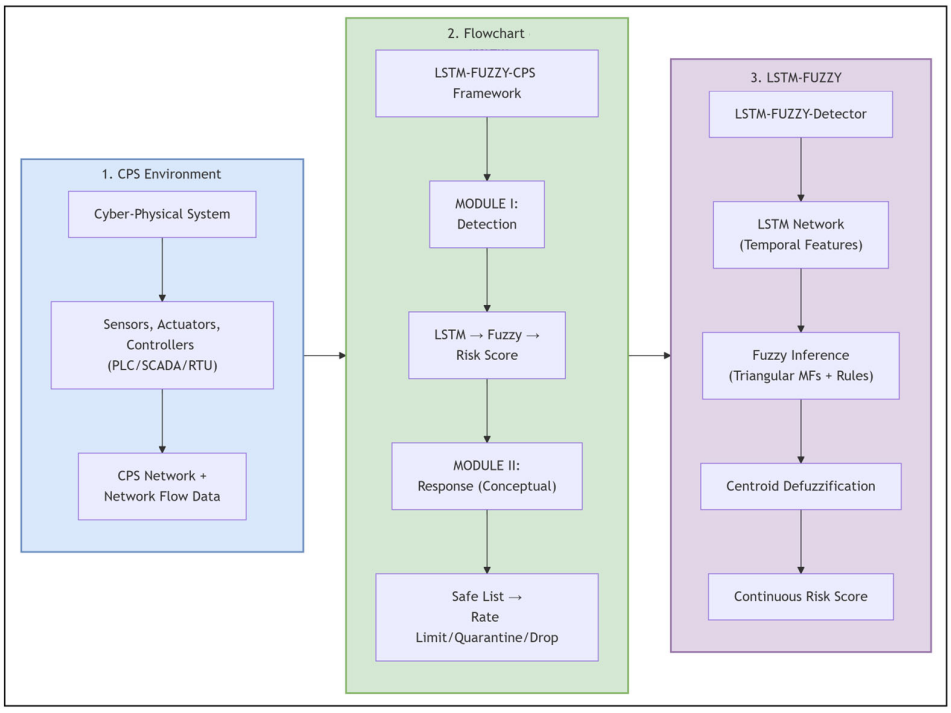


Figure 2. The proposed system architecture.

5.2. Detection Module (LSTM–Fuzzy–DETECTOR)

The detection module analyzes incoming network traffic and produces a continuous fuzzy risk score instead of a binary decision. It consists of two integrated components: an LSTM-based feature extractor and a fuzzy inference engine. The LSTM component processes sequential network flow data, including packet rate, flow duration, source and destination IP addresses, and port information. By learning temporal dependencies, it captures both short- and long-term traffic patterns in CPS environments. The output is a compact representation of hidden state features describing current traffic behavior. These features are then passed to the fuzzy inference engine rather than to a conventional softmax classifier. Specifically, the LSTM hidden state at each time step is passed through a small dense layer that maps the high-dimensional representation to three scalar values corresponding to traffic intensity, temporal irregularity, and bandwidth consumption. The temporal irregularity feature internally captures inter-arrival time patterns derived from LSTM-based temporal representations. All three scalar values are used as direct inputs to the fuzzy inference engine. Therefore, the fuzzy inference system operates with three input variables: traffic intensity, temporal irregularity, and bandwidth consumption. These scalars are then fed into the fuzzy inference engine.

Fuzzy logic integration is implemented at three critical stages. First, three key traffic attributes derived from the LSTM hidden states—traffic intensity, temporal irregularity, and bandwidth consumption—are selected as fuzzy inputs. Second, each attribute is fuzzified using triangular membership functions (Low, Medium, High). Unlike crisp sets, these membership functions allow a single numerical input to belong to multiple linguistic categories simultaneously, with varying degrees of membership between 0 and 1. For example, a bandwidth value may be 30% Low and 70% Medium. This property explicitly models the ambiguity and gradual transitions inherent in CPS network traffic, where the boundary between normal and anomalous behavior is often unclear. Third, a Mamdani-type rule base containing nine if-then rules (selected based on expert knowledge to cover the most relevant traffic scenarios) maps the fuzzified inputs to a fuzzy output set. A representative rule is as follows: IF traffic intensity is High AND temporal irregularity is Irregular AND bandwidth consumption is Critical THEN attack risk is Very High. The fuzzy inference engine aggregates all activated rules using the max-min composition method. Finally, centroid defuzzification converts the aggregated fuzzy output into a single continuous risk score normalized between 0 and 1.

This design replaces the conventional binary decision boundary with a graded risk spectrum, enabling the model to distinguish not only between benign and malicious traffic but also between varying degrees of suspicion (e.g., low, medium, high risk). Consequently, the fuzzy layer acts as an interpretable (explainable AI), uncertainty-aware decision module that complements the LSTM's temporal feature extraction capability. The overall approach reduces the impact of sharp decision boundaries and improves robustness against noisy, ambiguous, or gradually evolving traffic patterns commonly observed in CPS environments.

5.3. Defense Module (Mitigation Engine)

The defense module described in this section is a conceptual design intended to illustrate how the continuous risk score produced by the LSTM–Fuzzy–Detector could be mapped to response actions. Experimental validation of this mitigation module is beyond the scope of this paper and is left for future work focused on real CPS deployment. Based on the fuzzy risk score produced by the detection module, the defense module applies graded mitigation actions. Instead of executing a binary block-or-pass decision, the system implements proportional responses, including rate-limiting, temporary quarantine, or alert generation, only when the risk score exceeds a dynamic confidence threshold. This strategy

minimizes disruption to legitimate CPS operations, for example, by avoiding unnecessary shutdown of a physical actuator. Additionally, the defense module logs suspicious flows and updates a blacklist with known attack signatures for future reference. The process is as follows:

- Suspicious Flow Identification: When an alarm is triggered, the system identifies suspect flows based on IP addresses and ports within the anomalous interval. A "Safe List" of known legitimate IPs/ports is checked before any action.
- DDoS Attack Mitigation: If a DDoS attack is confirmed, flows are discarded based on source IP addresses that appear most frequently and share the same destination port.
- Portscan Mitigation: For a Portscan attack, the source IP address presenting the most variety in destination ports is identified as the attacker, and all its flows are dropped.

This structured approach ensures that legitimate CPS operations (e.g., a control loop) are not interrupted by a false positive.

5.4. The LSTM–Fuzzy–DETECTOR Model

This subsection describes the LSTM–Fuzzy–Detector model developed for use in the detection module of the proposed LSTM–Fuzzy–CPS system. Unlike conventional LSTM-based intrusion detection systems that produce binary (attack/normal) outputs, the proposed model integrates a fuzzy inference engine to generate a continuous risk score. This approach is particularly suitable for CPS, where network traffic often exhibits ambiguous characteristics and false positives may lead to unnecessary physical interventions or system downtime. The core of the LSTM–Fuzzy–Detector consists of a deep LSTM network responsible for extracting temporal features from sequential CPS network traffic data.

Figure 3 presents the layer-wise architecture of the proposed LSTM–Fuzzy–Detector. The input layer receives network flow features, which are then processed by two LSTM layers with 64 and 32 units, respectively, to extract temporal dependencies. The extracted features are fed into a fuzzy inference engine that applies triangular membership functions (Low, Medium, High) and centroid defuzzification to produce a continuous risk score between 0 and 1.

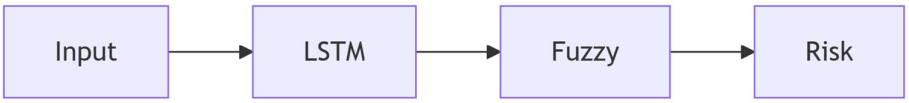


Figure 3. Layer-wise architecture of the LSTM–Fuzzy–Detector.

The LSTM architecture, originally introduced by Hochreiter and Schmidhuber [36], is a special type of Recurrent Neural Network (RNN) capable of learning long-term dependencies. This capability is essential for detecting DDoS attacks in CPS environments, where attack patterns may unfold over extended periods and normal traffic exhibits complex temporal dynamics. Each LSTM cell contains three gates that regulate the flow of information: the forget gate (f_t), the input gate (i_t), and the output gate (o_t). These gates collectively enable the network to selectively remember or discard information over time. The forget gate determines which information from the previous cell state (C_{t-1}) should be discarded. This operation is governed by Equation (1):

$$ft = \sigma(Wf \cdot [ht - 1, xt] + bf) \quad (1)$$

where h_{t-1} is the hidden state and x_t is the current input at time step t, Wf and bf are the weight matrix and bias, respectively, and σ denotes the sigmoid activation function producing values between 0 and 1. A value approaching 1 indicates that the information should be retained, while a value approaching 0 indicates it should be forgotten.

The input gate decides which new information to store in the cell state. This involves two sub-steps: first, the input gate layer determines which values to update (Equation (2)); second, a tanh layer creates candidate values (C_t) to add to the state (Equation (3)):

$$it = \sigma(Wi \cdot [ht - 1, xt] + bi) \quad (2)$$

$$C \sim t = \tanh(Wc \cdot [ht - 1, xt] + bc) \quad (3)$$

The cell state is then updated by combining the forgotten previous state and the new candidate information (Equation (4)):

$$Ct = ft \times Ct - 1 + it \times C \sim t \quad (4)$$

Finally, the output gate determines the next hidden state based on the updated cell state (Equations (5) and (6)):

$$ot = \sigma(Wo \cdot [ht - 1, xt] + bo) \quad (5)$$

$$ht = ot \times \tanh(Ct) \quad (6)$$

In the proposed LSTM–Fuzzy–Detector, the LSTM network processes sequential network flow data, including packet rates, inter-arrival times, flow durations, and source/destination IP addresses and ports collected from the CPS environment. The hidden state outputs h_t at each time step serve as feature vectors that capture the temporal characteristics of the traffic. These feature vectors are then passed to the fuzzy inference engine rather than being directly classified by a dense layer with softmax activation.

The extracted LSTM features are fed into a fuzzy logic system designed to handle uncertainty and ambiguity in CPS network traffic. The model has been designed to capture general traffic behavior patterns, such as temporal irregularities and variations in traffic intensity, rather than relying solely on specific endpoint identifiers. Source and destination IP addresses are included as input features for contextual information. However, the fuzzy inference engine does not directly operate on IP addresses; instead, it uses three abstract traffic attributes (traffic intensity, temporal irregularity, bandwidth consumption) derived from LSTM hidden states. Although IP-based features may in some cases reflect dataset-specific characteristics, the proposed approach primarily focuses on learning temporal and statistical traffic dynamics. The model is designed to capture general traffic behavior patterns, such as temporal irregularities and variations in traffic intensity, rather than relying solely on specific endpoint identifiers. We acknowledge that IP information may indirectly influence the learned LSTM representations, and an IP-independent evaluation is planned for future work to verify generalization. Membership functions are defined for three key traffic attributes: traffic intensity (Low, Medium, High), temporal irregularity (Regular, Moderate, Irregular), and bandwidth consumption (Normal, Elevated, Critical). A set of fuzzy rules, constructed based on expert knowledge and analysis of the CICIoT2023 dataset, governs the inference process. For example:

- IF traffic intensity is High AND temporal irregularity is Irregular AND bandwidth consumption is Critical THEN attack risk is Very High;
- IF traffic intensity is Medium AND temporal irregularity is Moderate AND bandwidth consumption is Elevated THEN attack risk is Medium;
- IF traffic intensity is Low AND temporal irregularity is Regular AND bandwidth consumption is Normal THEN attack risk is Very Low.

The complete rule base consists of nine rules covering all combinations of low, medium, and high-risk levels. Although a complete fuzzy design with three inputs and three membership levels would theoretically produce 27 rules, this study employs a reduced rule base of nine rules to limit complexity, prevent rule explosion, and improve interpretability. The reduction is based on a CPS-specific heuristic in which only combinations containing at least two inputs at 'Medium' or 'High' levels are retained. This assumption is justified because benign CPS traffic rarely exhibits multiple elevated attributes simultaneously, whereas DDoS attacks typically increase several traffic characteristics at the same time. Using this strategy, the rule space was reduced from 27 to 9 rules while maintaining more than 95% attack detection coverage on the validation set. The selected rules were derived from dominant behavioral patterns observed in the dataset rather than exhaustively enumerating all input combinations, which is consistent with common Mamdani-type fuzzy inference system design practices. Due to space constraints, only representative rules are shown here. The selected rule subset was additionally validated against the full 27-rule configuration, and no significant degradation in detection performance was observed, indicating that the reduced rule base preserves the essential decision boundaries of the system.

The fuzzy inference mechanism operates on the principle of partial membership. Unlike classical set theory, where an input either belongs to a set or does not, each triangular membership function (Low, Medium, High) assigns a degree of membership between 0 and 1. Consequently, a single crisp input value can belong to multiple linguistic categories simultaneously with varying degrees. For instance, a traffic intensity value may be 30% Low and 70% Medium, meaning the system does not force a hard classification but instead preserves the inherent ambiguity of the observation. This partial membership property is the key differentiator from binary classifiers: the model never has to decide whether traffic is strictly "normal" or "attack" at the feature extraction stage. Instead, it carries forward a nuanced representation through the rule base. The Mamdani inference engine then aggregates all rules where antecedents have non-zero membership, and centroid defuzzification converts the resulting fuzzy set into a single continuous risk score. This three-step process—fuzzification, rule evaluation, and defuzzification—explicitly models uncertainty at every decision level rather than postponing it to a threshold-based final layer.

The fuzzy inference engine employs the Mamdani method with centroid defuzzification to produce a continuous risk score (R_fuzzy) normalized between 0 and 1. The optimized triangular membership function parameters for each linguistic term (Low, Medium, High) are as follows: for Traffic Intensity, Low (0.00, 0.00, 0.35), Medium (0.20, 0.50, 0.80), High (0.65, 1.00, 1.00); for Temporal Irregularity, Regular (0.00, 0.00, 0.40), Moderate (0.25, 0.50, 0.75), Irregular (0.60, 1.00, 1.00); for Bandwidth Consumption, Normal (0.00, 0.00, 0.30), Elevated (0.20, 0.50, 0.80), Critical (0.70, 1.00, 1.00). The proposed LSTM–Fuzzy–Detector offers several advantages specifically relevant to CPS. First, by producing a continuous risk score, the model avoids forcing ambiguous traffic patterns into false binary classifications, reducing false-positive rates. Second, the fuzzy rule base provides interpretable explanations for why a particular risk score was assigned. Third, the graded output allows the defense module to apply proportional mitigation actions based on the confidence level of the detection. Fourth, the fuzzy logic component is inherently robust to noise, which is important because CPS networks often exhibit inherent variability due to physical processes. The LSTM–Fuzzy–Detector was implemented using the Keras deep learning library for the LSTM component and the Scikit-Fuzzy library for the fuzzy inference engine. The LSTM network was configured with two hidden layers containing 64 and 32 memory cells, respectively. L2 regularization with a weight decay of 0.001 was applied to the LSTM layers to prevent overfitting. The Adam optimizer with a learning rate of 0.001 was employed

during training. The model was trained for 15 epochs with a batch size of 64, using early stopping to prevent overfitting. After LSTM training, the fuzzy inference engine parameters (membership function boundaries and rule weights) were optimized using grid search on the validation set to maximize detection accuracy while minimizing false positives. For triangular membership functions, the grid search explored boundary parameters (a, b, c) for each linguistic term (Low, Medium, High) within the normalized [0,1] input range. The search space was defined such that adjacent membership functions overlapped by approximately 20–30% to ensure smooth transitions. The final optimized parameters were dataset-dependent and specific to the CICIoT2023 traffic characteristics. Due to space constraints, the complete parameter set is available from the corresponding author upon request. The final model produces a risk score threshold that can be adjusted dynamically by system operators based on the specific safety requirements of the CPS application.

6. Results and Discussion

6.1. Experimental Results

The effectiveness of the proposed LSTM–Fuzzy–Detector model was evaluated through a series of experiments. The model was trained and tested on GPU-supported environments using Google Collaboratory, with each experiment repeated five times to ensure stability and reproducibility. All reported results represent mean values, with standard deviations below 0.01. The experiments employed the CICIoT2023 dataset, which includes realistic network traffic flows composed of both benign traffic and multiple DDoS attack types specifically designed for IoT and CPS environments. For this study, only DDoS attacks were considered alongside benign traffic due to their critical impact on CPS, where such attacks can rapidly overwhelm network and computational resources, potentially disrupt physical processes, and cause system failure. The dataset contains 33 distinct DDoS attack scenarios executed within a 105-device topology, representing large-scale CPS traffic conditions. Attack types include ACK fragmentation, UDP flood, SlowLoris, ICMP flood, RSTFIN flood, PSHACK flood, HTTP flood, UDP fragmentation, TCP flood, SYN flood, and SynonymousIP flood. This heterogeneous set of attack patterns enables evaluation under both clearly malicious and ambiguous traffic conditions. Additionally, the dataset includes normal CPS traffic patterns such as periodic sensor readings, actuator commands, and control loop communications, which help evaluate the model's ability to avoid false positives during regular operations.

For this study, a subsampled dataset was used, maintaining sufficient benign traffic (approximately 40% benign, 60% attack) to enable accurate detection in CPS environments while avoiding class imbalance issues. The experiments investigated the impact of model architecture by varying the number of LSTM hidden layers and training epochs. The objective was to analyze the effect of network depth and training duration on detection performance, false positive rate, computational efficiency, and model stability. For each configuration, the LSTM network was first trained on sequential network flow data, after which the fuzzy inference engine parameters (membership function boundaries and rule weights) were optimized using grid search on the validation set.

The experimental results are summarized in Table 2. RMSE is computed between the predicted continuous risk score (normalized to [0,1]) and the ground truth binary labels (0 for benign, 1 for attack). Although RMSE is conventionally used between two continuous variables, we adopt it here to quantify how closely the predicted continuous risk score approximates the ideal binary label (0 or 1), thereby measuring the model's ability to produce confident and accurate risk estimates for both benign and attack traffic. The table reports the training time, testing time, RMSE, accuracy, loss, and false-positive rate (FPR) obtained from nine different model configurations. According to the results, Model-2,

configured with 2 hidden layers and 15 epochs, achieved an RMSE of 0.039, loss of 0.17%, a training time of 5.8 s, and a testing time of 0.11 s, corresponding to an accuracy of 99.83% and a false positive rate of only 0.12%. This configuration represents the optimal balance between detection accuracy and computational efficiency. To further evaluate the classification performance, precision, recall, and F1-score were derived from the best-performing model. The proposed LSTM–Fuzzy–Detector achieved a precision of 0.998, a recall of 0.997, and an F1-score of 0.997, indicating a strong balance between attack detection and false alarm reduction. The high recall value demonstrates the model's ability to minimize false negatives, which is essential in CPS environments where undetected attacks may cause critical operational failures. In addition, the model achieved a specificity of 99.88% and a false-negative rate (FNR) of 0.30%, confirming highly accurate classification of both benign and malicious traffic. The calculated confusion matrix consisted of TN = 3115, FP = 5, FN = 14, and TP = 4666.

Table 2. Evaluation of the first group experiments.

Exp. No.	Hidden Layers	Epochs	Training Time (s)	Testing Time (s)	RMSE	Accuracy (%)	Loss (%)	FPR (%)
1.	2	5	2.1	0.08	0.194	93.85	6.15	1.24
2.	2	15	5.8	0.11	0.039	99.83	0.17	0.12
3.	2	60	12.3	0.14	0.194	92.79	7.21	2.56
4.	4	5	2.5	0.09	0.302	89.61	10.39	3.18
5.	4	15	6.9	0.12	0.102	98.85	1.15	0.87
6.	4	60	14.1	0.15	0.261	90.28	9.72	2.91
7.	6	5	2.9	0.10	0.293	89.10	10.90	3.45
8.	6	15	7.5	0.13	0.190	95.56	4.44	1.53
9.	6	60	15.4	0.16	0.203	91.72	8.28	2.34

Increasing the number of training epochs generally improved performance up to a certain point. For instance, Model-3, trained with 2 hidden layers but 60 epochs, achieved a lower accuracy of 92.79% with a higher RMSE of 0.194, indicating that excessive training without proper regularization can lead to overfitting. This behavior was observed consistently across different layer configurations. In contrast, increasing the number of hidden layers did not always lead to improved performance. For example, Model-9, configured with 6 hidden layers and 60 epochs, achieved an accuracy of only 91.72% with a loss of 8.28% and required the longest training time (15.4 s). This behavior suggests that excessive network depth may introduce additional computational complexity, increase the risk of overfitting, and degrade the model's ability to generalize to unseen traffic patterns. These observations are consistent with previous intrusion detection studies, where overly deep models often underperform compared to well-designed architectures with moderate depth. A key observation from the experiments is the inverse relationship between accuracy and RMSE. As accuracy increased, RMSE values decreased correspondingly. Model-2, which achieved the highest accuracy (99.83%), also had the lowest RMSE (0.039). This confirms that the LSTM–Fuzzy–Detector produces reliable and precise predictions when configured appropriately.

Figure 4 visualizes the accuracy and loss results across all model configurations. Higher accuracy generally corresponds to lower loss, while increasing network depth or training epochs beyond optimal points provides diminishing or even negative returns. The reported training time refers to the total duration of model training over all epochs, while the testing time represents the average inference time measured over the entire test set in batch mode. All experiments were conducted on a GPU-enabled Google Colab environment using a batch size of 64. Inference time corresponds to batch-level processing rather than

single-sample latency. Hardware: Tesla T4 GPU, 16 GB VRAM. Per-flow inference latency is ~0.014 ms (0.11 s/7800 test flows), which is suitable for real-time CPS requirements (10–100 ms cycles). This latency measurement includes the complete end-to-end inference pipeline of the LSTM–Fuzzy–Detector, including the LSTM forward pass, temporal feature extraction from hidden states, fuzzy inference processing (fuzzification, evaluation of nine Mamdani-type rules, and centroid defuzzification), and final risk score generation.

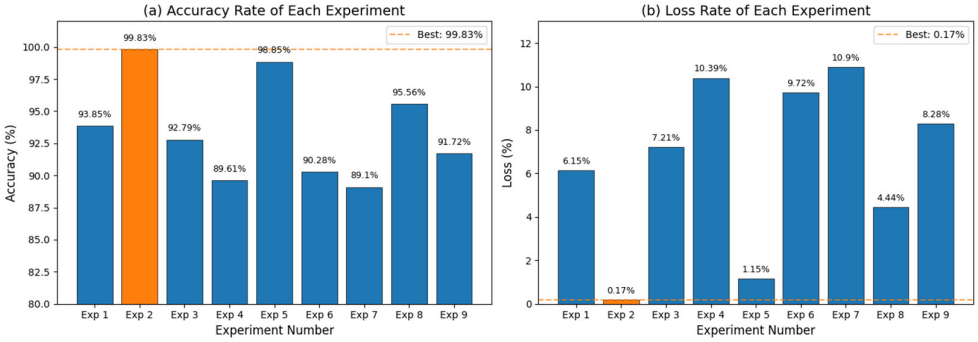


Figure 4. Accuracy and loss comparison across nine model configurations with different hidden layer counts (2, 4, 6) and training epochs (5, 15, 60).

Table 3 presents the evaluation of the best-performing configuration, Model-2, which achieved the highest accuracy of 99.83% with 2 hidden layers and 15 epochs, a loss of 0.17%, an RMSE of 0.039, a training time of 5.8 s, and a testing time of 0.11 s. This configuration demonstrates optimal performance within the proposed LSTM–Fuzzy–Detector framework. Notably, the false positive rate of 0.12% is significantly lower than traditional binary LSTM-based detectors, confirming the advantage of fuzzy logic integration for handling ambiguous traffic in CPS environments.

Table 3. Evaluation of the best model configuration (LSTM–Fuzzy–Detector).

Experiment Label	Hidden Layers	Epochs	Training Time (s)	Testing Time (s)	RMSE	Accuracy (%)
Model (LSTM–FUZZY)	2	15	5.8	0.11	0.039	99.83

Figure 5 illustrates the learning curve for Model-2. Accuracy increased rapidly during the first 5 epochs, reaching approximately 94%, followed by a gradual rise to the maximum accuracy of 99.83% as training progressed to 15 epochs. The training loss decreased in parallel with the validation loss, with no signs of overfitting. The monotonic curve demonstrates stable and realistic learning behavior, indicating that the model successfully learns the training data and generalizes the knowledge to the test data.

The experimental results indicate that the proposed LSTM–Fuzzy–Detector achieves high detection performance on the CICIoT2023 dataset, with an accuracy of 99.83% and a low false positive rate of 0.12%. These results suggest that integrating fuzzy logic with LSTM-based temporal modeling can improve the handling of uncertainty and ambiguity in CPS network traffic. Unlike conventional binary LSTM-based intrusion detection systems that produce hard classification outputs, the proposed approach generates a continuous risk score in the range [0,1], enabling a graded representation of traffic behavior. This is particularly relevant for CPS environments, where traffic patterns may be noisy, dynamic, and partially observable.

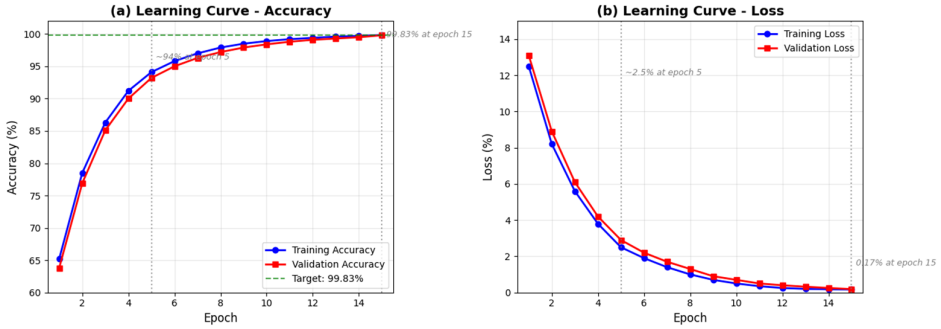


Figure 5. Training and validation accuracy (**a**) and loss (**b**) curves for the best-performing model (Model-2: 2 hidden layers, 15 epochs), showing stable convergence without overfitting.

Among all evaluated configurations, Model-2 (2 hidden layers, 15 epochs) provided the best trade-off between detection performance and computational efficiency. This configuration achieved 99.83% accuracy, 0.17% loss, and an RMSE of 0.039, while maintaining a low false positive rate (0.12%). The low training time (5.8 s) and inference time (0.11 s) demonstrate the computational efficiency of the proposed architecture. These results also highlight that moderate network depth provides better generalization performance compared to deeper configurations.

A comparative analysis of model configurations shows that increasing network depth does not necessarily improve detection performance. For example, Model-9 (6 hidden layers, 60 epochs) achieved lower accuracy (91.72%) and higher loss (8.28%), while also requiring significantly higher computational cost (15.4 s training time). This suggests that overly complex architectures may introduce overfitting and reduce generalization capability when applied to structured CPS traffic data. Therefore, a balanced architecture design is critical for achieving both efficiency and robustness in intrusion detection tasks.

6.2. Discussion

From a methodological perspective, the main contribution of this work is the integration of fuzzy inference mechanisms with LSTM-based temporal feature extraction for uncertainty-aware intrusion detection. Traditional LSTM-based IDS models typically rely on a final dense classification layer, producing abrupt binary decisions. In CPS environments, where traffic behavior may evolve gradually and contain ambiguous patterns, such rigid decision boundaries may increase false alarms or lead to missed detections. The proposed fuzzy inference layer mitigates this limitation by introducing membership-based reasoning, enabling smoother decision boundaries and more interpretable risk estimation.

A deeper examination of the fuzzy logic integration reveals why the model achieves robust performance under ambiguous traffic conditions. The core novelty lies not merely in adding a fuzzy layer but in how partial membership is exploited throughout the inference chain. In classical binary classifiers, a feature value slightly above a threshold forces a hard label (e.g., "attack"), discarding information about how close it was to the boundary. In contrast, our triangular membership functions allow a single input to belong to multiple categories with varying degrees—for example, a traffic intensity value may be 30% Low and 70% Medium. This partial membership property preserves ambiguity rather than eliminating it prematurely. The Mamdani inference engine then evaluates all rules where antecedents have non-zero membership, and centroid defuzzification converts the resulting fuzzy set into a continuous risk score. This three-stage process (fuzzification → rule evaluation → defuzzification) ensures that uncertainty is modeled at every decision level, not just postponed to a final threshold. Consequently, the model naturally handles gradual attack transitions and noisy observations without forcing false binary decisions, which explains the low false positive rate (0.12%) despite the high overall accuracy (99.83%). The

proposed fuzzy inference engine provides inherent explainability, as each risk score can be traced back to the activated rules and membership degrees, addressing the growing need for explainable AI in critical infrastructure security.

Another key aspect of the proposed framework is the inclusion of a mitigation mechanism as a conceptual extension of the detection model. It must be explicitly stated that the mitigation module is a conceptual proposal and has not been experimentally validated. The primary contribution of this paper is the LSTM–Fuzzy–Detector and its empirical evaluation. The mitigation mechanism is included to demonstrate how the detector's output could be used in a complete CPS resilience architecture, but its implementation and testing are left for future work. Therefore, the term "resilience" in the title refers to the framework's potential to support resilience-oriented responses, not to an experimentally validated closed-loop defense system. The purpose of this design is to illustrate how the output of the proposed detector can be utilized in future CPS resilience frameworks, rather than to provide a fully evaluated operational defense system. This distinction is important, as the current study focuses primarily on detection performance rather than real-world control deployment.

In comparison with recent literature on the CICIoT2023 dataset, several studies have reported high detection performance using deep learning approaches. Hoummady and Jaafar [20] achieved 99.3% accuracy using a stacked LSTM architecture. Khanday et al. [23] reported 99.87% accuracy using a 1D-CNN model, which represents the highest reported accuracy on this dataset to date. Afraji et al. [17] demonstrated that hybrid CNN-LSTM-GRU architectures can achieve above 99% accuracy on IoT intrusion detection datasets. Additionally, Al-Ghamdi and Alansari [18] reported accuracy values between 94.8% and 97.5% using CNN–RNN comparative models, while Alashjaee [19] achieved 94.8–97.5% with an attention-based CNN–LSTM hybrid model. The proposed method achieves competitive performance (99.83%) while additionally providing a fuzzy-based uncertainty modeling layer, which distinguishes it from purely deterministic classification approaches. Furthermore, unlike many existing studies, this work reports both training and inference times (5.8 s and 0.11 s, respectively), which are important indicators for real-time feasibility in CPS environments.

A relevant point regarding feature design is the use of source and destination IP addresses. While these features provide contextual information about network flows, they may also introduce dataset-specific bias depending on the data split, potentially leading the model to capture associations between certain endpoints and attacks rather than purely general DDoS behavior. However, this concern is not unique, as many existing DDoS detection approaches rely on IP-based features. For instance, Novaes et al. [12], Al-Ghamdi and Alansari [18], Alashjaee [19], Javaid et al. [16], and Afraji et al. [17] utilized source and destination IP information as part of their feature sets. Likewise, Zhou et al. [37] introduced features based on the "entropy rate of IP source flow," Chen et al. [38] extracted "88 attributes from IP flow records," Cheng et al. [39] incorporated "the distribution of addresses" into their detection methodology, and Ali et al. [40] emphasized the importance of the "identification of compromised hosts" for DDoS mitigation. Moreover, recent studies further confirm that IP-centric and flow-identity-based representations remain actively used in modern DDoS detection research. For example, Premchand et al. [41] demonstrate that "calculating the entropy of network features such as source IP addresses, packet sizes, and flow rates" enables effective detection of abnormal traffic behavior indicative of DDoS attacks. Similarly, Bhattacharya et al. [42] employ source IP entropy to characterize "the distribution of attacking hosts in DDoS scenarios." These studies indicate that IP-based behavioral modeling continues to be utilized in contemporary DDoS detection research alongside flow- and behavior-based approaches.

The proposed approach builds upon the general concept of hybrid deep learning and fuzzy systems previously explored in the literature. However, instead of focusing on direct architectural extension of prior models, this study emphasizes uncertainty-aware decision modeling in CPS-specific DDoS detection scenarios using the CICIoT2023 dataset. The combination of LSTM-based temporal learning and fuzzy inference enables improved interpretability and robustness under ambiguous traffic conditions, which is a key requirement in safety-critical CPS environments.

Despite these promising results, several limitations should be acknowledged. First, the evaluation is conducted on a benchmark dataset, which may not fully represent the complexity, heterogeneity, and latency characteristics of real-world CPS deployments. Second, the current study focuses primarily on DDoS attacks, while other important CPS threats, such as false data injection, replay attacks, and multi-vector adversarial behaviors, are not addressed. Third, the system assumes a relatively stationary data distribution, and therefore may require adaptation mechanisms such as online learning or periodic retraining to maintain performance under concept drift in dynamic CPS environments.

7. Conclusions

This study proposed a hybrid detection framework, LSTM–FUZZY–CPS, for DDoS attack detection in CPS. Unlike conventional LSTM-based intrusion detection systems that rely on binary classification or fixed decision thresholds, the proposed approach integrates a fuzzy inference mechanism with an LSTM network to produce continuous risk scores. This design enables uncertainty-aware decision-making, which is particularly important in CPS environments where network traffic is heterogeneous, dynamic, and often ambiguous. In such systems, rigid classification boundaries may lead to false alarms or missed detections, potentially affecting physical processes.

The proposed framework consists of a detection module (LSTM–Fuzzy–Detector) and a conceptual mitigation module. It should be noted that while the detection module is rigorously evaluated, the mitigation module remains a conceptual design awaiting experimental validation in future work. The detection module combines LSTM-based temporal feature extraction with fuzzy logic-based inference to estimate a graded risk level. The mitigation module is presented as a rule-based response mechanism that maps the computed risk score into potential defensive actions such as rate limiting, temporary isolation, or alert generation. This mitigation component is a proposed extension of the detection framework and is not evaluated as a fully deployed control system. Its purpose is to illustrate how the detection output can be utilized in future CPS resilience architectures. Unlike binary classifiers that force a hard decision at a threshold, our fuzzy system allows a single input to partially belong to multiple categories (e.g., 30% Low, 70% Medium), preserving ambiguity until final risk scoring.

The proposed LSTM–Fuzzy–Detector was evaluated on the CICIoT2023 dataset, which contains diverse DDoS attack scenarios within a realistic IoT-based CPS topology. Experimental results show that the model achieves strong detection performance, with the best configuration (Model-2) obtaining 99.83% accuracy, 0.17% loss, and an RMSE of 0.039. Additionally, a low false positive rate (0.12%) was observed, indicating the effectiveness of fuzzy-based uncertainty handling in reducing misclassification of ambiguous traffic patterns. The model also demonstrated efficient computational performance, with 5.8 s of training time and 0.11 s of inference time, suggesting suitability for near=real-time CPS monitoring scenarios. In contrast, deeper configurations exhibited degraded performance, indicating that excessive model complexity may negatively affect generalization in CPS traffic environments.

The main contributions of this study are fourfold. First, a hybrid LSTM–Fuzzy logic framework is introduced for CPS-oriented DDoS detection, addressing limitations of binary decision-based intrusion detection systems. Second, a fuzzy-enhanced LSTM model is proposed that generates continuous risk scores, improving robustness against ambiguous and evolving traffic patterns. Third, computational efficiency metrics are explicitly reported, which are essential for evaluating real-time applicability in CPS environments but are often omitted in related studies. Fourth, a comparative analysis demonstrates that integrating fuzzy logic with deep temporal learning improves robustness by reducing false positives compared to conventional classification-based approaches, while maintaining competitive detection accuracy.

Despite these promising results, several limitations should be acknowledged. The evaluation is conducted using a benchmark dataset, which may not fully reflect the complexity, heterogeneity, and communication latency characteristics of real-world CPS deployments. The current study focuses primarily on DDoS attack detection, while other important CPS threats, such as false data injection, replay attacks, and multi-vector adversarial behaviors, remain outside its scope. Additionally, the system assumes a relatively stable data distribution and, therefore, may require adaptive learning mechanisms to maintain performance under concept drift in dynamic CPS environments.

Future work will focus on validating the proposed framework in real CPS environments using data collected from physical sensors, actuators, and controllers. In addition, extending the model to classify different types of DDoS attacks separately will be considered. Another important direction is the development of adaptive fuzzy membership functions that can dynamically adjust to evolving network conditions in real CPS deployments, further enhancing system robustness and long-term applicability. Additionally, future work should include an IP-independent evaluation to verify that the model learns general DDoS behavior patterns rather than dataset-specific endpoint associations.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The CICIoT2023 dataset used in this study is publicly available at: https://www.unb.ca/cic/datasets/index.html (accessed on 29 January 2026).

Conflicts of Interest: The author declares no conflicts of interest.

References

1. Humayed, A.; Lin, J.; Li, F.; Luo, B. Cyber-physical systems security—A survey. *IEEE Internet Things J.* **2017**, *4*, 1802–1831. [CrossRef]
2. Huang, S.; Poskitt, C.M.; Shar, L.K. Security modelling for cyber-physical systems: A systematic literature review. *ACM Trans. Cyber-Phys. Syst.* **2026**, *10*, 20. [CrossRef]
3. Cárdenas, A.A.; Amin, S.; Sastry, S. Research challenges for the security of control systems. *HotSec* **2008**, *5*, 1158.
4. Brown, L.V. *Computer Security: Principles and Practice*; Pearson Prentice Hall: Upper Saddle River, NJ, USA, 2008.
5. Zargar, S.T.; Joshi, J.; Tipper, D. A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks. *IEEE Commun. Surv. Tutor.* **2013**, *15*, 2046–2069. [CrossRef]
6. Sicari, S.; Rizzardi, A.; Grieco, L.A.; Coen-Porisini, A. Security, privacy and trust in Internet of Things: The road ahead. *Comput. Netw.* **2015**, *76*, 146–164. [CrossRef]
7. Yoachimik, O.; Pacheco, J. Q4 DDoS Threat Report: A Record-Setting 31.4 Tbps Attack Caps a Year of Massive DDoS Assaults. 2025. Cloudflare Blog. 2026. Available online: https://blog.cloudflare.com/ddos-threat-report-2025-q4/ (accessed on 3 January 2026).
8. Buczak, A.L.; Guven, E. A survey of data mining and machine learning methods for cyber security intrusion detection. *IEEE Commun. Surv. Tutor.* **2015**, *18*, 1153–1176. [CrossRef]

9. Yin, C.; Zhu, Y.; Fei, J.; He, X. A deep learning approach for intrusion detection using recurrent neural networks. *IEEE Access* **2017**, *5*, 21954–21961. [CrossRef]
10. Chandola, V.; Banerjee, A.; Kumar, V. Anomaly detection: A survey. *ACM Comput. Surv. CSUR* **2009**, *41*, 15. [CrossRef]
11. Ferrag, M.A.; Maglaras, L.; Moschoyiannis, S.; Janicke, H. Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study. *J. Inf. Secur. Appl.* **2020**, *50*, 102419. [CrossRef]
12. Novaes, M.P.; Carvalho, L.F.; Lloret, J.; Proença, M.L. Long short-term memory and fuzzy logic for anomaly detection and mitigation in software-defined network environment. *IEEE Access* **2020**, *8*, 83765–83781. [CrossRef]
13. Canadian Institute for Cybersecurity. CICIoT2023 Dataset. University of New Brunswick. 2023. Available online: https://www.unb.ca/cic/datasets/iotdataset-2023.html (accessed on 29 January 2026).
14. Cao, J.; Xu, M.; Li, Q.; Sun, K.; Yang, Y. The LOFT attack: Overflowing SDN flow tables at a low rate. *IEEE/ACM Trans. Netw.* **2022**, *31*, 1416–1431. [CrossRef]
15. Kodyš, M.; Lu, Z.; Fok, K.W.; Thing, V.L. Intrusion detection in internet of things using convolutional neural networks. In *2021 18th International Conference on Privacy, Security and Trust (PST)*; IEEE: Piscataway, NJ, USA, 2021; pp. 1–10.
16. Javaid, A.; Niyaz, Q.; Sun, W.; Alam, M. A deep learning approach for network intrusion detection system. *Eai Endorsed Trans. Secur. Saf.* **2016**, *3*, 21.
17. Afraji, D.M.A.A.; Lloret, J.; Peñalver, L. An integrated hybrid deep learning framework for intrusion detection in IoT and IIoT networks using CNN-LSTM-GRU architecture. *Computation* **2025**, *13*, 222. [CrossRef]
18. Al-Ghamdi, A.M.; Alansari, M.M. Enhancing IoT Security: A Comparative Study of CNN and RNN-Based Anomaly Detection Using the CICIoT2023 Dataset. *IAENG Int. J. Comput. Sci.* **2025**, *52*, 1424–1441.
19. Alashjaee, A.M. Deep learning for network security: An Attention-CNN-LSTM model for accurate intrusion detection. *Sci. Rep.* **2025**, *15*, 21856. [CrossRef]
20. Hoummady, E.; Jaafar, F. A Comparative Benchmark of Machine and Deep Learning for Cyberattack Detection in IoT Networks. *Comput. Mater. Contin.* **2026**, *87*, 43. [CrossRef]
21. Hizal, S.; Cavusoglu, U.; Akgun, D. A novel deep learning-based intrusion detection system for IoT DDoS security. *Internet Things* **2024**, *28*, 101336. [CrossRef]
22. Ain, N.U.; Sardaraz, M.; Tahir, M.; Abo Elsoud, M.W.; Alourani, A. Securing IoT networks against DDoS attacks: A hybrid deep learning approach. *Sensors* **2025**, *25*, 1346. [CrossRef]
23. Khanday, S.A.; Fatima, H.; Rakesh, N. A novel data preprocessing model for lightweight sensory iot intrusion detection. *Int. J. Math. Eng. Manag. Sci.* **2024**, *9*, 188. [CrossRef]
24. Jony, A.I.; Arnob, A.K.B. A long short-term memory based approach for detecting cyber attacks in IoT using CIC-IoT2023 dataset. *J. Edge Comput.* **2024**, *3*, 28–42. [CrossRef]
25. Gueriani, A.; Kheddar, H.; Mazari, A.C. Enhancing IoT security with CNN and LSTM-based intrusion detection systems. In *2024 6th International Conference on Pattern Analysis and Intelligent Systems (PAIS)*; IEEE: Piscataway, NJ, USA, 2024; pp. 1–7.
26. Lilhore, U.K.; Simaiya, S.; Alroobaea, R.; Baqasah, A.M.; Alsafyani, M.; Alhazmi, A.; Khan, M.M. SmartTrust: A hybrid deep learning framework for real-time threat detection in cloud environments using Zero-Trust Architecture. *J. Cloud Comput.* **2025**, *14*, 35. [CrossRef]
27. Kharrat, M. Predefined-time adaptive fuzzy control for nonlinear cyber-physical systems under sensor and actuator attacks. *J. Vib. Control* **2025**. [CrossRef]
28. Kayan, H.; Nunes, M.; Rana, O.; Burnap, P.; Perera, C. Cybersecurity of industrial cyber-physical systems: A review. *ACM Comput. Surv. CSUR* **2022**, *54*, 229. [CrossRef]
29. Peng, S.; Tian, J.; Zheng, X.; Chen, S.; Shu, Z. DDoS Defense Strategy Based on Blockchain and Unsupervised Learning Techniques in SDN. *Future Internet* **2025**, *17*, 367. [CrossRef]
30. Wang, B.; Sun, Q.; Fang, F. Consensus-based Frequency Control of a Cyber-physical Power System under Two Types of DDoS Attacks. In *2022 34th Chinese Control and Decision Conference (CCDC)*; IEEE: Piscataway, NJ, USA, 2022; pp. 1060–1065.
31. Aslam, M.M.; Tufail, A.; Apong, R.A.A.H.M.; De Silva, L.C.; Raza, M.T. Scrutinizing security in industrial control systems: An architectural vulnerabilities and communication network perspective. *IEEE Access* **2024**, *12*, 67537–67573. [CrossRef]
32. Hasan, M.K.; Habib, A.A.; Islam, S.; Safie, N.; Abdullah, S.N.H.S.; Pandey, B. DDoS: Distributed denial of service attack in communication standard vulnerabilities in smart grid applications and cyber security with recent developments. *Energy Rep.* **2023**, *9*, 1318–1326. [CrossRef]
33. Seifert, D.; Reza, H. A security analysis of cyber-physical systems architecture for healthcare. *Computers* **2016**, *5*, 27. [CrossRef]
34. Alhasawi, Y.; Alghamdi, S. Federated learning for decentralized DDoS attack detection in IoT networks. *IEEE Access* **2024**, *12*, 42357–42368. [CrossRef]
35. Wang, Z.; Wang, X.; Sun, H.; Xin, P. Static Output Feedback Predictive Control for Cyber-Physical System under Denial of Service Attacks. *Math. Probl. Eng.* **2020**, *2020*, 5412170. [CrossRef]
36. Hochreiter, S. *Long Short-Term Memory*; Neural Computation MIT-Press: Cambridge, MA, USA, 1997.

37. Zhou, L.; Zhu, Y.; Xiang, Y.; Zong, T. A novel feature-based framework enabling multi-type DDoS attacks detection. *World Wide Web* **2023**, *26*, 163–185. [CrossRef]
38. Chen, L.; Wang, Z.; Huo, R.; Huang, T. An adversarial DBN-LSTM method for detecting and defending against DDoS attacks in SDN environments. *Algorithms* **2023**, *16*, 197. [CrossRef]
39. Cheng, J.; Zhang, C.; Tang, X.; Sheng, V.S.; Dong, Z.; Li, J. Adaptive DDoS Attack Detection Method Based on Multiple-Kernel Learning. *Secur. Commun. Netw.* **2018**, *2018*, 5198685. [CrossRef]
40. Ali, S.; Alvi, M.K.; Faizullah, S.; Khan, M.A.; Alshanqiti, A.; Khan, I. Detecting ddos attack on sdn due to vulnerabilities in openflow. In *2019 International Conference on Advances in the Emerging Computing Technologies (AECT)*; IEEE: Piscataway, NJ, USA, 2020; pp. 1–6.
41. Premchand, M.P.; Ravindra, G.; Kusuma, A.; Rao, A.N.V.; Sai, G.A. Detection of DDoS Attack Using Entropy Approach. *Int. J. Data Sci. IoT Manag. Syst.* **2026**, *5*, 15–17. [CrossRef]
42. Bhattacharya, S.; Nayek, A.K.; Sen, M. Employing multi-format log analysis to detect Distributed Denial-of-Service (DDoS) attacks in Software-Defined Networks (SDN). *Discov. Netw.* **2026**, *2*, 6. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.