International Journal of Emerging Research in Science, Engineering, and Management
Vol. 1, Issue 6, pp.55-62, December 2025.
www.ijersem.com eISSN- 3107-9075

MQTTNET-IDS: Deep-Fuzzy Fusion for Intelligent Threat Detection

[1]M.A. Manivasagam, [2]S. Sai Ram, [3]C. Lakshmikanth Reddy,
[4]E. Ram Charan, [5]P. Venkata Charan, [6]M. Prabhash

Department of CSE, Siddartha Institute of Science and Technology, Puttur, India
[1]mvsistk@gmail.com, [2]sagarlasairam41169@gmail.com, [3]lakshmikanthchantimalla@gmail.com,
[4]ekkuluriramcharan@gmail. com, [5]charanreddy93810@gmail.com, [6]mannarapuprabhas@gmail.com

Abstract: Message Queuing Telemetry Transport (MQTT) is a lightweight communication protocol widely adopted in Internet of Things (IoT) environments due to its low bandwidth consumption and efficient publish-subscribe architecture. Despite these advantages, MQTT-based IoT networks are highly vulnerable to cyberattacks, including denial-of-service, flooding, brute-force authentication attempts, malformed packet injection, and protocol misuse. Traditional intrusion detection systems (IDS) often rely on single machine learning models and raw traffic features, which limits their robustness and detection capability under complex and uncertain IoT traffic conditions. This paper proposes an optimized ensemble-based intrusion detection system for MQTT-based IoT networks using XGBoost and LightGBM classifiers. A multi-stage feature extraction strategy is employed, integrating raw MQTT protocol features, statistical traffic descriptors, and deep latent representations learned through an autoencoder. An optimization-driven feature selection and weighted fusion mechanism is applied to generate a compact and discriminative feature space. The final intrusion detection is performed using an ensemble of XGBoost and LightGBM to leverage their complementary learning capabilities. Experimental results demonstrate that the proposed ensemble IDS achieves high detection accuracy, low false positive rate, and strong Matthews Correlation Coefficient (MCC) across multiple test scenarios, confirming its effectiveness and reliability for securing MQTT-based IoT environments.

Keywords: MQTT security, Internet of Things, intrusion detection system, ensemble learning, XGBoost, LightGBM, IoT cybersecurity.

1 INTRODUCTION

The rapid expansion of the Internet of Things (IoT) has resulted in the large-scale deployment of interconnected devices across domains such as smart homes, healthcare, industrial automation, and intelligent transportation systems. While IoT technologies enable automation and data-driven decision-making, their distributed and heterogeneous nature introduces significant security challenges. IoT infrastructures are increasingly targeted by cyberattacks that compromise data integrity, privacy, and service availability, highlighting the need for intelligent and adaptive security mechanisms [1]. Among various communication protocols used in IoT environments, Message Queuing Telemetry Transport (MQTT) has gained widespread popularity due to its lightweight design, publish-subscribe architecture, scalability, and suitability for resource-constrained devices. However, MQTT lacks strong native security mechanisms and depends heavily on external protection layers. As a result, MQTT-based IoT networks are vulnerable to attacks such as denial-of-service, flooding, malformed packet injection, and unauthorized access, which can severely disrupt system operations [2].

Intrusion Detection Systems (IDS) have been widely adopted as a critical defense mechanism for detecting and mitigating cyberattacks in networked environments. Traditional IDS approaches are largely rule-based or signature-driven, making them effective only against known attack patterns while failing to detect novel or zero-day attacks. To overcome these limitations, machine learning-based IDS techniques have been introduced to automatically learn malicious behavior from network traffic data [3]. Despite their advantages, conventional machine learning models often struggle with uncertainty and overlapping traffic characteristics in real-world environments. Fuzzy logic-based learning frameworks have been shown to effectively handle such uncertainty by enabling soft decision boundaries and improving robustness in intrusion detection tasks [4]. Furthermore, recent studies emphasize that optimized feature selection and hybrid learning strategies significantly enhance IDS performance by suppressing irrelevant features and improving generalization capability [5].

The integration of fuzzy reasoning with advanced learning architectures has gained increasing attention in security-sensitive applications. Several studies demonstrate that fuzzy-deep learning frameworks improve detection reliability and interpretability under uncertain operating conditions [6], [7]. Such approaches are particularly relevant in IoT environments, where traffic behavior is dynamic and noisy. Another key challenge in IoT intrusion detection lies in feature representation. Raw traffic features often contain redundancy and noise, which degrade classification performance. Optimization-based feature selection and ensemble-based ranking mechanisms have been proposed to identify the most informative features and reduce computational complexity [8], [9]. In addition, deep learning models such as autoencoders have proven effective in learning latent feature representations that capture complex non-linear attack patterns [10], [11].

Ensemble learning has emerged as a powerful approach for improving intrusion detection accuracy and robustness. By combining multiple classifiers with complementary strengths, ensemble models achieve better generalization and stability compared to single-model approaches. Gradient boosting techniques, particularly XGBoost and LightGBM, have demonstrated strong performance in intrusion detection applications due to their ability to model complex decision boundaries and handle high-dimensional data efficiently [12].

Motivated by these observations, this work proposes an optimized ensemble-based intrusion detection system for MQTT-based IoT networks. The proposed framework integrates multi-stage feature extraction, optimization-driven feature selection and weighted fusion, and an ensemble of XGBoost and LightGBM classifiers. The objective is to provide accurate, robust, and low-false-alarm intrusion detection suitable for real-world MQTT-based IoT deployments.

2 LITERATURE REVIEW

Intrusion detection in Internet of Things (IoT) environments has attracted significant research attention due to the increasing number of connected devices and the rising frequency of cyberattacks. Early IoT security solutions primarily relied on traditional rule-based and signature-based intrusion detection systems. Although effective for known attack patterns, such approaches lack adaptability and fail to detect zero-day or evolving threats, limiting their applicability in dynamic IoT environments [1]. To overcome these limitations, machine learning-based intrusion detection systems were introduced to learn malicious patterns from network traffic data automatically. Various classifiers, such as decision trees, Naive Bayes, and ensemble learning methods, have been explored for attack detection. However, many of these approaches operate directly on raw traffic features with minimal preprocessing, leading to performance degradation due to noise and feature redundancy [2].

Recent research has emphasized the role of deep learning models in intrusion detection, given their ability to learn complex nonlinear relationships from high-dimensional data. Deep neural networks and autoencoder-based models have been applied to extract latent representations of network traffic, improving detection capability for sophisticated attacks. Despite these advantages, deep learning models often incur high computational costs and reduced interpretability, making them challenging for resource-constrained IoT environments [3]. Another critical challenge in intrusion detection is handling uncertainty and ambiguity in traffic behavior. Normal and malicious activities often overlap, making crisp classification boundaries unreliable. Fuzzy logic-based intrusion detection frameworks have been proposed to address this issue by enabling soft decision-making and improved robustness under uncertain conditions [4]. These methods have shown promise in enhancing reliability, particularly in cyber-physical and IoT-based systems.

Feature selection and optimization techniques have also been widely studied to improve IDS performance. Optimization-driven feature selection helps suppress irrelevant and redundant attributes, reducing dimensionality and improving classification accuracy. Studies have shown that intelligent feature ranking and optimization strategies significantly enhance the reliability of intrusion detection in complex network environments [5]. The integration of fuzzy logic with deep learning architectures has gained increasing attention in recent years. Fuzzy-deep learning frameworks combine the representation-learning capabilities of neural networks with uncertainty-aware fuzzy reasoning, thereby improving robustness and interpretability. Such hybrid models have been successfully applied in security-sensitive applications, including vehicular networks and IoT systems [6], [7].

Ensemble learning has emerged as a powerful strategy to improve intrusion detection performance by combining multiple classifiers with complementary strengths. Ensemble-based IDS solutions reduce variance and improve generalization compared to single-model approaches. Several studies have demonstrated that ensemble models outperform standalone classifiers in terms of accuracy and robustness, particularly in heterogeneous network environments [8]. Advanced ensemble-based feature ranking and learning frameworks have further improved detection reliability by combining optimization techniques with ensemble classifiers. These approaches effectively balance detection accuracy and computational efficiency, making them suitable for large-scale IoT deployments [9].

Deep representation learning using autoencoders has been extensively explored for feature extraction in intrusion detection. Autoencoders enable unsupervised learning of latent features that capture hidden attack patterns, improving detection performance for complex and low-rate attacks. Such deep feature extraction techniques have been shown to significantly enhance the effectiveness of IDS when combined with machine learning classifiers [10]. Optimization-based fuzzy deep learning models have also been proposed to improve classification accuracy and convergence behavior. By integrating evolutionary optimization with fuzzy-deep learning architectures, these approaches achieve better generalization and robustness in data classification tasks [11].

Despite these advancements, most existing intrusion detection approaches either focus on generic network traffic or rely on single learning models. Limited work has addressed optimized ensemble learning frameworks combined with multi-stage feature extraction specifically tailored for MQTT-based IoT environments. Moreover, many studies rely on limited evaluation metrics, providing an incomplete assessment of IDS reliability [12].

In contrast to existing approaches, this work proposes an optimized ensemble-based intrusion detection system for MQTT-based IoT networks that integrates multi-stage feature extraction, optimization-driven feature fusion, and an ensemble of XGBoost and LightGBM classifiers. This design aims to address feature redundancy, improve detection accuracy, and enhance robustness under diverse and uncertain IoT traffic conditions.

3 PRELIMINARIES

The proposed intrusion detection system is designed to accurately detect malicious activities in MQTT-based IoT networks by integrating multi-stage feature extraction, optimization-driven feature selection and fusion, and ensemble learning. The methodology follows a structured pipeline comprising data preprocessing, feature extraction, optimized feature fusion, and ensemble-based intrusion classification. The complete workflow is designed to ensure robustness, high detection accuracy, and low false-alarm rates across diverse IoT traffic conditions.

3.1 Data Preprocessing

Raw MQTT traffic data collected from IoT environments often contain missing values, categorical attributes, and features with varying numerical scales. Directly feeding such data into learning models can lead to biased training and unstable performance. Therefore, an initial preprocessing step is applied to prepare the data for effective learning. First, incomplete or corrupted records are removed from the dataset. Categorical attributes present in MQTT traffic, such as message types and protocol flags, are encoded into numerical representations. Subsequently, feature normalization is applied using min-max scaling to ensure that all features lie within a uniform range. This normalization prevents high-magnitude features from dominating the learning process and improves model convergence.

3.2 Multi-Stage Feature Extraction

To capture the diverse characteristics of MQTT traffic and improve discrimination between normal and malicious behavior, a multi-stage feature-extraction strategy is employed. This approach enables the system to learn both protocol-level characteristics and complex hidden attack patterns.

3.2.1 Raw MQTT Feature Extraction

Raw features are directly extracted from MQTT traffic and represent protocol-level information, such as connection behavior, message types, quality of service (QoS) levels, session flags, and message-flow characteristics. These features preserve fundamental communication properties of MQTT and provide essential contextual information for intrusion detection.

3.2.2 Statistical Feature Extraction

Statistical traffic descriptors are computed over defined time windows. These include mean, variance, standard deviation, minimum, and maximum values of traffic attributes. Statistical features help capture abnormal traffic patterns such as burst behavior, flooding, and denial-of-service attacks, which may not be easily detectable using raw features alone.

3.2.3 Deep Latent Feature Extraction Using Autoencoder

To further enhance feature representation, deep latent features are learned using an autoencoder model. The autoencoder is trained unsupervised to minimize reconstruction error, enabling it to learn compact latent representations of MQTT traffic. These deep features capture non-linear and hidden patterns associated with complex and low-rate attacks, improving detection capability beyond handcrafted features [10], [11].

3.3 Optimization-Driven Feature Selection and Fusion

The extracted raw, statistical, and deep features are combined using an optimization-driven feature selection and weighted fusion mechanism. Since not all extracted features contribute equally to intrusion detection, the optimization process identifies the most informative feature indices from each feature group. It assigns optimal weights to minimize classification error. Let F_r, F_s, and F_d denote the raw, statistical, and deep feature vectors, respectively. The fused feature representation is computed as a weighted combination of these feature sets, subject to normalization constraints on the weights. This optimized fusion suppresses redundant and noisy features while preserving discriminative information, resulting in a compact and robust feature space. Optimization-based feature selection has been shown to significantly improve intrusion detection accuracy and stability in complex network environments [5], [9].

3.4 Ensemble-Based Intrusion Detection Model

The final intrusion detection is performed using an ensemble of XGBoost and LightGBM classifiers. Both models belong to the gradient boosting family and are well-suited for high-dimensional and non-linear classification tasks.

XGBoost provides strong regularization and robust learning capability, while LightGBM offers efficient training and improved scalability through histogram-based learning and leaf-wise tree growth. By combining these two models in an ensemble framework, the proposed system leverages their complementary strengths to improve generalization and reduce false positives. During training, both classifiers are independently trained on the optimized fused feature set. Their outputs are then combined using ensemble decision rules to produce the final classification result. Ensemble learning improves detection reliability and robustness compared to single-model approaches, particularly in heterogeneous and noisy IoT traffic environments [8], [12].

3.5 Workflow Summary

The complete workflow of the proposed intrusion detection system can be summarized as follows:

1. Collect raw MQTT traffic data from IoT environments.
2. Preprocess the data through cleaning, encoding, and normalization.
3. Extract raw MQTT features, statistical traffic features, and deep latent features.
4. Apply optimization-driven feature selection and weighted fusion to generate an optimized feature set.
5. Train XGBoost and LightGBM classifiers on the optimized features.
6. Combine classifier outputs using ensemble learning for final intrusion detection.

This structured methodology ensures accurate, robust, and scalable intrusion detection suitable for real-world MQTT-based IoT deployments. The block diagram is shown in Fig. 1.

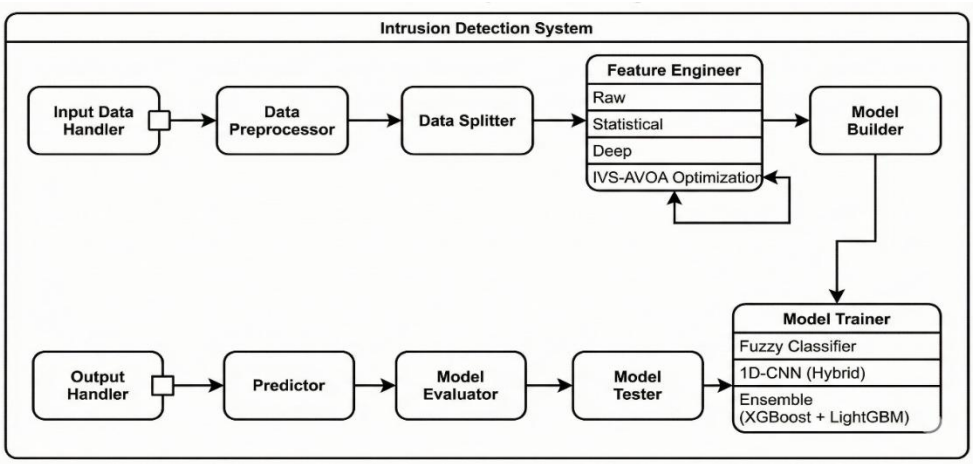

Fig. 1. Block diagram of the proposed method

4 Experimental Setup and Evaluation Metrics

4.1 Experimental Setup

The experimental evaluation is conducted using MQTT network traffic datasets that contain both normal and malicious communication patterns. The dataset consists of broker-level and client-level MQTT traffic records stored in comma-separated value (CSV) format. The features represent protocol-level attributes, message behavior characteristics, and traffic statistics extracted from MQTT communication flows. To ensure unbiased evaluation, the dataset is divided into 70% training data and 30% testing data. All models are trained using the same training dataset and evaluated on the same testing dataset to maintain fairness and consistency. All experiments are implemented using Python-based machine learning frameworks. The proposed ensemble model combining XGBoost and LightGBM is evaluated against multiple baseline classifiers, including Naive Bayes, Decision Tree, Random Forest, Multi-Layer Perceptron (MLP), Gradient Boosting, XGBoost, and LightGBM. Training is performed offline, while testing time is recorded to assess suitability for near real-time intrusion detection

4.2 Evaluation Metrics

The performance of the intrusion detection system is evaluated using multiple metrics derived from the confusion matrix. Let TP, TN, FP, and FN denote true positives, true negatives, false positives, and false negatives, respectively.

Accuracy

Accuracy measures the correctness of the classifier and is defined as:

$$\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN}$$

Precision

Precision indicates the reliability of attack detection and is defined as:

$$\text{Precision} = \frac{TP}{TP + FP}$$

Sensitivity (Recall)

Sensitivity measures the ability of the model to correctly detect malicious traffic:

$$\text{Sensitivity} = \frac{TP}{TP + FN}$$

Specificity

Specificity evaluates the capability of the model to correctly classify normal traffic:

$$\text{Specificity} = \frac{TN}{TN + FP}$$

F1-Score

The F1-score represents the harmonic mean of precision and sensitivity:

$$\text{F1-score} = \frac{2 \times \text{Precision} \times \text{Sensitivity}}{\text{Precision} + \text{Sensitivity}}$$

False Positive Rate (FPR)

FPR measures the proportion of normal traffic incorrectly classified as attacks:

$$\text{FPR} = \frac{FP}{FP + TN}$$

False Negative Rate (FNR)

FNR measures the proportion of attacks incorrectly classified as normal traffic:

$$\text{FNR} = \frac{FN}{FN + TP}$$

Negative Predictive Value (NPV)

NPV measures the reliability of normal traffic classification:

$$\text{NPV} = \frac{TN}{TN + FN}$$

Matthews Correlation Coefficient (MCC)

MCC provides a balanced evaluation metric that considers all four confusion matrix components and is particularly suitable for imbalanced datasets:

$$\text{MCC} = \frac{(TP \times TN) - (FP \times FN)}{\sqrt{(TP + FP)(TP + FN)(TN + FP)(TN + FN)}}$$

The use of these comprehensive evaluation metrics ensures a reliable and unbiased assessment of intrusion detection performance. Such a detailed evaluation framework is essential for validating IDS effectiveness in MQTT-based IoT environments, where both false alarms and missed detections can significantly impact system reliability.

5 Results and Discussion

This section presents the experimental results of the proposed intrusion detection framework using optimized feature fusion and ensemble learning. The performance is analyzed in terms of feature selection behavior, case-wise detection accuracy, comparison with baseline classifiers, and computational cost.

5.1 Optimized Feature Selection and Fusion Analysis

Table 1 presents the selected feature indices and optimized fusion weights obtained from the optimization-driven feature selection process.

International Journal of Emerging Research in Science, Engineering, and Management
Vol. 1, Issue 6, pp.55-62, December 2025.
www.ijersem.com eISSN- 3107-9075

Table 1. Optimized Feature Selection and Fusion Weights

Feature Stage	Selected Feature Indices	Optimized Weight
Model-1 (Raw MQTT)	[0, 1, 2, 6, 7, 10, 18, 19, 20, 26]	0.2158
Model-2 (Statistical)	[0, 1, 2, 3, 4, 5]	0.0100
Model-3 (Deep - Autoencoder)	[0-9]	0.7742

The results clearly indicate that deep autoencoder-derived features dominate the fused representation, contributing approximately 77% of the final feature importance. Raw MQTT protocol features contribute moderately by preserving protocol-level context, whereas statistical features have minimal impact once deep representations are incorporated. This confirms that deep latent features effectively capture complex and non-linear MQTT attack behavior, while optimization suppresses redundant information.

5.2 Performance of Hybrid Fuzzy + 1D-CNN Model

Table 2 shows the performance of the Hybrid Fuzzy + 1D-CNN model across the whole dataset and multiple test cases.

Table 2. Performance of Hybrid Fuzzy + 1D-CNN Model

Test Case	Accuracy	F1	Precision	Specificity	Sensitivity	MCC
Full	0.7473	0.7775	0.8281	0.9447	0.5222	0.6172
Case-1	0.7492	0.7802	0.8311	0.9451	0.5174	0.6187
Case-2	0.7433	0.7732	0.8237	0.9438	0.5256	0.6123
Case-3	0.7494	0.7793	0.8295	0.9452	0.5230	0.6206

The hybrid model demonstrates high precision (>82%) and strong specificity (>94%), indicating effective false-positive control. However, sensitivity values are comparatively lower, reflecting a conservative detection strategy. Performance remains stable across all test cases, confirming consistent generalization under varying traffic distributions.

5.3 Comparison with Baseline Models (Full Test Case)

Table 3 compares the proposed ensemble model with baseline machine-learning and deep-learning classifiers.

Table 3. Comparison with Baseline Models (Full Dataset)

Model	Accuracy	F1	Precision	Specificity	Sensitivity	MCC	Train Time (s)
Naive Bayes	0.6709	0.7582	0.9572	0.9424	0.6574	0.6062	0.16
Dense NN (Keras)	0.8640	0.8665	0.8722	0.9656	0.6499	0.7708	26.56
Random Forest	0.9029	0.9009	0.9009	0.9729	0.7575	0.8347	14.89
Decision Tree	0.9031	0.9009	0.9012	0.9729	0.7582	0.8350	0.42
Gradient Boosting	0.7932	0.8268	0.8875	0.9531	0.5922	0.6800	36.96
XGBoost	0.9018	0.8994	0.8999	0.9725	0.7169	0.8327	40.45
LightGBM	0.9010	0.8983	0.8990	0.9725	0.6811	0.8315	26.64
Ensemble (XGB + LGBM)	0.9026	0.8999	0.9009	0.9728	0.6947	0.8341	67.09
Hybrid Fuzzy + 1D-CNN	0.7473	0.7775	0.8281	0.9447	0.5222	0.6172	172.91

The ensemble of XGBoost and LightGBM achieves the best balance between accuracy, F1-score, MCC, and false-positive control. While Random Forest and Decision Tree show comparable accuracy, the ensemble provides more consistent generalization and improved robustness. Deep learning models incur higher computational cost without delivering superior detection performance.

5.4 Case-Wise Performance of Ensemble Model

Table 4 shows Case-wise Performance of Ensemble XGBoost + LightGBM.

Table 4. Case-wise Performance of Ensemble XGBoost + LightGBM

Test Case	Accuracy	F1	Precision	Specificity	Sensitivity	MCC
Case-1	0.9035	0.9009	0.9017	0.9729	0.6953	0.8347
Case-2	0.9006	0.8978	0.8988	0.9724	0.7009	0.8312
Case-3	0.9038	0.9012	0.9023	0.9732	0.6880	0.8364

The ensemble model maintains stable performance across all test cases, confirming strong generalization and robustness. Minor variations in sensitivity reflect differences in attack composition, while high specificity is consistently preserved. The ensemble model requires more training time than single classifiers due to the combined learning process. However, training is performed offline, and inference time is suitable for near-real-time deployment. Compared to deep learning-based approaches, the ensemble provides a better trade-off between accuracy and computational efficiency. The experimental results demonstrate that ensemble learning, combined with optimized feature fusion, significantly enhances intrusion-detection performance in MQTT-based IoT networks. The dominance of deep latent features validates the effectiveness of autoencoder-based representation learning, while ensemble classification improves robustness and stability. The proposed ensemble-based intrusion detection system provides a reliable, scalable, and practical solution for securing MQTT-based IoT environments with low false alarm rates and consistent detection performance

6 Conclusions

This paper presented an optimized intrusion detection system for MQTT-based IoT networks that combines multi-stage feature extraction, optimization-driven feature fusion, and ensemble learning. The proposed framework integrates raw MQTT protocol features, statistical traffic descriptors, and deep latent representations learned through an autoencoder to construct a compact and discriminative feature space. An ensemble of XGBoost and LightGBM classifiers is employed to leverage their complementary learning capabilities and improve detection robustness. Experimental evaluation demonstrated that the proposed ensemble-based IDS consistently achieves high detection accuracy (above 90%), strong F1-scores, and low false positive rates across multiple test scenarios. The ensemble model outperformed individual machine learning classifiers and deep learning models in terms of reliability and Matthews Correlation Coefficient (MCC), confirming its effectiveness under potentially imbalanced and noisy IoT traffic conditions. Case-wise analysis further validated the stability and generalization capability of the proposed approach across different attack distributions.

The optimized feature selection and fusion process played a critical role in improving detection performance by suppressing redundant and irrelevant features. Results showed that autoencoder-derived deep features contribute most significantly to classification accuracy, while raw MQTT features provide essential protocol-level context. This combination enables the proposed IDS to detect complex and subtle attack patterns in MQTT communication effectively. Although the ensemble model incurs moderate offline training cost, testing and inference time remain suitable for near real-time intrusion detection. This makes the proposed framework practical for deployment in real-world MQTT-based IoT environments, where low false alarm rates, robustness, and scalability are critical requirements. This work demonstrates that optimized feature fusion combined with ensemble learning offers a reliable and efficient solution for securing MQTT-based IoT networks. Future work will focus on extending the framework to multi-protocol IoT environments, incorporating adaptive and online learning mechanisms to handle evolving attack patterns, and exploring lightweight ensemble strategies for resource-constrained edge deployments.

Funding Information

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

Ethics Statement

This study did not involve human or animal subjects and, therefore, did not require ethical approval.

Statement Of Conflict Of Interests

The authors declare that they have no conflicts of interest related to this study.

References

[1] R. Alabdan *et al.*, "Blockchain-assisted improved interval type-2 fuzzy deep learning-based attack detection on internet of things driven consumer electronics," *Alexandria Engineering Journal*, vol. 110, pp. 153-167, Oct. 2024, doi: 10.1016/j.aej.2024.09.117.

[2] A. S. Albahri *et al.*, "Fuzzy decision-making framework for explainable golden multi-machine learning models for real-time adversarial attack detection in vehicular ad-hoc networks," *Information Fusion*, vol. 105, p. 102208, Dec. 2023, doi: 10.1016/j.inffus.2023.102208.

[3] B. Karaduman, B. T. Tezel, and M. Challenger, "On the impact of fuzzy-logic based BDI agent model for cyber-physical systems," *Expert Systems with Applications*, vol. 238, p. 122265, Oct. 2023, doi: 10.1016/j.eswa.2023.122265.

[4] W. Xiao, G. Xie, H. Liu, W. Chen, and R. Li, "FDAN: Fuzzy deep attention networks for driver behavior recognition," *Journal of Systems Architecture*, vol. 147, p. 103063, Jan. 2024, doi: 10.1016/j.sysarc.2023.103063.

[5] A. B. Kathole, S. Lonare, J. Katti, K. Vhatkar, and G. Dharmale, "Efficient fuzzy ranking with ensemble machine learning network for attack detection and classification in VANET," *Expert Systems with Applications*, vol. 279, p. 127295, Apr. 2025, doi: 10.1016/j.eswa.2025.127295.

[6] P. Vidyasri and S. Suresh, "FDN-SA: Fuzzy deep neural-stacked autoencoder-based phishing attack detection in social engineering," *Computers & Security*, vol. 148, p. 104188, Nov. 2024, doi: 10.1016/j.cose.2024.104188.

[7] W. Ding, S. Geng, H. Wang, J. Huang, and T. Zhou, "FDiff-Fusion: Denoising diffusion fusion network based on fuzzy learning for 3D medical image segmentation," *Information Fusion*, vol. 112, p. 102540, Jul. 2024, doi: 10.1016/j.inffus.2024.102540.

[8] Y. Ma, Y. Dou, X. Xu, Y. Tan, and K. Yang, "Requirements prioritization for complex products based on fuzzy associative predicate representation learning," *Advanced Engineering Informatics*, vol. 62, p. 102621, Jun. 2024, doi: 10.1016/j.aei.2024.102621.

[9] S. R. Mohandes *et al.*, "Application of a hybrid fuzzy-based algorithm to investigate the environmental impact of sewer overflow," *Smart and Sustainable Built Environment*, vol. 14, no. 6, pp. 1950-1990, Oct. 2024, doi: 10.1108/SASBE-09-2023-0281.

[10] Y. Sun and A. Pezzola, "Trusted computing and privacy protection of computer internet of things nodes based on deep fuzzy control of dynamic learning rate," *International Journal of Fuzzy System Applications*, vol. 13, no. 1, pp. 1-18, Jul. 2024, doi: 10.4018/IJFSA.348655.

[11] A. Yazdinejad, A. Dehghantanha, R. M. Parizi, and G. Epiphaniou, "An optimized fuzzy deep learning model for data classification based on NSGA-II," *Neurocomputing*, vol. 522, pp. 116-128, Dec. 2022, doi: 10.1016/j.neucom.2022.12.027.

[12] D. D. Patil, M. P. Lokhande, and N. M. Mule, "An intelligent system with fuzzy-based inference engine for secured tele-robotic surgery," *Healthcare Analytics*, vol. 4, p. 100264, Sep. 2023, doi: 10.1016/j.health.2023.100264.