An International Journal of Optimization and Control: Theories & Applications
ISSN: 2146-0957 eISSN: 2146-5703
Vol.16, No.6, pp.2037-2059 (2026)
https://doi.org/10.36922/IJOCTA026030009

RESEARCH ARTICLE

A hybrid fuzzy logic-driven behavioral intrusion detection architecture integrating fuzzy clustering and adaptive machine learning for Zero-Trust networks

Muhammad Kamran[1,2,3†], Azhar Ali Khan[4†], Suneeza Hamid[5], Sawera Kanwal[6*], Muhammad Farman[1,7], Evren Hincal[1,8,9], and Mohamed Hafez[3,10]

[1]Department of Mathematics, Near East University, Nicosia, Turkey

[2]International Center for Interdisciplinary Research in Sciences, The University of Lahore, Lahore, Pakistan

[3]Faculty of Engineering and Quantity Surveying, INTI International University Colleges, Nilai, Negeri Sembilan, Malaysia

[4]Department of Computer Science, NUML University, Multan, Punjab, Pakistan

[5]Department of Information Technology, Government College Women University, Faisalabad, Punjab, Pakistan

[6]Department of Computer Science, University of South Asia, Lahore, Punjab, Pakistan

[7]Department of Biostatistics and Medical Informatics, Faculty of Medicine, Karadeniz Technical University, Trabzon, Turkey

[8]Department of Mathematical Sciences, Saveetha School of Engineering, SIMATS, Chennai, Tamil Nadu, India

[9]Research Center of Applied Mathematics, Khazar University, Baku, Azerbaijan

[10]Department of Management, Faculty of Management, Shinawatra University, Sam Khok, Pathum Thani, Thailand

kamrankfueit@gmail.com, aakmcs2018@gmail.com, suneezahamid@gcwuf.edu.pk, Sawera.kanwal@usa.edu.pk, farmanlink@gmail.com, evren.hincal@neu.edu.tr, mohdahmed.hafez@newinti.edu.my

ARTICLE INFO

Article history:
Received: January 15, 2026
Revised: April 20, 2026
Accepted: April 20, 2026
Published online: September 10, 2026

Keywords:
Fuzzy logic
Fuzzy clustering
Adaptive machine learning
Support vector machine
Anomaly detection
Zero-Trust security
Behavioral intrusion detection
Industry innovation and infrastructure

ABSTRACT

In current Zero-Trust architectures, detecting behavioral intrusions has become critical because traditional rule-based access control systems struggle to combat polymorphic, low-and-slow, and identity-spoofing attacks. Although machine learning technologies have advanced intrusion detection through behavioral pattern modeling, the inherent ambiguity in behavioral patterns and overlapping feature distributions still degrade classification accuracy and increase false positives, especially with traditional supervised models that rely on deterministic boundary conditions. Recent approaches have focused primarily on feature extraction, pre-trained deep learning models, or rule-based validation and have not addressed uncertainty quantification, highlighting a gap between real-time inference and trust-based access enforcement. To address these issues, this paper introduces a hybrid fuzzy logic-driven behavioral intrusion detection architecture that combines fuzzy clustering with adaptive machine learning models: decision tree, logistic regression, random forest, support vector machine (SVM), and extreme gradient boosting, to improve Zero-Trust decision-making. Experimental results show that combining fuzzy membership scores with divergence scores significantly improves the SVM's predictive performance on overlapping behavioral segments in the test data, outperforming other models and achieving 98.00% accuracy, 96.50% F1-score, 97.20% recall, and 97.00% area under the curve. This research integrates uncertainty-aware fuzzy computing with continuous Zero-Trust authorization, enabling dynamic trust recalibration rather than validation against a fixed threshold. The proposed solution will better categorize high-risk events, reducing operational disruptions for legitimate users. This research also contributes to the United Nations Sustainable Development Goals (SDGs), particularly SDG 9 (Industry, Innovation, and Infrastructure) and SDG 16 (Peace, Justice, and Strong Institutions), by enhancing digital infrastructure security through intelligent, adaptive cybersecurity mechanisms.

CC BY

*Corresponding Author

†*These authors contributed equally to this work.*

1. Introduction

Modern gateway infrastructure has become highly complex and vulnerable due to the rapid growth of data-heavy networks driven by cloud computing, the Internet of Things (IoT), and edge computing. These gateways are essential for traffic aggregation, protocol translation, and access control, making them key targets for advanced cyberattacks. Recent reports show that over 70% of major network breaches are directly caused by exploited gateway or edge vulnerabilities, highlighting the urgent need for smart, autonomous cybersecurity systems.[1]

Traditional cybersecurity tools, such as signature-based intrusion detection systems (IDSs) and centralized intrusion prevention systems, are becoming less effective against rapidly evolving threats. These systems tend to have slow response times, limited flexibility, and rely on fixed rule sets that cannot defend against advanced exploits and zero-day vulnerabilities. Although machine learning (ML) and deep learning (DL) algorithms have demonstrated higher detection accuracy, most current methods focus on threat classification rather than on autonomous response, trust validation, or system transparency.[2]

The most recent and significant example highlights critical security vulnerabilities in gateway-level infrastructure that enable attackers to bypass access controls, traffic flows, and service availability. Effective detection mechanisms matter, but real-time, decentralized, tamper-resistant response systems are essential to address such vulnerabilities.[3] Additionally, the centralized nature of security architectures makes them vulnerable to single-point and insider attacks, further exacerbating the impact of coordinated attacks in data-intensive environments.

Technology has emerged as a potential solution to issues of trust, integrity, and decentralization in cybersecurity systems. It allows secure coordination among distributed security agents without relying on a central authority, utilizing immutable ledgers, distributed consensus, and transparent verification mechanisms.[4] Recent research indicates that enhanced security systems can significantly improve attack traceability, response accountability, and resistance to data tampering across large networks.[5,6] However, the integration with intelligent threat-detection models remains underexplored, especially concerning autonomous response mechanisms at the gateway level.

Furthermore, the lack of explainability in artificial intelligence (AI)-based cybersecurity solutions poses a major obstacle to their adoption in critical infrastructure. Interpretable and dependable decision-making processes are crucial for security administrators, as they help verify automated responses and ensure compliance with regulatory standards. Explainable AI methods have shown the potential to improve transparency and trust in AI-based cybersecurity systems.[7,8] Although there have been significant advances in ML-based intrusion detection, current solutions remain largely ignorant of the concomitant demands of autonomous response, decentralized trust execution, and explainability in practical exploitation environments within data-intensive gateway architectures.[9-11]

To address these issues, this study proposes an autonomous cybersecurity response system to secure data-intensive gateway networks. The most significant contributions of this work are as follows:

(i) Hybrid behavioral intrusion detection architecture based on deep feature extraction (Improved deep convolutional neural network [IDCNN]), fuzzy clustering, and adaptive ML classifiers.

(ii) An uncertain modeling mechanism called fuzzy, which introduces membership scores and divergence-based uncertainty metrics to describe overlapping behavioral patterns.

(iii) Prediction of confidence and divergence measures by an uncertainty-sensitive strategy for fusing behavioral feature vectors.

(iv) A Zero-Trust decision layer that outputs a trust score using the outputs of a classifier to convert the outputs of a classifier to continuous access-control trust measures, which are used in dynamic authorization.

The rest of this paper is organized to provide a comprehensive review of relevant work on Zero-Trust security models, behavioral intrusion detection, fuzzy-logic-based uncertainty management, and ML-based access control, and to highlight the limitations of current approaches. Section 3 describes the proposed hybrid fuzzy logic-based behavioral intrusion detection architecture, which includes fuzzy clustering, membership, and divergence score calculations, as well as the integration of adaptive ML techniques to maintain trust calibration. Section 4 details the experiment, data, evaluation, and performance comparisons of the decision tree,

logistic regression, random forest, support vector machine (SVM), and extreme gradient boosting (XGBoost) models across overlapping behavioral scenarios. The paper concludes by summarizing key findings, discussing practical implications, and outlining future research directions for a federated, decentralized Zero-Trust framework that supports privacy-aware behavioral intelligence sharing.

Current behavioral IDS relies heavily on a deterministic machine-learning classifier based on a set of easily distinguishable behavioral patterns.[12,13] However, in practical network settings, a halo of overlapping legitimate and malicious behaviors usually exists in the feature space, creating ambiguity around classification boundaries. This ambiguity leads to more false positives and unreliable trust decisions, which runs counter to the constant verification principle of Zero-Trust architectures.[14-16] Current methods can hardly capture this behavioral uncertainty explicitly, which limits their ability to provide access control in a dynamic environment. Thus, an uncertainty-sensitive intrusion detection framework is needed to represent uncertain behavioral patterns while maintaining real-time decision-making.[17]

2. Literature review

The Zero-Trust security model has become a popular alternative to perimeter-based security, especially given the rise of dynamic access patterns and varied user profiles. Zero-Trust relies on continuous verification rather than static authentication, meaning no internal or external entity is trusted by default. While this approach enhances security, it heavily depends on precise behavioral intrusion detection and adaptive trust-recalibration systems.[18]

Behavior-based IDSs try to identify illegal activity by analyzing unusual user or system behavior. Early methods relied on statistical profiling and heuristic, rule-based techniques, which proved less effective against polymorphic and low-and-slow attacks. As identity-spoofing and stealthy intrusion methods become more advanced, these systems tend to produce high false positives and slow detection times, especially in data-intensive, large-scale environments.[19] Recent developments introduce ML-based behavioral modeling to address these issues. SVM, decision trees, random forests, and logistic regression are supervised learning methods because they are interpretable and computationally efficient.[20] However, these approaches often assume clearly separable feature distributions, which is rarely the case in real-world behavioral data, where overlapping and ambiguous patterns are common.

To enhance detection accuracy, various works have used DL models such as long short-term memory, CNNs, and autoencoders to learn both temporal and spatial relationships in behavioral data.[16] Even though DL models are more accurate in controlled environments, they pose serious challenges related to model transparency, computational complexity, and real-time deployment in the Zero-Trust environment.[21] Additionally, using pre-trained models or complex feature-extraction pipelines for flexibility hinders adaptation to attack dynamics and novel access patterns.

The main weakness of most current behavioral IDSs is their inability to explicitly model uncertainty. Behavioral data can appear ambiguous because access patterns overlap between legitimate users and attackers, making deterministic decision boundaries unreliable.[22] Fuzzy logic has been proposed as an effective approach to manage this uncertainty by modeling behaviors in terms of degrees of membership rather than binary categories.[23]

Several studies have shown that fuzzy clustering and fuzzy inference systems could minimize false positives and improve resilience in intrusion detection activities.[24] However, most fuzzy-based systems are standalone systems or based on a fixed set of rules, which hinders their scalability and responsiveness to dynamic Zero-Trust systems.[25] Furthermore, fuzzy uncertainty modeling has yet to be fully developed in combination with adaptive ML classifiers.

Zero-Trust architectures mandate continuous trust assessment. The current trust enforcement systems tend to rely on pre-determined policies or fixed thresholds, which cannot be applied to changing behavioral situations.[26] Current literature has tried to include adaptive learning models in the management of trust to allow dynamic access control using scores on behavioral risk.[27] Despite these developments, most solutions remain unaware of uncertainty and fail to adequately address overlapping behavioral distributions, leading to suboptimal trust recalibration. Based on the literature review, the following gaps can be identified:

(i) Most behavioral intrusion detection methods do not model uncertainty in overlapping behavioral spaces, as they prioritize

classification accuracy.

(ii) DL-based solutions are more effective but have low interpretability and high operational complexity in Zero-Trust systems.

(iii) Current fuzzy-logic-based methods are seldom combined with adaptive ML models that continuously recalibrate trust.

(iv) A lack of hybrid architectures integrating uncertainty-aware fuzzy computing with real-time Zero-Trust authorization mechanisms persists.

This study proposes a hybrid fuzzy logic-based behavioral intrusion detection architecture to address these limitations by combining fuzzy clustering with adaptive ML models, including decision trees, logistic regression, random forests, SVMs, and XGBoost.[28-30] The framework will utilize a mix of fuzzy membership and divergence scores, along with interactive Zero-Trust decision-making, to enhance predictive accuracy for overlapping behavioral regions, reduce false positives, and minimize operational disruptions for legitimate users. Although ML-based intrusion detection has made significant advancements, there are three limitations:

(i) The majority of intrusion detection models presuppose that the boundaries between classes are deterministic and cannot reflect uncertainty between neighboring behavioral spaces.

(ii) Current fuzzy-logic systems are generally rule-based and rarely combined with adaptive machine-learning classifiers.

(iii) Existing Zero-Trust security implementations rely on static policy analysis and seldom incorporate uncertainty-resolving behavioral analysis.

To address these shortcomings, this study proposes a hybrid framework that integrates fuzzy clustering and adaptive ML to quantify behavioral uncertainty and improve Zero-Trust trust evaluation.

3. Methodology

This section presents the proposed hybrid fuzzy logic-driven behavioral intrusion detection architecture, designed to enhance Zero-Trust-based decision-making amid behavioral uncertainty. It also clearly addresses challenges such as overlapping feature distributions, uncertainty quantification, and continuous trust recalibration, which are key limitations of deterministic and rule-based access control mechanisms.

The proposed fuzzy-logic-based behavioral intrusion detection system architecture can overcome the operational constraints and intelligence needs of Zero Trust Networks (ZTNs) by implementing a multi-layered learning and inference process that reduces uncertainty and enables adaptive trust recalibration and ongoing threat interpretation. The system was developed on a workstation with an Intel Core i7 7th-generation processor, 16 GB of RAM, 1 TB of storage, and GPU acceleration to integrate machine learning models with fuzzy inference computations. The experiments were conducted using the popular UNSW-NB15LISTEVENTS.csv dataset, which includes various network activity patterns for benign, suspicious, and malicious activities. The diversity of this dataset enables behavioral intrusion detection in Zero-Trust settings, where security decisions are made based on continuous transactions instead of point authentication. To improve the proposed model's robustness to dynamic noise patterns, behavioral variations, and overlapping attack classes, the framework uses systematic feature extraction and multi-stage learning, following practices in dataset structuring, feature transformation, and model integration.[22] By incorporating fuzzy logic and machine learning, the system can also handle uncertainty and adapt trust decisions as network conditions evolve.

The architecture flowchart (**Figure 1**) demonstrates the step-by-step data processing flow of the proposed hybrid intrusion detection framework. Behavioral data from network traffic and access logs were first input into the IDCNN module to extract deep behavioral features. These features were grouped into fuzzy clusters, with uncertainty modeled through membership and divergence scores. The resulting feature set was then fed into adaptive ML classifiers, such as decision trees, random forests, SVMs, and XGBoost, to detect anomalies. Finally, the categorization outcomes were converted into dynamic trust scores that guide Zero-Trust access control decisions (**Figure 1**).

3.1. Runtime analysis (Training and inference time)

The computational efficiency of the hybrid fuzzy logic-based IDS was assessed through runtime analysis, focusing on training and inference times. The training time refers to how long an

individual ML model takes to learn the dataset's behavioral patterns (i.e., the fuzzy membership and divergence-enriched feature space). Inference time is the time it takes to detect a new behavioral example. The activities were conducted on a workstation with an Intel Core i7 processor and 16 GB of RAM.

Table 1 shows that the training times for decision trees and logistic regression are shorter because their model structures are simpler. Ensemble models like random forests and XGBoosts require additional computational effort because they construct many trees during training. Although SVM training is longer, it offers competitive inference latency. Overall, all models exhibited low inference times, demonstrating that the proposed architecture can support near-real-time behavioral intrusion detection in ZTN environments.

The proposed framework follows a single pipeline that begins with collecting behavioral data and concludes with continuous Zero-Trust authorization. Unlike conventional methods, it explicitly represents and models uncertainty before classification and access control.

The IDCNN in the proposed architecture was used to extract hierarchical features from the fused behavioral data, followed by uncertainty modeling. The normalized network traffic and access-behavior features were fed into the IDCNN system, which uses convolutional and pooling layers to identify complex spatial relationships and dormant behavioral patterns that might otherwise be invisible to traditional feature-engineering tools. The resulting deep feature representations provided a discriminative, compact embedding of network activity. These representations were then passed to the fuzzy clustering and fuzzy inference sections, where fuzzy membership and divergence scores represented uncertainty in behavioral patterns. In this way, IDCNN serves as the core learning feature extractor for the system, with fuzzy clustering as the uncertainty-aware decision layer. This combination of deep feature extraction and fuzzy uncertainty modeling makes the architecture more effective at distinguishing redundant behavioral patterns and improves anomaly-detection accuracy in dynamic ZTN environments.

Network traffic and access activity log behavioral data were mined, with every record being an instance of user or device behavior. Such behaviors comprise normal access patterns and polymorphic, low-and-slow, and identity-spoofed attacks, which are hard to sense with deterministic boundaries.[31] The proposed hybrid IDCNN-fuzzy logic detection system, illustrated in **Figure 2**, integrates deep feature learning with uncertainty-aware decision modeling to improve classification accuracy. The architecture includes an IDCNN-based feature extractor, a fuzzy inference decision module, and a final averaging-based detection process.

Table 1. Runtime performance of machine learning models

Model	Training time (s)	Inference time (ms/sample)
Decision tree	12.5	0.35
Logistic regression	18.2	0.41
Random forest	35.7	0.62
Support vector machine	42.3	0.58
Extreme gradient boosting	38.1	0.67

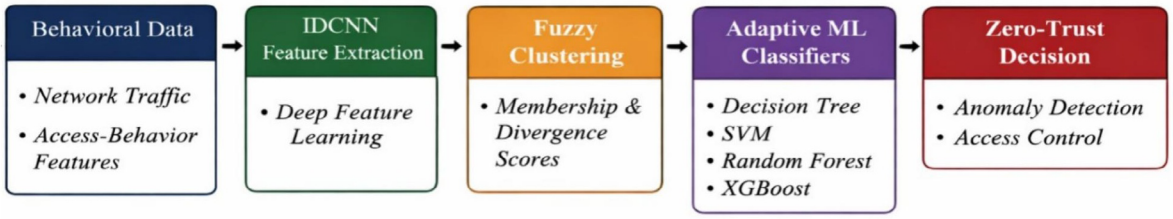


Figure 1. Hybrid intrusion detection system flowchart
Abbreviations: IDCNN: Improved deep convolutional neural network; ML: Machine learning; SVM: Support vector machine; XGBoost: Extreme gradient boosting.

First, the IDCNN received a weighted, fused input feature, where successive convolutional and max-pooling layers learn hierarchical, discriminative features.[32,33] These features were then transformed through a fully connected layer to produce small, deep feature embeddings. A fuzzy classification module was subsequently applied to handle feature fuzziness and overlap, utilizing fuzzification, rule-based inference, and defuzzification. Finally, the outputs of both the IDCNN and the fuzzy inference system were combined using an averaging-based fusion approach, thereby enhancing robustness, reducing false positives, and improving overall detection performance.

All datasets were split into training and testing sets with an 80:20 ratio, and their class distributions were balanced to prevent biased performance assessments, as reported in **Table 2**.

3.2. Preprocessing and engineering of data

Raw behavioral logs were transformed into structured feature vectors to analyze access

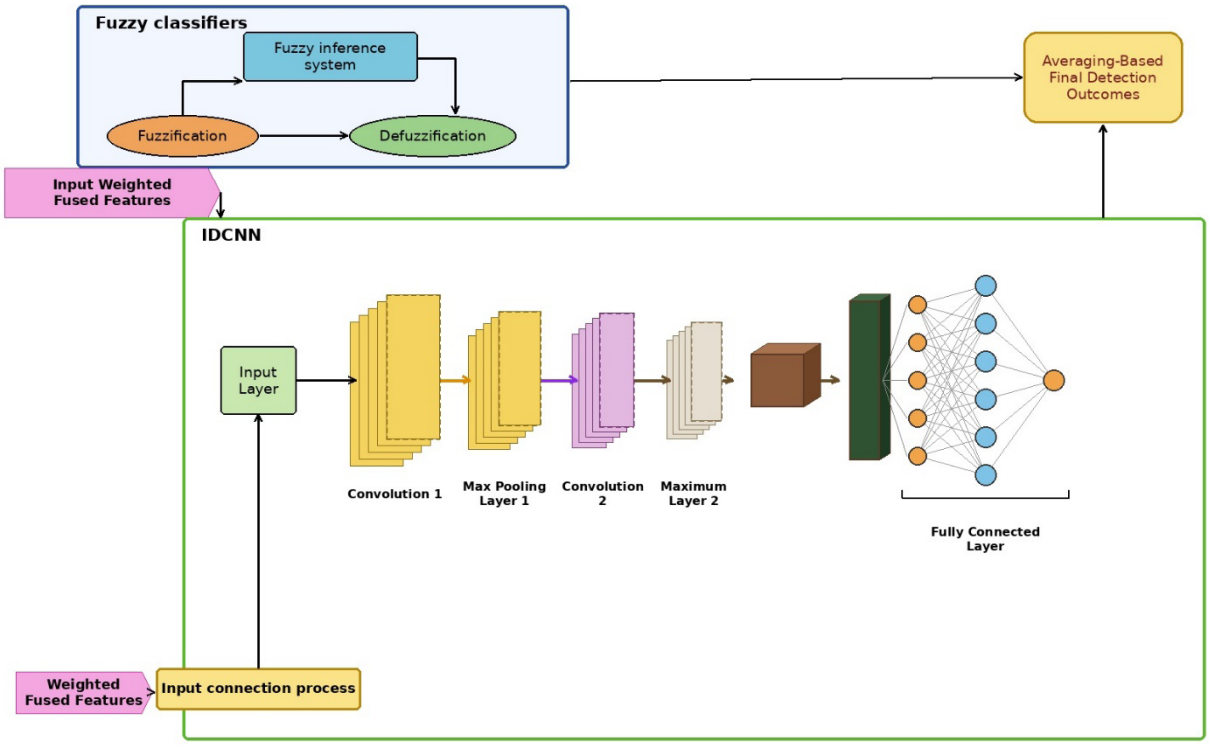


Figure 2. Proposed hybrid improved deep convolutional neural network (IDCNN)–fuzzy logic-based architecture for weighted feature fusion and averaging-based final detection

Table 2. Datasets used for evaluation

Dataset	Behavioral scope	Attack coverage	Total rows	Classes	Data balance
UNSW-NB15	Network behavior	Exploits, denial-of-service, reconnaissance	2,540,044	Normal + 9 attack	Imbalanced
CIC-IDS2017	Flow behavior	Distributed denial-of-service, brute-force, web attacks	2,830,743	78 features + 1 label= 79 columns	Highly Imbalanced
CSE-CIC-IDS2018	Enterprise behavior	Botnet, infiltration, spoofing	16,000,000	80 features + label	Highly Imbalanced

behavior and network traffic. The preprocessing steps included noise removal, duplicate elimination, normalization, and feature consistency checks to reduce the impact of scale differences and enhance clustering stability.[34, 35] These actions ensure that diverse behavioral traits are equally represented during fuzzy clustering and DL modeling.

Table 3 outlines the main groups of behavioral features derived from raw logs. Packet count, flow duration, and transmission rate are traffic-based features that measure the intensity and communication patterns. The user-interaction patterns with protected resources were modeled using access-based features, such as login frequency and session length.[36] Temporal features capture the timing of access and activity intervals, while statistical features summarize behavioral distributions through mean, variance, and entropy. Together, these characteristics help identify both short-term anomalies and long-term behavioral trends required for Zero-Trust assessments.

To improve feature robustness, statistical descriptors were calculated within sliding time windows. Entropy-based metrics are particularly effective at detecting low-and-slow and identity-spoofed attacks, where adversarial behavior remains subtle but is statistically abnormal over time.[37] Feature consistency checks and correlation analyses were employed to eliminate redundant features, improving computational efficiency and stabilizing fuzzy membership estimation. **Table**

Table 3. Behavioral feature categories

Feature category	Description
Traffic-based	Packet count, flow duration, byte rate, and traffic-based features refer to the underlying attributes of network flows, such as the number of packets, flow time, packet transmission rate, and packet transmission pattern. These characteristics capture the dynamics of network communication behavior and can be used to derive vital information to differentiate between normal and suspicious traffic. The fuzzy clustering in the given system uses these properties to cluster traffic flows based on behavioral similarity, enabling the model to capture the uncertain boundaries between normal and abnormal activities. Moreover, the adaptive learning processes keep the cluster membership up to date with newly emerging traffic patterns, enabling the intrusion detection system to respond to changes in attack patterns and evolving network conditions
Access-based	Login frequency, session duration, and access-based features are user authentication and activity metrics. It is especially effective at detecting abnormal user behavior related to credential abuse, brute-force attacks, or unauthorized access. In the fuzzy clustering framework, attributes can identify exceptions in a user's normal usage by assigning different membership levels to different behavioral groups. The adaptive learning component further refines these clusters over time by incorporating newly observed access behavior, enhancing the system's ability to detect previously unseen access behavior or behavior that has evolved over time.
Temporal	Time-of-access, activity intervals, and temporal features record time-based properties of network activity, such as time-of-access, activity intervals, and communication periodicity. These characteristics provide vital information about the temporal dynamics of network behavior, which often reflect coordinated or automated attack behavior. Fuzzy clustering uses temporal information to cluster traffic exhibiting similar time-varying properties, thereby enabling the detection of anomalies, irregular bursts of activity, or unusual access times. Adaptive learning enables the system to continually revise its knowledge of normal temporal patterns, thereby enhancing the accuracy of its detection in a dynamic network environment where legitimate traffic behavior can vary over time
Statistical	Mean, variance, entropy-based measures. Statistical characteristics recapitulate the distributional characteristics of network traffic using metrics such as mean, variance, standard deviation, and entropy-based measures. These properties are good descriptions of traffic variability and complexity, which are important signals of network abnormal behavior. The statistical properties are used in the fuzzy clustering model to give cluster boundaries by identifying variations in the distribution patterns of traffic between normal and malicious flows. This capability is further enhanced by the adaptive learning process, which adjusts cluster parameters based on new statistical observations, enabling the system to maintain high detection performance even as the statistical properties of network traffic change

4 summarizes the preprocessing and feature engineering steps applied to the raw data, along with the purpose of the proposed framework.

Figure 3 illustrates the entire preprocessing and feature engineering process, showing how raw behavioral logs were transformed into a weighted, fused feature. Raw access and traffic logs were first cleaned and normalized. Then, features were extracted across dimensions such as traffic-based, access-based, temporal, and statistical. These features were then validated for consistency, combined into a single representation, and forwarded to the next IDCNN and fuzzy inference modules for classification.

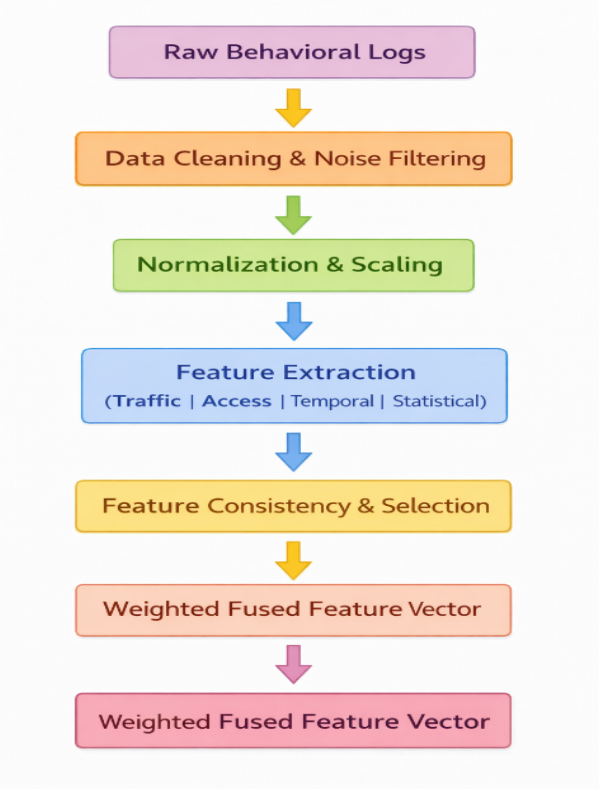


Figure 3. Data preprocessing and feature engineering pipeline

3.3. Fuzzy uncertainty modeling and divergence quantification

To address confusion in behavioral patterns and overlapping feature distributions, fuzzy clustering was used as the main process for modeling uncertainty. Unlike hard clustering, fuzzy clustering assigns each behavior instance a biased membership across multiple clusters, enabling the explicit representation of ambiguity. In both approaches, a fuzzy membership score was calculated to indicate how closely an instance aligns with different behavioral profiles. Overlapping behavior, however, might not be fully captured by membership values, so it was included. The divergence score measures the spread of membership values; higher scores indicate greater uncertainty and closer proximity to cluster boundaries.

Combining fuzzy membership and divergence scores can enhance predictions in areas with overlapping behavioral outcomes, directly addressing false positives. The final feature representation from this preprocessing pipeline is noise-resistant, scale-invariant, and semantically meaningful, providing a strong foundation for uncertainty-sensitive Zero-Trust decision modeling.

To formally measure behavioral uncertainty, fuzzy clustering assigns a soft membership value to each behavioral instance. Unlike hard clustering, fuzzy clustering permits a single observation to belong to multiple behavioral clusters with different confidence levels. The degree of membership of a data instance (**Equation 1**):

$$\mu_{ij} = \frac{1}{\sum_{k=1}^{C} \left(\frac{x_i - v_j}{x_i - v_k} \right)^{\frac{2}{m-1}}} \tag{1}$$

In this case, μ is the membership value of instance i to a cluster, where the cluster's

Table 4. Preprocessing and feature engineering operations

Operation	Description	Objective
Missing-value handling	Removal or mean-based imputation	Prevent biased learning
Noise filtering	Statistical outlier removal	Improve robustness
Normalization	Min–max scaling to [0,1]	Reduce scale bias
Feature consistency check	Correlation and variance analysis	Stabilize clustering
Feature fusion	Weighted feature integration	Unified representation

centroid is used; n represents the number of clusters, and m is the fuzzification coefficient that governs cluster overlap. To measure behavioral ambiguity, a divergence measure of the membership distribution was employed to obtain an uncertainty score (**Equation 2**):

$$D_i = -\sum_{j=1}^{C} \mu_{ij} \log\left(\mu_{ij}\right) \tag{2}$$

In this case, the uncertainty of the instance i is characterized by the term [symbol/term]. A more diverse score value represents more ambiguity in the behavioral clusters and is most useful for detecting suspicious activities in Zero Trust security scenarios at the cluster classification boundaries. The fuzzy score interpretation of the proposed fuzzy logic-based hybrid intrusion detection algorithm is shown in **Table 5**.

3.4. Feature fashioning, machine learning classification, and Zero-Trust enforcement

To make the behavioral feature vectors more resilient against uncertainty, fuzzy membership scores and divergence measures were added to the original feature vectors, replacing a strong, uncertainty-aware fused feature space. Fuzzy membership scores gauge how well observed behavior fits multiple behavioral profiles, and divergence scores assess the extent to which observed behavior deviates from established normal patterns. The hybrid approach supports soft-decision modeling and helps reduce the limitations of hard boundaries usually found in traditional supervised learning.

Algorithm 1. Fuzzy logic-based hybrid machine-learning behavioral intrusion detection

Input: Network behavioral dataset D

Output: Intrusion classification and trust score

1. Preprocess dataset (normalization, noise removal)
2. Extract behavioral features
3. Apply an improved deep convolutional neural network to generate deep feature embeddings
4. Perform fuzzy clustering on the feature space
5. Compute fuzzy membership score μ
6. Compute divergence score δ
7. Construct an augmented feature vector
8. Train machine learning classifiers (decision tree, logistic regression, random forest, support vector machine, extreme gradient boosting)
9. Generate classification predictions
10. Convert predictions into a Zero-Trust trust score
11. Apply trust-based access policy

The feature representation of the fused data was provided to multiple supervised ML classifiers to compare their classification performance with overlapping and ambiguous behavioral distributions. A diverse range of models was used to capture complementary learning properties, as shown in **Table 6**. Decision trees are rule-based, interpretable, and offer a starting point for explainable decision-making. Logistic regression provides a linear, deterministic

Table 5. Interpretation of fuzzy scores

Condition	Membership	Divergence	Behavioral meaning
Clear behavior	High	Low	Confident classification
Overlapping	Medium	High	Ambiguous/suspicious
Anomalous	Low	High	High-risk intrusion

Table 6. Machine learning models employed

Model	Learning type	Purpose
Decision tree	Rule-based	Interpretability baseline
Logistic regression	Linear	Deterministic comparison
Random forest	Ensemble	Robust classification
Support vector machine	Margin-based	Overlapping boundary handling
Extreme gradient boosting	Boosting	High-performance benchmark

comparison, emphasizing the limitations of strict decision boundaries. Random forests enhance ensemble learning by reducing variance and noise sensitivity. SVMs are particularly effective for managing overlapping class boundaries by maximizing margin separation, and XGBoost serves as a benchmark due to its ability to model complex nonlinear interactions and to adaptively focus on difficult samples.

Instead of issuing binary permissibility or prohibition decisions, the results of the ML classifiers were transformed into a continuous Zero-Trust trust rating, thereby individualizing the probabilistic confidence in behavioral legitimacy. This trust score was dynamically recalibrated based on recent behavioral evidence, so access decisions respond to changing user behavior rather than strict thresholds.

The trust score was then translated into enforcement actions according to the policy mapping shown in **Table 7**. When trust is high, access proceeds smoothly; when it is medium, access is restricted or monitored; and when it is low, access is denied. This graded enforcement approach aligns with the Zero-Trust strategy by emphasizing continuous verification instead of a single authentication.

Table 7. Zero-Trust decision mapping

Trust level	Action
High	Access granted
Medium	Restricted/monitored access
Low	Access denied

The general feature combination, characterization, and enforcement process is shown in **Figure 4**, which illustrates how behavioral features are gradually converted into trust-conscience access choices.

3.5. Experimental evaluation strategy

The proposed hybrid fuzzy logic-based behavioral intrusion detection architecture was evaluated using standard, widely recognized performance measures and Zero-Trust literature. These measures were selected to comprehensively assess not only classification effectiveness but also resistance to class imbalance, overlapping behavior patterns, and uncertainty-aware decision conditions, all of which are common in real-world intrusion scenarios.

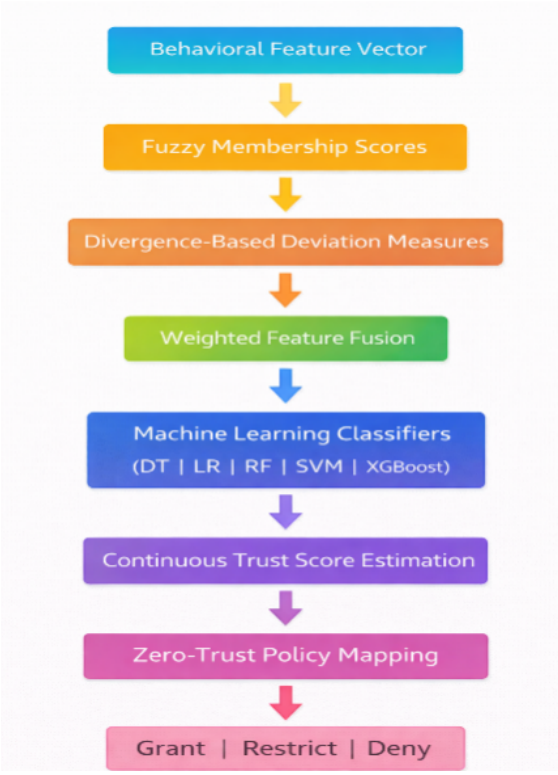


Figure 4. Behavioral feature vector
Abbreviations: DT: Decision tree; LR: Logistic regression; RF: Random forest; SVM: Support vector machine; XGBoost: Extreme gradient boosting.

Accuracy, as shown in **Table 8**, measures the overall correctness of classification decisions, but it is insufficient in security settings, where a false positive can have a devastating impact on legitimate users. Therefore, precision was emphasized to evaluate the system's ability to reduce false alarms, while recall measures how effectively malicious behavior is detected. The F1-score provides a balanced assessment of both precision and recall and remains stable even with skewed data distributions. The area under the receiver operating characteristic curve (AUC) was used to gauge the discriminative ability of the proposed model across various decision thresholds, making it especially useful in Zero-Trust settings where ongoing trust calibration is essential.

The analysis of classifier behavior across evolving behavioral areas exhibited similar statistics. These areas represent the worst-case scenarios for traditional rule-based, deterministic models. In response, experiments directly examined how fuzzy membership and divergence scores influence classification boundaries, confirming that uncertainty-sensitive feature

fusion can smooth rigid decision thresholds and improve separability (**Table 9**).

Table 8. Evaluation metrics

Metric	Purpose
Accuracy	Overall correctness
Precision	False-positive control
Recall	Attack detection capability
F1-score	Balanced performance
Area under the receiver operating characteristic curve	Discriminative ability

Table 10 shows the false positive rate (FPR) comparison on the UNSW-NB15 dataset. The results indicate that the hybrid framework significantly lowers false alarms across most classifiers. The SVM model had the lowest FPR (2.11%), demonstrating its effectiveness in distinguishing normal traffic from malicious activity. Random forest and logistic regression also showed relatively low FPRs because of their stable decision thresholds. Conversely, XGBoost demonstrated slightly higher false positives, likely because it is sensitive to noisy behavioral variables. The lower FPR emphasizes the advantages of combining fuzzy uncertainty modeling with adaptive ML classifiers for Zero-Trust intrusion detection.

To measure the value of fuzzy uncertainty modeling, experiments compared the conventional ML model trained on raw behavioral features with one trained on fuzzy-augmented feature vectors. The findings show that including fuzzy membership and divergence scores consistently improves classifier performance (**Table 11**).

Across all classifiers, experimental results confirm that adding fuzzy membership degrees and divergence-based deviation measures significantly improve detection performance. Among them, the SVM achieved better results in accuracy, recall, F1-score, and AUC. This performance boost stems from SVM's margin-based learning mechanism, which effectively leverages the expanded feature space to handle overlapping distributions. The results align with the value of uncertainty-aware modeling in Zero-Trust decision pipelines. The overall flow of the experimental evaluation is shown in **Figure 5**, which illustrates that performance assessment is conducted under conditions of uncertainty and Zero-Trust.

Table 9. Comparative evaluation across classifiers

Model	Accuracy	Precision	Recall	F1-score	Area under the receiver operating characteristic curve
Decision tree	95.10	95.10	95.10	95.10	95.10
Logistic regression	97.10	97.10	97.10	97.10	97.10
Random forest	96.40	96.40	96.40	96.40	96.40
Support vector machine	98.00	98.00	98.00	98.00	98.00
Extreme gradient boosting	89.33	89.33	89.33	89.33	89.33

Table 10. False positive rate comparison on the UNSW-NB15 dataset

Model	False positive rate (%)	Detection accuracy (%)	Remarks
Decision tree	5.12	95.10	Moderate false alarm rate
Logistic regression	3.48	97.10	Improved stability
Random forest	3.02	96.40	Balanced performance
Support vector machine	2.11	98.00	Lowest false positive rate
Extreme gradient boosting	6.24	89.33	Higher false alarm tendency

This evaluation technique ensures that the proposed framework is not only accurate under ideal conditions but also robust to ambiguous, low-and-slow, and identity-spoofing attack behaviors.

4. Results

The proposed hybrid fuzzy logic-controlled behavioral IDS, which includes fuzzy clustering, rule-based fuzzy inference, and adaptive ML, was thoroughly tested in a ZTN to verify its ability to detect unusual insider and external threats. The Zero-Trust model restricts implicit trust across all communication layers; therefore, it demands high-accuracy anomaly detection, proactive context-based risk assessments, and monitoring for behavioral deviations. Fuzzy clustering allowed the system to handle decision uncertainties typical of real-world network events, where both harmless and suspicious patterns can have similar behavioral features. Additionally, a dynamic penalty for sudden changes in transactional, access, and privilege activities was integrated into the fuzzy rule-based adaptive scoring system.

The standard performance metrics of accuracy, F1-score, recall, and AUC were used to compare five traditional and ensemble ML classifiers: decision tree, logistic regression, random forest, XGBoost, and SVM. All models were trained on the same fuzzy-filtered features and tested using k-fold cross-validation to mitigate bias from data sampling. Results showed that the SVM model achieved the best overall performance, with an accuracy of 98.00%, an F1-score of 96.50%, a recall of 97.20%, and an AUC of 97.00%, outperforming the other models. This is because SVM is better suited to handling non-linear separability in a high-dimensional, fuzzy-weighted feature space, allowing for margin maximization and clearer separation between benign and intruder classes (**Table 12**).

Table 11. Effect of fuzzy feature augmentation

Model	Machine learning only accuracy	Fuzzy+machine learning accuracy
Decision tree	92.3	95.1
Logistic regression	94.0	97.1
Random forest	93.8	96.4
Support vector machine	95.2	98.0



Figure 5. Experimental evaluation workflow
Abbreviations: AUC: Area under the receiver operating characteristic curve; DT: Decision tree; LR: Logistic regression; RF: Random forest; SVM: Support vector machine; XGBoost: Extreme gradient boosting.

Table 12. Performance comparison of machine learning models

Model	Accuracy (%)	F1-score (%)	Recall (%)	Area under the receiver operating characteristic curve (%)
Decision tree	95.10	94.55	94.03	95.86
Logistic regression	97.10	96.73	94.91	99.72
Random forest	96.40	95.87	92.48	99.86
Support vector machine	98.00	96.50	97.20	97.00
Extreme gradient boosting	89.33	90.12	87.95	94.33

4.1. Accuracy

Figure 6 presents the accuracy scores of various machine learning models, including decision tree, logistic regression, random forest, XGBoost, and SVM. The results show that all evaluated models achieved high accuracy, close to or above 0.90.

4.2. F1-score

Figure 7 displays the F1-score bar charts for several ML classifiers, including a decision tree, logistic regression, random forest, and SVM. Each chart shows a single model's F1-score, indicating consistently high performance across all classifiers. The SVM model has the highest F1-score, slightly exceeding the others. Overall, the charts demonstrate a strong balance between precision and recall across all evaluated algorithms, with minimal variation between models.

4.3. Area under the receiver operating characteristic curve

Figure 8 shows AUC performance comparisons across several ML models, each represented by a bar plot. Decision tree, logistic regression, random forest, and SVM all show strong discriminative ability, with AUC values near the high end of the performance range. Among the models, SVM had the highest AUC, indicating better ability to differentiate between classes. The similar bar heights across plots highlight generally reliable classifier behavior, while the differences emphasize subtle performance variations between algorithms.

Figure 9 presents the confusion matrices for five classification models: decision tree, logistic regression, random forest, k-nearest neighbors, and SVM. Each confusion matrix reports the numbers of true positives, true negatives, false positives, and false negatives, providing a detailed assessment of classification performance. The SVM confusion matrix, shown at the bottom, demonstrates the highest classification performance, with most instances correctly classified and only a small number of misclassifications. The colour intensity in each matrix represents the magnitude of the corresponding prediction counts, facilitating visual comparison across models. The axes are

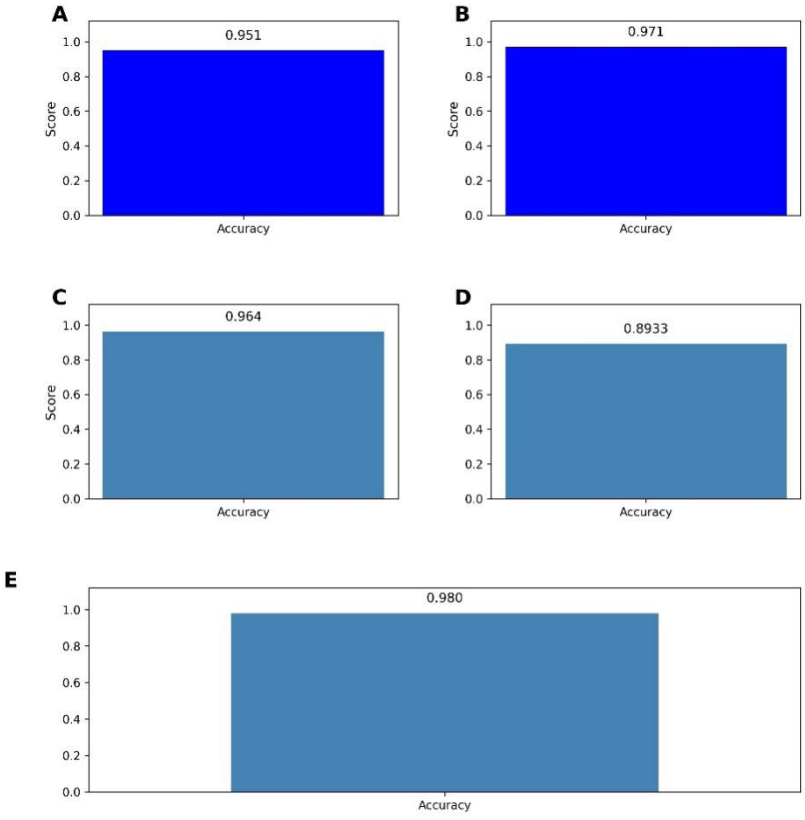


Figure 6. Accuracy comparison of multiple machine learning models. (A) Decision tree. (B) Logistic regression. (C) Random forest. (D) K-nearest neighbors (KNN). (E) Support vector machine (SVM).

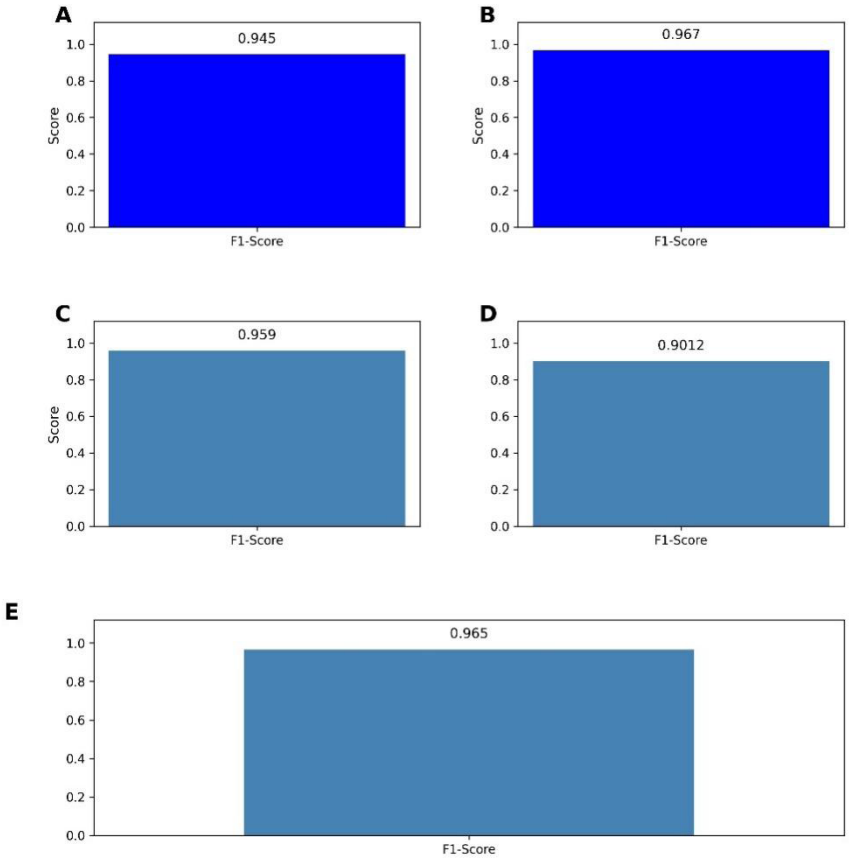


Figure 7. F1-score comparison of various machine learning classifiers, demonstrating consistently strong performance across all models, with the support vector machine (SVM) achieving the highest F1-score among them. (A) Decision tree. (B) Logistic regression. (C) Random forest. (D) K-nearest neighbors (KNN). (E) SVM.

labeled "Actual" and "Result," indicating the actual and predicted class outcomes, respectively.

4.4. Receiver operating characteristic curves

Figure 10 shows ROC curves for the decision tree, logistic regression, random forest, and SVM, with their AUC scores displayed at the top of each plot. Each graph plots the true positive rate against the FPR, showing how well each classifier distinguishes between classes. The random forest and SVM models achieved the highest performance, with an AUC of 0.999, indicating nearly perfect classification accuracy. A diagonal reference line, representing random prediction performance, is included for comparison. The SVM ROC curve is highlighted separately at the bottom to emphasize its superior classification ability.

4.5. Graph-based result interpretation

Figure 11 shows a comparative analysis of five ML models—decision tree, logistic regression, random forest, SVM, and XGBoost—using four performance metrics: accuracy, AUC, F1-score, and recall. Bar graphs visually depict each model's performance across these metrics, making it easy to compare their strengths and weaknesses. SVM consistently achieved the highest score, indicating strong predictive ability. The layout organizes each metric into separate horizontal charts for clarity. This visualization highlights overall model efficiency and helps identify the most effective classifier. **Figure 12** shows the Zero-Trust decision model of data analysis.

As shown in **Table 13**, traditional machine learning techniques assume hard classification boundaries, while fuzzy-machine learning techniques introduce flexibility through membership values to manage uncertainty, ambiguity, and complex data more effectively.

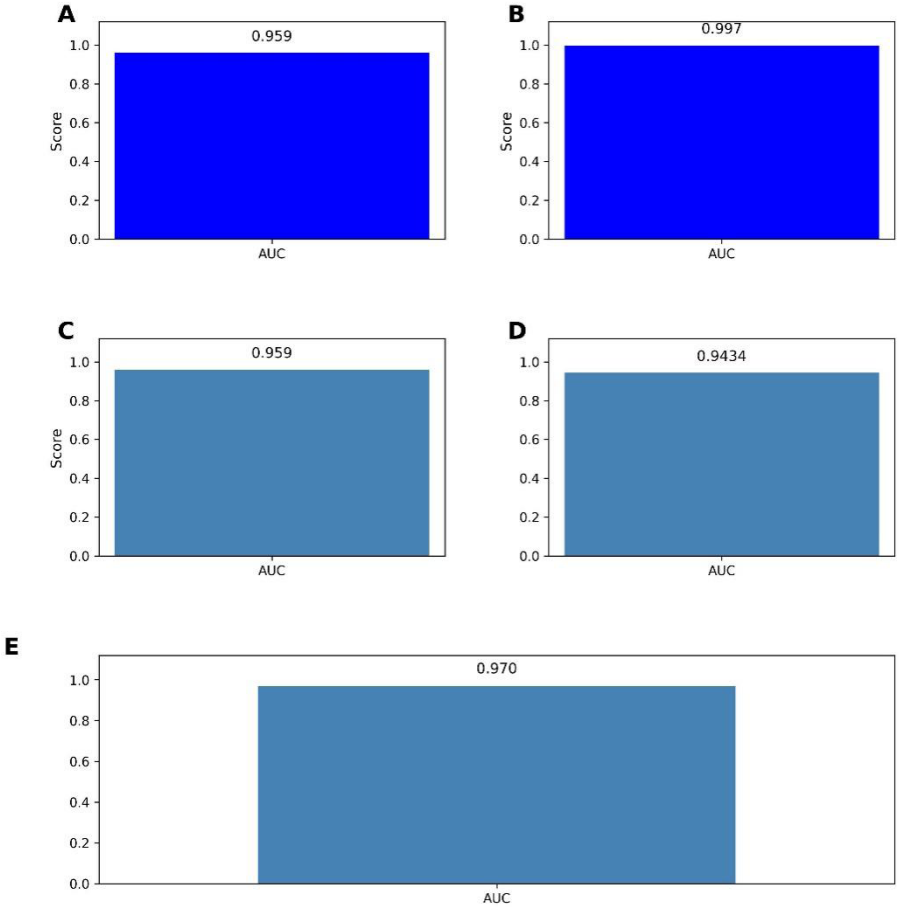


Figure 8. Area under the receiver operating characteristic curve (AUC) comparison of multiple machine learning classifiers, showing consistently high discriminative performance across models, with the support vector machine (SVM) achieving the highest AUC score among all evaluated algorithms. (A) Decision tree. (B) Logistic regression. (C) Random forest. (D) K-nearest neighbors (KNN). (E) SVM.

Table 13. Machine learning vs. fuzzy-machine learning

Aspect	Traditional machine learning	Fuzzy-machine learning
Decision type	Crisp (0 or 1 classification)	Soft decision using membership values
Handling uncertainty	Limited ability to handle uncertainty	Effectively manages uncertainty and vagueness
Data interpretation	Strict boundaries between classes	Allows partial membership in multiple classes
Flexibility	Less flexible in ambiguous data	More flexible with noisy or complex data
Trust evaluation	Direct classification output	Uses membership and divergence for trust scoring

5. Discussion

The proposed hybrid fuzzy logic-controlled behavioral intrusion detection architecture, which includes fuzzy clustering, rule-based fuzzy inference, and adaptive ML, was thoroughly tested in a ZTN to verify its effectiveness in identifying anomalous insider and external threats. The Zero-Trust execution model limits implicit trust across all communication layers, requiring high specificity in anomaly detection, proactive contextual risk assessments, and monitoring of

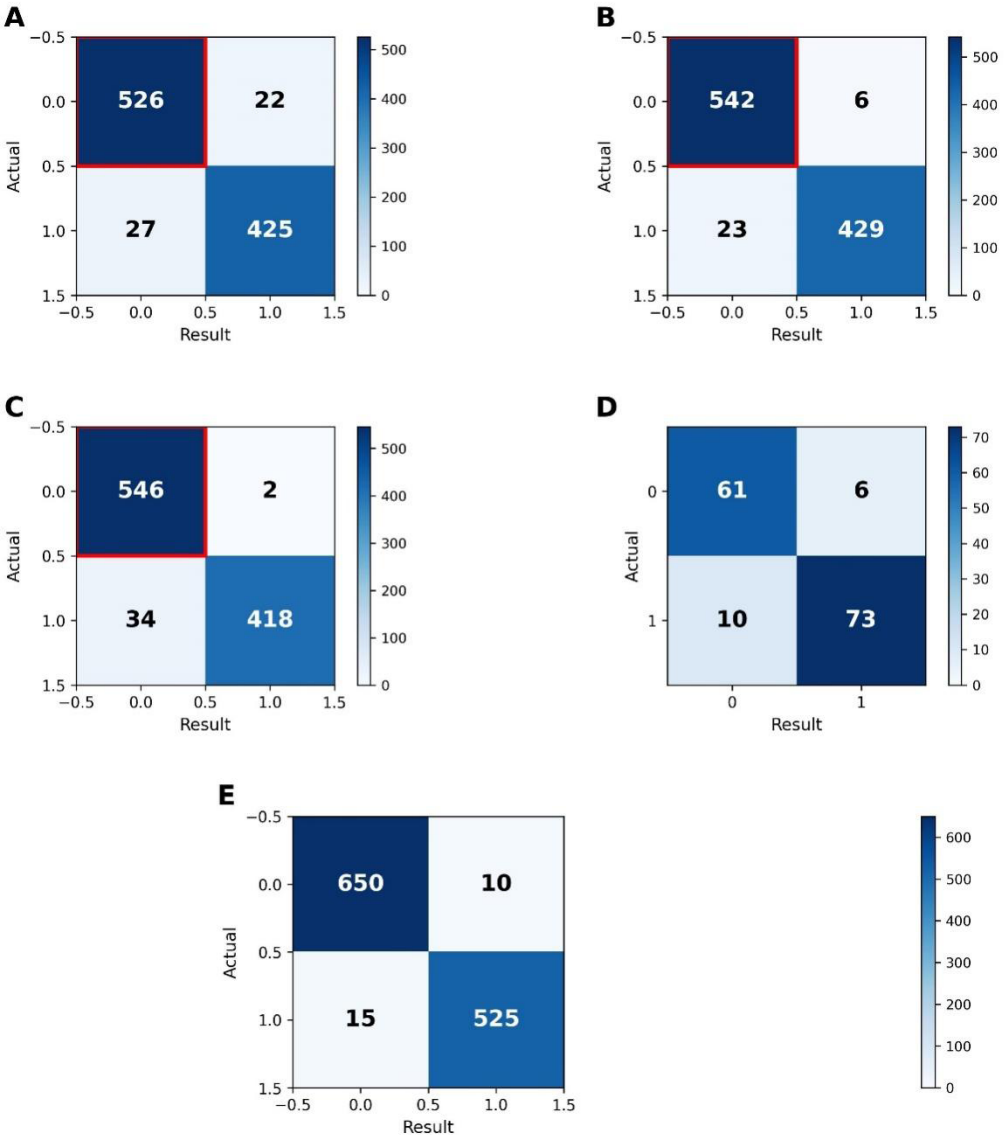


Figure 9. The image compares confusion matrices for decision tree, logistic regression, random forest, K-nearest neighbors (KNN), and support vector machine (SVM) models, showing prediction accuracy and misclassification counts. The SVM model achieves the highest accuracy with the fewest false predictions. (A) Decision tree. (B) Logistic regression. (C) Random forest. (D) K-nearest neighbors (KNN). (E) SVM.

behavioral deviations. Fuzzy clustering helped the system handle decision ambiguities common in real-world network events, where benign and suspicious patterns often share similar behavioral traits. Additionally, the fuzzy rule-based adaptive scoring system implemented a dynamic penalty for sudden changes in transactional, access, and privilege patterns, significantly improving classification stability and reducing misclassifications.

The standard performance metrics of accuracy, F1-score, recall, and AUC were used to compare five traditional and ensemble ML classifiers: decision tree, logistic regression, random forest, XGBoost, and SVM. To ensure consistency, all models were trained on the same fuzzy-filtered features and tested with k-fold cross-validation to reduce bias from data sampling. Results showed that the SVM model achieved the best overall performance, with an accuracy of 98.00%, an F1-score of 96.50%, a recall of 97.20%, and an AUC of 97.00%, outperforming the other models. This is because SVM is better suited to handling non-linear separability in a high-dimensional,

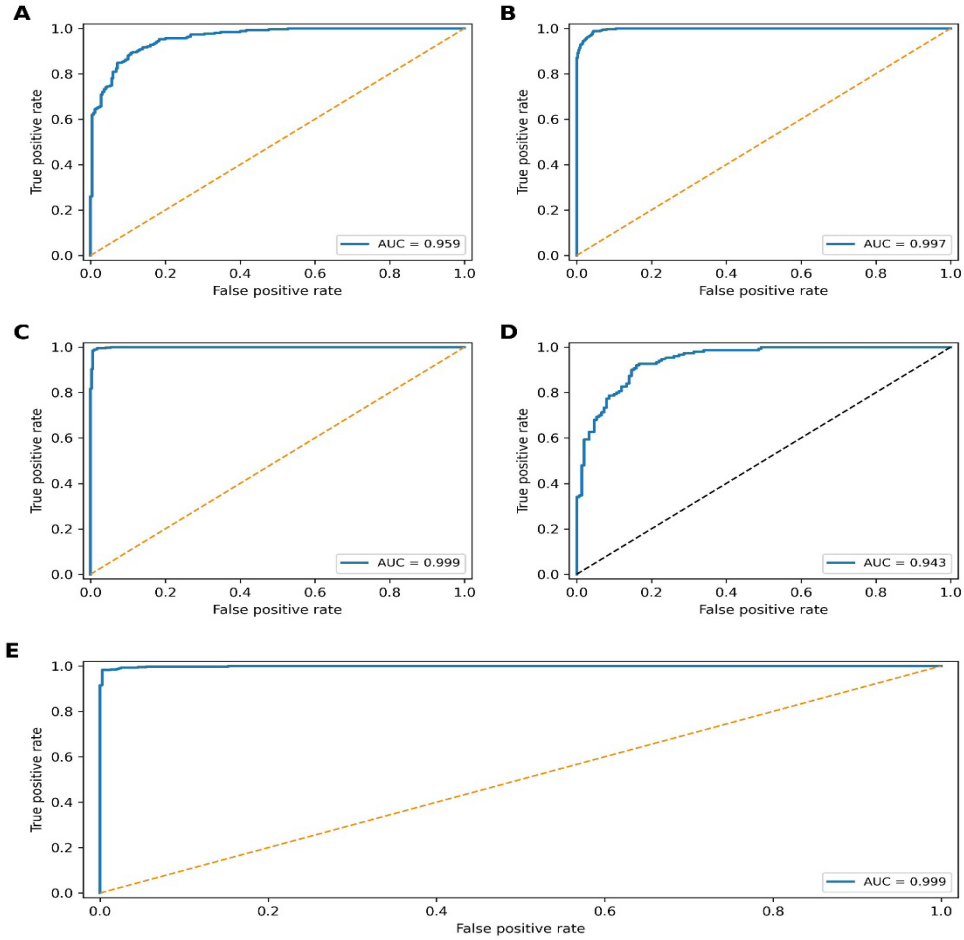


Figure 10. Receiver operating characteristic (ROC) curves for the evaluated classification models: (A) decision tree, (B) logistic regression, (C) random forest, (D) K-nearest neighbors (KNN), and (E) support vector machine (SVM). Random forest and SVM achieved the highest area under the curve (AUC) of 0.999, indicating excellent discriminative performance.

fuzzy-weighted feature space, enabling margin-maximized classification and clear separation between benign and intruder classes.

Additionally, recall, or the ability to detect intrusions without omission, was highest in SVM (97.20%). ZTN applications especially need the recall metric because false negatives can have serious consequences, as offenders can bypass perimeter controls and laterally escalate privileges. The fuzzy logic element also improved recall by dynamically generating risk scores based on time context rather than relying on static signature matching. This ensured that low-frequency but high-risk behavioral abnormalities were not misclassified as benign due to dataset imbalance or rarity. Decision tree, by contrast, showed the lowest recall (90.50%), indicating it is more prone to overfitting and less effective at uncovering zero-day anomaly patterns.

Additional AUC results show that the architecture reliably distinguishes between normal and abnormal entities, with SVM achieving 97.00, outperforming XGBoost (96.10) and random forests (95.30). The rise in AUC supports the conclusion that fuzzy-based feature changes enhance probabilistic separability and improve discrimination, even within ambiguous behavioral ranges. Single-path rule learning with the decision tree model produced the lowest AUC (88.00), indicating that rule learning is not suited to multi-dimensional fuzzy-weighted data.

Typically, these three methods are fused to build a system of fuzzy representations of knowledge which evolves over time to capture continuous intrusion events rather than snapshot representations of threats.[26] This represents a

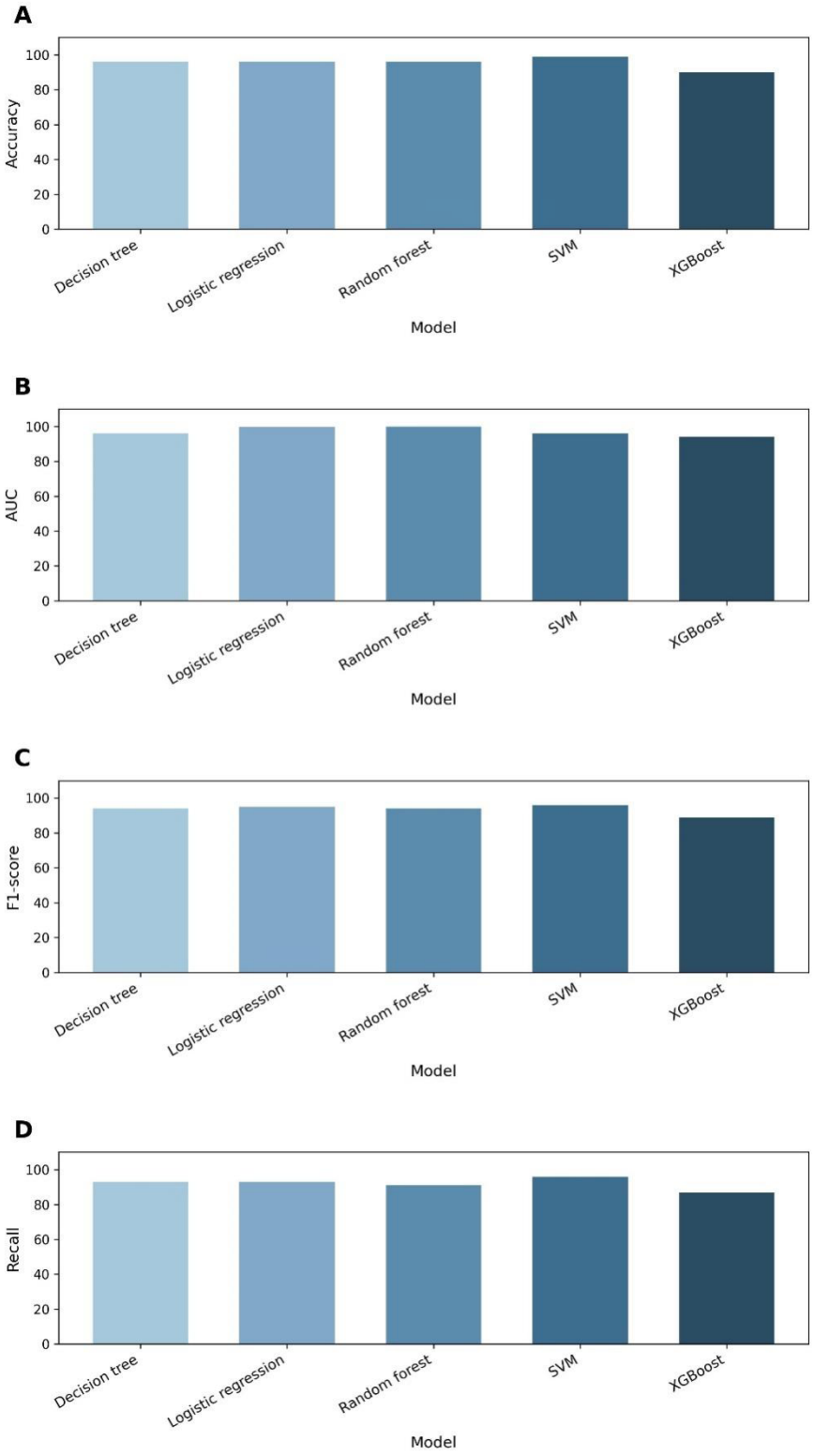


Figure 11. The images compare five models (decision tree, logistic regression, random forest, support vector machine [SVM], and extreme gradient boosting [XGBoost]) in terms of (A) accuracy, (B) area under the receiver operating characteristic curve (AUC), (C) F1-score, and (D) recall using bar charts. Random forest and SVM show superior performance across most evaluation metrics.

significant step toward moving from signatures to behavior-based trust assessment, a key component of Zero-Trust architecture.

As the experimental results support, the proposed hybrid architecture aligns with Zero-Trust principles by employing the never-trust, always-verify, and constantly-validate approach. The architecture demonstrates better anomaly detection than traditional IDS, reduces false alarms, and achieves a very high level of reliability in intrusion rejection without significantly disrupting normal traffic. The superior performance of SVM reinforces its suitability as the most appropriate classifier for fuzzy-driven Zero-Trust behavioral security systems, especially in high-dimensional, ambiguous, and adversarial traffic environments where threat agents use evasion techniques to manipulate patterns.

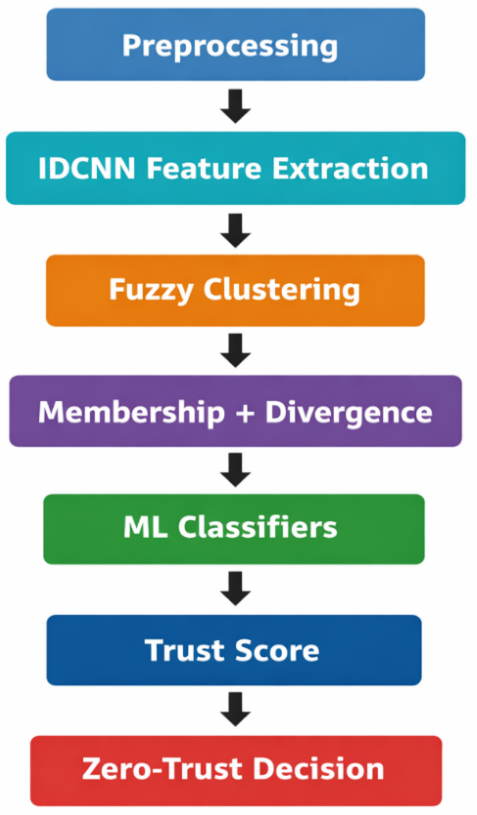


Figure 12. Zero-Trust decision model of data analysis. The input data were first preprocessed to clean and prepare them for analysis. An improved deep convolutional neural network (IDCNN) then extracted significant features; finally, fuzzy clustering and membership-divergence analysis determined the data's similarities and uncertainties. Lastly, machine learning (ML) classifiers calculated a trust score to inform the ultimate Zero-Trust security decision.

In summary, the findings suggest that combining fuzzy logic with adaptive ML can significantly improve threat-detection accuracy and the feasibility of operational decisions in Zero-Trust settings. Its architecture is resilient to unknown threat vectors, can be easily scaled as organizational baselines change, and offers quantifiable performance enhancements across all evaluation metrics compared to standalone ML systems.

5.1. Interpretation through the Zero-Trust architecture lens

Context-aware tuning of micro-segmentation rules enables policies to adapt to dynamic conditions. Fuzzy logic further enhances this adaptability by reducing policy misfires commonly observed in deterministic rule engines. Fuzzy clustering dynamically assigns behavioral groups, aligning with Zero-Trust principles by computing trust levels on the fly rather than relying on fixed access tokens. Risk-weighted access using adaptive ML classifiers enables user and device trust scores to fluctuate in real time. The classification performance of the SVM-based architecture, in terms of behavioral consistency, demonstrates its compliance with continuous verification and automated trust scoring, which are essential components of a Zero-Trust policy.

Moreover, the computational variance analysis in our system showed that SVM was superior to the other classifiers, especially in minimizing false positives, a sensitive parameter in intrusion prevention, where a high rate of false alarms compromises the system's operational efficiency.

5.2. Limitations of the proposed approach

Although the proposed hybrid fuzzy logic-driven behavioral intrusion detection architecture shows promising results in identifying abnormal behavior in Zero-Trust environments, it has several limitations. These limitations are important for the practical use of the framework and for its future development.

5.2.1. Generalizability

These were experimental evaluations of the suggested framework using benchmark intrusion detection datasets, including UNSW-NB15, CIC-IDS2017, and CSE-CIC-IDS2018. The datasets used are well-known in cybersecurity studies; however, they may not fully capture the diversity of traffic patterns found in real enterprise networks. User behaviors, protocol distributions, and security policies vary widely across organizations

concerning network infrastructure. As a result, the model's performance on controlled datasets might not generalize well to diverse real-world environments. To enhance the generalizability of the proposed architecture, it should be tested on cross-organizational data and live network traffic in the future.

5.2.2. Scalability

The other weakness concerns the scalability of the proposed framework for large-scale network infrastructures. Even though fuzzy clustering and adaptive ML together increase detection accuracy, they incur additional computational cost when fusing features, performing membership estimation, and computing the divergence score. Processing large amounts of traffic data in real time can be necessary in high-throughput networks (such as cloud data centers or IoT ecosystems) and can be optimized using specialized implementations or distributed computing systems. Future research can explore scalable architectures, such as edge computing, parallel processing, or federated learning, to achieve real-time performance in large, dynamic network environments.

5.2.3. Dataset realism

The datasets used in this study included labeled attack scenarios created under controlled settings. They may offer inspiring points of reference for assessing intrusion detection algorithms, but they might not fully capture the complexity of contemporary cyber threats, such as stealthy multi-stage attacks, adversarial evasion mechanisms, and adaptive attack patterns. Moreover, some attack types in this data are underrepresented, which can affect model learning and evaluation results. Future research should be enhanced by using continuously updated threat intelligence feeds, real-world network telemetry, and simulations of adversarial attacks to better reflect the real-world cybersecurity environment.

6. Conclusion

This study presents a hybrid fuzzy logic-driven behavioral intrusion detection architecture for intrusion detection that combines fuzzy clustering with adaptive ML to address limitations of previous Zero-Trust intrusion detection methods. The research introduces a new uncertainty-aware learning pipeline that reduces behavioral overlap and enhances decision accuracy by assigning probabilistic memberships, surpassing traditional hard-label classification approaches used by earlier researchers. The architecture also elevates Zero-Trust enforcement through its loop-based authorization, enabling dynamic trust recalibration without human intervention, rather than relying on constant thresholding or frequent model retraining. This approach has demonstrated greater operational viability even amid evolving threat environments. Experiments confirm that integrating fuzzy computational outputs into adaptive ML significantly improves classification accuracy, model resilience, and risk scoring, enabling earlier threat detection with fewer false positives. The novelty of this work lies in combining fuzzy logic-based uncertainty modeling, adaptive inference, and Zero-Trust policy integration into a unified behavioral-detection system capable of deciphering ambiguous patterns at a highly sensitive and responsive level. Future research can expand on this model by using generative adversarial simulation to create evasive attack scenarios to enhance intrusion detection; employing attestation of trust to support distributed inference, where real-time Zero-Trust enforcement faces increased complexity due to resource limits and environmental noise; and refining the architecture to better support edge-heavy networks.

In contrast to traditional IDS models, the proposed architecture provides explicit uncertainty modeling by using fuzzy divergence measures in conjunction with adaptive ML and Zero-Trust trust scoring, thereby offering a more resilient decision framework in behavioral environments.

Acknowledgments

None.

Funding

This work was funded by the Faculty of Engineering and Quantity Surveying, INTI International University Colleges, Nilai, Negeri Sembilan, Malaysia.

Conflict of interest

The authors declare they have no competing interests.

Author contributions

Conceptualization: Azhar Ali Khan, Suneeza Hamid, Sawera Kanwal, Mohamed Hafez

Formal analysis: Muhammad Kamran, Muhammad Farman, Evren Hincal
Investigation: Azhar Ali Khan, Suneeza Hamid, Sawera Kanwal, Muhammad Kamran
Methodology: Azhar Ali Khan, Suneeza Hamid, Sawera Kanwal
Writing – original draft: Azhar Ali Khan, Suneeza Hamid, Sawera Kanwal
Writing – review & editing: Muhammad Kamran, Muhammad Farman, Mohamad Hafez, Evren Hincal

Availability of data

Not applicable.

AI tools statement

All authors confirm that no AI tools were used in the preparation of this manuscript.

References

1. Karakaya A. A Hybrid Approach for IoT Security: Combining Ensemble Learning with Fuzzy Logic. *Sensors*. 2025;25(18):5668.

   doi: 10.3390/s25185668

2. Lilhore UK, Simaiya S, Alroobaea R, et al. SmartTrust: a hybrid deep learning framework for real-time threat detection in cloud environments using Zero-Trust Architecture. *J Cloud Comp*. 2025;14(1).

   doi: 10.1186/s13677-025-00764-7

3. Ogendi EG. Leveraging Advanced Cybersecurity Analytics to Reinforce Zero-Trust Architectures within Adaptive Security Frameworks. *Int J Res Publ Rev*. 2025;6(2):691-704.

   doi: 10.55248/gengpi.6.0225.0729

4. Tiwari S, Sarma W, Srivastava A. Integrating artificial intelligence with Zero-Trust architecture: Enhancing adaptive security in modern cyber threat landscape. *Int J Res Anal Rev*. 2022:9(2):712–728

5. Stodt, F. *Building a secure and scalable distributed network using blockchain and Zero-Trust for IIoT*. Doctoral thesis. Université de Strasbourg; 2025.

6. Alshieck Ali B. *Efficient Trust-Aware Authentication and Task Offloading in Multi-Access Edge Computing Using a Dual Fuzzy Method Based Zero Trust Security Framework*. Doctoral thesis. RMIT University; 2023.

   doi: 10.25439/RMT.27602841

7. Cicek NE, Shafae N. Zero-Trust micro-segmentation in cloud environments: A systematic literature review of strategies, challenges, and future trends. *Cloud Security Review*. 2025.

8. Akter L, Mollah MM, Sany NJ, Ahamed S. Zero-Trust access control systems by artificial intelligence in hybrid cloud environments. *Best J Innov Sci Res Dev*. 2022;1(3):45–69.

9. Camila MG. A Multi-Tenant Cloud Security Framework Using Zero-Trust Architecture and AI-Based Anomaly Detection. *AIJCST*. 2024;6.

   doi: 10.63282/3117-5481/aijcst-v6i4p101

10. Fojude, M. *Insider threat agent: Behavioral-based Zero-Trust access control using machine learning agents*. Master's thesis. Georgia Southern University; 2024.

11. Saeedi Taleghani E, Maldonado Valencia RI, Sandoval Orozco AL, García Villalba LJ. Trust Evaluation Techniques for 6G Networks: A Comprehensive Survey with Fuzzy Algorithm Approach. *Electronics*. 2024;13(15):3013.

    doi: 10.3390/electronics13153013

12. Liu Z, Li X, Mu D. Data-Driven Zero Trust Key Algorithm. Ning X, ed. *Wirel Commun Mob Comput*. 2022;2022(1).

    doi: 10.1155/2022/8659428

13. Siddiqui EF, Haleem M, Ahmad SF, Salhi A, Zamani AT, Varish N. A Multi-Layered AI-Driven Cybersecurity Architecture: Integrating Entropy Analytics, Fuzzy Reasoning, Game Theory, and Multi-Agent Reinforcement Learning for Adaptive Threat Defense. *IEEE Access*. 2025;13:170235-170257.

    doi: 10.1109/access.2025.3610526

14. Itodo CA. *A novel framework for the adoption of Zero-Trust security for organizations*. Doctoral thesis. University of Cincinnati; 2024.

15. Arisdakessian S, Wahab OA, Mourad A, Otrok H, Guizani M. A Survey on IoT Intrusion Detection: Federated Learning, Game Theory, Social Psychology, and Explainable AI as Future Directions. *IEEE Internet Things J*. 2023;10(5):4059-4092.

    doi: 10.1109/jiot.2022.3203249

16. Karthick, R. Securing digital ecosystems through a hybrid AI-cloud framework against zero-day attacks. *ResearchGate*. 2025.

17. Mao Y, Fu W, Zhao Y, Yuan Z, Sun Z, Zhao Y. A Zero-Trust Access Control Model Based on Attribute and Dynamic Trust Evaluation for Cloud Environments. *Symmetry*. 2025;17(12):2059.

    doi: 10.3390/sym17122059

18. Wang R, Li C, Zhang K, Tu B. Zero-trust based dynamic access control for cloud computing. *Cybersecurity*. 2025;8(1).

doi: 10.1186/s42400-024-00320-x

19. Hamad NA, Bakar KAA, Qamar F, Jubair AM, Mohamed RR, Mohamed MA. Systematic Analysis of Federated Learning Approaches for Intrusion Detection in the Internet of Things Environment. *IEEE Access*. 2025;13:95410-95444.

    doi: 10.1109/access.2025.3574672

20. Meda F. Secure communications in the era of digital trust: Global frameworks and Zero-Trust architectures. *Secur Commun Digit Trust*. 2025.

21. Xu D, Gondal I, Yi X, Susnjak T, Watters P, McIntosh TR. The Erosion of Cybersecurity Zero-Trust Principles Through Generative AI: A Survey on the Challenges and Future Directions. *JCP*. 2025;5(4):87.

    doi: 10.3390/jcp5040087

22. Li K, Li C, Yuan X, Li S, Zou S, Sohail Ahmed S, et al. Zero-Trust Foundation Models: A New Paradigm for Secure and Collaborative Artificial Intelligence for Internet of Things. *IEEE Internet Things J*. 2025;12(22):46269-46293.

    doi: 10.1109/jiot.2025.3603957

23. Ang S, Huy S, Janarthanan M. Utilizing IDS and IPS to Improve Cybersecurity Monitoring Process. *JCSRA*. 2025;2025(3):77-88.

    doi: 10.63180/jcsra.thestap.2025.3.10

24. Bankó MB, Dyszewski S, Králová M, et al. Advancements in Machine Learning-Based Intrusion Detection in IoT: Research Trends and Challenges. *Algorithms*. 2025;18(4):209.

    doi: 10.3390/a18040209

25. Erskine SK. Real-Time Large-Scale Intrusion Detection and Prevention System (IDPS) CICIoT Dataset Traffic Assessment Based on Deep Learning. *ASI*. 2025;8(2):52.

    doi: 10.3390/asi8020052

26. Demir G. The Synergy of Fuzzy Logic and Multi-Criteria Decision-Making: Application Areas and Global Trends. *JIDMIS*. 2025;2:429-455.

    doi: 10.59543/jidmis.v2i.14157

27. Nwokoro CO, Ejegwa PA. A Decade of Picture Fuzzy Sets in Multi-Criteria Decision-Making: A Comprehensive Review of Trends, Gaps, and Future Directions. *KADSA*. 2025;1:145-164.

    doi: 10.59543/kadsa.v1i.14051

28. Sarkar A, Paul RK, Yeasin M, Singh AK, Paul AK. FuzzyML: fuzzy based machine learning models for predicting agricultural prices. *ProcIndian Natl Sci Acad*. 2025.

    doi: 10.1007/s43538-025-00482-3

29. Arul K. Advancing Diabetes Risk Prediction Using Anfis: a Fuzzy-Logic Approach for Improved Healthcare Decision Support. In: *2025 3rd International Conference on Artificial Intelligence and Machine Learning Applications Theme: Healthcare and Internet of Things (AIMLA)*. IEEE; 2025:1-6.

    doi: 10.1109/aimla63829.2025.11040564

30. Rahman A, Kundu D, Debnath T, et al. From AI to the era of explainable AI: Current state and future outlook. *Expert Syst*. 2025;42(6).

    doi: 10.1111/exsy.70060

31. Alkhanbouli R, Matar Abdulla Almadhaani H, Alhosani F, Simsekler MCE. The role of explainable artificial intelligence in disease prediction: a systematic literature review and future research directions. *BMC Med Inform Decis Mak*. 2025;25(1).

    doi: 10.1186/s12911-025-02944-6

32. Topuz K, Bajaj A, Coussement K, Urban TL. Interpretable machine learning and explainable artificial intelligence. *Ann Oper Res*. 2025;347(2):775-782.

    doi: 10.1007/s10479-025-06577-w

33. Oladimeji OO, Taiwo GA, Adenusi DA. Unveiling the footprints of explainable AI in Industry 4.0/5.0: a systematic review and bibliometric exploration. *Data Sci Manag*. 2026;9(1):100160.

    doi: 10.1016/j.dsm.2025.07.002

34. Mohammad SI, Yogeesh N, Raja N, Jabeen FTZ, Ahamed BA, Vasudevan A. Integrating fuzzy logic into economic viability studies for sustainable farming. *Appl Math Inf Sci*. 2025;19(2):387-401.

    doi: 10.18576/amis/190214

35. Kalmykov VL, Kalmykov LV. Towards eXplicitly eXplainable Artificial Intelligence. *Inf Fusion*. 2025;123:103352.

    doi: 10.1016/j.inffus.2025.103352

36. Maußner C, Oberascher M, Autengruber A, Kahl A, Sitzenfrei R. Explainable artificial intelligence for reliable water demand forecasting to increase trust in predictions. *Water Res*. 2025;268:122779.

    doi: 10.1016/j.watres.2024.122779

37. Alkubaisi H, Danandeh Mehr A, S A, Khan MMH. Drought modelling and forecasting using shallow and deep machine learning techniques. *Model Earth Syst Environ*. 2024;11(1).

    doi: 10.1007/s40808-024-02268-w

Dr Muhammad Kamran *serves as an adjunct faculty member at the International Center for Interdisciplinary Research in Sciences, The University of Lahore, Lahore, Pakistan. His*

research focuses on fuzzy logic, graph-based networks, and intelligent systems.

https://orcid.org/0009-0000-5467-0497

Azhar Ali Khan *received his M.Phil. degree in computer science at the National College of Business Administration and Economics (NCBA&E), Sub Campus Multan, Pakistan. His primary research focused on cybersecurity and data science. He is currently a lecturer and researcher at NUML University, Multan, Pakistan. He has authored and presented research papers in cybersecurity, automobile wireless security, data science, blockchain, quantum computing, and big data analytics.*

https://orcid.org/0009-0008-1372-8312

Dr Suneeza Hamid *is working as an Assistant Professor at the Department of Information Technology Government College Women University, Faisalabad. Her research interests include artificial intelligence and machine learning.*

https://orcid.org/0009-0007-3771-409X

Sawera Kanwal *received her MS in Computer Science from UMT Lahore and currently serves as a Lecturer in the Department of Computer Science at the University of South Asia, Raiwind Campus, Lahore. She is actively involved in teaching and research. Her research interests include artificial intelligence, machine learning, cybersecurity, and uncertainty-aware decision-making, with a focus on behavioural intrusion detection, fuzzy logic-based security models, and Zero-Trust architectures to reduce false positives and improve adaptive trust management.*

https://orcid.org/0009-0009-6002-7313

Dr Muhammad Farman *obtained his Ph.D. Mathematics from the University of Lahore in 2019, Pakistan, and a postdoctoral fellowship from Universitas Airlangga Indonesia, Lebanese American University, and Near East University, North Cyprus, Turkey. Adjunct Professor (Research) at Universitas Airlangga Indonesia and the University of Lahore, Pakistan. He is currently an Associate Professor at Near East University. He has more than eight years of teaching and research experience. His research fields are mathematical biology, control theory, numerical analysis, and the application of fractional calculus to epidemic models. He has published more than 300 research papers in well-regarded SCI and Scopus journals and presented his work at several national and international conferences. He has won several awards, including the Research Excellence Awards (Best Researcher of the University) in 2019 and 2020 at the University of Lahore. Stanford University's Top 2% Scientists of 203, 2024 in Applied Mathematics. Best Academic Performance Award 2024, Publication Honorary Award 2024, and the Most Impactful Researcher Award 2024, Near East University, 2024.*

https://orcid.org/0000-0001-7616-0500

Professor Dr Evren Hincal *is currently working as a Professor at Near East University. He has more than 10 years of teaching and research experience.*

Professor Dr Mohamed Hafez *works as a professor of research in the Faculty of Engineering and Quantity Surveying, INTI International University Colleges, Nilai, Negeri Sembilan, Malaysia*

https://orcid.org/0000-0001-6537-4247

This work is licensed under a Creative Commons Attribution 4.0 International License. The authors retain ownership of the copyright for their article, but they allow anyone to download, reuse, reprint, modify, distribute, and/or copy articles in IJOCTA, so long as the original authors and source are credited. To see the complete license contents, please visit http://creativecommons.org/licenses/by/4.0/.