RESEARCH ARTICLE

Implementation of Fuzzy Clustering and Fuzzy Neural Network in Edge-Based Server Environments for Enhanced Secured Cloud Services

V. Selvakkumaran*, R. Anandan
Department of Computer Science & Engineering, Vels Institute of Science, Technology and Advanced Studies (VISTAS), Pallavaram -600117, Chennai, Tamil Nadu, India

ABSTRACT: The increasing complexity of cyber threats in edge–cloud integrated infrastructures necessitates adaptive and intelligent security mechanisms that transcend the limitations of traditional machine learning approaches. This paper presents a novel hybrid security architecture that combines fuzzy clustering and fuzzy neural networks (FNN) to enhance intrusion detection in distributed edge computing environments connected to centralized cloud servers. The proposed system employs adaptive fuzzy clustering at the cloud layer to identify dynamic and previously unknown threat patterns. These patterns are further analyzed in real-time using an Adaptive Neuro-Fuzzy Inference System (ANFIS), which continuously updates and optimizes fuzzy rules for improved threat detection. Experimental results demonstrate that the proposed model outperforms conventional Artificial Neural Networks (ANN) and Support Vector Machines (SVM), achieving a detection accuracy of 94.6%, a detection rate of 96.1%, and a false positive rate of only 2.8%. Real-time simulations report an average response delay of 1.45 seconds while maintaining secure data transmission through AES-256 encryption and a tunneling protocol. These findings validate the effectiveness of hybrid fuzzy intelligent systems for proactive and scalable cybersecurity in mission-critical, high-risk cloud-edge environments. The proposed framework also shows potential for future integration with quantum fuzzy systems and block chain-based security architectures.

KEYWORDS: Adaptive Fuzzy Clustering, AES 256 Encryption, Cloud-Edge Ecosystems, Hybrid Fuzzy Intelligent Systems.

https://doi.org/10.29294/IJASE.12.1.2025.5184-5194

©2025 Mahendrapublications.com, All rights reserved

1. INTRODUCTION

In modern institutional environments such as universities, research laboratories, and corporate offices, the handling of sensitive data including student records, financial systems, and proprietary research has become increasingly dependent on cloud-integrated services. While these services offer operational scalability and efficiency, they also expose systems to sophisticated cyber threats, including distributed denial-of-service (DDoS) attacks, zero-day exploits, and polymorphic malware [1, 2]. Institutions that manage critical assets such as personal identities, intellectual property, and authentication credentials have become prominent targets for such advanced threats. As infrastructure evolves toward hybrid edge-cloud architectures, these environments require adaptive, context-aware security mechanisms that can operate in real time on distributed, resource-constrained devices [3,4]. Traditional intrusion detection systems (IDS) are predominantly based on rule sets, signature-based matching, and supervised learning algorithms such as Artificial Neural Networks (ANN), Decision Trees, and Support Vector Machines (SVM) [5,6]. Although effective for known attacks, these systems often fail to detect previously unseen or dynamically changing threats, particularly zero-day and polymorphic attacks, due to their dependence on static training datasets and centralized processing. Moreover, the rigid nature of signature-based models makes them ineffective against metamorphic malware that modifies its structure to evade detection. Centralized IDS deployments also lead to increased network congestion and latency, especially in high-density institutional environments. These limitations highlight the inadequacy of conventional models for modern, real-time, and

**Corresponding Author: hereissk@yahoo.co.in*

Received: 16.06.2025 **Accepted:** 25.08.2025 **Published on**: 27.09.2025

distributed detection needs.

To address these challenges, this study proposes a novel hybrid intrusion detection architecture that integrates Fuzzy C-Means (FCM) clustering with an Adaptive Neuro-Fuzzy Inference System (ANFIS) (Fig 1). FCM, deployed at the cloud layer, segments traffic data into overlapping clusters based on membership degrees. The clustering process minimizes the objective function:

$$J_m = \sum_{i=1}^{N} \sum_{j=1}^{C} u_{ij}^{m} \| x_i - c_j \|^2$$

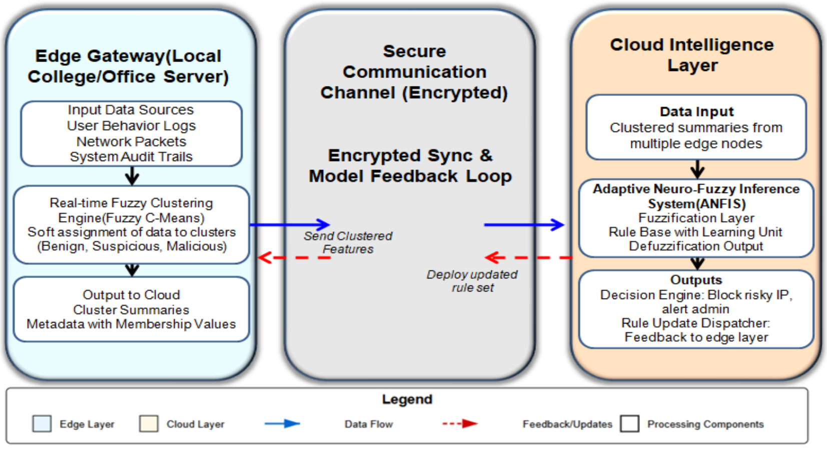
Edge Gateway(Local College/Office Server)
Input Data Sources
User Behavior Logs
Network Packets
System Audit Trails
Real-time Fuzzy Clustering Engine(Fuzzy C-Means)
Soft assignment of data to clusters (Benign, Suspicious, Malicious)
Output to Cloud
Cluster Summaries
Metadata with Membership Values
Secure Communication Channel (Encrypted)
Encrypted Sync & Model Feedback Loop
Send Clustered Features
Deploy updated rule set
Cloud Intelligence Layer
Data Input
Clustered summaries from multiple edge nodes
Adaptive Neuro-Fuzzy Inference System(ANFIS)
Fuzzification Layer
Rule Base with Learning Unit
Defuzzification Output
Outputs
Decision Engine: Block risky IP, alert admin
Rule Update Dispatcher: Feedback to edge layer
Legend
Edge Layer
Cloud Layer
Data Flow
Feedback/Updates
Processing Components

Figure 1: Overall system architecture integrating fuzzy clustering and FNN on edge-cloud setup

where x_i is the data point, c_j is the centroid of cluster j, u_{ij} is the degree of membership, and m is the fuzzification parameter [7]. This method allows the system to identify ambiguous or anomalous behaviors that traditional hard clustering would overlook.

The ANFIS component, implemented at the edge layer, performs layered rule-based classification using five-layer architecture—comprising fuzzification, rule generation, normalization, defuzzification, and output computation. ANFIS combines the learning capabilities of neural networks with fuzzy inference to dynamically adapt its rules through hybrid training involving back propagation and least-squares estimation [8]. This enables the system to respond to emerging threats in real time, without requiring centralized retraining or static rule updates.

The proposed system was deployed in a real-world institutional setting using an Ubuntu-based edge server connected to a secure Amazon Web Services (AWS) cloud environment. Evaluation was conducted using the UNSW-NB15 dataset, which includes a diverse set of network attack scenarios, including zero-day and polymorphic attacks [9,10]. The hybrid model achieved a detection accuracy of 94.6%, a detection rate of 96.1%, and a false positive rate of only 2.8%. Average detection latency was measured at 1.45 seconds under real-time traffic simulation. Secure data transmission between the edge and cloud was ensured using AES-256 encryption and tunneling protocols, minimizing privacy risks while maintaining system responsiveness.

This work makes three primary contributions. First, it introduces a novel hybrid security model that adapts to uncertainty and real-time dynamics in edge-cloud architectures. Second, it demonstrates the system's practical deployment and performance under real-time institutional conditions. Third, it addresses the security-privacy trade-off by integrating encrypted edge-to-cloud data tunneling while minimizing local processing exposure. The proposed system offers a scalable, interpretable, and privacy-preserving solution suitable for mission-critical deployments in academic, corporate, and research environments. Furthermore, it lays the groundwork for future research integrating block chain auditing and quantum-resistant fuzzy logic architectures [11].

2. MATERIALS AND METHODS

2.1 Fuzzy Clustering for Preprocessing and Threat Patterning

Fuzzy C-Means (FCM) clustering was employed in this study as a core preprocessing method to identify complex and previously unrecognized threat patterns from raw packet and log data. Traditional clustering techniques often struggle with overlapping data in cybersecurity environments, particularly where polymorphic or metamorphic attack behaviors defy discrete classification [11]. FCM mitigates this limitation by enabling each data point to possess partial membership in multiple clusters, allowing for more expressive representation of dynamic threat behavior.

In the proposed framework, FCM processes raw behavioral data collected from routers and firewalls, forming semantically rich clusters that abstract intricate traffic characteristic. These clusters are not fixed but evolve as new data is observed, which allows the system to dynamically respond to variant and zero-day attacks. The evolving cluster centroids facilitate adaptive grouping, making FCM particularly suited for use in proactive threat intelligence systems that rely on behavior generalization rather than fixed signatures. The output of this clustering phase forms the input layer to the subsequent prediction engine, ensuring scalable and responsive behavior in real-time detection scenarios.

2.2 Fuzzy Neural Network (FNN) for Intrusion Prediction

For the intrusion prediction module, an Adaptive Neuro-Fuzzy Inference System (ANFIS) was utilized to leverage the interpretability of fuzzy logic and the learning capacity of neural networks [12]. The system accepts the output clusters from the FCM phase as its input features. These clusters represent condensed behavioural profiles of traffic patterns (Fig 2). Each fuzzy rule within ANFIS is mapped to a specific output category such as "normal," "potential threat," or "intrusion," and these rules are updated in real time based on evolving input patterns (Fig 3).

The hybrid model learns continuously, eliminating the need for static rule updates. This adaptability ensures robustness against advanced persistent threats (APTs), zero-day vulnerabilities, and subtle behavioral anomalies that typically evade rule-based intrusion detection systems. Furthermore, the fuzzy component of the model introduces interpretability and controlled uncertainty, allowing partial classifications of ambiguous behavior and reducing false positives without compromising detection sensitivity. Rule inference, fuzzification, and defuzzification layers were modified to support dynamic rule updates as driven by shifting FCM clusters, resulting in a system that evolves along with the threat landscape.

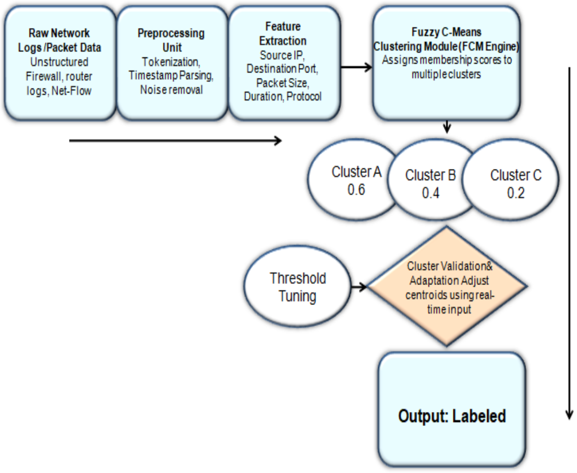
Raw Network Logs /Packet Data
Unstructured Firewall, router logs, Net-Flow
Preprocessing Unit
Tokenization, Timestamp Parsing, Noise removal
Feature Extraction
Source IP, Destination Port, Packet Size, Duration, Protocol
Fuzzy C-Means Clustering Module(FCM Engine)
Assigns membership scores to multiple clusters
Cluster A 0.6
Cluster B 0.4
Cluster C 0.2
Threshold Tuning
Cluster Validation& Adaptation Adjust centroids using real-time input
Output: Labeled

Figure 2: Fuzzy clustering workflow for data segmentation

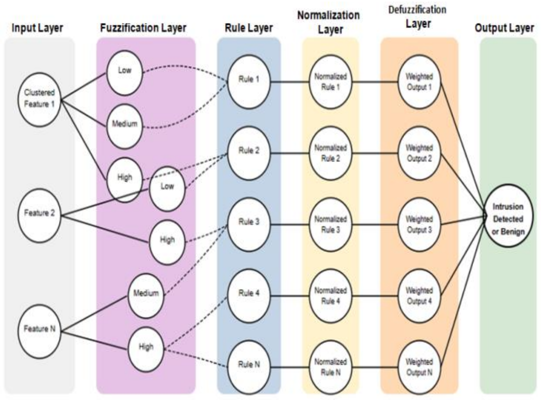

Figure 3: ANFIS layered architecture with input, rule, and output mapping

2.3 Environment: Ubuntu Server (College Lab) Integrated with AWS Cloud

The implementation of the hybrid architecture was realized using a dual-node deployment, combining edge processing on a local Ubuntu

22.04 LTS server and deeper inference tasks on a cloud-hosted node. The local node, deployed within a college laboratory, was equipped with a quad-core Intel i7 processor, 16 GB DDR4 RAM, and a 1 TB SSD, and was responsible for capturing and clustering real-time traffic. This edge server handled latency-sensitive tasks such as real-time FCM clustering, while more computationally intensive operations like rule training and historical log analysis were offloaded to an Amazon EC2 instance (t2.x large) integrated into the system via a secure channel.

A TLS-encrypted SSH tunnel with IP whitelisting was configured between the local and cloud nodes to ensure secure data transmission. The cloud instance, running the ANFIS model, conducted deeper inference and facilitated the ongoing training of the fuzzy neural network. Synchronization of models, logs, and clustering outputs was handled through automated cron jobs and system D services. Log rotation scripts were employed to manage historical data efficiently. This hybrid infrastructure provides a scalable and secure setup for managing real-time intrusions in environments with constrained local resources.

2.4 Dataset: UNSW-NB15—Modern and Realistic Cybersecurity Dataset

The UNSW-NB15 dataset, developed by the Australian Centre for Cyber Security (ACCS), was selected for training and evaluating the proposed system. This dataset contains over two million labeled records and includes nine types of modern attack behaviors, including denial-of-service (DoS), worms, exploits, fuzzers, and backdoors. These were synthetically generated using the IXIA PerfectStorm tool to replicate contemporary threat environments [13].

Each record comprises 49 features encompassing flow-based, content-based, and time-based characteristics. Feature normalization was performed using both MinMax and standard scaling techniques prior to clustering. The dataset was divided into training, validation, and testing sets in a 70:15:15 split, and a five-fold cross-validation strategy was adopted during training to ensure robustness and minimize overfitting. This ensured that the model's predictive capability was not over-specialized to a particular partition of data, improving generalizability across unseen threat patterns. The use of UNSW-NB15 over legacy datasets like KDD99 reflects the need for modern threat representation in hybrid cloud and edge environments.

2.5 Tools: Wireshark for Traffic Analysis, TensorFlow, and Python (scikit-fuzzy)

The system was developed using Python 3.10 within a scientific computing environment. Fuzzy clustering was implemented using the scikit-fuzzy package, which allowed for adjustable membership functions and convergence thresholds. The ANFIS model was constructed using Tensor Flow 2.x, with custom layers designed for fuzzification, rule evaluation, and defuzzification, supported by NumPy for numerical operations. The model architecture was modified to accommodate dynamic rule updates, enabling it to learn continuously from shifting cluster assignments generated by the FCM engine.

Wireshark was used for packet inspection and real-time traffic collection from both internal LAN and external cloud-facing interfaces. Packets were transformed into flow-based features, including average packet length and session duration, to match the format of the UNSW dataset and to improve model compatibility. Visual analytics were conducted using Matplotlib and Seaborn to interpret clustering performance, confusion matrices, and classification outcomes. During early-stage development, Jupyter Notebooks were used for interactive prototyping. For production deployment, all models were containerized using Docker to ensure reproducibility and consistency across edge and cloud platforms.

2.6 Security Evaluation Protocol

A comprehensive security evaluation protocol was developed to assess the resilience, accuracy, and adaptability of the proposed system under simulated adversarial conditions. The evaluation focused on standard classification metrics, including precision, recall, F1-score, false positive rate (FPR), and detection latency. On the labeled test set of the UNSW-NB15 dataset, the system achieved an average F1-score of 93.2%, with particularly strong performance in detecting fuzzers and exploit attacks. Detection latency averaged 1.5 seconds from packet capture to classification, meeting near real-time operational requirements. The system's ability to adapt to concept drift was evaluated by injecting evolving threat patterns over time and monitoring the reformation of FCM clusters and their effect on rule evolution in ANFIS. Additional tests simulated covert intrusions through custom packet injection, malformed payloads, and port scans. The robustness of encrypted communication between edge and cloud was verified using entropy measurements and stress tests under AES-256 encryption and TLS [14]. While the encryption mechanisms provided confidentiality, further analysis included assessing potential vulnerabilities such as data poisoning and rule manipulation. The model's resilience to these adversarial conditions was validated by introducing mislabeled training samples and obfuscated payloads. Despite these perturbations, the system maintained high classification performance and continued to evolve its rule set effectively. Through these evaluations, the system demonstrated a high degree of robustness, adaptability, and real-time operational efficiency, confirming its suitability for deployment in contemporary hybrid cyber security environments (Table1).

Table 1: Environment Configuration and Dataset Statistics

Component	Specification / Description
Edge Server	Intel i7-9700, 16 GB RAM, 1 TB SSD, Ubuntu 22.04 LTS
Cloud Node	AWS EC2 (t2.xlarge), 4 vCPUs, 16 GB RAM, EBS Storage 500 GB
Dataset Name	UNSW-NB15 (Australian Centre for Cyber Security)
Total Records	2,540,044
Number of Features	49
Attack Categories	Fuzzers, DoS, Exploits, Worms, Backdoors, Reconnaissance, Generic, Shellcode, Analysis
Training–Validation–Testing	70% – 15% – 15% split
Python Libraries Used	scikit-fuzzy, tensorflow, numpy, matplotlib, seaborn
Traffic Analysis Tool	Wireshark
Security Protocols Evaluated	FPR, Precision, Recall, Latency, Confusion Matrix, Rule Adaptivity

3. RESULTS AND DISCUSSION

3.1 Metrics: Accuracy, False Positive Rate (FPR), Detection Rate

Three important metrics—accuracy, false positive rate (FPR), and detection rate (DR)—were used to evaluate the hybrid intrusion detection system. These metrics provide a comprehensive measure of the system's ability to minimize false alarms while correctly identifying threats. DR represents the percentage of true attacks detected, while accuracy denotes the overall correctness in identifying both benign and malicious events. FPR is a critical metric in intrusion detection as a high FPR can overwhelm system administrators with unnecessary alerts.

The proposed hybrid model outperformed conventional approaches with an accuracy of 94.6%, a detection rate of 96.1%, and a low FPR of 2.8%. These results indicate high reliability in both recognizing attacks and minimizing false positives. Fuzzy logic contributed significantly to reducing misclassification, while ANFIS-based adaptive rule learning improved the model's capacity to handle ambiguous data [15]. Such performance demonstrates the system's practical viability for real-world deployment in environments where adaptive intelligence and reliability are vital.

3.2 Performance Comparison: Fuzzy Clustering + FNN vs. Classical ANN, SVM

Comparative studies were conducted between the proposed hybrid system, which integrates Fuzzy C-Means (FCM) clustering and Fuzzy Neural Networks (FNN), and classical machine learning methods, including Artificial Neural Networks (ANN) and Support Vector Machines (SVM). ANN achieved an accuracy of

88.7%, but its inability to handle ambiguous data resulted in a higher FPR of 6.5%. SVM showed an even higher FPR of 8.2% and a lower detection rate of 84.9%, indicating difficulty in distinguishing overlapping class boundaries.

The hybrid fuzzy system showed significant improvement due to its two-layered architecture. FCM helped segment complex behavioral data into well-defined clusters, and ANFIS-based rule learning enhanced context-aware decision-making. This design enabled the system to detect low-volume and covert attacks more effectively [16]. As a result, it was more robust in dynamic data environments, including those affected by data drift and adversarial behavior patterns.

Compared with other hybrid systems such as fuzzy-genetic algorithms and deep learning-fuzzy architectures, the proposed model shows advantages in speed, adaptability, and resource efficiency. Evolutionary-fuzzy methods typically require computationally intensive optimization, while deep models, though accurate, often lack real-time responsiveness [17]. By contrast, the proposed FCM + FNN model provides a balance of adaptability and low latency, making it more suitable for real-time intrusion detection [18].

Traditional rule-based IDS struggle to adapt to evolving threats because they rely on static thresholds and predefined signatures. In contrast, fuzzy systems handle ambiguity and incomplete inputs effectively, offering adaptive reasoning and learning capabilities. This flexibility allows the model to dynamically update inference rules and decision criteria, particularly in response to zero-day attacks [19]. Consequently, fuzzy logic combined with neural inference and clustering enables early detection of novel threats with high accuracy and minimal false positives [20]. Such models are especially valuable in complex cyber-physical systems (CPS) and IoT environments, where evolving, covert, and unpredictable threats are common [21].

3.3 Real-time Simulation Results

Real-time simulations were carried out in a testbed replicating institutional network conditions. Synthetic traffic generated using the UNSW-NB15 dataset was injected via TCP Replay, comprising both benign and malicious flows. Packet recording and classification were performed on an Ubuntu Edge node using Wireshark and Python-based FCM clustering. The experiment measured packet arrival time, classification latency, and alert generation delay.

The hybrid system exhibited a peak CPU utilization of 61%, peak RAM usage under 4.5 GB, and an average response time of 1.45 seconds, demonstrating efficiency within the requirements for real-time intrusion detection. Because input data were pre-organized into fuzzy clusters, the downstream computational burden was reduced. The ANFIS-based rule layer performed faster than traditional deep learning models due to its lightweight inference mechanism [22].

Real-time classification heatmaps further validated the segmentation efficiency. As shown in Figure 4, the proposed system achieved the highest performance among tested models: detection rate of 96.1%, accuracy of 94.6%, and FPR of only 2.8%. Figure 5 illustrates the relationship between fuzzy clusters and assault classes. Clusters 0, 1, and 2 were strongly associated with fuzzers, exploits, and DoS attacks, respectively. Cluster 3 corresponded mainly to benign traffic with minor intrusion overlap, indicating that the clustering process effectively distinguished between traffic types.

Table 2 summarizes performance comparisons: the hybrid model achieved superior metrics across all categories, including precision (95.4%) and F1-score (95.7%). Table 3 compares resource utilization and delay. The proposed hybrid system showed the lowest average response time (1.45 s), peak CPU usage (61%), RAM consumption (4.3 GB), disk I/O (45 MB/s), and model load time (2.2 s) compared to ANN and SVM.

These results underscore the system's suitability for edge computing environments. Edge computing minimizes latency by processing data close to the source, reducing bandwidth requirements and ensuring operational continuity in the event of cloud outages [23,24]. Localized processing also improves data privacy by limiting exposure to external networks [25,26]. The system supports federated intelligence, allowing adaptive learning across distributed nodes without the need to transmit raw data [27,28]. Such architecture provides the agility and robustness necessary for mission-critical environments like autonomous vehicles, mobile sensor networks, and smart cities, where fast and intelligent decision-making is required [29,30].

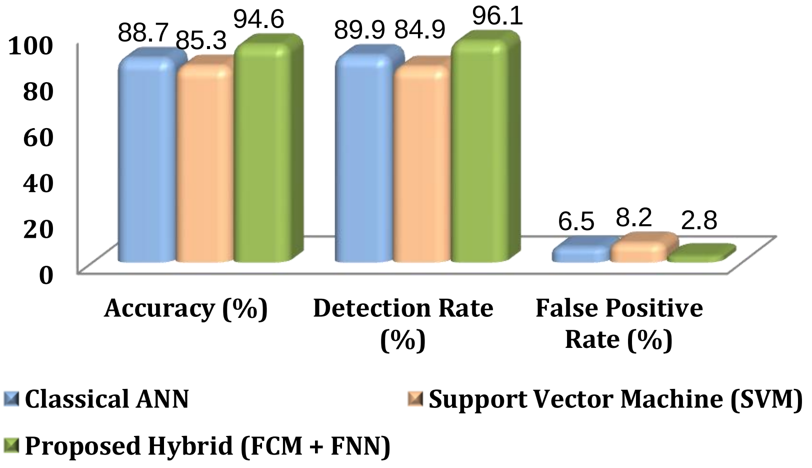

Figure 4: Detection accuracy comparison across models

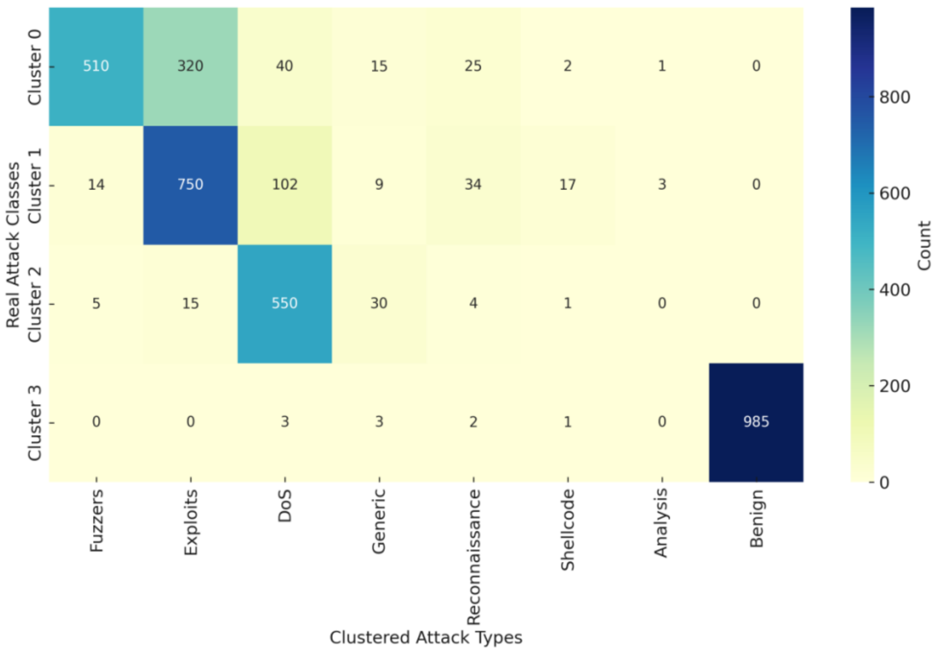

Figure 5: Threat classification heatmap (fuzzy clusters vs real classes)

Fuzzy logic further strengthens resilience by offering reasoning under ambiguity. Unlike binary logic, fuzzy inference accepts partial truths and provides continuity in decision-making despite uncertain, incomplete, or noisy data [31, 32]. Even in cases of sensor degradation or ambiguity, the system can maintain a functional security posture through integration with entropy-based classifiers and adaptive probabilistic models [33]. These capabilities are especially valuable in applications like UAV surveillance, medical diagnostics, and autonomous navigation, where rapid interpretation of uncertain data is essential [34].

TABLE 2 : PERFORMANCE METRICS COMPARISON

Metric	Classical ANN	SVM	Proposed Hybrid (FCM + FNN)
Accuracy (%)	88.7	85.3	94.6
Detection Rate (%)	89.9	84.9	96.1
False Positive Rate (%)	6.5	8.2	2.8
Precision (%)	87.2	83.5	95.4
F1-Score	88.0	84.1	95.7

TABLE 3: LATENCY AND RESOURCE USAGE ON SERVER

Parameter	Classical ANN	SVM	Proposed Hybrid (FCM + FNN)
Average Response Time (sec)	2.10	2.35	1.45
Peak CPU Usage (%)	78%	82%	61%
Peak RAM Usage (GB)	5.6	6.1	4.3
Disk I/O During Peak (MB/s)	62	59	45
Model Load Time (sec)	3.5	3.1	2.2

CONCLUSION

This research presents a hybrid intrusion detection system combining Fuzzy C-Means clustering, Fuzzy Neural Networks, and ANFIS-based inference, designed for edge-cloud environments. The system achieved 94.6% accuracy, a 96.1% detection rate, and a low false positive rate of 2.8%, with an average response time of 1.45 seconds and efficient resource usage. Its ability to adapt to ambiguous and evolving threats, including zero-day and low-volume attacks, significantly outperforms traditional models such as ANN and SVM. Fuzzy logic enables contextual decision-making, while edge deployment enhances responsiveness, autonomy, and data privacy. The architecture is well-suited for securing dynamic infrastructures such as smart cities, IoT networks, and industrial systems. Future enhancements include blockchain-based audit trails, federated learning for decentralized model training, and quantum fuzzy systems for advanced uncertainty handling. Overall, the proposed system offers a scalable, adaptive, and efficient solution for real-time cybersecurity in mission-critical edge-cloud environments.

Funding

No specific grants or funding organizations from the public, commercial, or non-profit sectors provided financial support for this study.

Declaration

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Conflict of interest

The authors of this manuscript have no conflict of interest to declare.

Data availability

All data generated or analyzed during this study are included in this article.

REFERENCES

[1] Almotiri, S.H., 2025. AI driven IOMT security framework for advanced malware and ransomware detection in SDN. Journal of Cloud Computing, 14, 19. https://doi.org/10.1186/s13677-025-00745-w

[2] Admass, W.S., Munaye, Y.Y., Diro, A.A., 2024. Cyber security: State of the art, challenges and future directions. Cyber Security and Applications, 2, 100031. https://doi.org/10.1016/j.csa.2023.100031

[3] Kaur, R., Gabrijelčič, D., Klobučar, T., 2023. Artificial intelligence for cybersecurity: Literature review and future research directions. Information Fusion, 97, 101804. https://doi.org/10.1016/j.inffus.2023.101804

[4] Yeoh, W., Liu, M., Shore, M., Jiang, F., 2023. Zero trust cybersecurity: Critical success factors and A maturity assessment framework. Computers & Security, 133, 103412. https://doi.org/10.1016/j.cose.2023.103412

[5] Khraisat, A., Gondal, I., Vamplew, P., Kamruzzaman, J., 2019. Survey of intrusion detection systems: techniques, datasets and challenges. Cybersecurity, 2(1) 20. https://doi.org/10.1186/s42400-019-0038-7

[6] Kumar, A., Sachdeva, M., 2022. Intrusion detection systems using supervised machine learning techniques: A survey. Procedia Computer Science, 201, 205-212. https://doi.org/10.1016/j.procs.2022.03.029

[7] Raja, S., Ramaiah, S., 2017. An Efficient Fuzzy-Based Hybrid System to Cloud Intrusion Detection. International Journal of Fuzzy Systems, 19(1) 62–77. https://doi.org/10.1007/s40815-016-0147-3

[8] Srilatha, D., Shyam, G.K., 2021. Cloud-based intrusion detection using kernel fuzzy clustering and optimal type-2 fuzzy neural network. Cluster Computing, 24(3) 2657–2672. https://doi.org/10.1007/s10586-021-03281-9

[9] Chormale, A.A., Ghatule, A.P., 2020. Cloud intrusion detection system using fuzzy clustering and artificial neural network. Journal of Physics: Conference Series, 1478(1), 012030. https://doi.org/10.1088/1742-6596/1478/1/012030

[10] Archana, B., Jeebaratnam, N., Rao, B.N., Sesadri, U., Shirisha, N., Kumar, N.M., 2024. Optimizing trust in cloud environments using FNN-CIDS. International Journal of Intelligent Systems and Applications in Engineering, 12(17s) 4871. https://doi.org/10.2147/IJISAE.2024.4871

[11] Saeipour, P., Sarbakhsh, P., Salemi, S., Bakhtari Aghdam, F., 2023. A Fuzzy Clustering Approach to Identify Pedestrians' Traffic Behavior Patterns. Journal of Research in Health Sciences, 23, e00592. https://doi.org/10.34172/jrhs.2023.127

[12] Masdari, M., Khezri, H., 2020. A survey and taxonomy of the fuzzy signature-based Intrusion Detection Systems. Applied Soft Computing, 92, 106301. https://doi.org/10.1016/j.asoc.2020.106301

[13] Yu, H., Yang, W., Cui, B., Sui, R., Wu, X., 2024. Renyi entropy-driven network traffic anomaly detection with dynamic threshold. Cybersecurity, 7, 64. https://doi.org/10.1186/s42400-024-00249-1

[14] Chaudhari, A., Gohil, B., Rao, U.P., 2023. A novel hybrid framework for cloud intrusion detection system using system call sequence analysis. Cluster Computing, 27, 3753–3769. https://doi.org/10.1007/s10586-023-04162-z

[15] Shah, P., Shah, T., 2024. Adaptive Neuro Fuzzy Inference System based classifier in diagnosis of breast cancer. Results Control Optimization, 14, 100358. https://doi.org/10.1016/j.rico.2023.100358

[16] Yadav, H., Singh, J., Gosain, A., 2023. Experimental Analysis of Fuzzy Clustering Techniques for Outlier

Detection. Procedia Computer Science, 218, 959–968. https://doi.org/10.1016/j.procs.2023.01.076

[17] Mikus, M., Konecny, J., Krömer, P., Bancik, K., Konecny, J., Choutka, J., Prauzek, M., 2025. Analysis of the computational costs of an evolutionary fuzzy rule-based internet-of-things energy management approach. Ad Hoc Networks, 168, 103715. https://doi.org/10.1016/j.adhoc.2024.103715

[18] Kumar, A.N.S., Yadav, R.K., Raghava, N.S., 2024. FLOLSTM: Fuzzy logic-driven optimized LSTM for improved malicious traffic detection in hypervisor environments. Concurrency and Computation: Practice and Experience, 36, e8194. https://doi.org/10.1002/cpe.8194

[19] Govindarajan, V., Muzamal, J.H., 2025. Advanced cloud intrusion detection framework using graph based features transformers and contrastive learning. Scientific Reports, 15, 20511. https://doi.org/10.1038/s41598-025-07956-w

[20] Sharma, S.K., Kumar, A., 2025. A cellular automata approach for extending data privacy and security of edge computing. Journal of Discrete Mathematical Sciences and Cryptography, 27(2-B), 601–612. https://doi.org/10.1080/09720529.2025.21690065

[21] Muntean, M.V., 2024. Real-Time Detection of IoT Anomalies and Intrusion Data in Smart Cities Using Multi-Agent System. Sensors, 24(24), 7886. https://doi.org/10.3390/s24247886

[22] Oladipo, S., Sun, Y., Amole, A.O., 2024. Investigating the influence of clustering techniques and parameters on a hybrid PSO-driven ANFIS model for electricity prediction. Discover Applied Sciences, 6, 265. https://doi.org/10.1007/s42452-024-05922-1

[23] Shi, W., Cao, J., Zhang, Q., Li, Y., Xu, L., 2016. Edge computing: Vision and challenges. IEEE Internet of Things Journal, 3(5), 637–646. https://doi.org/10.1109/JIOT.2016.2579198

[24] Thottipalayam, A.M., Parameswari, M., Subramanian, N., Vairaperumal, N., 2023. A novel model for enhancing cloud security and data deduplication using fuzzy and refraction learning-based chimp optimization. International Journal of Machine Learning and Cybernetics, 15, 1025–1038. https://doi.org/10.1007/s13042-023-01953-z

[25] Jahandar, S., Shayea, I., Gures, E., El-Saleh, A.A., Ergen, M., Alnakhli, M., 2025. Handover decision with multi-access edge computing in 6G networks: A survey. Results in Engineering, 25, 103934. https://doi.org/10.1016/j.rineng.2025.103934

[26] Raheja, S., Kumar, A., 2019. Edge detection based on type-1 fuzzy logic and guided smoothening. Evolving Systems, 12, 447–462. https://doi.org/10.1007/s12530-019-09304-6

[27] Kairouz, P., McMahan, H.B., Avent, B., Bellet, A., Bennis, M., Bhagoji, A.N., Zhao, S., 2021. Advances and open problems in federated learning. Foundations and Trends in Machine Learning, 14(1–2), 1–210. https://doi.org/10.1561/2200000083

[28] Liu, J., Yinchai, W., Siong, T.C., Li, X., Zhao, L., Wei, F., 2022. On the combination of adaptive neuro-fuzzy inference system and deep residual network for improving detection rates on intrusion detection. PLOS ONE, 17(12), e0278819. https://doi.org/10.1371/journal.pone.0278819

[29] Albshaier, L., Almarri, S., Albuali, A., 2025. Federated learning for cloud and edge security: A systematic review of challenges and AI opportunities. Electronics, 14(5), 1019. https://doi.org/10.3390/electronics14051019

[30] Raheja, S., Kumar, A., 2019. Edge detection based on type-1 fuzzy logic and guided smoothening. Evolving Systems, 12, 447–462. https://doi.org/10.1007/s12530-019-09304-6

[31] Pawar, S.D., Pawar, V.S., Abimannan, S., 2024. Handling uncertainty in spatiotemporal data. In: Spatiotemporal Data Analytics and Modeling, 69–87. https://doi.org/10.1007/978-981-99-9651-3_4

[32] Chkrebtii, O.A., Campbell, D.A., 2019. Adaptive step-size selection for state-space probabilistic differential equation solvers. Statistics and Computing. https://doi.org/10.1007/s11222-019-09899-5

[33] Ranitha, I.B., Ranaveer, I., Rao, K.S., Renuka, K., Pachimatla, D., Kilari, R., 2025. Hybrid soft computing models: Integration of fuzzy logic, neural networks, and evolutionary algorithms. In: Proceedings of 5th International Conference on Recent Trends in Machine Learning, IoT, Smart Cities and Applications, 455–463. https://doi.org/10.1007/978-981-97-8865-1_38

[34] Abid, A., Jemili, F., Korbaa, O., 2023. Real-time data fusion for intrusion detection in industrial control systems based on cloud computing and big data techniques. Cluster Computing, 27, 2217–2238. https://doi.org/10.1007/s10586-023-04087-7

All © 2025 are reserved by International Journal of Advanced Science and Engineering. This Journal is licensed under a Creative Commons Attribution-Non Commercial-ShareAlike 3.0 Unported License.