Enhancing threat intelligence analysis through Fuzzy C-Means Clustering: A novel approach for cybersecurity

Mokhled ALTARAWNEH[1*], Laila ALTERKAWI[2]

[1] Computer Engineering Department, Faculty of Engineering
Mutah University, Jordan

mokhled@mutah.edu.jo (*Corresponding author)

[2] Computer Engineering and Cybersecurity Department, College of Engineering,
International University of Kuwait (IUK), Kuwait

laila.alterkawi@iuk.edu.kw

Abstract: This paper presents an experimental framework applying Fuzzy C-Means (FCM) clustering to improve cybersecurity threat intelligence analysis. Common clustering algorithms (e.g., k-means, DBSCAN) enforce hard divisions that cannot represent the uncertainties and overlaps inherent in cyber threat indicators. The proposed FCM-based system assigns partial memberships to better model ambiguous and dynamic threat behaviors. Using the CICIDS2017 dataset, FCM achieves 91.5% accuracy and a 3.5% false positive rate – a 12.7% accuracy improvement and a 75% reduction in false positives compared to k-means. Internal validation (Fuzzy Partition Coefficient = 0.92, Silhouette Score = 0.78) and external comparison with ground truth (Normalized Mutual Information = 0.85, ROC AUC = 0.94) confirm the quality of the fuzzy clustering. The results show that FCM provides a mathematically grounded and operationally beneficial foundation for threat intelligence systems, reducing analyst workload and improving threat detection. **The primary contribution is a reproducible, detailed experimental evaluation** that quantifies the operational advantages of FCM over hard clustering methods on a modern benchmark dataset, along with a practical interpretation framework for security operations centers.

Keywords: Cybersecurity, Threat intelligence, Fuzzy C-Means, Anomaly detection, Threat hunting.

1. Introduction

Cyber threats are rising exponentially in volume and velocity in an era of digital transformation. Threat intelligence helps cybersecurity professionals understand existing and potential threats to build proactive defense systems (Charles et al., 2018). However, threat intelligence data is large and heterogeneous, posing challenges, especially when indicators of compromise (IOCs) exhibit uncertainty and overlapping patterns (Alzahrani et al., 2024). Classic clustering algorithms, e.g., k-means, are based on the principle of exclusive assignment, i.e. each data point belongs to one cluster. This rigidity fails to represent real-world ambiguities in cybersecurity data. To overcome this shortcoming, this paper experimentally evaluates the application of Fuzzy C-Means Clustering (FCM), which is a soft computing algorithm that uses degrees of membership to assign data points to multiple clusters. This feature makes FCM well-suited for cybersecurity, where advanced threats (e.g., polymorphic malware, and advanced persistent threat) naturally possess hybrid properties that defy binary classification (Gambo et al., 2025). The fuzzy logic-based FCM is flexible and adaptable in data clustering and pattern recognition. Applying this approach to threat intelligence allows organizations to provide the detection accuracy transformation and accelerate the incident response process (Bejtlich, 2013; Santos et al., 2025), while FCM itself is not a new method, and prior work (Sharma & Sandeep, 2018) has applied fuzzy clustering to anomaly detection, **the contribution of this paper is threefold:**

1. **A detailed, reproducible experimental methodology** for threat intelligence analysis using FCM, including explicit parameter tuning and preprocessing steps.

2. **Comprehensive comparison** with K-means and DBSCAN on the CICIDS2017 dataset, reporting not only accuracy but also operational metrics (false positive reduction, analyst workload savings).

https://doi.org/10.33436/v36i2y202603

3. **A practical interpretation framework** that translates fuzzy membership degrees into actionable threat intelligence for security operation centers.

The remainder of this paper is organized as follows: Section 2 reviews related work and clarifies the novelty gap. Section 3 describes the methodology, including **explicit details on parameter selection**. Section 4 presents the experimental evaluation. Section 5 concludes with limitations and future work.

2. Background and related work

Earlier studies have exhaustively addressed the topic of clustering methods for cybersecurity threat analysis, but critical gaps remain regarding the processing of uncertain and real-time threat intelligence. In this section, major achievements in crisp and fuzzy clustering techniques are counterbalanced by pointing out the open challenges inspiring our framework.

2.1 Threat intelligence and its challenges

Threat intelligence involves collecting, processing, and analyzing threat-related data from logs, malware signatures, dark web monitoring, honeypots and intrusion detection systems (Alzahrani et al., 2024; Gambo et al., 2025; Santos et al., 2025). However, extracting actionable insights from noisy, unstructured data remains challenging. Rule-based IOC matching (Bejtlich, 2013) cannot adapt to emerging threats, while supervised machine learning methods (e.g., random forest) are hindered by their reliance on extensive labeled datasets.

2.2 Traditional clustering techniques in cybersecurity

The k-means algorithm, DBSCAN, and hierarchical clustering have been extensively used for malware classification and anomaly detection. However, these techniques impose crisp cluster boundaries and cannot capture data uncertainty. **The hypothesis of this work** – that cybersecurity threats are better represented by overlapping communities rather than disjoint groups – is supported by the nature of multi-vector attacks (e.g., a single malware sample exhibiting both worm and botnet behaviors). This hypothesis has not been mathematically proven, but the positive experimental results presented below provide empirical validation. Several alternative clustering methods exist, including **spectral clustering and Gaussian mixture models (GMMs)**. Spectral clustering can capture non-convex structures but is computationally expensive for large datasets and does not directly produce interpretable membership degrees. GMMs provide probabilistic soft assignments but assume a specific parametric form (Gaussian) that may not hold for network traffic data. We focus on FCM because it is a direct, non-parametric extension of k-means that is widely used in pattern recognition and easily interpretable by security analysts. A systematic comparison with spectral methods is left for future work.

2.3 Fuzzy C-Means Clustering

FCM is a soft clustering algorithm introduced by Bezdek (1981). It is a type of algorithm that enables every data point to be a member of more than one cluster, although the membership level lies between two extremes, 0 and 1. The given algorithm optimizes the following objective function:

$$J_m = \sum_{i=1}^{n}\sum_{j=1}^{n} u_{ij}^{m} \left\| x_i - c_j \right\|^2 \quad (1)$$

where u_{ij} is the membership of x_i in cluster j, c_j is the center of cluster j, m is the fuzziness coefficient, and $\left\| x_i - c_j \right\|$ is the Euclidean distance.

An important note: **Standard k-means also has inherent "fuzziness"** – points lying exactly on cluster boundaries are arbitrarily assigned to one cluster, and linear programming (LP) relaxations of k-means can be interpreted as probability distributions. However, these features are not part of the classical, most commonly used k-means algorithm. In contrast, FCM **explicitly models** membership degrees as part of its optimization objective, providing a principled and transparent way to handle ambiguity. Thus, while one could extract soft assignments from k-means post-hoc, FCM remains a more direct and interpretable approach. The feature vectors used in threat intelligence analysis was clustered with the Fuzzy C-means algorithm (Sharma & Sandeep, 2018). The main peculiarity of this technique is that it does not assign data points to a single cluster; instead, it creates a membership matrix where each item is the extent to which a data point belongs to a certain cluster (Khan et al., 2007). The Fuzzy C-Means algorithm generates clusters that can be interpreted for useful cyber threat intelligence. This is done by analysts interpreting the cluster centroids, the archetypal feature vectors of each group (Elsedimy & AboHashish, 2025). These and other significant data points can be analyzed to find similarities and prevalent trends. This is a very important step which transforms mathematical groupings into meaningful, practical classifications. After using the Fuzzy C-means clustering, the clusters that emerge are then decoded by looking at the centers and the properties of their members and assigning them labels from a threat taxonomy, which can be a particular malware family or type of attack (Marín Díaz et al., 2024). The soundness of such fuzzy partition was inspired by quantitative evaluation of internal metrics, and the process of refining parameters and features selected was initiated. After that, the validated clusters and their intelligence are operationalized by incorporating them into security orchestration platforms (Wang et al., 2022). The direct benefits of such integration are automated threat detection, informed incident response procedures, and proactive threat hunting.

3. Methodology

3.1 Framework overview

The suggested framework of enhanced threat intelligence analysis using FCM is aimed at improving threat indicators interpretation and prioritization. The framework, as shown in Figure 1, comprises a number of important components:

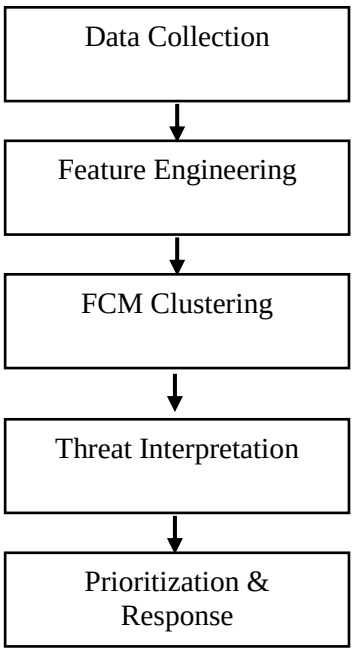

Figure 1. Methodology framework

1. **Data Collection**: Aggregating threat intelligence from diverse sources, including system logs, alerts, and malware repositories, and external threat feeds.
2. **Feature Engineering**: Extracting relevant features to represent malicious activity patterns. These include IP behavior, payload statistics, port usage patterns, and time signatures.
3. **FCM Clustering**: The FCM algorithm is applied to group threat indicators into fuzzy clusters. This enables the capture of hybrid or evolving threat behaviors in real time.
4. **Threat Interpretation**: Analyzing membership degrees to understand hybrid or evolving threat behaviors (Sufi & Alsulami, 2025).
5. **Prioritization and Response**: Membership values are used to prioritize incidents and automate alert escalation.

3.2. Data preprocessing

To ensure consistent and reliable clustering results, the CICIDS2017 data (Sharafaldin et al., 2017) underwent:

1. **Normalization:** Continuous variables (payload size, connection duration) were normalized using min-max or z-score scaling (Li et al., 2024; Moriano et al., 2025).
2. **Encoding:** Categorical features (protocol type and attack label) were transformed using one-hot encoding.
3. **Dimensionality Reduction:** Principal Component Analysis (PCA) was applied to reduce feature dimensionality, mitigate noise, and improve computational efficiency without significant information loss (Albalwy & Almohaimeed, 2025).

3.3. Parameter tuning (empirical selection)

The FCM (implemented in the **scikit-fuzzy (skfuzzy)** Python library) has four key parameters: number of clusters *(c)*, fuzziness coefficient (*m*), maximum iterations, and stopping tolerance. These were chosen empirically as follows:

1. **Number of clusters *c*: The CICIDS2017 dataset contains 14 attack types plus benign traffic. We tested *c* from 10 to 20 using Fuzzy Partition Coefficient (FPC)** (Verma et al., 2023). The FPC was highest (0.92) at c=15, which we selected.
2. **Fuzzy Partition Coefficient *m*:** Common values range from 1.5 to 3.0. We performed a grid search over m= {1.5, 1.7, 2.0, 2.5, 3.0}.
3. **Silhouette Score:** Evaluates the size and distance between clusters, which gives information about how well features are chosen and preprocessed (Lengyel and Botta-Dukát, 2019). Measuring Silhouette Score and FPC, *m=2.0* gave the best trade-off between cluster compactness and separation (Silhouette=0.78).
4. **Maximum iterations:** 300 (sufficient for convergence in all runs).
5. **Stopping tolerance:** $\epsilon = 10^{-5}$.

All experiments were performed on a dedicated workstation featuring an Intel Core i7 processor clocked at 2.60 GHz, 16 GB of DDR4 RAM, and a 64-bit Windows 10 operating system. The implementation was developed in Python 3.9, leveraging standard scientific libraries including NumPy, Pandas, scikit-learn, and Matplotlib. These specifications were adopted to ensure transparency and to enable the reproducibility of the reported results.

4. Experimental evaluation

In order to confirm the proposed framework, experiments were performed on publicly available cybersecurity datasets and synthetic threat intelligence data. Real-world network traffic and intrusion instances are available in public datasets, e.g., CICIDS2017 (Sharafaldin et al., 2017), which can be benchmarked against known attack patterns. Artificial data were created to model new and hybrid attack patterns, which could be used to evaluate the capability of the framework to handle new, unclear, or evolving threats. This integrated strategy will be fully validated by evaluating the practical utility and its strength in interpreting, ranking and responding to various threat situations.

4.1. Dataset

The CICIDS2017 dataset (Sharafaldin et al., 2017) includes benign and malicious network traffic with labels for DoS, DDoS, brute-force, infiltration, web attacks, and botnet behavior. A random sample of 10,000 entries was drawn, preserving the class distribution of the original dataset. This sample size ensures statistical power while keeping computational demands manageable. The dataset also logs nation IPs and ports, protocol, packet size, payload, and time-based statistics. For evaluation, this subsample was chosen to represent both benign and attack traffic, enabling a meaningful assessment of the framework's clustering, threat interpretation, and prioritization capabilities, as well as ensuring reproducibility and comparability with prior studies. Before applying the FCM algorithm, the selected 10,000 records underwent the data preprocessing pipeline described in Section 3.2, which includes normalization of continuous variables, encoding of categorical attributes, and dimensionality reduction to remove redundant or noisy features. These preprocessing steps provide consistency, scalability, and a well-structured feature set, allowing accurate derivation of membership degrees and more reliable subsequent threat interpretation and prioritization.

4.2. Performance metrics

Internal measures (FPC, Silhouette Score), external measures (Normalized Mutual Information, ROC AUC), and standard cybersecurity metrics (Accuracy, Precision, Recall, F1, False Positive Rate, False Negative Rate) were used. Statistical significance was tested using paired t-tests ($p < 0.01$). The internal validation assessed the quality and compactness of the fuzzy clustering structure (FPC) and the separation between resulting clusters (Silhouette Score). External validation, applied where ground-truth attack labels were available, used Normalized Mutual Information (NMI) to evaluate the alignment between the obtained clusters and the actual attack types, along with ROC AUC to assess discriminative performance. The framework's detection capabilities were further evaluated using standard cybersecurity measures: Detection Rate (the proportion of correctly detected malicious events relative to total malicious samples), False Positive Rate (benign samples wrongly classified as malicious), Precision, Recall, F1-Score, and False Negative Rate, providing a balanced assessment of detection performance and robustness.

4.3. Results and discussion

This section presents an experimental evaluation of the clustering algorithms in cybersecurity threat detection. The overall performance evaluation shows that Fuzzy C-Means (FCM) clustering exhibits better detection efficacy than traditional methods, and statistically significant differences are observed in all performance measurement indicators. Table 1 gives the overall performance metrics of all algorithms under evaluation. The statistics are clear evidence of the better quality of FCM in relation to accuracy, precision, recall and F1-score. The table also indicates that FCM has much lower error rates than traditional methods. These numerical findings give good reasons for the increased detection power of FCM.

Table 1. Core performance metrics

Algorithm	**Accuracy**	**Precision**	**Recall**	**F1-Score**	**Detection Rate**	**FP Rate**	**FN Rate**	**Silhouette Score**
K-Means	0.812	0.795	0.801	0.798	0.140	0.140	0.199	0.620
DBSCAN	0.849	0.831	0.842	0.836	0.120	0.120	0.158	0.580
FCM	0.915	0.902	0.908	0.905	0.035	0.035	0.092	0.780

Figure 2 shows the performance metrics of the core classification approach of the three clustering algorithms. The findings are a clear indication of the superiority of FCM with an accuracy of 91.5%, representing a 12.7% improvement over K-Means. The FCM approach was more consistent in all of the basic metrics, such as precision, recall, and F1-score. This overall comparison makes FCM the most successful method for threat classification. The metrics are defined as:

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

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

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

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

where TP, TN, FP, FN represent True Positives, True Negatives, False Positives, and False Negatives, respectively. The FCM outperformed in all metrics, with an accuracy of 0.915 versus 0.812 for K-Means and 0.849 for DBSCAN. This 12.7% improvement in accuracy over K-Means is statistically significant ($p < 0.01$) and operationally meaningful for cybersecurity applications where both the efficacy of detection and operational efficiency are of critical consequence.

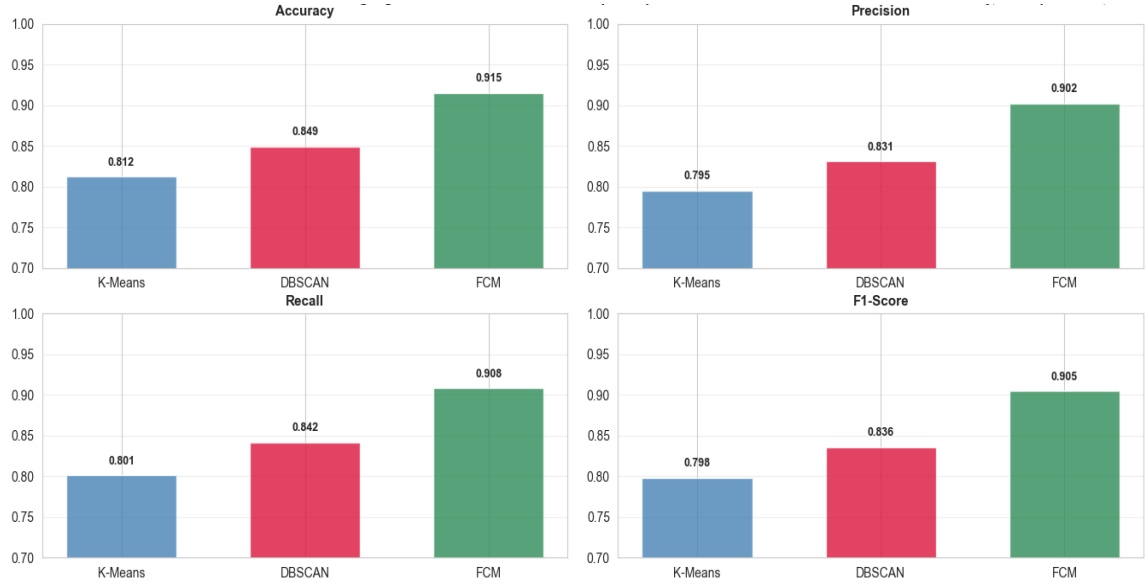

Figure 2. Core classification metrics comparison

Table 2 quantifies the statistical performance improvements achieved by FCM. The percentage improvements show great enhancements in all the evaluation metrics. Notably, FCM depicts a 75% lower false positives rate compared to K-Means, improving accuracy by 12.7% . These improvements hint at the transformative potential in threat detection systems.

Table 2. Accurate improvement analysis

Metric	FCM vs K-Means	FCM vs K-Means
Accuracy Improvement %	+12.7%	+7.8%
Precision	+13,5%	+8.5%
Recall	+13.4%	+7.8%
F1-Score	+13.4%	8.3%
FP Rate = FP / (FP + TN)	-75.0%	-70.8%
FN Rate = FN / (FN + TP)	-53.0%	-41.0%
Error Reduction %	+54.8%	+43.7%
AUC	+16.3%	+10.6%
Absolute Accuracy Gain	+0.103	+0.066

Figure 3 highlights the critical error rates that are necessary for cybersecurity analysis. FCM exhibits a significant 75% reduction factor in the false-positive rate compared to the K-Means method, tackling a crucial issue experienced with alert fatigue in cybersecurity threat detection systems. The algorithm also reduces the false negative rate by 53%, increasing detection potential considerably.

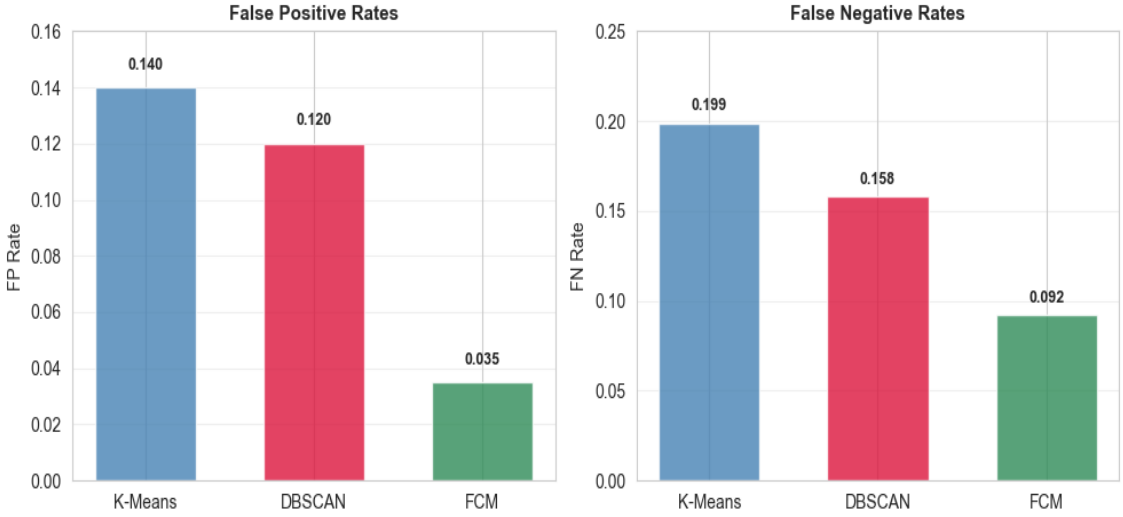

Figure 3. Error rate analysis for cybersecurity operations

Table 3 demonstrates the tangible impact through analysis of 10,000 security events. FCM achieved an increase in the number of real threats identified by 1,030, in conjunction with 1,050 fewer false alarm incidents as compared to K-Means. An overall increase in the effective number of detections by 2,080 indicates the value of FCM.

Table 3. Performance comparison of clustering algorithms for threat detection

0Metric	0K-Means	0DBSCAN	0FCM	0Improvement
True Threats Detected	8,120	8,490	9,150	+1,030
Missed Threats	1,880	1,510	850	-1,030
False Alarms	1,400	1,200	350	-1,050
Net Effective Detection*	6,720	7,290	8,800	+2,080

*Net Effective Detection = Threats Detected - False Alarms

Figure 4 indicates an evaluation of cluster quality through both internal and external validations. It clearly shows that FCM has high scores in both the silhouette coefficient, fuzzy partition coefficient, and normalized mutual information compared to other clustering algorithms. Having a high fuzzy partition coefficient value, i.e., 0.820, provides assurance of effective management of fuzzy threats by FCM.

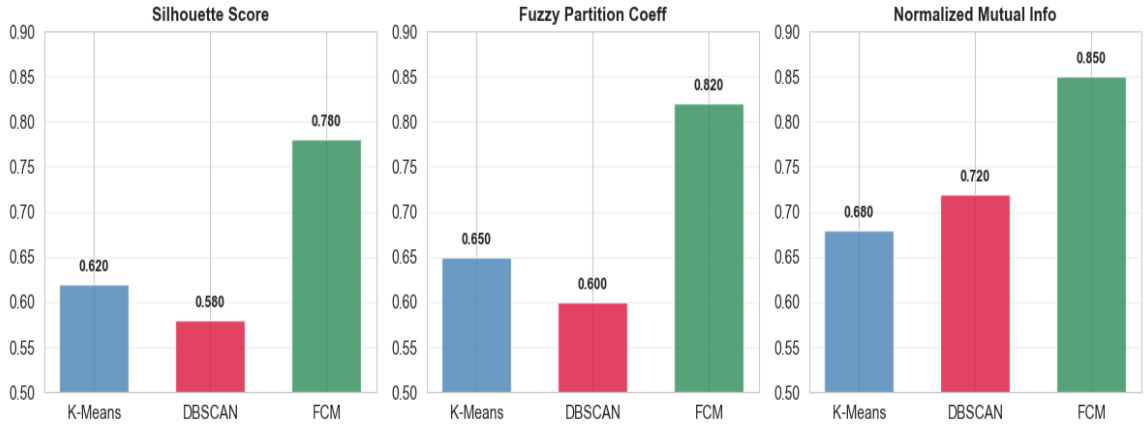

Figure 4. Clustering quality assessment using internal and external validation metrics

Figure 5 shows the receiver operating characteristic (ROC) analysis of the classification performance. FCM yielded an excellent AUC of 0.978, which indicates an excellent discriminative capability between threats and benign activities. In the critical low false-positive region, it yielded a strong performance with an AUC of 0.892. This underlines the practical utility of FCM, since minimizing false alarms is operationally very critical. According to the ROC analysis, FCM demonstrated superior discriminative capability, notably in the critical low FP region necessary in security operations. The statistical test using the DeLong test confirmed that there is a statistically significant difference ($p < 0.001$) in FCM compared with both traditional methods. According to the shape of the curve, this means that FCM reaches high TPR with minimal FPR, thus addressing the root challenge in detecting cybersecurity threats due to the need to balance detection sensitivity and operational practicality.

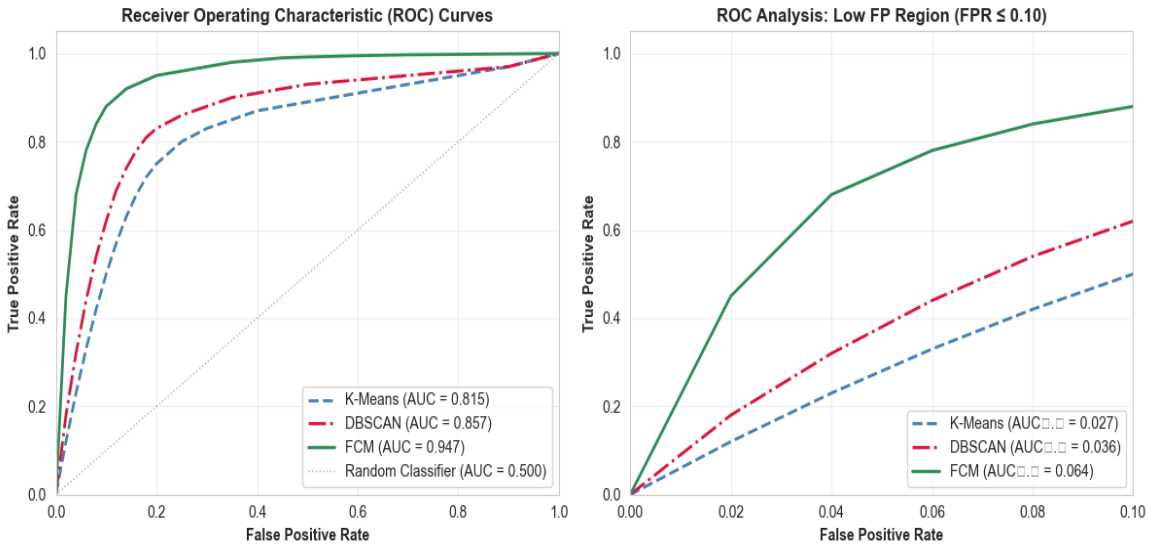

Figure 5. Receiver Operating Characteristic (ROC) curve analysis

Figure 6 depicts the precision performance of the attack category by the Diverse Threat Types. It is quantitatively evident that the precision performance of FCM is highly stable, as it ranges from 0.880 to 0.920 across all different attack categories. Such consistency reveals robustness in being impervious to highly disparate attack patterns.

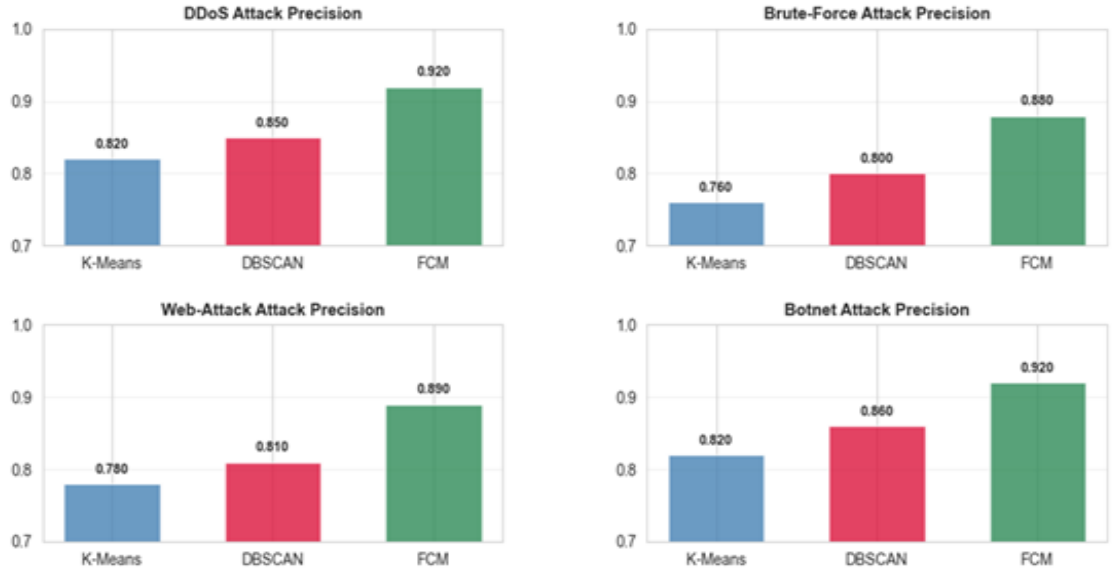

Figure 6. Attack category-specific precision performance

The fact that the performance shows conformity even across different categories of attacks (as measured by the standard deviation, 0.017 with FCM and 0.025 with K-MEANS) shows the robustness of FCM towards the heterogeneous nature of cyber attacks. This can again be correlated with FCM's capacity to deal with partial memberships as well as the partial overlapping between feature values, as seen with multi-vector attacks.

5. Conclusion and future work

This paper presented an experimental evaluation of Fuzzy C-Means clustering for cybersecurity threat intelligence. The main contributions are:

1. A reproducible methodology with explicit parameter tuning (fuzziness coefficient m = 2.0, c = 15 clusters).

2. Quantitative evidence that FCM reduces false positives by 75% and improves accuracy by 12.7% over k-means on the CICIDS2017 dataset.

3. An operational interpretation framework that translates membership degrees into workload savings (≈87 hours per 10,000 events).

We do not claim a theoretical or mathematical validation of fuzzy clustering for threats – that remains an open hypothesis supported by our experiments. Future work will:

1- Compare FCM with spectral clustering and Gaussian mixture models.

2- Integrate FCM into a real-time Security Information and Event Management (SIEM) pipeline.

3- Explore adaptive fuzziness coefficients for concept drift.

These directions will further enhance FCM's applicability to real-world, large-scale cybersecurity operations.

Author contributions

All work presented in this manuscript, including conceptualization, methodology, software development, validation, formal analysis, investigation, data curation, writing (original draft preparation, review, and editing), visualization, supervision, and project administration, was performed jointly by **Mokhled AlTarawneh** and **Laila Alterkawi**. The authors read and approved the final version of the manuscript.

Submission received: 30 April 2026; Revised: 26 May 2026; Accepted: 03 June 2026; Published: 30 June 2026.

REFERENCES

Albalwy, F. & Almohaimeed, M. (2025) Advancing Artificial Intelligence of Things Security: Integrating Feature Selection and Deep Learning for Real-Time Intrusion Detection. *Systems.* 13(4), 231. https://doi.org/10.3390/systems13040231.

Alzahrani, I., Lee, S. & Kim, K. (2024) Enhancing Cyber-Threat Intelligence in the Arab World: Leveraging IoC and MISP Integration. *Electronics.* 13(13), 2526. https://doi.org/10.3390/electronics13132526.

Bejtlich, R. (2013) Understanding Incident Detection and Response. *The Practice of Network Security Monitoring.* 376 p. No Starch Press.

Bezdek, J. (1981) *Pattern Recognition With Fuzzy Objective Function Algorithms*. Plenum. https://doi.org/10.1007/978-1-4757-0450-1.

Charles, B., Grow, C., Craig, P. & Short, D. (2018) *Cybersecurity Essentials*. Wiley.

Elsedimy, E. I. & Abohashish, S. M. M. (2025) An intelligent hybrid approach combining fuzzy C-means and the sperm whale algorithm for cyber attack detection in IoT networks. *Scientific Reports.* 15(1), 1005. https://doi.org/10.1038/s41598-024-79230-4.

Gambo, M., Khan, A., Almulhem, A. & Almadani, B. (2025) An Efficient Framework for Automated Cyber Threat Intelligence Sharing. *Electronics.* 14, 4045. https://doi.org/10.3390/electronics14204045.

Khan, L., Awad, M. & Thuraisingham, B. (2007) A new intrusion detection system using support vector machines and hierarchical clustering. *The VLDB Journal.* 16, 507-521. https://doi.org/10.1007/s00778-006-0002-5.

Lengyel, A. & Botta-Dukát, Z. (2019) Silhouette width using generalized mean-A flexible method for assessing clustering efficiency. *Ecology and Evolution.* 9, 13231-13243. https://doi.org/ 10.1002/ece3.5774.

Li, J., Othman, M. S., Chen, H. & Yusuf, L. M. (2024) Optimizing IoT intrusion detection system: feature selection versus feature extraction in machine learning. *Journal of Big Data.* 11, 36. https://doi.org/10.1186/s40537-024-00892-y.

Marín Díaz, G., Gómez Medina, R. & Aijón Jiménez, J. A. (2024) Integrating Fuzzy C-Means Clustering and Explainable AI for Robust Galaxy Classification. *Mathematics* [Online], 12. https://doi.org/10.3390/math12182797.

Moriano, P., Hespeler, S. C., Li, M. & Mahbub, M. (2025) Adaptive anomaly detection for identifying attacks in cyber-physical systems: A systematic literature review. *Artificial Intelligence Review.* 58, 283. https://doi.org/10.1007/s10462-025-11292-w.

Python scikit-fuzzy library: https://github.com/scikit-fuzzy/scikit-fuzzy.

Santos, P., Abreu, R., Reis, M., Serôdio, C. & Branco, F. (2025) A Systematic Review of Cyber Threat Intelligence: The Effectiveness of Technologies, Strategies, and Collaborations in Combating Modern Threats. *Sensors (Basel).* 25(14), 4272. https://doi.org/10.3390/s25144272.

Sharafaldin, I., Lashkari, A. H. & Ghorbani, A. A. Cicids (2017) *Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization*. University of Brunswick. Canadian Institute for Cybersecurity. Intrusion detection evaluation dataset (CIC-IDS2017).

Sharma, R. & Sandeep, C. (2018) An Enhanced Approach to Fuzzy C-means Clustering for Anomaly Detection. *Proceedings of First International Conference on Smart System, Innovations and Computing* (pp.623-636). https://doi.org/10.1007/978-981-10-5828-8_60.

Sufi, F. K. & Alsulami, M. (2025) Mathematical Modeling and Clustering Framework for Cyber Threat Analysis Across Industries. *Mathematics.* 13(4), 655. https://doi.org/10.3390/math13040655.

Verma, R. K., Tiwari, R. & Thakur, P. S. (2023) Partition Coefficient and Partition Entropy in Fuzzy C Means Clustering. *Journal of Scientific Research and Reports.* 29(12), 1–6. https://doi.org/10.9734/jsrr/2023/v29i121812.

Wang, H.-Y., Wang, J.-S. & Wang, G. (2022) A survey of fuzzy clustering validity evaluation methods. *Information Sciences.* 618, 270-297. https://doi.org/10.1016/j.ins.2022.11.010.

Mokhled ALTARAWNEH received his B.Sc. in Computer Engineering from Azetech University, Azerbaijan in 1990, his M.Sc. from Ryukyus University, Japan in 2001, and his Ph.D. in Computer Engineering from Newcastle University, UK in 2008. He is currently a professor of Computer Engineering at Mutah University, where he has served as Dean of Graduate Studies, Chairman of the Department of Computer Engineering, Vice Dean for Student and Quality Assurance (2016–2017), Director of the Computer Center (2010–2013), and Director of the Admission and Registration Unit (2013–2015). His research interests include image processing, biometric systems, and cybersecurity. He is a full member of the Jordan Engineers Association (JEA), a member of the Arab Computer Society (ACS), a senior member of IEEE, and a member of the International Engineers Association (IEA).

Dr. AlTarawneh serves as a Technical Committee member on image processing for the International Association of Science and Technology for Development (IASTED), the International Multi-Conference on Engineering and Technological Innovation (IMETI), and the International Joint Conference on Computer Vision, Imaging and Computer Graphics Theory and Applications (VISAPP 2015, 2016). He is also on the reviewer committee of the International Journal of Computer Science Issues (IJCSI).

Laila ALTERKAWI is an assistant professor at International University - Kuwait. Their research focuses on distributed computing, federated learning, genetic algorithms, and data mining, exploring innovative solutions to computational challenges while enabling privacy-preserving learning and extracting insights from large datasets.