Intrusion Detection in IoT using Gaussian Fuzzy Mutual Information-based Feature Selection

Abdullah Hussain Abu Saq
Department of Information Systems, College of Computer Science and Information Systems, Najran University, Saudi Arabia
ahabusaq@nu.edu.sa (corresponding author)

Anazida Zainal
Department of Computer Science, Faculty of Computing, Universiti Teknologi Malaysia, Johor Bahru, Malaysia
anazida@utm.my

Bander Ali Saleh Al-Rimy
School of Computing, University of Portsmouth, UK
bander.al-rimy@port.ac.uk

Abdulrahman Alyami
Department of Information Systems, College of Computer and Information Sciences, Jouf University, Sakaka, Saudi Arabia
am.yami@ju.edu.sa

Hamad Ali Abosaq
Computer Science Department, College of Computer Science and Information Systems, Najran University, Saudi Arabia
haabosaq@nu.edu.sa

Received: 30 June 2024 | Revised: 14 August 2024 and 1 September 2024 | Accepted: 8 September 2024

 DOI: https://doi.org/10.48084/etasr.8268

ABSTRACT

The proliferation of Internet of Things (IoT) devices has revolutionized various sectors by enabling real-time monitoring, data collection, and intelligent decision-making. However, the massive volume of data generated by these devices presents significant challenges for data processing and analysis. Intrusion Detection Systems (IDS) for IoT require efficient and accurate identification of malicious activities amidst vast amounts of data. Feature selection is a critical step in this process, aiming to identify the most relevant features that contribute to accurate intrusion detection, thus reducing computational complexity and improving model performance. Traditional Mutual Information-based Feature Selection (MIFS) methods face challenges when applied to IoT data due to their inherent noise, uncertainty, and imprecision. This study introduces a novel Fuzzy Mutual Information-based Feature Selection (Fuzzy-MIFS) method that integrates fuzzy logic with Gaussian membership functions to address these challenges. The proposed method enhances the robustness and effectiveness of the feature selection process, resulting in improved accuracy and efficiency of IDSs in IoT environments. Experimental results demonstrate that the Fuzzy-MIFS method consistently outperformed existing feature selection techniques across various neural network models, such as CNN, LSTM, and DBN, showcasing its superior performance in handling the complexities of IoT data. The results show that Fuzzy-MIFS increased the accuracy from 0.962 to 0.986 for CNN, from 0.96 to 0.968 for LSTM, and from 0.96 to 0.97 for DBN.

Keywords-IDS; IoT; deep learning; cyber attacks

I. INTRODUCTION

The proliferation of Internet of Things (IoT) devices has revolutionized various sectors, enabling real-time monitoring, data collection, and intelligent decision-making [1, 2]. However, the massive volume of data generated by these devices poses significant challenges for data processing and analysis. Intrusion Detection Systems (IDS) for IoT must efficiently and accurately identify malicious activities among vast amounts of data [3]. To achieve this, feature selection becomes a critical step, aiming to identify the most relevant features that contribute to accurate intrusion detection, thus reducing computational complexity and improving model performance. Mutual Information-based Feature Selection (MIFS) is a widely adopted method for feature selection, particularly suited for IDS applications in IoT due to its ability to measure the dependency between features and the target variable [4, 5]. MIFS quantifies the amount of information gained about the target variable through each feature, allowing the identification of the most informative features [6]. Despite its effectiveness, traditional MIFS faces several challenges when applied to IoT data, which are often characterized by noise, uncertainty, and imprecision due to various factors such as sensor inaccuracies, communication errors, and environmental interference.

The inherent characteristics of IoT data can significantly hinder the performance of traditional MIFS, which relies on precise probabilistic measures [7]. As a result, traditional MIFS may not adequately handle these uncertainties, leading to suboptimal feature selection and reduced IDS performance. This issue highlights a critical research gap: the need for a feature selection method that can effectively manage the uncertainty and imprecision inherent in IoT data [8]. Addressing this gap requires an innovative approach that can address these specific challenges. Fuzzy logic is a promising solution to handle ambiguity in IoT data. This study proposes a novel Fuzzy Mutual Information-based Feature Selection (Fuzzy-MIFS) method using the Gaussian membership function to address the limitations of traditional MIFS in IDS for IoT. The proposed method uses fuzzy sets and a membership function to represent imprecise data, improving the resilience and efficiency of feature selection. This approach aims to improve the accuracy and efficiency of feature selection, ultimately enhancing the performance of IDS in detecting malicious activities in IoT environments. The integration of fuzzy logic into traditional MIFS aims to advance feature selection for IDS in IoT, providing a more robust and effective approach to managing the complexities of IoT data. A robust feature selection process that can handle the noisy and uncertain nature of IoT data is critical to the development of efficient and reliable IDSs.

A. Current Study Contributions

- Integration of Fuzzy Logic with MIFS: This study introduces a novel approach that integrates fuzzy logic with the MIFS framework, enhancing the robustness of feature selection in the presence of noisy and uncertain IoT data. This integration allows for better handling of the inherent uncertainties in IoT data, leading to more reliable feature selection.
- Utilization of Gaussian Membership Functions: This study employs Gaussian membership functions to model gradual transitions and uncertainties in IoT data, improving the accuracy and efficiency of the feature selection process. The smooth and continuous nature of Gaussian membership functions makes them particularly suited for representing imprecise data generated by IoT devices.
- Enhanced Performance of IDS in IoT: The proposed Fuzzy-MIFS method demonstrates significant improvements in IDS performance, providing a more reliable and effective means of detecting malicious activities in IoT environments. The enhanced feature selection process leads to better model performance, which is crucial for the timely and accurate detection of intrusions.

B. Related Works

IoT security is a critical concern due to the diverse range of devices and networks interconnected within such ecosystems. With the proliferation of IoT devices, the attack surface for potential security breaches has expanded, necessitating robust security measures to protect sensitive data and ensure the integrity of IoT systems [9]. IDSs play a crucial role in enhancing the security of IoT environments by continuously monitoring network activities, detecting anomalies, and responding promptly to potential threats [10, 11].

IDSs are essential to identify malicious traffic and unauthorized access attempts on IoT networks, particularly in sensitive domains such as healthcare, where the consequences of security breaches can be severe [9, 10]. By leveraging machine learning algorithms and advanced security frameworks, IDSs can effectively mitigate security risks and protect IoT devices from evolving cyber threats [10]. Additionally, the integration of biometrics and blockchain technologies into IoT security solutions further enhances authentication and trust mechanisms, contributing to a more secure IoT ecosystem [12, 13]. Overall, IDSs serve as a cornerstone in the defense against security vulnerabilities in IoT networks, playing a crucial role in maintaining the confidentiality, integrity, and availability of IoT systems amidst growing cybersecurity challenges.

IDSs are essential for safeguarding IoT environments by monitoring, analyzing, and detecting anomalies in network activities [9]. The increasing number of IoT devices has led to an increase in security risks and vulnerabilities, highlighting the need for robust IDS solutions to protect against potential intrusions [14]. These systems are crucial for responding promptly to security breaches in IoT networks, ensuring the integrity and security of IoT ecosystems [15]. The development of IDSs for IoT involves sophisticated techniques such as deep learning-driven approaches, hybrid models, and feature selection methods tailored to the unique characteristics and challenges of these environments [16-18]. Using advanced technologies such as artificial intelligence and machine learning, IDS for IoT can improve detection accuracy, scalability, and efficiency, strengthening defense mechanisms against cyber threats [19, 20]. Furthermore, the integration of explainable feature sets and lightweight approaches in IDS design contributes to improving the overall performance and

effectiveness of intrusion detection in IoT settings [21, 22]. In general, IDS for IoT is a critical aspect of cybersecurity in the interconnected world of IoT, ensuring continuous monitoring and protection of IoT devices and networks against potential security breaches.

The use of fuzzy logic in IoT systems covers a wide range of applications, including routing protocols, monitoring, and IDS systems. Fuzzy logic has been proposed for energy-efficient routing in wireless sensor networks, emphasizing the benefits of cross-layer approaches in IoT systems [23]. Moreover, the application of fuzzy logic in IoT extends to diverse areas, such as intelligent transportation systems, smart city platforms, and industrial control systems, highlighting its wide impact in optimizing IoT functionality [24-28]. The utilization of fuzzy logic in IoT-based decision-making processes, risk-cautioning frameworks, and intelligent tourist attractions underscores its significance in enhancing the intelligence and efficiency of IoT systems [25-27]. Moreover, fuzzy logic has been used in IoT systems for applications such as smart agriculture, hydroponics, and intelligent monitoring systems, demonstrating its adaptability across different domains [29-31]. In the realm of IoT, the integration of fuzzy logic with other technologies has shown promising results. For instance, the combination of fuzzy logic with neural networks on wireless nodes has been explored for environmental monitoring, highlighting the potential of hybrid approaches in IoT applications [32].

Fuzzy-based IDS modeling for IoT environments has been investigated in several studies. For instance, a fuzzy-based self-tuning Long Short-Term Memory (LSTM) IDS was proposed, using fuzzy logic to dynamically adjust the number of epochs when training an LSTM-based IDS [33]. In [34], fuzzy inference was used for the classification of intrusions in IoT networks. In [35], fuzzy logic was used to classify intrusions as normal, low, medium, or high. In [36], fuzzy logic was employed as part of the trust management mechanism to address irregular behaviors of malicious nodes, allowing them to trick neighbors into believing that they are honest or escape network punishment. Fuzzy logic was also used in [37] to detect jamming attacks by processing uncertain and imprecise data collected from local IoT nodes. This study used a set of predefined rules to interpret the data, allowing the system to make informed decisions about potential jamming activities in the network. In [38], fuzzy logic was used to dynamically evaluate the security levels of IoT devices and users considering factors such as behavior, network conditions, and resource availability. This approach translated these factors into fuzzy sets and applied predefined rules to calculate a numerical security level, which guided the adjustment of encryption keys and security measures in real time. The use of fuzzy logic enables a flexible and adaptive security management system that effectively responds to varying conditions in a decentralized IoT environment.

In [39], fuzzy logic was employed through an Adaptive Neuro-Fuzzy Inference System (ANFIS) to accurately classify potential intrusions by handling uncertainty and imprecision in the detection process. Additionally, fuzzy membership functions were optimized using a hybrid Jaya Shark Smell Optimization (JSSO) algorithm, improving detection accuracy and reducing false alarms.

The literature summarized above reveals that existing IDS solutions for IoT use fuzzy logic for classification and attack detection, aiding decision-making under uncertainty. However, these methods struggle to identify the source of uncertainty, particularly in noisy IoT data. Addressing uncertainty at the data level, especially during feature selection, could improve IDS performance [40]. This study emphasizes mutual information in feature selection as a method of improving IDS in IoT environments. Information theory-based techniques have been used as feature selection techniques for IDS in IoT. In [40], Mutual Information Feature Selection (MIFS) was used to select a set of features that represent attack patterns against the Internet of Medical Things. Similarly, Redundancy Coefficient Gradual Upweighting was incorporated into MIFS (RCGU-MIFS) to address the issue of data insufficiency during the early phases of cyber attacks [41]. In [42], Minimum Redundancy Maximum Relevance (MRMR) was used to select the top features for ransomware attack detection modeling. Similarly, Joint Mutual Information (JMI) was used in [43] as a feature selection method to reduce data dimensionality. Furthermore, Joint Mutual Information Maximization (MJMI) was proposed in [44] to select the best features to prevent model overfitting. Although information theory-based techniques can reduce data dimensionality and prevent overfitting, these techniques are unable to inspect data uncertainty, due to the reliance on information that assumes that the relationship between input features and class labels is clear and easy to capture. This assumption does not hold for evasive intrusion attacks against IoT. Therefore, a method that can deal with data uncertainty when evaluating feature relevance is needed.

Combining MIFS and fuzzy logic is promising in addressing uncertainty in data and optimizing decision-making in IoT applications, including latency-sensitive tasks [45]. The growth of IoT in healthcare settings has been a topic of research interest, aiming to leverage IoT technologies for sustainable development and improve healthcare management [46]. Furthermore, the application of fuzzy logic in IoT systems has been explored in various domains, such as quality of service evaluation in smart homes, drug storage systems, and energy management, showcasing its versatility and applicability in IoT contexts [47, 48].

II. METHODOLOGY

The proposed Fuzzy MIFS method consists of several key steps: data fuzzification, calculation of fuzzy mutual information, feature ranking, and feature selection.

A. Gaussian Membership Functions

To handle the uncertainty and imprecision in IoT data, a Gaussian membership function, defined in (1), was used to fuzzify the input data.

$$\mu(x; c, \sigma) = exp\left(-\frac{(x-c)^2}{2\sigma^2}\right) \quad (1)$$

where c is the center (mean) and σ is the standard deviation of the Gaussian function. These parameters are determined for

each feature based on the data distribution, providing a smooth and continuous way to model the uncertainty in the data.

B. Data Fuzzification

The fuzzification process converts the crisp values of each feature into fuzzy values using the Gaussian membership function. First, for each feature X_i and the target variable Y, the mean c_i and standard deviation σ_i were calculated. For each feature X_i and each data point x_{ij} in the dataset, the fuzzy value was computed using the Gaussian membership function $(x_{ij}) = \mu(x_{ij}; c_i, \sigma_i)$. Similarly, the target variable Y was fuzzified for each data point y_j using $\tilde{y}_j = \mu(y_j; c_Y, \sigma_Y)$.

C. Calculation of Fuzzy Mutual Information

Once the data is fuzzified, the fuzzy mutual information between each feature and the target variable is calculated. This involves several steps. First, the fuzzy entropy $H(\tilde{X}_i)$ for each fuzzified feature (2) and $H(\tilde{Y})$ (3) for the fuzzified target variable are computed:

$$H(\tilde{X}_i) = -\sum_{k=1}^{n} \tilde{x}_{ik} \log(\tilde{x}_{ik}) \quad (2)$$

$$H(\tilde{Y}) = -\sum_{k=1}^{n} \tilde{y}_k \log(\tilde{y}_k) \quad (3)$$

Next, the joint fuzzy entropy $H(\tilde{X}_i, \tilde{Y})$ for each pair of fuzzified feature and target variable is calculated using

$$H(X, Y) = -\sum_{i=1}^{m} \tilde{x}_{ik}.y_k \log(\tilde{x}_{ik}.y_k) \quad (4)$$

Finally, the fuzzy mutual information $I(\tilde{X}_i; \tilde{Y})$ is computed using

$$I(\tilde{X}_i; Y) = H(\tilde{X}_i) - H(\tilde{Y}) - H(\tilde{X}_i, \tilde{Y}) \quad (5)$$

D. Feature Ranking

After calculating the fuzzy mutual information values, the features were ranked based on these values. Higher fuzzy mutual information values indicate stronger relationships with the target variable. Thus, the features were sorted in descending order of their fuzzy mutual information values.

E. Feature Selection

The final step is feature selection, which involves choosing the most relevant features based on their ranked fuzzy mutual information values. A threshold was set for the fuzzy mutual information value to select features, or alternatively, the top N features were selected based on their fuzzy mutual information values. Features that meet the threshold criteria or are within the top N ranked features are chosen for further processing or model building.

Algorithm 1 shows the pseudocode of the Fuzzy-MIFS technique. It begins by defining the necessary inputs and outputs for the algorithm. The input consists of a data matrix X, where each column represents a feature, and each row represents a data sample and a target vector Y, which contains the target values for each data sample. The output is a set of selected features that are deemed most relevant for the target variable based on their fuzzy mutual information values.

Algorithm 1: Fuzzy MIFS

```
Input: Data matrix X, target vector Y
Output: Selected features
1: Define Gaussian membership functions
   for each feature X_i and target Y
2: Fuzzify data:
   For each feature X_i in X:
     Calculate mean (c_i) and standard
     deviation (σ_i)
     For each value x_ij in X_i:
       Compute fuzzy value x_ij = μ(x_ij; c_i, σ_i)
   Fuzzify target variable Y similarly
3: Calculate Fuzzy Mutual Information:
   For each fuzzified feature X̃_i:
     Compute fuzzy entropy H(X̃_i)
     Compute fuzzy entropy H(Ỹ)
     Compute joint fuzzy entropy H(X̃_i, Ỹ)
     Compute fuzzy mutual information
     I(X̃_i; Ỹ) = H(X̃_i) + H(Ỹ − H(X̃_i, Ỹ)
4. Rank features based on fuzzy mutual
   information values I(X̃_i; Ỹ)
5. Select features:
   Set a threshold or determine top N
   features
   Select features that meet the
   threshold or are in the top N
Return selected features
```

The first step is to define the Gaussian membership function for each feature X_i and the target variable Y. These membership functions are used to fuzzify the data, converting the crisp values into fuzzy values that can better handle the uncertainty and imprecision present in IoT data. For each feature X_i, the mean c_i and standard deviation σ_i are calculated. Then, for each value x_{ij} in the feature X_i, the fuzzy value $\tilde{x}_{ij}$ is calculated using the Gaussian membership function. This process is repeated for the target variable Y, resulting in fuzzified target values $\tilde{y}_j$.

Next, the calculation of fuzzy mutual information is described. For each fuzzified feature $\tilde{X}_i$, the fuzzy entropy $H(\tilde{X}_i)$ is computed, which quantifies the uncertainty within the fuzzified feature. Similarly, the fuzzy entropy $H(\tilde{Y})$ is calculated for the fuzzified target variable. The joint fuzzy entropy $H(\tilde{X}_i, \tilde{Y})$ is then determined, which measures the combined uncertainty of the feature and the target variable. Using these entropy values, the fuzzy mutual information $I(\tilde{X}_i, \tilde{Y})$ is computed for each feature, indicating the amount of information shared between the feature and the target variable.

Following the calculation of fuzzy mutual information values, the features are ranked based on these values. Features with higher fuzzy mutual information values are considered to have stronger relationships with the target variable. The technique then proceeds to the feature selection step, where features are selected based on their ranks. A threshold is set for the fuzzy mutual information value, or alternatively, the top N features are selected. Features that meet the threshold criteria or

are within the top N ranked features are chosen for further processing or model building.

Finally, the selected features are returned. This structured approach ensures that the most relevant features are selected, improving the accuracy and robustness of feature selection for IDS in IoT environments. By integrating fuzzy logic and Gaussian membership functions, the Fuzzy-MIFS method effectively manages the uncertainty and imprecision inherent in IoT data, leading to more reliable and effective IDSs.

III. RESULTS AND ANALYSIS

The study used the WUSTL-EHMS-2020 dataset [49], consisting of network traffic parameters and biometric information from patients. The dataset was obtained from a real-time testbed for an Energy Harvesting and Management System (EHMS). The testbed architecture comprises four fundamental components: medical monitoring sensors, a data transmission gateway, network infrastructure, and a display and control unit. The dataset was meticulously curated to include diverse incursion scenarios and typical operations. It contains numerous records, ensuring a diverse and representative sample for both training and testing purposes. The dataset was divided into two subsets for training and testing, with a ratio of 80:20. The training set was used to construct the model, while the testing set was used exclusively to evaluate its performance. To improve reliability and mitigate the likelihood of overfitting, cross-validation was included in the training process. The original training dataset was partitioned into various subsets using the bagging approach, resulting in the formation of several smaller datasets. Subsequently, these datasets were used to train distinct classifiers within the ensemble. This strategy improved the classifiers' ability to make generalizations by exposing them to several subsets of the data during the model training phase, thus increasing variety and resilience.

The proposed technique was developed and evaluated using several tools and utilities, such as Python, Skfeature, TensorFlow, Keras, Scikit Learn, and NumPy. The organization of data instances, the execution of algorithms, and the examination of results were performed on a PC with an Intel Core i7-4790 CPU @ 3.60 GHz and 16 GB of RAM. This study assessed the effectiveness of the Fuzzy-MIFS method by measuring its accuracy (Acc) as the main performance metric.

$$ACC = \frac{TP+TN}{TP+TN+FP+FN} \quad (6)$$

In the experiments, the hyperparameters of the CNN, LSTM, and DBN models were adjusted with the same values. The number of epochs was adjusted to 50, the learning rate was 0.001, the batch size was 64, the dropout rate was 0.20, and regularization was 0.001 (L2).

The performance of the proposed Fuzzy-MIFS method across different neural network models, including CNN, LSTM, and DBN, demonstrates its effectiveness in handling feature selection across a broad spectrum of data-driven architectures. This study used the top N features as a threshold to measure the accuracy of the proposed technique. The results showed that the top N approach consistently yielded higher performance across all models, especially in complex neural networks such as CNN and LSTM. This demonstrates that the top N thresholding approach is preferable for optimizing IDS performance in IoT environments as it helps to focus on the most informative features.

Starting with five features, the CNN model showed an accuracy of 0.945, closely followed by LSTM at 0.944, with DBN leading slightly with 0.951. With 10 features, all three models maintained similar performance levels, with the CNN slightly trailing at 0.943, while LSTM stays consistent at 0.944 and DBN slightly better at 0.948. Increasing the number of features up to 15 shows a continued improvement in accuracy for all models, with CNN reaching 0.956, LSTM at 0.953, and DBN at 0.958.

TABLE I. EVALUATION RESULTS

Number of features	5	10	15	20	25	30	35	40
CNN	0.945	0.943	0.956	0.960	0.967	0.986	0.978	0.974
LSTM	0.944	0.944	0.953	0.964	0.968	0.963	0.957	0.957
DBN	0.951	0.948	0.958	0.962	0.970	0.964	0.959	0.959

A notable improvement in accuracy is observed as the number of features increases further, particularly with the CNN and DBN models. Using 20 features, the CNN model achieves an accuracy of 0.960, and the LSTM model surpasses this slightly with 0.964, while the DBN model shows a similar performance at 0.962. The highest accuracies were recorded at 25 features, with CNN at 0.967, LSTM at 0.968, and DBN at the top with 0.970. Beyond 25 features, although the accuracy generally remains high, the most significant jump is seen with the CNN model at 30 features, marking a peak accuracy of 0.986. Beyond this point, increasing the number of features to 35 and 40, there is a slight decrease in accuracy across all models, but the levels remain robust, demonstrating the ability of the proposed Fuzzy-MIFS to effectively manage larger feature sets while maintaining high performance in varied neural network environments. This study compared the performance of the proposed Fuzzy-MIFS technique with several well-known feature selection methods, including RCGU-MIFS [41], MIFS [40], MRMR [42], JMI [43], and MJMI [44]. Each of these methods was chosen for their established effectiveness in feature selection for IDSs. The results from the accuracy comparison between the proposed Fuzzy-MIFS and other approaches using a CNN model demonstrate FMIFS's superior performance across a range of feature counts from 5 to 40. FMIFS consistently outperformed RCGU-MIFS, MIFS, MRMR, JMI, and MJMI in most scenarios. For instance, with five features, Fuzzy-MIFS achieved an accuracy of 0.960, compared to its closest competitor, RCGU-FIMS, at 0.944. The trend continues as the number of features increases, with Fuzzy-MIFS recording the highest accuracy of 0.992 at 25 features, significantly outperforming other methods, where the second-highest was RCGU-MIFS at 0.963. This pattern is evident across different subsets of features, indicating the robustness and effectiveness of Fuzzy-MIFS in handling feature selection for CNN models.

The analysis of these results reveals that the introduction of the fuzzy mechanism in Fuzzy-MIFS plays a crucial role in its

superior performance. The fuzzy mechanism addresses the inherent uncertainty and imprecision in IoT data, which traditional MIFS-based methods struggle to manage effectively. By integrating fuzzy logic, Fuzzy-MIFS can capture nuanced relationships and dependencies between features and the target variable more accurately than traditional methods. This ability to account for the uncertainty and gradual variations in the data leads to a more informed and effective feature selection process, as evidenced by the higher accuracy rates. The improvement in accuracy with an increase in the number of features further supports the effectiveness of the fuzzy approach in improving the reliability and efficiency of feature selection, particularly in complex models such as CNNs, where precise feature selection is critical to performance.

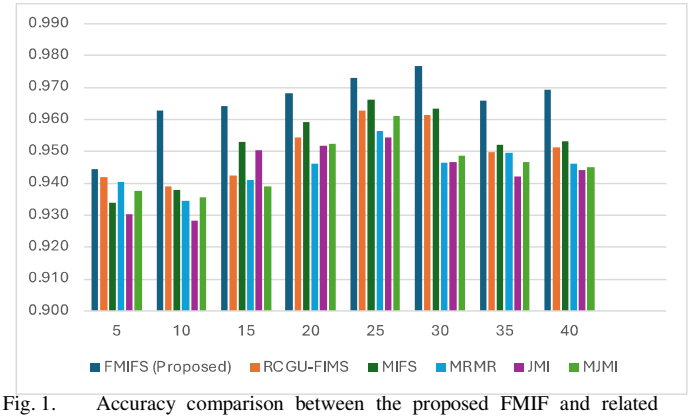

Fig. 1. Accuracy comparison between the proposed FMIF and related works using CNN.

The results of the accuracy comparison between the proposed Fuzzy-MIFS and other related works using an LSTM model show that Fuzzy-MIFS consistently leads in performance across a range of feature counts from 5 to 40. Initially, with five features, Fuzzy-MIFS achieves an accuracy of 0.944, marginally surpassing the nearest competitors, RCGU-MIFS and MRMR, with accuracies of 0.942 and 0.940, respectively. As the number of features increases, Fuzzy-MIFS continues to maintain the highest accuracy, reaching a peak of 0.968 at 25 features. In particular, Fuzzy-MIFS achieves superior performance in all feature sets, demonstrating a consistent improvement over other methods, such as MIFS, MRMR, JMI, and MJMI, particularly in configurations with higher numbers of features. The introduction of fuzzy logic allows Fuzzy-MIFS to better handle the inherent uncertainty and imprecision in the data, which is particularly beneficial for LSTM models that are sensitive to the quality of input features due to their reliance on learning from sequences. This capability to accurately account for data variations enhances the feature selection process, ensuring that the most relevant and informative features are retained. The consistent outperformance of Fuzzy-MIFS across varying feature counts suggests that its fuzzy mechanism effectively captures and utilizes the subtle dependencies and relationships within the data. This leads to a more robust and effective model, capable of achieving higher accuracy in complex predictive tasks involving sequencial data, like those commonly handled by LSTMs.

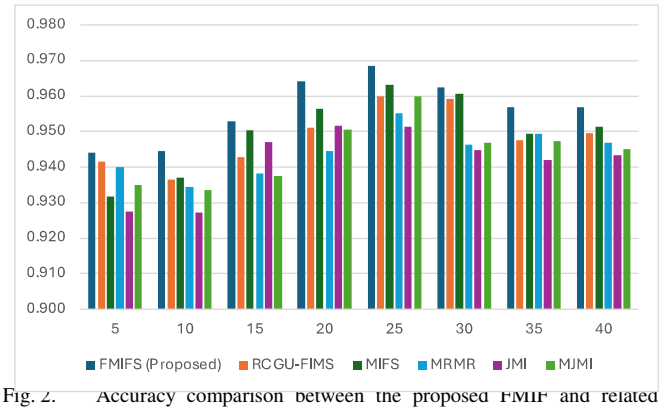

Fig. 2. Accuracy comparison between the proposed FMIF and related works using LSTM

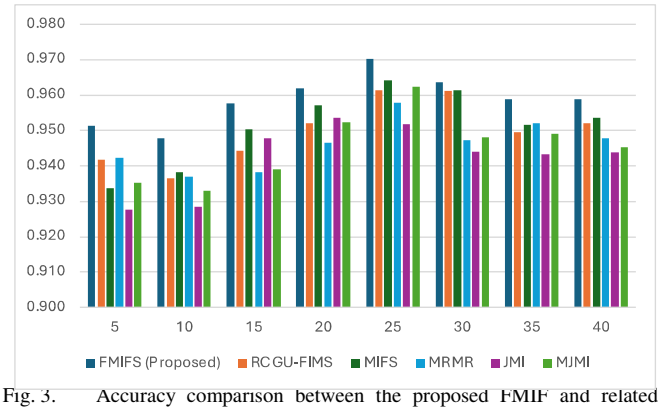

Fig. 3. Accuracy comparison between the proposed FMIF and related works using DBN.

The integration of fuzzy logic in feature selection addresses the critical challenge of uncertainty and imprecision inherent in IoT data, which can significantly impact the learning capabilities of a DBN. The fuzzy mechanism implemented in Fuzzy-MIFS effectively captures and utilizes the nuances within the data, allowing for a more accurate and robust selection of features that are truly informative for the predictive tasks at hand. This is particularly beneficial for a DBN, which relies on a layered structure where the quality of input directly influences overall learning and feature representation in subsequent layers. By enhancing the precision of feature selection, Fuzzy-MIFS ensures that the DBN model is not only fed with high-quality inputs but also optimized for higher performance through the effective management of data intricacies. This results in improved predictive accuracy, demonstrating the practical advantages of employing fuzzy logic to extend the capabilities of traditional mutual information-based approaches in complex and uncertain data environments like those encountered in IoT applications.

IV. CONCLUSION

This study presented a novel Fuzzy-MIFS method to enhance the performance of IDSs in IoT environments. By integrating fuzzy logic with Gaussian membership functions, the proposed method effectively addresses the inherent uncertainties and imprecisions of IoT data, which traditional MIFS methods struggle to manage. The proposed Fuzzy-MIFS method was evaluated against several existing feature selection

techniques using three different neural network models: CNN, LSTM, and DBN. Across all models and various feature counts, Fuzzy-MIFS demonstrated superior accuracy, highlighting its robustness and effectiveness in feature selection. The results of this study indicate that the fuzzy mechanism within Fuzzy-MIFS plays a crucial role in capturing the nuanced relationships and dependencies between the features and the target variable. This leads to more informed and effective feature selection, significantly enhancing the performance of an IDS in detecting malicious activities. The ability of Fuzzy-MIFS to maintain high accuracy across different neural network models and feature counts underscores its versatility and applicability in diverse IoT contexts. Future work may explore further optimization of the fuzzy membership function and the extension of this approach to IoT applications beyond intrusion detection, thus broadening the impact and utility of the Fuzzy-MIFS method in the field of IoT security.

REFERENCES

[1] O. Abu Alghanam, W. Almobaideen, M. Saadeh, and O. Adwan, "An improved PIO feature selection algorithm for IoT network intrusion detection system based on ensemble learning," *Expert Systems with Applications*, vol. 213, Mar. 2023, Art. no. 118745, https://doi.org/10.1016/j.eswa.2022.118745.

[2] R. Alsulami, B. Alqarni, R. Alshomrani, F. Mashat, and T. Gazdar, "IoT Protocol-Enabled IDS based on Machine Learning," *Engineering, Technology & Applied Science Research*, vol. 13, no. 6, pp. 12373–12380, Dec. 2023, https://doi.org/10.48084/etasr.6421.

[3] S. Subramani and M. Selvi, "Multi-objective PSO based feature selection for intrusion detection in IoT based wireless sensor networks," *Optik*, vol. 273, Feb. 2023, Art. no. 170419, https://doi.org/10.1016/j.ijleo.2022.170419.

[4] Y. Lyu, Y. Feng, and K. Sakurai, "A Survey on Feature Selection Techniques Based on Filtering Methods for Cyber Attack Detection," *Information*, vol. 14, no. 3, Mar. 2023, Art. no. 191, https://doi.org/10.3390/info14030191.

[5] N. A. Alsharif, S. Mishra, and M. Alshehri, "IDS in IoT using Machine Learning and Blockchain," *Engineering, Technology & Applied Science Research*, vol. 13, no. 4, pp. 11197–11203, Aug. 2023, https://doi.org/10.48084/etasr.5992.

[6] S. Al-Emari, Y. Sanjalawe, D. Alsmadi, E. Alduweib, and A. Alharbi, "Employing Mutual Information Feature Selection and LightGBM for Intrusion Detection in IoT." ICIC International, 2024, https://doi.org/10.24507/icicel.18.06.597.

[7] M. Gautam, S. Ahuja, and A. Kumar, "Intrusion Detection Techniques in Internet of Things: A Bird's Eye View," in *2024 11th International Conference on Computing for Sustainable Global Development (INDIACom)*, New Delhi, India, Feb. 2024, pp. 622–628, https://doi.org/10.23919/INDIACom61295.2024.10499013.

[8] Z. Ling and Z. J. Hao, "An Intrusion Detection System Based on Normalized Mutual Information Antibodies Feature Selection and Adaptive Quantum Artificial Immune System," *International Journal on Semantic Web and Information Systems*, vol. 18, no. 1, pp. 1–25, Jan. 2022, https://doi.org/10.4018/IJSWIS.308469.

[9] A. A. Anitha and L. Arockiam, "ANNIDS: Artificial Neural Network based Intrusion Detection System for Internet of Things," *International Journal of Innovative Technology and Exploring Engineering*, vol. 8, no. 11, pp. 2583–2588, Sep. 2019, https://doi.org/10.35940/ijitee.K1875.0981119.

[10] F. Hussain *et al.*, "A Framework for Malicious Traffic Detection in IoT Healthcare Environment," *Sensors*, vol. 21, no. 9, Jan. 2021, Art. no. 3025, https://doi.org/10.3390/s21093025.

[11] H. Y. I. Khalid and N. B. I. Aldabagh, "A Survey on the Latest Intrusion Detection Datasets for Software Defined Networking Environments," *Engineering, Technology & Applied Science Research*, vol. 14, no. 2, pp. 13190–13200, Apr. 2024, https://doi.org/10.48084/etasr.6756.

[12] A. Wells and A. B. Usman, "Trust and Voice Biometrics Authentication for Internet of Things," *International Journal of Information Security and Privacy*, vol. 17, no. 1, pp. 1–28, Jan. 2023, https://doi.org/10.4018/IJISP.322102.

[13] Q. A. Arshad, W. Z. Khan, F. Azam, M. K. Khan, H. Yu, and Y. B. Zikria, "Blockchain-based decentralized trust management in IoT: systems, requirements and challenges," *Complex & Intelligent Systems*, vol. 9, no. 6, pp. 6155–6176, Dec. 2023, https://doi.org/10.1007/s40747-023-01058-8.

[14] A. M. Banaamah and I. Ahmad, "Intrusion Detection in IoT Using Deep Learning," *Sensors*, vol. 22, no. 21, Jan. 2022, Art. no. 8417, https://doi.org/10.3390/s22218417.

[15] S. H. S. Ariffin *et al.*, "Intrusion Detection System (IDS) Accuracy Testing for Software Defined Network Internet of Things (SDN-IOT) Testbed," *ELEKTRIKA- Journal of Electrical Engineering*, vol. 21, no. 3, pp. 23–27, Dec. 2022, https://doi.org/10.11113/elektrika.v21n3.361.

[16] G. Thamilarasu and S. Chawla, "Towards Deep-Learning-Driven Intrusion Detection for the Internet of Things," *Sensors*, vol. 19, no. 9, Jan. 2019, Art. no. 1977, https://doi.org/10.3390/s19091977.

[17] A. Khraisat, I. Gondal, P. Vamplew, J. Kamruzzaman, and A. Alazab, "A Novel Ensemble of Hybrid Intrusion Detection System for Detecting Internet of Things Attacks," *Electronics*, vol. 8, no. 11, Nov. 2019, Art. no. 1210, https://doi.org/10.3390/electronics8111210.

[18] J. Wu, H. Dai, Y. Wang, K. Ye, and C. Xu, "Heterogeneous Domain Adaptation for IoT Intrusion Detection: A Geometric Graph Alignment Approach," *IEEE Internet of Things Journal*, vol. 10, no. 12, pp. 10764–10777, 2023, https://doi.org/10.1109/JIOT.2023.3239872.

[19] R. Khilar *et al.*, "Artificial Intelligence-Based Security Protocols to Resist Attacks in Internet of Things," *Wireless Communications and Mobile Computing*, vol. 2022, no. 1, 2022, Art. no. 1440538, https://doi.org/10.1155/2022/1440538.

[20] O. Shende, R. K. Pateriya, P. Verma, and A. Jain, "CEBM: Collaborative Ensemble Blockchain Model for Intrusion Detection in IoT Environment." Research Square, 2021, https://doi.org/10.21203/rs.3.rs-702181/v1.

[21] M. M. Alani and A. Miri, "Towards an Explainable Universal Feature Set for IoT Intrusion Detection," *Sensors*, vol. 22, no. 15, Jan. 2022, Art. no. 5690, https://doi.org/10.3390/s22155690.

[22] P. R. Agbedanu, R. Musabe, J. Rwigema, I. Gatare, T. J. Maginga, and D. K. Amenyedzi, "Towards achieving lightweight intrusion detection systems in Internet of Things, the role of incremental machine learning: A systematic literature review." F1000Research, Nov. 24, 2022, https://doi.org/10.12688/f1000research.127732.1.

[23] M. Nasri, A. Helali, and H. Maaref, "Energy-efficient fuzzy logic-based cross-layer hierarchical routing protocol for wireless Internet-of-Things sensor networks," *International Journal of Communication Systems*, vol. 34, no. 9, 2021, Art. no. e4808, https://doi.org/10.1002/dac.4808.

[24] Q. Yin, "Design and Application of Smart City Internet of Things Service Platform Based on Fuzzy Clustering Algorithm," *Mobile Information Systems*, vol. 2022, no. 1, 2022, Art. no. 8405306, https://doi.org/10.1155/2022/8405306.

[25] M. P. Pitchai, M. Ramachandran, F. Al-Turjman, and L. Mostarda, "Intelligent Framework for Secure Transportation Systems Using Software-Defined-Internet of Vehicles," *Computers, Materials & Continua*, vol. 68, no. 3, pp. 3947–3966, 2021, https://doi.org/10.32604/cmc.2021.015568.

[26] W. Zang, "Construction of Mobile Internet Financial Risk Cautioning Framework Based on BP Neural Network," *Mobile Information Systems*, vol. 2022, no. 1, 2022, Art. no. 3374674, https://doi.org/10.1155/2022/3374674.

[27] X. Guo, T. Zeng, Y. Wang, and J. Zhang, "Fuzzy TOPSIS Approaches for Assessing the Intelligence Level of IoT-Based Tourist Attractions," *IEEE Access*, vol. 7, pp. 1195–1207, 2019, https://doi.org/10.1109/ACCESS.2018.2881339.

[28] M. I. Tariq, N. A. Mian, A. Sohail, T. Alyas, and R. Ahmad, "Evaluation of the Challenges in the Internet of Medical Things with Multicriteria

Decision Making (AHP and TOPSIS) to Overcome Its Obstruction under Fuzzy Environment," *Mobile Information Systems*, vol. 2020, no. 1, 2020, Art. no. 8815651, https://doi.org/10.1155/2020/8815651.

[29] A. D. Indriyanti, "Design and Build Smart Agriculture Using Cognitive Internet of Things (C IoT)," *Journal Research of Social Science, Economics, and Management*, vol. 1, no. 7, Feb. 2022, https://doi.org/10.59141/jrssem.v1i7.113.

[30] A. R. A. Tahtawi and R. Kurniawan, "Kendali pH untuk sistem IoT hidroponik deep flow technique berbasis fuzzy logic controller," *Jurnal Teknologi dan Sistem Komputer*, vol. 8, no. 4, pp. 323–329, Oct. 2020, https://doi.org/10.14710/jtsiskom.2020.13822.

[31] S. Titi, H. B. Elhadj, and L. C. Fourati, "A Fuzzy-Ontology Based Diabetes Monitoring System Using Internet of Things," in *The Impact of Digital Technologies on Public Health in Developed and Developing Countries*, Hammamet, Tunisia, 2020, pp. 287–295, https://doi.org/10.1007/978-3-030-51517-1_25.

[32] R. Yauri, J. Lezama, and M. Rios, "Evaluation of a wireless low-energy mote with fuzzy algorithms and neural networks for remote environmental monitoring," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 23, no. 2, Aug. 2021, https://doi.org/10.11591/ijeecs.v23.i2.pp717-724.

[33] M. Alalhareth and S. C. Hong, "An Adaptive Intrusion Detection System in the Internet of Medical Things Using Fuzzy-Based Learning," *Sensors*, vol. 23, no. 22, Jan. 2023, Art. no. 9247, https://doi.org/10.3390/s23229247.

[34] F. S. Alrayes *et al.*, "Optimal Fuzzy Logic Enabled Intrusion Detection for Secure IoT-Cloud Environment," *Computers, Materials & Continua*, vol. 74, no. 3, pp. 6737–6753, 2023, https://doi.org/10.32604/cmc.2023.032591.

[35] J. B. Awotunde, F. E. Ayo, R. Panigrahi, A. Garg, A. K. Bhoi, and P. Barsocchi, "A Multi-level Random Forest Model-Based Intrusion Detection Using Fuzzy Inference System for Internet of Things Networks," *International Journal of Computational Intelligence Systems*, vol. 16, no. 1, Mar. 2023, Art. no. 31, https://doi.org/10.1007/s44196-023-00205-w.

[36] S. R. Zahra and M. A. Chishti, "A generic and lightweight security mechanism for detecting malicious behavior in the uncertain Internet of Things using fuzzy logic- and fog-based approach," *Neural Computing and Applications*, vol. 34, no. 9, pp. 6927–6952, May 2022, https://doi.org/10.1007/s00521-021-06823-9.

[37] M. Savva, I. Ioannou, and V. Vassiliou, "Performance evaluation of a Fuzzy Logic-based IDS (FLIDS) technique for the Detection of Different Types of Jamming Attacks in IoT Networks," in *2023 21st Mediterranean Communication and Computer Networking Conference (MedComNet)*, Island of Ponza, Italy, Jun. 2023, pp. 93–100, https://doi.org/10.1109/MedComNet58619.2023.10168848.

[38] S. S. Pandi *et. al.*, "Advancing IoT security with flame: A hybrid approach combining fuzzy logic and artificial lizard search optimization," *Computers & Security*, vol. 145, Oct. 2024, Art. no. 103984, https://doi.org/10.1016/j.cose.2024.103984.

[39] M. A. Alohali, M. Elsadig, F. N. Al-Wesabi, M. Al Duhayyim, A. Mustafa Hilal, and A. Motwakel, "Enhanced Chimp Optimization-Based Feature Selection with Fuzzy Logic-Based Intrusion Detection System in Cloud Environment," *Applied Sciences*, vol. 13, no. 4, Jan. 2023, Art. no. 2580, https://doi.org/10.3390/app13042580.

[40] M. Alalhareth and S. C. Hong, "An Improved Mutual Information Feature Selection Technique for Intrusion Detection Systems in the Internet of Medical Things," *Sensors*, vol. 23, no. 10, Jan. 2023, Art. no. 4971, https://doi.org/10.3390/s23104971.

[41] B. A. S. Al-rimy *et al.*, "Redundancy Coefficient Gradual Up-weighting-based Mutual Information Feature Selection technique for Crypto-ransomware early detection," *Future Generation Computer Systems*, vol. 115, pp. 641–658, Feb. 2021, https://doi.org/10.1016/j.future.2020.10.002.

[42] Y. A. Ahmed, B. Koçer, S. Huda, B. A. S. Al-rimy, and M. M. Hassan, "A system call refinement-based enhanced Minimum Redundancy Maximum Relevance method for ransomware early detection," *Journal of Network and Computer Applications*, vol. 167, Oct. 2020, Art. no. 102753, https://doi.org/10.1016/j.jnca.2020.102753.

[43] P. Zhang, G. Liu, and J. Song, "MFSJMI: Multi-label feature selection considering join mutual information and interaction weight," *Pattern Recognition*, vol. 138, Jun. 2023, Art. no. 109378, https://doi.org/10.1016/j.patcog.2023.109378.

[44] M. Bennasar, Y. Hicks, and R. Setchi, "Feature selection using Joint Mutual Information Maximisation," *Expert Systems with Applications*, vol. 42, no. 22, pp. 8520–8532, Dec. 2015, https://doi.org/10.1016/j.eswa.2015.07.007.

[45] Y. Shi, J. Chu, C. Ji, J. Li, and S. Ning, "A Fuzzy-Based Mobile Edge Architecture for Latency-Sensitive and Heavy-Task Applications," *Symmetry*, vol. 14, no. 8, Aug. 2022, Art. no. 1667, https://doi.org/10.3390/sym14081667.

[46] N. Radwan and M. Farouk, "The Growth of Internet of Things (IoT) In The Management of Healthcare Issues and Healthcare Policy Development," *International Journal of Technology, Innovation and Management*, vol. 1, no. 1, pp. 69–84, Sep. 2021, https://doi.org/10.54489/ijtim.v1i1.8.

[47] L. A. Saddik, B. A. Khalifa, and B. Fateh, "Evaluation quality of service for internet of things based on fuzzy logic: a smart home case study," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 25, no. 2, Feb. 2022, Art. no. 825, https://doi.org/10.11591/ijeecs.v25.i2.pp825-839.

[48] S. M. Othman and M. B. Abdulrazzaq, "Fuzzy logic system for drug storage based on the internet of things: a survey," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 29, no. 3, Mar. 2023, Art. no. 1382, https://doi.org/10.11591/ijeecs.v29.i3.pp1382-1392.

[49] A. A. Hady, A. Ghubaish, T. Salman, D. Unal, and R. Jain, "Intrusion Detection System for Healthcare Systems Using Medical and Network Data: A Comparison Study," *IEEE Access*, vol. 8, pp. 106576–106584, 2020, https://doi.org/10.1109/ACCESS.2020.3000421.

AUTHORS' PROFILES

Abdullah Abu Saq is currently a Ph.D. candidate at the Faculty of Computing, Universiti Teknologi Malaysia. His research interests include, but are not limited to, cyber security, IoT, IDS, and information assurance.

Anazida Zainal received a B.Sc. in Computer Science from Rutgers University, NJ, USA, in 1990, and an M.Sc. in Computer Science and a Ph.D. in Computer Science and Network Security from Universiti Teknologi Malaysia (UTM) in 2000 and 2011, respectively. She is currently an Assistant Professor in the Faculty of Computing, and a member of the Information Assurance and Security Research Group (IASRG), UTM. Her research interests include cyber threat intelligence, security analytics, network security, and anomaly detection.

Bander A. Al-Rimy is currently a faculty member of the School of Computing, University of Portsmouth, UK. He received a Ph.D. in computer science from Universiti Teknologi Malaysia, in 2019, an M.Sc. in Information Technology from Open University Malaysia in 2013, and a B.Eng. in Computing from Sana'a University in 2003. He is the recipient of several academic awards including, but not limited to, the UTM Best Student Award, the UTM Service Excellence Award, and the OUM Distinction Award. His research interests include malware analysis, cyber security, computer networks, and artificial intelligence.

Abdulrahman Alyami is an Assistant Professor in Information Systems at the College of Computer and Information Sciences, Jouf University, Sakaka, Saudi Arabia.

Hamad Abu Saq is an assistant professor at Computer Science, College of Computer Science and Information Systems, Najran University, Saudi Arabia.