Journal of Information & Optimization Sciences
ISSN 0252-2667 (Print), ISSN 2169-0103 (Online)
Vol. 47 (2026), No. 1, pp. 353–369
DOI : 10.47974/JIOS-2150

A fuzzy mutual information-based intrusion detection system for enhancing cybersecurity in smart energy grids

Ch. Kodanda Ramu *
T. Srinivasa Rao †
Department of Computer Science and Engineering
GITAM (Deemed to Be University)
Visakhapatnam 530045
Andhra Pradesh
India

Abstract

The shift from traditional power grids to smart grids has enhanced efficiency, reliability, and flexibility through advanced digital communication, automation, and real-time control. However, this increased connectivity expands the attack surface, exposing smart grids to diverse cyber threats and legacy system vulnerabilities. Cybersecurity is, thus, essential to ensure reliable, safe, and secure energy services in smart grid scenarios. This paper proposes a novel FMI-Reduct-Based NIDS Classifier, which integrates a fuzzy approach along with Conditional Mutual Information (CMI) and the Quick Reduct Algorithm (QRA) to prioritize the most relevant features in smart grid data effectively. This methodology not only improves classification performance but also significantly boosts detection capabilities, providing a robust solution for addressing the challenges posed by evolving cyber threats in a smart grid. Extensive experiments using public and benchmark datasets such as NSL-KDD and UNSW-NB15 demonstrate that the proposed FMI-Reduct-Based Classifier outperforms traditional classifiers in precision, recall, and overall detection rate. The limitations and future research works are discussed thoroughly.

Subject Classification: *03B52, 68T01, 93C95, 68M25.*

Keywords: *Smart energy security, Ensemble learning, Cyber-physical resilience, Sustainable infrastructure, Benchmark datasets.*

* *E-mail:* **kvr.chintu1978@gmail.com (Corresponding Author)**
† *E-mail:* **sthamada@gitam.edu**

1. Introduction

Intrusion Detection Systems (IDS) are pivotal in safeguarding modern networks against cyber threats such as Distributed Denial of Service (DDoS) attacks, malware, and phishing campaigns [1]. In the realm of smart energy, networks, encompassing Distributed Energy Resources (DERs), smart meters, Phasor Measurement Units (PMUs), and Advanced Metering Infrastructure (AMI)—the integration of Internet of Things (IoT) devices and legacy protocols introduces complex cybersecurity challenges [2]. These challenges are further intensified by the dynamic nature of network traffic and the high dimensionality of data, which often overwhelm traditional IDS frameworks [3].

Researchers have proposed several innovative soft computing systems for smart energy grid cybersecurity to accurately model overall security levels [4]. A good number of studies adopted fuzzy logic [5-6], fuzzy cognitive maps (FCMs), expert systems [7], which offered an amicable solution capable of revealing weak links, and vulnerabilities of automation systems. Further, supervised machine learning models, including Support Vector Machines (SVM), Random Forests (RF), and Deep Neural Networks (DNNs) have demonstrated promise in improving IDS performance [8, 1]. However, these models are frequently benchmarked using legacy datasets such as NSL-KDD [8]. While NSL-KDD provides structured, labeled data and includes attack types like Denial of Service (DoS), User-to-Root (U2R), Remote-to-Local (R2L), and Probing, conceptually relevant to smart grid environments, for example, attacks on SCADA, AMI, and PMU systems, it has significant limitations in practical smart grid applications. Specifically, NSL-KDD is constructed from simulated attacks on outdated 1990s network architectures and lacks support for modern industrial protocols such as IEC 61850 and DNP3, which are fundamental to smart grid communications.

Moreover, the dataset does not capture physical layer data, device-level interactions, or critical operational features—such as load profiles, voltage or frequency anomalies, and real-time control commands that are essential for detecting sophisticated cyber-physical attacks like false data injection or load-altering events [2, 1]. Consequently, while NSL-KDD serves as a baseline for benchmarking, its applicability to real-world smart grid cybersecurity is limited [8], highlighting the need for domain-specific datasets that better capture the complexity of smart grid operations [2, 1]. To address these limitations, this paper proposes a Fuzzy Mutual Information-Based Intrusion Detection System (FMI-IDS), combining

fuzzy logic's capacity to handle uncertainty [1] with Conditional Mutual Information (CMI) and the Quick Reduct Algorithm (QRA) for feature selection. This hybrid approach enhances the detection of subtle attack patterns in complex smart grid environments and improves classification accuracy, as demonstrated through comparative evaluations using NSL-KDD [8] and UNSW-NB15 [9] datasets, respectively.

2. Literature survey

Recent advancements in IDS for smart grids and IoT environments have leveraged a combination of deep learning, ensemble methods, and feature selection techniques to enhance detection accuracy and address evolving cyber threats. For instance, [10] developed a hybrid CNN-LSTM model utilizing the UNSW-NB15 dataset, achieving high accuracy in detecting intrusions within industrial IoT networks. Similarly, [11] proposed a CNN-GRU-FL approach that integrates federated learning (FL) to preserve data privacy while maintaining robust intrusion detection capabilities in smart grid environments. In the realm of feature selection, [12] introduced IDS-XGbFS, employing XGBoost with recent feature selection techniques to enhance VANET safety. [13] proposed an intrusion detection model using election-based feature selection combined with K-NN, demonstrating improved detection rates on the UNSW-NB15 dataset. Addressing the challenges of IoT edge computing, [14] designed an effective intrusion detection approach that combines ensemble learning with feature selection methods, achieving notable results on the Bot-IoT dataset.

A research study [15] explored advanced machine learning techniques for big data analytics in smart grids, highlighting the role of scalable algorithms in processing vast amounts of network data. In the context of SDN-based SCADA systems, [16] proposed an ensemble learning framework for DDoS detection, thereby enhancing the resilience of critical control systems. A research [17] introduced a hybrid deep learning approach combining CNN and BiLSTM for network intrusion detection in SDN environments, achieving improved detection rates. Said et al. [18] proposed a novel network intrusion detection method that integrates Temporal Convolution Networks (TCN), Bidirectional Gated Recurrent Units (BiGRU), and attention mechanisms to capture complex temporal patterns in network traffic. A research study [19] presented a double-layer feature fusion-based network intrusion detection system using CNN and GRU, demonstrating enhanced performance in detecting sophisticated

cyberattacks. Collectively, these studies underscore the ongoing evolution of intrusion detection methodologies, emphasizing the integration of advanced machine learning techniques, feature selection methods, and ensemble learning to address the multifaceted security challenges in smart grid and IoT environments.

3. Data and Analysis Methodology

The following diagram, as shown in Figure 1, visually demonstrates four common types of cyber-attacks on a simplified smart grid infrastructure.

The control center is the core hub for managing smart grid operations and a prime target for attacks. Substations transform and relay voltage between the control center and end-users. Smart meters, as edge devices, record consumption and enable communication with utilities but are also vulnerable entry points. The attacker, shown in red, represents a threat from external networks via the internet cloud.

Attack types include:

a) DoS – Disrupts service availability
b) U2R – Gains low-level access and escalates to admin rights
c) R2L – Remote attacker gains unauthorized local access, and
d) Probing– Scans network for vulnerabilities without launching an attack.

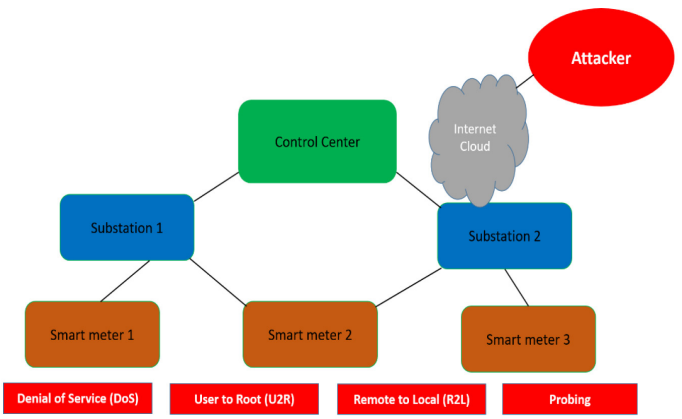

Figure 1

Four common types of cyber-attacks on a smart grid infrastructure

3.1 *Datasets used*

3.1.1. KDD CUP 99

The KDD CUP 99 dataset, derived from DARPA 98 (http://www.ll.mit.edu/r-d/datasets/1998-darpa-intrusion-detection-evaluation-dataset) and developed by MIT Lincoln Laboratory, evaluates intrusion detection systems. It is widely used for testing IDS and anomaly-based detection methods (AB-IDS). The dataset has three-feature categories—principal, traffic, and content features—and covers four major attack types: DoS, Probe, U2R, and R2L. However, issues like data redundancy and imbalance affect model performance. To overcome these, the NSL-KDD dataset was introduced as an improved version of KDD 99.

3.1.2. NSL KDD

Since its release in 1999, researchers have widely used the KDD-CUP 99 dataset for anomaly and misuse detection. Derived from 4 GB of DARPA 98 data, it contains about 4 million entries. However, the NSL-KDD dataset

Table 1

Dataset-wide Binary Classification Distribution

S. No	NSL-KDD Subsets	Number of Instances		
		Total	Normal%	Attack%
1	KDD_Train(+)	1,25,973	67343(53.45%)	58630 (46.55%)
2	KDD_Test(+)	25,544	9711 (38.02%)	15833 (61.98%)
3	KDD_Test(+21)	11,850	4344 (36.65%)	7506 (63.35%)

Table 2

Dataset-wide Multi Classification Distribution

S. No.	NSL-KDD Subsets	Number of Instances				
		Normal%	DoS %	Probe %	U2R %	R2L %
1	KDD_Train (+)	67343 53.45%	45927 36.45%	11656 9.25%	995 0.78%	52 0.07%
2	KDD_Test (+)	9711 38.02%	7460 29.20%	2885 11.29%	2421 9.48%	67 0.26%
3	KDD_Test (+21)	4344 36.65%	2885 24.34%	2402 20.27%	2152 18.16%	67 0.58%

refines KDD 99 by addressing duplicate biases, offering a more balanced IDS evaluation. The dataset has 42 features—both numerical and categorical—representing normal traffic and 22 attack types. Tables 1–3 detail the attack distribution and feature types; continuous features (bolded) may require fuzzification depending on the method used.

Table 3
Dataset-Wide Features and its Type

Category	Feature	Type
Basic Features	duration, protocol type, service, flag, **src_bytes**, **dst_bytes**, land, wrong_fragment, urgent	Categorical/ Numeric
Content Features	**hot**, num_failed_logins, logged_in, **num_compromised**, **root_shell**, **su_attempted**, **num_root**, **num_file_creations**, **num_shells**, **num_access_files**, num_outbound_cmds, is_host_login, is_guest_login	Numeric/ Boolean
Time-Based Features	**count**, srv_count, **serror_rate**, srv_serror_rate, **rerror_rate**, srv_rerror_rate, same_srv_rate, diff_srv_rate, srv_diff_host_rate	Numeric
Host-Based Features	**dst_host_count**, **dst_host_srv_count**, **dst_host_same_srv_rate**, **dst_host_diff_srv_rate**, **dst_host_same_src_port_rate**, dst_host_srv_diff_host_rate, **dst_host_serror_rate**, dst_host_srv_serror_rate, **dst_host_rerror_rate**, dst_host_srv_rerror_rate	Numeric
Predicted Variable	attack type (normal, DoS, U2R, R2L, Probe)	Categorical

3.1.3 UNSW-NB15

The dataset, created using the advanced IXIA test bed setup tool [20], incorporates modern attacks to provide a realistic evaluation environment for current intrusion detection systems (IDS). Developed in Australia as an enhanced version of the KDD 99 dataset, the NSL-KDD is periodically updated using the CVE lexicon, which catalogs well-documented security vulnerabilities. This dataset captures a fusion of contemporary network conditions, including nine distinct attacks. Two scenarios were simulated in the IXIA tested: one generating one attack per second until 50 GB of

pcap data was collected, and another generating ten attacks per second for an additional 50 GB. The extracted dataset includes 51 features grouped into flow (5), basic (13), content (8), time (9), connections (7), general (5), others (5) characteristics. The UNSW-NB15 dataset presents significant challenges in classifying network attacks due to the complexity and diversity of its nine attack categories, which include Fuzzers, DoS, Backdoors, Exploits, and Worms, among others, as shown in Table 4. A major issue is the high-class overlap, where attacks like Fuzzers and Reconnaissance exhibit behaviors similar to normal traffic, increasing false positives and false negatives. The dataset also suffers from class imbalance, with fewer instances of rare attacks like Worms and Shell code, leading to biased classification models. Additionally, the mix of categorical and continuous features, such as protocol types and packet sizes, adds complexity to the classification process. These challenges highlight the importance of using effective data cleaning techniques and ways to choose the best features to make intrusion detection better when working with this specific dataset.

Table 4

Distribution of Multi-class UNSW-NB 15 Dataset

S. No	Attacks	TRAIN (75%)	VALIDATION (25%)	Total (Train Set) (100%)	TESTSET
1	Generic	30,081	9919	40,000	18,871
2	DoS	9237	3027	12,264	4089
3	Worms	99	31	130	44
4	Exploits	25,034	8359	33,393	11,132
5	Fuzzers	13,608	4576	18,184	6062
6	Backdoor	1330	416	1746	583
7	Shell code	854	279	1133	378
8	Analysis	1477	523	2000	677
9	Reconnaissance	7875	2616	10,491	3496
10	Normal	41,911	14,089	56,000	37,000

3.2. *Methodology*

3.2.1 FMI-IDS Approach

Smart grids, by design, integrate a complex ecosystem of interconnected devices such as smart meters, sensors, Phasor Measurement

Units (PMUs), and control centers—operating under diverse protocols such as IEC 61850 and DNP3. This interconnectedness, while essential for efficiency, introduces vulnerabilities such as false data injection, load-altering attacks, and denial-of-service (DoS). Traditional intrusion detection systems often struggle to cope with the heterogeneity, high-dimensionality, and uncertainty inherent in smart grid data. Moreover, conventional binary classifiers may fail to capture subtle variations in traffic patterns—such as slight deviations in packet size or connection count—that distinguish legitimate operations from attacks. The proposed Fuzzy Mutual Information-Based Intrusion Detection System (FMI-IDS) effectively addresses these limitations by integrating fuzzy logic with mutual information-based feature selection. In real-world smart grid environments, network features like packet size and connection count rarely have sharp boundaries between normal and malicious behavior. For example, a packet size of 1200 bytes might be normal for one application but indicative of a DoS attack in another. Fuzzy logic provides a framework to quantify these uncertainties using membership functions. Let us consider the fuzzy rules defined in the system:

For packet size (x), the system assigns degrees of membership to «DoS» and «Port Scan» categories using piecewise linear functions:

1. a) For DoS: μ_DoS(x) transitions from 0 (non-suspicious) to 1 (highly suspicious) as x increases from 500 to 1500 bytes (Eq. 1).
2. b) For Port Scanning: μ_Scan(x) peaks for smaller packets (64–200 bytes) typical of probe attacks (Eq. 2).
3. Similarly, for connection count (y):
4. c)μ_DoS(y) peaks for moderate counts (50–100), as multiple connections per second may indicate flooding (Eq. 3).
5. d) μ_Scan(y) peaks for 20–50 connections, typical of scan bursts (Eq. 4).

These fuzzy membership functions enable the system to represent degrees of suspicion instead of binary decisions, accommodating gray areas where traffic may not be clearly normal or malicious.

3.2.2 Aggregation through Fuzzy Operators

Once membership degrees are computed for individual features, FMI-IDS combines them using the max operator:

For each packet, the system computes:

6. a)μ_Total DoS(x, y) = max(μ_DoS(x), μ_DoS(y)) (Eq. 5)
7. b) μ_Total Scan(x, y) = max(μ_Scan(x), μ_Scan(y)) (Eq. 6)

This aggregation accounts for scenarios where a single strong indicator (e.g., unusually large packet size) may suffice to flag an attack, ensuring the system is sensitive to critical features while tolerating noise.

3.2.3. Classification through Defuzzyfication

The final classification is performed using the maximum membership principle:

If μ_Total DoS > μ_Total Scan, classify as DoS.

If μ_Total Scan > μ_Total DoS, classify as Port Scan.

If both values are approximately equal, flag as ambiguous, prompting further analysis.

This soft decision-making is crucial in smart grids, where false positives (misclassifying normal operations as attacks) can lead to unnecessary service interruptions, and false negatives (missing attacks) can compromise grid stability.

3.2.4. Feature Selection with Mutual Information

While fuzzy logic manages uncertainty, Mutual Information (MI) identifies the most relevant features (e.g., packet size, connection count, flow duration) by measuring how much information they provide about the attack classes.

This FMI approach:

a) Reduces the impact of irrelevant or redundant features.
b) Improves classification accuracy and computational efficiency.
c) Tailors detection to smart grid-specific patterns like load profiles, control commands, and SCADA traffic.

The proposed methodology, as shown in Figure 2, processes raw network traffic data by first converting continuous features into fuzzy sets using triangular membership functions. Since the dataset has no missing values, preprocessing focuses on fuzzification. For feature selection, CMI identifies relevant features, while QRA eliminates redundancies, refining the feature set. The reduced feature space, called FMI-Reduct, is then used to train an ensemble classifier combining C4.5, SVM, and k-NN models.

This ensemble, supported by a decision-making system, enhances detection accuracy and reduces false alarms. Finally, a majority voting mechanism aggregates predictions from the base classifiers during validation, ensuring robust detection of network intrusions.

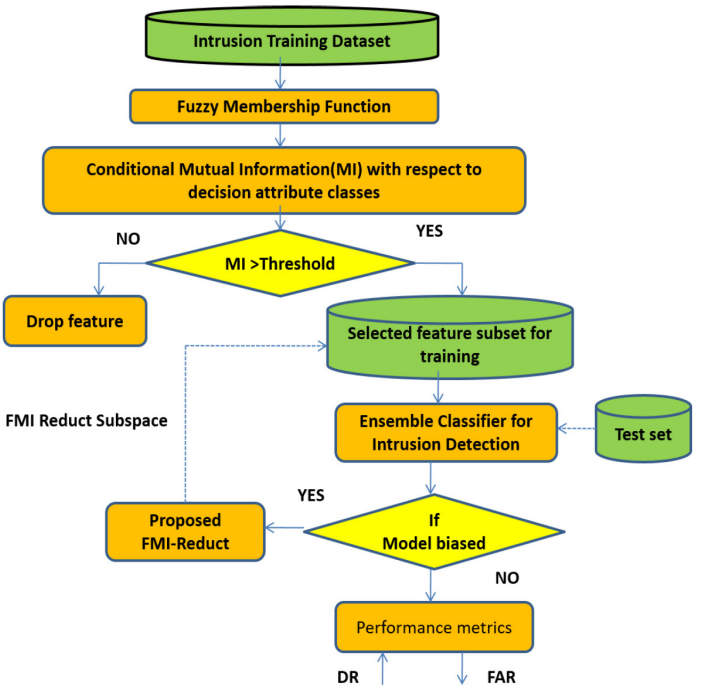

Figure 2

The Flow of FMI-Reduct Ensemble NIDS Classification

4. Results and Discussion

In constructing the ensemble classification model, classifiers such as DT, SVM, and K-NN were tuned separately for both the NSL-KDD and UNSW-NB15 datasets to achieve optimal performance. The experiments were done using two popular datasets: NSL-KDD and UNSW-NB15 were chosen for their comprehensive representation of both modern and traditional network attack scenarios. The input (training and test) data format for the chosen algorithms underwent necessary pre-processing: continuous features were transformed using fuzzy logic to handle overlapping issues. The categorical features were encoded using one-hot encoding. This ensured that both numerical and non-numerical input

types of data were compatible with all chosen methods and classifiers in the ensemble model. The reduction or relevant network feature selection in the proposed NIDS framework was performed using the CMI and QRA for selecting 'reduct' features. The individual base classifiers were carefully tuned for optimal performance and evaluation, including DT, SVM and K-NN, and were integrated into an ensemble framework.

4.1 *Significance of the Feature Selection Data*

The presented data in Table 5 highlights the critical role of feature selection in improving intrusion detection for smart grid cyber security.

Table 5

The relevant features selected from proposed and existing techniques.

Dataset	Total Features (Nos.)	Algorithm	Reduced Features	Total Reduced (Nos.)
NSL_ KDD	42	IG	1, 2, 3, 5, 6, 9, 10, 12, 14, 17, 20, 23, 24, 29, 31, 32, 34, 36, 38, 39, 40	21
		PCA	1, 2, 3, 5, 6, 8, 10, 12, 14, 17, 20, 23, 25, 28, 30, 32, 34, 36, 37, 39, 40, 41	22
		IG + PCA	1, 2, 3, 5, 6, 9, 11, 12, 14, 16, 18, 24, 27, 30, 32, 37, 39	17
		FMI	1, 5, 6, 7, 9, 10, 11, 12, 13, 16, 17, 22, 29, 33, 34, 40, 41	17
		QRA (FMI-Reduct)	5, 6, 7, 11, 12, 13, 22, 33, 40, 41	10
UNSW_ NB15	51	IG	1, 2, 3, 5, 7, 10, 12, 14, 15, 17, 18, 20, 21, 23, 25, 27, 28, 30, 31, 34, 35, 37, 39, 40	23
		PCA	1, 2, 3, 4, 6, 7, 10, 11, 13, 14, 16, 17, 18, 19, 20, 21, 22, 24, 26, 27, 29, 30, 33, 35, 38, 40	26
		IG + PCA	1, 3, 5, 7, 10, 12, 13, 15, 17, 19, 21, 23, 25, 27, 29, 35	16
		FMI	6, 9, 10, 11, 13, 14, 15, 16, 20, 21, 23, 34, 35, 36, 37, 38, 41, 42, 45	19
		QRA (FMI-Reduct)	6, 10, 11, 15, 16, 20, 23, 37, 38, 41, 42, 45	12

By comparing methods—Information Gain (IG), Principal Component Analysis (PCA), IG + PCA, Fuzzy Mutual Information (FMI), and the proposed QRA (FMI-Reduct)—across benchmark datasets (NSL-KDD, UNSW-NB15), the study demonstrates how redundant and irrelevant features can be effectively reduced. For the NSL-KDD dataset (42 features), the QRA approach achieves the most compact representation, reducing to 10 features, while maintaining essential discriminatory information. Similarly, for the UNSW-NB15 dataset (51 features), QRA reduces to 12 features. This significant reduction—from 42 to 10 and from 51 to 12—not only streamlines computational complexity but also enhances model performance by focusing on the most relevant attributes. The data underscores the strength of the FMI-Reduct approach in isolating core features, ensuring better detection accuracy and efficiency in complex, evolving smart grid environments.

The models were evaluated on Precision, Recall, DR, and Accuracy-Score and FAR to ensure a comprehensive analysis of their performance. All experiments were carried out in a Python environment with Scikit-learn and SciPy libraries on a system with an Intel Core i5-2400 processor (3.10 GHz), 4 GB of RAM, and a 32-bit operating system to test both the latest methods and our new methods.

4.2 Results of Individual Base Classifier

To provide a detailed discussion of individual base classifiers and their performance compared to the ensemble model, we analyze the

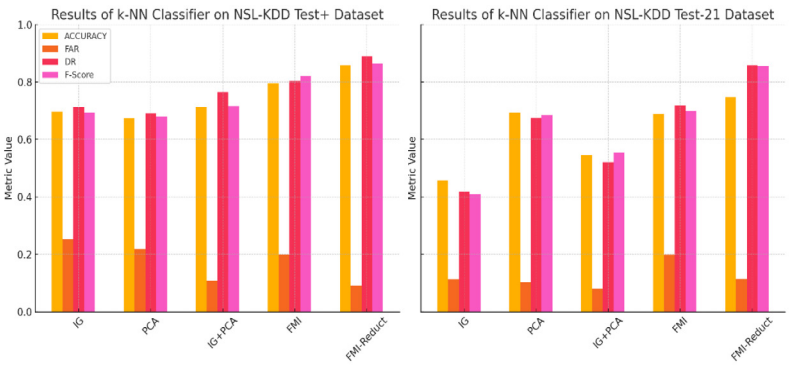

Figure 3

3a). Results of k-NN Classifier on NSL-KDD Test+ Dataset (left panel) and 3b) NSL-KDD Test-21 Dataset (right panel).

results, highlighting the distinct performance characteristics of K-NN, SVM, and DT classifiers and how they compare to the ensemble classifier.

It is obvious from Figures 3a and 3b that the FMI-Reduct approach consistently demonstrates superior detection performance, achieving higher accuracy, detection rates, and F-Scores while maintaining lower false alarm rates. This highlights the efficacy and robustness of the FMI-Reduct methodology for intrusion detection in diverse environments. Despite its simplicity, K-NN's lack of robustness in distinguishing minority attacks limits its overall effectiveness compared to other classifiers.

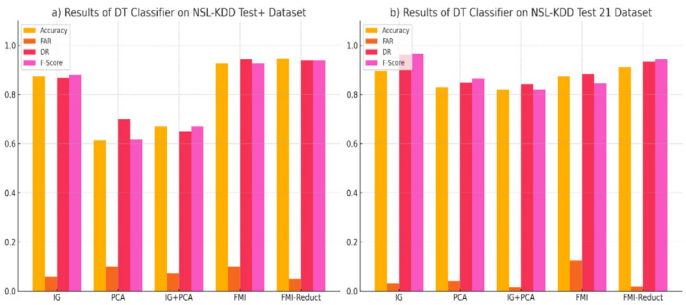

Figure 4

4a). Results of DT Classifier on NSL-KDD Test+ Dataset (left panel) and 4b) NSL-KDD Test-21 Dataset (right panel).

Figures 4a and 4b illustrate that the FMI-Reduct method consistently outperforms others across all key metrics—Accuracy, Detection Rate (DR), False Alarm Rate (FAR), and F-Score—highlighting its superior capability

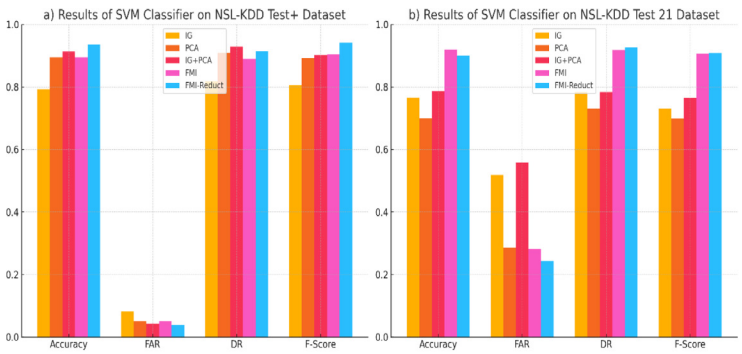

Figure 5

5a). Results of SVM Classifier on NSL-KDD Test+ Dataset (left panel) and 5b) NSL-KDD Test-21 Dataset (right panel).

in reducing feature overlap and enhancing classification performance. Notably, the FMI-Reduct achieves the highest Accuracy and lowest FAR, demonstrating its effectiveness in real-world intrusion detection scenarios. Despite this, DT remains efficient in classifying high-frequency attack types.

The bar diagrams, as shown in Figures 5a and 5b, compare the performance of various feature selection techniques—IG, PCA, IG+PCA, FMI, and FMI-Reduct—on the SVM classifier for NSL-KDD Test+ and Test 21 datasets. FMI-Reduct consistently shows the highest accuracy and F-Score, lowest FAR, and strong detection rate across both datasets, highlighting its effectiveness in improving intrusion detection performance. In addition to the NSL-KDD results, how well each individual model works on the UNSW-NB15 dataset also reveals important insights.

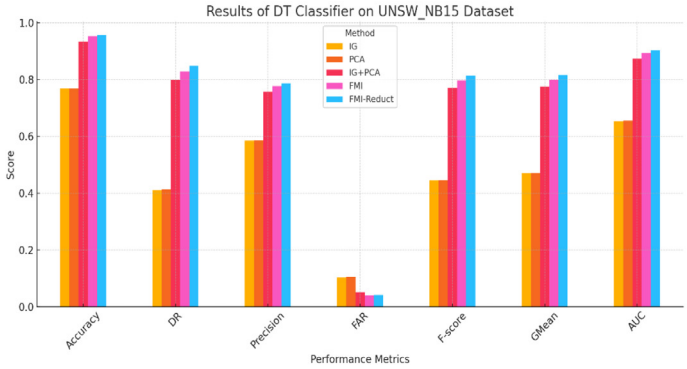

Figure 6

Results of DT Classifier on UNSW_NB15 Dataset

Figure 6 depicts, the bar diagram, that the FMI-Reduct method outperforms other feature selection methods, achieving the highest accuracy, detection rate, and AUC while maintaining a low false alarm rate. FMI also performs well, while IG and PCA deliver lower results across most metrics. This highlights the importance of fuzzy-based methods for improved intrusion detection in smart grids. Nevertheless, the proposed FMI ensemble classifier significantly improves upon the individual classifiers' performance by combining their strengths. The ensemble approach leverages the diversity of base classifiers and their complementary strengths, resulting in a more balanced and accurate detection across all attack types. The ensemble model shows a marked improvement in accuracy, precision, and a reduced false alarm rate, particularly for complex and low frequency attacks like U2R and R2L. By

using a technique called FMI-Reduct feature selection, the ensemble classifier can significantly reduce the amount of data it needs to process without losing important information. This makes the classifier more efficient and accurate.

6. Conclusion and Future Scope

Experimental results on NSL-KDD and UNSW-NB15 demonstrate that FMI-Reduct outperforms traditional feature selection methods such as IG, PCA, and IG+PCA in terms of accuracy, detection rate, precision, and false alarm rate. FMI-Reduct achieves up to 93% accuracy on UNSW-NB15, effectively classifying complex attacks like U2R and R2L while maintaining lower false alarm rates. These improvements are attributed to the fuzzy logic's ability to handle uncertainties and the powerful feature selection achieved by CMI-QRA. Overall, this research highlights that the FMI-Reduct-Based NIDS is critical for securing modern energy infrastructure against evolving cyber-physical threats. For future work, the same feature subset can be tested using deep learning approaches to evaluate comparative results with existing feature selection (optimization techniques). Additionally, real-time implementations on larger, more diverse datasets should be investigated to ensure scalability and adaptability to emerging network attack patterns. Expanding the approach to other domains, such as anomaly detection in IoT networks, would also validate the robustness of the proposed methodology in diversified environments.

References

[1] Y. Li, X. Wei, Y. Li, Z. Dong, and M. Shahidehpour, "Detection of false data injection attacks in smart grid: A secure federated deep learning approach," arXiv preprint arXiv:2209.00778 (2022). [Online]. Available: https://arxiv.org/abs/2209.00778

[2] X. Lin, D. An, F. Cui, and F. Zhang, "False data injection attack in smart grid: Attack model and reinforcement learning-based detection method," *Frontiers in Energy Research*, vol. 10, p. 1104989 (2022).

[3] X. Niu, J. Li, and J. Sun, "Dynamic detection of false data injection attack in smart grid using deep learning," arXiv preprint arXiv:1808.01094 (2018). [Online]. Available: https://arxiv.org/abs/1808.01094

[4] K. Demertzis, L. S. Iliadis, and V.-D. Anezakis, "An innovative soft computing system for smart energy grids cybersecurity," *Advances in Building Energy Research*, vol. 12, no. 1, pp. 3–24 (2018), doi: 10.1080/17512549.2017.1325401.

[5] S. Ahmad and Z. A. Baig, "Fuzzy-based optimization for effective detection of smart grid cyberattacks," *International Journal of Smart Grid and Clean Energy,* vol. 1, no. 1, pp. 15–21 (2012). [Online]. Available: http://www.ijsgce.com/uploadfile/2012/1011/20121011122129685.pdf

[6] J. Wang, Q. Wang, W. Q. Ma, and D. H. Yao, "Fuzzy knowledge representation and reasoning of the smart grid based on medium logic and its application," in Proc. 2nd Int. Conf. Computer Science and Electronics Engineering (ICCSEE), Paris, France, pp. 2786. [Online] (2013). Available: http://www.atlantis-press.com/php/download_paper.php?id=5126

[7] S. Mohagheghi, "Integrity assessment scheme for situational awareness in utility automation systems," *IEEE Transactions on Smart Grid*, vol. 5, pp. 592–601 (2014), doi: 10.1109/TSG.2013.2283260.

[8] M. Tavallaee, E. Bagheri, W. Lu, and A. A. Ghorbani, "A detailed analysis of the KDD CUP 99 data set," in *IEEE Symp. Computational Intelligence for Security and Defense Applications*, pp. 1–6. [Online] (2009). Available: https://ieeexplore.ieee.org/document/5356528

[9] N. Moustafa and J. Slay, "UNSW-NB15: A comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set)," in *MilCIS, IEEE* (2015), doi: 10.1109/MilCIS.2015.7348942.

[10] U. AlHaddad, A. Basuhail, M. Khemakhem, F. E. Eassa, and K. Jambi, "Ensemble model based on hybrid deep learning for intrusion detection in smart grid networks," *Sensors,* vol. 23, no. 17, p. 7464 (2023), doi: 10.3390/s23177464.

[11] F. Zhai, T. Yang, H. Chen, B. He, and S. Li, "Intrusion detection method based on CNN–GRU–FL in a smart grid environment," *Electronics,* vol. 12, no. 5, p. 1164 (2023), doi: 10.3390/electronics12051164.

[12] S. A. Amaouche, A. Guezzaz, S. Benkirane, and M. Azrour, "IDS-XGbFS: A smart intrusion detection system using XGBoost with recent feature selection for VANET safety," *Cluster Computing*, vol. 27, no. 3, pp. 3521–3535 (2024), doi: 10.1007/s10586-023-04157-w.

[13] M. Mohy-eddine, A. Guezzaz, S. Benkirane, and M. Azrour, "An intrusion detection model using election-based feature selection and

K-NN," *Microprocessors and Microsystems*, art. no. 104966 (2023), doi: 10.1016/j.micpro.2023.104966.

[14] M. Mohy-eddine, A. Guezzaz, S. Benkirane, and M. Azrour, "Malicious detection model with artificial neural network in IoT-based smart farming security," *Cluster Computing*, vol. 27, no. 6, pp. 7307–7322 (2024), doi: 10.1007/s10586-024-04334-5.

[15] R. K. Viral and D. Asija, "Advanced machine learning methods for big data analytics used in smart grid," in Big Data Analytics Framework for Smart Grids, 1st ed., R. Viral, D. Asija, and S. Salkuti, Eds. Boca Raton, FL: CRC Press, pp. 79–97 (2023), doi: 10.1201/9781032665399-5.

[16] S. Oyucu, O. Polat, M. Türkoğlu, H. Polat, A. Aksöz, and M. T. Ağdaş, "Ensemble learning framework for DDoS detection in SDN-based SCADA systems," *Sensors,* vol. 24, no. 1, p. 155 (2024), doi: 10.3390/s24010155.

[17] B. R. Said, Z. Sabir, and I. Askerzade, "CNN-BiLSTM: A hybrid deep learning approach for network intrusion detection system in software-defined networking with hybrid feature selection," *IEEE Access*, vol. 11, pp. 138732–138747 (2023), doi: 10.1109/ACCESS.2023.3340142.

[18] Y. Song, N. Luktarhan, Z. Shi, and H. Wu, "TGA: A novel network intrusion detection method based on TCN, BiGRU, and attention mechanism," *Electronics,* vol. 12, no. 13, p. 2849 (2023), doi: 10.3390/electronics12132849.

[19] Y. Imrana, Y. Xiang, L. Ali et al., "CNN-GRU-FF: A double-layer feature fusion-based network intrusion detection system using convolution neural network and gated recurrent units," *Complex Intelligent Systems,* vol. 10, pp. 3353–3370 (2024), doi: 10.1007/s40747-023-01313-y.

[20] S. Meftah, T. Rachidi, and N. Assem, "Network based intrusion detection using the UNSW-NB15 dataset," *International Journal of Computing and Digital Systems,* vol. 8, no. 5, pp. 478–487 (2019).

Received August, 2025