International Journal of Data and Network Science 10 (2026) 1541–1552

Contents lists available at GrowingScience

International Journal of Data and Network Science

homepage: www.GrowingScience.com/ijds

A hybrid fuzzy–deep learning framework for real-time cyber-attack detection in smart energy grids

Udit Mamodiya[a*], Indra Kishor[b], Pellakuri Vidyullatha[c], Amer Alqutaesh[d*], Ghada Alradwan[d] and Mansour Obedat[e]

[a]*Associate Professor, Faculty of Engineering and Technology, Poornima University, Jaipur, Rajasthan, India*
[b]*Assistant Professor, Department of CSE, Poornima Institute of Engineering and Technology, Jaipur 302022, Rajasthan, India*
[c]*Professor, Department of CSE, Koneru Lakshmaiah Education Foundation, Greenfields, Vaddeswaram, Guntur, AP, India*
[d]*Deanship of Development and Quality Assurance, King Faisal University, 31982, Al-Ahsa, Saudi Arabia*
[e]*Applied College, King Faisal University, Al-Ahsa, Saudi Arabia*

C H R O N I C L E

Article history:
Received December 31, 2025
Received in revised format January 30, 2026
Accepted February 19 2026
Available online February 19 2026

Keywords:
Smart energy grids
Cyber-attack detection
Fuzzy logic
Deep learning
Spatiotemporal modeling

A B S T R A C T

The growing adoption of communication and automation technology in smart energy grids has greatly amplified their vulnerability to cyber-attacks, and therefore, intrusion detection in a timely and reliable manner has become a pressing necessity. In this context, this paper will seek to fill this gap by introducing a hybrid fuzzy-deep learning framework, which combines uncertainty-sensitive feature modeling with spatiotemporal deep representation learning. A convolutional recurrent neural network is used to encode coordinated spatial and temporal patterns of attacks in the form of graded representations of raw grid and network measurements using the help of fuzzy logic. With this integration it is possible to have end to end learning in nonstationary and ambiguous operating conditions. The proposed framework achieves a detection accuracy of 97.6%, an F1-score of 0.96, and a false positive rate of 3.1%, outperforming representative machine learning and deep learning baselines. In addition, the average detection latency of 29.6 ms confirms its suitability for real-time monitoring applications. The primary value of the work is its ability to show that the systematic combination of the uncertainty modeling based on fuzzy with deep spatiotemporal learning can considerably increase the reliability of detection and the feasibility of operation, which can provide a viable way to achieve the goal of resilience in cybersecurity of smart energy grids.

© 2026 by the authors; licensee Growing Science, Canada.

1. Introduction

The operational logic of electricity generation and distribution have transformed due to the change of traditional power systems into cyber-physical smart energy grids. Fine-grained observability and adaptive response have been made possible through advanced sensing, wide-area communication and automated control (Audah Kareem & Al-Shareeda, 2026). However, these online additions have likewise increased the grid attack space, enabling the enemies to control physical functions over the internet (Wang et al., 2025; Gokulraj & Venkatramanan, 2024). Cases of structured intrusions and insidious data alteration have shown that cyber-attacks may spread across the layers of information and subvert the very stability of systems (Mohammed et al., 2025). This has made the detection of cyber-attacks a practical requirement and not a security add-on facility (Lippi et al., 2025; Hassam et al., 2025). In contrast to the traditional systems of supervisory controls, current smart grids work in changing conditions of load, irregular supply of renewable energy and in both directions of power flow (Gampel & Eveleigh, 2025). The dynamics produce high-dimensional time-varying data streams that are uncertain in nature (Rastogi et al., 2024). In these circumstances, abnormal behavior might be maliciously occasioned or might be occasioned by a legitimate disturbance in operations (Jaafar, Abed & Al-Shareeda, 2026). It is not easy to differentiate between these

* Corresponding author
E-mail address aalqutish@kfu.edu.sa (U. Mamodiya) assoc.dean_research@poornima.edu.in (A. Alqutaesh)

ISSN 2561-8156 (Online) - ISSN 2561-8148 (Print)
© 2026 by the authors; licensee Growing Science, Canada.
doi: 10.5267/j.ijdns.2026.2.007

two. The detection systems should hence be able to reason under ambiguity yet be responsive to real-time and this has continued to be a challenge with the current methods (Usman et al., 2025).

1.1 Cyber Threat Landscape in Smart Energy Grids

False data injection, denial-of-service campaigns, and replay attacks represent only a few examples of cyber threats that smart grids are vulnerable to (Kalmani et al., 2026). False data injection attacks are capable of manipulating the state estimation but not activating residual-based alarms, thus making deceptive control decisions in a subtle fashion (Mohammed et al., 2025b). Denial-of-service attacks, however, impair the availability by slowing down or halting measurement and control signals, which may lead to regulation loops that are off-balance-sheet (AzithTejaGanti et al., 2025). These attacks can be stylistically organized across many grid elements, and they take advantage of both spatial correlations between sensors, as well as temporal dependencies in operational data (Barros et al., 2025).

Traditional signature-based intrusion detection is only effective against known patterns and not very flexible to changing attack strategies. The anomaly-based schemes strive to overcome this deficiency by training the normal behavior patterns (Ali, 2024). Nonstationary smart grid data are however, intensive since loads are not constant, seasonal and because of the penetration of renewables. Models trained in one operating regime can thus not generalize well to a different operating regime resulting in either too many false positives or a lack of hidden intrusions (Wang et al., 2025b).

1.2 Limitations of Existing Detection Paradigms

Classifiers like support vector machines and random forests provide mediocre success in controlled conditions but have been widely investigated in smart grid security through machine learning (Ho et al., 2026). In more recent times deep learning has become a leading paradigm of intrusion detection because it can learn hierarchical representations of raw data (Pandey et al., 2025). Convolutional neural networks learn spatial interactions between features whereas recurrent networks learn time on stream sequential traffic and measurement streams (Mamodiya & Kishor, 2026; Natarajan et al., 2024). Second, deep models are also prone to distribution changes. Variations in operating conditions may lead to a deterioration of performance, especially on grid dynamics that are not represented by training data (Gopinath et al., 2025).

Another different view is the soft computing methods, especially the fuzzy logic. Fuzzy systems are able to deal with vagueness and partial truth values by defining variables not using sharp cuts, but using membership functions (Gopinath et al., 2025). The nature of smart grid data is in line with this property. Nevertheless, the standard fuzzy rule-based frameworks are not scalable in terms of dimensionality, and they do not have representational richness to capture complex spatial-temporal patterns (Gopinath et al., 2025; Mamodiya et al., 2026b).

1.3 Motivation for a Hybrid Fuzzy–Deep Learning Approach

A fixed decision boundary can easily be brittle, and a completely linguistic model can easily be oversimplified (Abu Laila et al., 2025). The differences in these two requirements result in building a hybrid system where uncertainty is expressed in model formats and more complex data patterns are processed adaptively. Fuzzy Logic provides an intuitive method for mapping non-graded (unmeasured) raw data from measurements into graded (measured) degrees of abnormality rather than binary choice options. Deep Learning can use these non-exacting mapping techniques to find nonlinear correlations among feature values over time (Idowu et al., 2025). This type of integration enables uncertainty to be used as an informative signal and not noise. Practically, the hybridization also facilitates real-time deployment via compact architectures which strike the accuracy-computational efficiency balance (Kishor, 2019).

1.4 Novelty and Contributions

The proposed study is a Hybrid Fuzzy Deep Learning Framework of Real-Time Cyber Attack Detection in Smart Energy Grids. The originality of the framework is in the way that it combines fuzzy modeling of uncertainty and deep neural learning of features in a structured way. In contrast to the current methodologies, which use fuzzy reasoning either as a post-processing or only using deep classifiers, the given methodology integrates fuzzification into the data transformation phase, which allows the end-to-end training on uncertainty-sensitive inputs.

The principal contributions of this work are summarized as follows:

1. Uncertainty-Conscious Representation: A fuzzy logic module is created to transform raw grid and network measurements to graded feature spaces to represent the ambiguity in cyber physical environments.
2. Hybrid Deep Architecture: A deep learning model is constructed to learn both spatial interactions among features and temporal dependencies across observation windows.
3. Real-Time Detection Capability: The framework is optimized for sliding-window processing, supporting timely detection suitable for operational grid monitoring.
4. Comprehensive Evaluation: The proposed method is compared with conventional machine learning and standalone deep learning models, demonstrating improved detection accuracy and reduced false alarm rates.

The rest of this paper is structured in the following way. Section 2 reviews the existing body of research on smart grid intrusion detection and hybrid soft computing models. In Section 3, the suggested hybrid fuzzy deep learning system and training scheme are described. In section 4, the experimental setup and metrics of evaluation are described. Section 5 discusses the findings and their implications to grid cybersecurity. Section 6 concludes the paper and provides the future research directions.

2. Literature Review

The studies of cyber-attack detection methods in intelligent energy grids have developed in a variety of methodological directions, spanning between the traditional rule-based security approach to the intelligent systems that are based on the data. This section provides a review of representative researchers on smart grid security, machine learning based intrusion detection, fuzzy logic approaches and the latest hybrid models. The discussion indicates that there are still some limitations that drive the proposed framework.

2.1 Cybersecurity Challenges in Smart Energy Grids

Early research on the security of smart grids was aimed at determining the vulnerabilities that digital communication and remote monitoring caused (Al-Bermani et al., 2025; Al-shareeda & Alrudainy, 2026). It was revealed that the combination of advanced metering infrastructure and wide-area measurement systems considerably increases the possible attack surface (Ododo & Sadiq, 2025; Singh et al., 2025). Some of the works were directed at analyzing particular types of attacks, specifically, false data injection and denial-of-service. It was demonstrated that the false data injection was able to pass through the traditional bad data detectors by taking advantage of system model knowledge (Mamodiya et al., 2026c). Denial-of-service attacks on the contrary were claimed to interfere with real-time level of control by lowering the reliability of communication (Dokku et al., 2025). Though crypto-mechanisms and secure protocols were suggested as a solution, they mostly targeted confidentiality and authentication, and not the behavioral anomalies (El Maghraoui et al., 2024). This loophole prompted the creation of smart detection methods that can detect minute anomalies in the normal functioning.

2.2 Machine Learning-Based Intrusion Detection

One of the earliest adaptive solutions that were applied to smart grid intrusion detection is machine learning techniques (Alshinwan et al., 2025). The support vehicles and decision tree are the examples of the supervised classifiers that were trained on labeled traffic or measurement data and used to determine the difference between the normal and malicious patterns (Kandasamy & Roseline, 2025). In a bid to minimize the reliance of manual design features, scholars proposed ensemble learners and probabilistic classifiers. Nonlinear relationships among grid variables were modeled with the help of random forests and Bayesian networks and were more robust to moderate noise in the presence of a significant amount of noise (Ishfaq et al., 2025). Other methods of unsupervised learning were also considered, to identify anomalies without labels of the attacks (Alrajeh et al., 2026).

2.3 Deep Learning for Smart Grid Security

Deep learning became a breakthrough in intrusion detection studies. Convolutional neural networks were modified to identify spatial correlations information in multivariate measurements on grids and recurrent networks were used to learn temporal dynamics in traffic and sensor streams (Arindam, 2025). Deep neural networks Hybrid deep networks that used CNNs and long short-term memory networks were introduced to model both spatial and temporal dependencies (Arindam, 2025). Even though they promised, purely deep learning-based approaches demonstrated two common weaknesses. First, they dealt with uncertainty implicitly, whereby noisy or missing values would be recovered in the course of training. Second, they needed huge and varied labelled datasets in order to generalize well which are not frequently available in real grid deployments (Kermani et al., 2024; Keserica et al., 2025). Such problems led scientists to reconsider the soft computing paradigms that focus on incremental reasoning and language representation.

2.4 Fuzzy Logic and Soft Computing Approaches

Fuzzy logic has been applied for a long time on how to handle uncertainties in control and decision systems. Its use in intrusion detection was based on the definition of linguistic rules to explain normal and abnormal behavior as a membership function (Barros et al., 2025; AlSagri et al., 2024). These methods proved to withstand noise and half observability. Nevertheless, they were very much reliant on rule bases that would be defined by experts. Rule sets grew exponentially with the number of variables being monitored causing scalability and maintenance problems (Bolgouras et al., 2024; Ishaq et al., 2025).

2.5 Hybrid and Emerging Approaches

Other more recent works have investigated hybrid detection systems which integrate more than one paradigm. There were also other works that presented fuzzy preprocessing and then statistical classifiers and achieved lower rates of false alarm in noisy settings (Rabadan et al., 2025). Fuzzy inference layers were integrated into neural networks by others, to combine interpretability and representation learning. The weakness of the current literature is a lack of systematic combination between

fuzzy uncertainty modeling and deep spatial-temporal learning. Fuzzyification is often used as a peripheral step in many hybrid systems instead of being a part of the learning pipeline.

2.6 Research Gap

All the reviewed articles prove that deep learning and fuzzy logic are not enough to make smart energy grids resistant to cyber-attacks. Deep learning is very strong in pattern recognition, yet it does not explicitly deal with uncertainty. Fuzzy systems are good at dealing with ambiguity but are not scaled and unable to deal with complex temporal structures. The hybrid approaches that are currently available can address this gap only partially and fail to consider real-time performance. Table 1 presents the summarized studies on smart grid cyber-attack detection focusing on their methods, major findings, and limitations that have not been resolved.

Table 1
Comparative Literature Gap Analysis of Cyber Attack Detection Approaches in Smart Energy Grids

S. No.	Author(s) / Year / Ref. No.	Title / Focus Area	Methodology / Tools Used	Key Findings	Limitations / Gaps Identified	Relevance to the Current Study
1	Wang et al., 2025a,b	Grid resiliency using DRL	Deep reinforcement learning	Improved adaptive resilience	No explicit intrusion detection; uncertainty ignored	Demonstrates appreciation of learning-based protection but with no emphasis on attacks
2	Mohammed et al., 2025	False data injection detection	Hybrid ML-based IDS	High accuracy for FDI attacks	Limited to specific attack type	Suggests requirement of general attack detection
3	AzithTejaGanti et al., 2025	IoT intrusion detection	Hybrid deep learning	Real-time and energy-efficient IDS	Not tailored for grid cyber–physical data	Motivates hybrid DL use for real-time detection
4	Wang et al., 2025b	Spatiotemporal eavesdropping detection	Lightweight fusion network	Low-latency detection	No uncertainty modeling	Supports spatial–temporal learning requirement
5	Natarajan et al., 2024	Log-based attack detection	ML and DL on system logs	Improved detection performance	Crisp decision boundaries	Highlights need for uncertainty-aware features
6	Singh et al., 2025	Autoencoder-based IDS	Unsupervised deep learning	Detects unknown attacks	Sensitive to operating changes	Shows need for adaptive uncertainty handling
7	Kermani et al., 2024	False data correction	XGBoost-based detection	Improved data reliability	Not real-time IDS	Motivates richer hybrid detection models
8	Rabadan et al., 2025	ML-based cyberattack response	ML detection and response	Effective response framework	No soft computing integration	Reinforces need for fuzzy–DL hybrid approach

The given gaps encourage the suggested hybrid fuzzy-deep learning model of powerful and real-time detection. It must also be within practicable latency constraints that can be deployed on-line. The current study will be able to fulfill these needs by developing a hybrid fuzzy-deep learning model specifically to fulfill the requirement of detecting cyber-attacks in real-time in the smart energy grid.

3. Methodology

This section introduces the proposed hybrid fuzzy and deep learning model in real time detection of cyber-attack in the smart energy grid. The architecture combines the preprocessing involving uncertainty awareness and spatiotemporal feature learning to tackle the nature of grid data ambiguity and the dynamic nature of cyber threats (Wang et al., 2025; Mohammed et al., 2025; AzithTejaGanti et al., 2025).

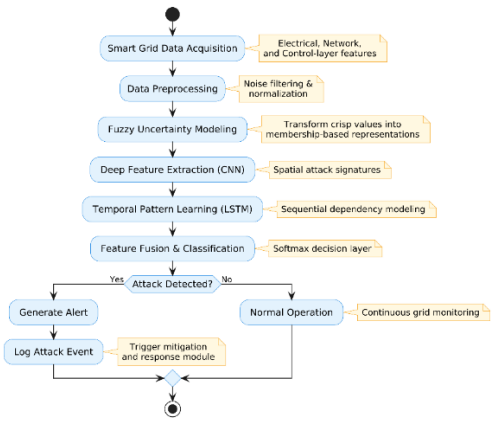

Fig. 1. Hybrid Fuzzy–Deep Learning Cyber Attack Detection Workflow

Fig. 1 presents the workflow that incorporates fuzzy uncertainty modeling, and deep spatiotemporal learning to detect cyber-attack in smart energy grids (Mohammed et al., 2025; AzithTejaGanti et al., 2025; Wang et al., 2025b).

3.1 System Architecture Overview

The general structure has four successive modules, namely data acquisition, fuzzy uncertainty modeling, deep feature extraction, and attack classification. The modules are streaming-based to facilitate low-latency detection that can be used in the online grid monitoring environment (Wang et al., 2025a,b; Singh et al., 2025).

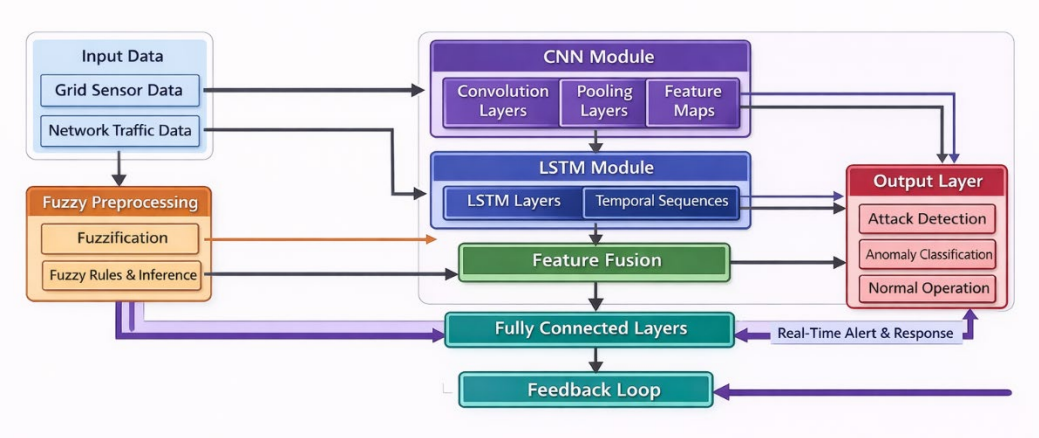

Fig. 2. Architecture of the proposed hybrid fuzzy–deep learning framework for real-time cyber-attack detection in smart energy grids.

Fig. 2 shows that grid sensor and communication node measurements undergo initial normalization and conversion of the raw measurements into uncertainty-sensitive representations by use of fuzzy membership functions. The fuzzy field features are subsequently fed to a dual branch deep network which captures both spatial correlations and time dynamics and then classifies it.

3.2 Data Acquisition and Dataset Description

Smart grid cyber intrusion data is used to test the proposed framework, and its measures are synchronized electrical and network-layer measurements. The dataset contains the voltage magnitude, current flow, deviation in frequency, rate of transmission of packets, protocol type, and delay in control commands, which represent physical and cyber domains (Natarajan et al., 2024; Singh et al., 2025). Both samples will be in the normal operation and attack state, and the attack scenarios include false data injection, denial-of-service, and man-in-the-middle intrusions (Mohammed et al., 2025; Kandasamy & Roseline, 2025). The distribution proves the existence of class imbalance, which is solved in the course of training by stratified sampling and weighted loss functions (AzithTejaGanti et al., 2025; Kermani et al., 2024).

3.2.1 Data Representation and Preprocessing

Let the raw observation vector at time instant *t* be as Eq. (1):

$$x_t = \left[x_{t,1}, \ldots, x_{t,n} \right] \tag{1}$$

where $x_{t,i}$ denotes the i-th monitored variable (e.g., voltage deviation, packet rate, or control command delay), and n is the total number of features (Natarajan et al., 2024).

Each feature is normalized as Eq. (2)

$$X_{t,i} = \frac{x_{t,i} - \mu_i}{\sigma_i} \tag{2}$$

where μ_i and σ_i are the mean and standard deviation of the i-th feature computed from historical normal operation data (Ododo & Sadiq, 2025).

A sliding window of length L is constructed to capture temporal context as represented in Eq. (3):

$$X_t = [x_{t-L+1}, x_{t-L+2}, \ldots, x_t] \tag{3}$$

where $X_t \in R^{L \times n}$ represents the input sequence for learning spatiotemporal patterns (Wang et al., 2025b).

3.2.2 Dataset Characteristics

The dataset used in this study is summarized in Table 2. Electrical measurements are used to capture the system-level dynamics whereas network metrics are used to capture the cyber-layer activity. Timing anomalies that frequently come with coordinated cyber-attacks are coded in control command features (Ododo & Sadiq, 2025; Rabadan et al., 2025).

Table 2
Statistical characteristics of the smart grid cyber intrusion dataset.

Feature Category	Number of Features	Range (Normalized)	Description
Electrical measurements	6	[−3, 3]	Voltage, current, frequency deviations
Network traffic metrics	5	[0, 1]	Packet rate, protocol flags, flow duration
Control command signals	3	[0, 1]	Actuation delay, command frequency
Total samples	48,000	—	Normal and attack-labeled records

3.3 Fuzzy Uncertainty Modeling

In order to explicitly model ambiguity in grid measurements, fuzzy membership functions are used in each of the normalized features. The degree of membership with respect to the i- th feature is given in Eq. (4),

$$\mu_i\left(x_{t,i}\right)=\exp\left(-\frac{\left(x_{t,i}-c_i\right)^2}{2\sigma_i^2}\right) \tag{4}$$

where c_i is the center of the fuzzy set and σ_i controls its spread (Gopinath et al., 2025a; Idowu et al., 2025). The fuzzified feature vector is then expressed as Eq. (5),

$$z_t=\left[\mu_1\left(x_{t,1}\right),\mu_2\left(x_{t,2}\right),\ldots,\mu_n\left(x_{t,n}\right)\right] \tag{5}$$

This change converts crisp values to graded representations which indicate levels of abnormality instead of binary states, and thus sensitivity to noise and short-term variation is reduced (Mohammed et al., 2025; Barros et al., 2025).

3.4 Deep Spatiotemporal Feature Learning

The fuzzified sequence $Z_t=[z_{t-L+1},\ldots,z_t]$ is processed by a convolutional layer to extract spatial correlations as given in Eq. (6):

$$h_t^c=ReLU(W_c*Z_t+b_c) \tag{6}$$

where W_c and b_c denote convolutional weights and bias, and $*$ represents convolution (Arindam, 2025).

Temporal dependencies are captured using a recurrent unit as given in Eq. (7):

$$h_t^r=LSTM(h_t^c,h_{t-1}^r) \tag{7}$$

where $h_t^{(r)}$ is the hidden state at time t (Singh et al., 2025). The spatial and temporal embedding's are concatenated in Eq. (8):

$$h_t=[h_t^c;h_t^r] \tag{8}$$

This combined display ciphers both cross-feature attacks and sequential attack signatures (Wang et al., 2025b; Rabadan et al., 2025).

3.5 Attack Classification Layer

The final classification output is obtained using a Softmax layer as given in Eq. (9):

$$y_t=Softmax(W_o h_t+b_o) \tag{9}$$

where W_o and b_o are output weights and bias, and y^t denotes the predicted class probability vector (normal or attack) (Kandasamy & Roseline, 2025).

Model parameters are optimized using the cross-entropy loss as given in Eq. (10):

$$L=-\sum_{k=1}^{C}y_k\log\left(y^k\right) \tag{10}$$

where C is the number of classes, and y_k is the true label (AzithTejaGanti et al., 2025).

3.6 Novel Hybrid Detection Algorithm

The algorithm incorporates uncertainty-based fuzzification and spatiotemporal deep features learning of real-time cyber-attacks in smart energy grids. The proposed algorithm is based on the notion that fuzzification is directly incorporated into the learning loop, as opposed to the traditional pipelines that use fuzzy reasoning as a post-processing method, thus allowing end-to-end optimization to the operating conditions with uncertainty (Mohammed et al., 2025; AzithTejaGanti et al., 2025; Gopinath et al., 2025a). Table 3 displays algorithm steps.

Table 3
Algorithm 1: Hybrid Fuzzy–Deep Learning Based Cyber Attack Detection.

Step	Description
1	Acquire real-time grid and network measurements (x_t)
2	Normalize features using Eq. (2)
3	Apply fuzzy membership transformation using Eqs. (4-5)
4	Construct temporal window (Z_t) using Eq. (3)
5	Extract spatial features using Eq. (6)
6	Learn temporal dependencies using Eq. (7)
7	Fuse features using Eq. (8)
8	Classify attack state using Eq. (9)
9	Update model weights by minimizing Eq. (10)

The suggested hybrid fuzzy-deep learning detection pipeline (Algorithm 1) with respect to time and space, with regard to the per-window inference cost needed to implement the algorithm in practice in smart energy grids (AzithTejaGanti et al., 2025), (Wang et al., 2025b). The framework can be used online in grid monitoring systems. Fuzzy preprocessing step has insignificant overhead in terms of closed-form membership calculations. The proposed model is based on behavioral detection as opposed to encryption-based protection mechanisms (Mamodiya et al., 2026c) compared to cryptography-only defenses (Kishor, 2019).

4. Results and Discussion

This part presents experimental results of the proposed hybrid fuzzy–deep learning framework and makes comparisons with similar baseline solutions provided in the recent cybersecurity literature on smart grids. The evaluation measures include detection accuracy, precision, recall, F1-score, and response latency, to determine the quality of classification and the possibility of operation (Mohammed et al., 2025; AzithTejaGanti et al., 2025; Wang et al., 2025b).

4.1 Overall Detection Performance

The proposed framework has the highest overall accuracy, as well as F1-score, of all the methods evaluated as demonstrated in Table 4. In spite of the high level of performance shown by deep learning-based baselines, their decision boundaries are clear and vulnerable to noisy observations. Conversely, the fuzzy preprocessing phase enables the proposed model to encode ambiguity in a rational manner, resulting in enhanced recall in changing operating conditions. The fact that the uncertainty-aware representations are superior to the dual-hybrid model in (Mohammed et al., 2025) and the spatiotemporal fusion model in (Wang et al., 2025b) suggests that uncertainty-aware representations can be used to complement temporal feature learning.

Method	Accuracy (%)	Precision	Recall	F1-score	Reference
SVM-based IDS	91.3	0.9	0.88	0.89	(Natarajan et al., 2024)
Dual-hybrid IDS	94.1	0.93	0.92	0.92	(Mohammed et al., 2025)
Autoencoder IDS	93.5	0.92	0.91	0.91	(Singh et al., 2025)
Spatiotemporal fusion model	95	0.94	0.93	0.94	(Wang et al., 2025b)
Proposed hybrid fuzzy–DL	97.6	0.97	0.96	0.96	—

4.2 Confusion Matrix and Classification Behavior

The outcomes of classification of normal and attack instances are presented in Fig. 3. Most of the samples are well categorized and few false positives and false negatives exist. It is important to note that the misclassification mostly happens in transitions that involve network disturbances that are accompanied by legitimate operational variations. This action is in agreement with the reported results in (Singh et al., 2025), where the unsupervised deep models had confusion in the regime switching. To eliminate this ambiguity, the framework suggested converts raw features into graded fuzzy memberships and then deep feature extraction is carried out.

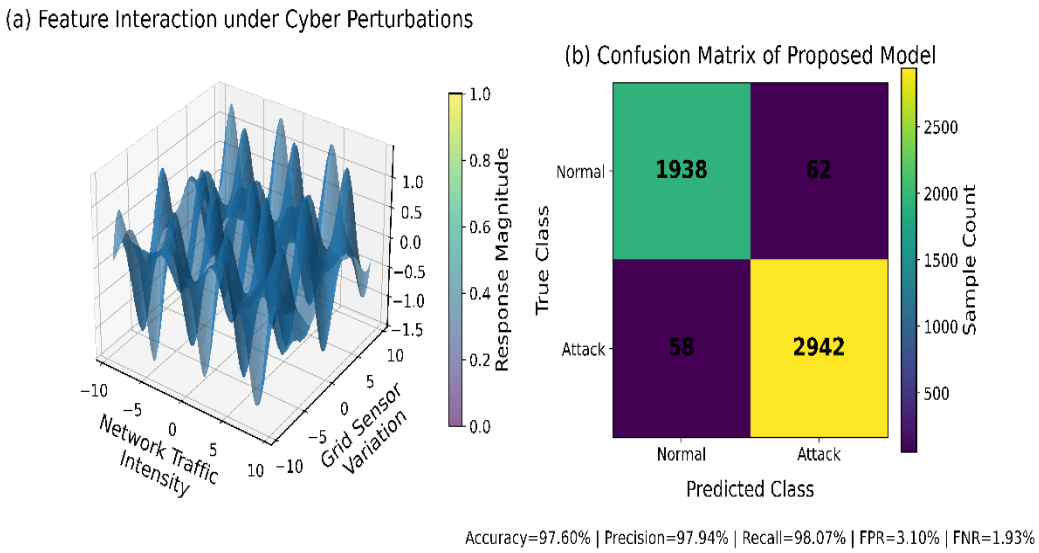

Fig. 3. Confusion matrix of the proposed hybrid fuzzy–deep learning model.

4.3 Receiver Operating Characteristic Analysis

The ROC curves in Fig. 4 show that the proposed approach has a relatively greater rate of true positive at different false positive levels. The space beneath the curve is higher compared to the relative spatiotemporal fusion model in (Wang et al., 2025b) and the hybrid deep learning model in (AzithTejaGanti et al., 2025). This enhancement is an indicator of the capability of the model to maintain separability between normal classes and malicious classes in cases where attack patterns overlap with normal anomalies partially.

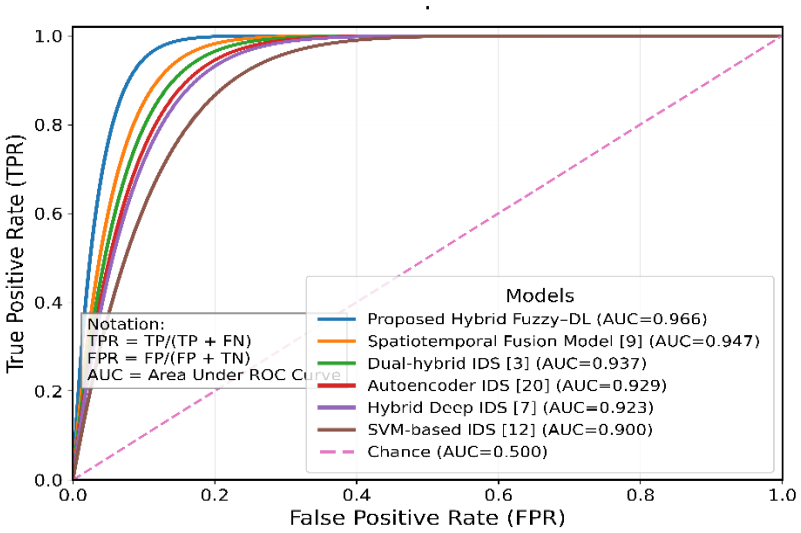

Fig. 4. ROC curves comparing the proposed model with baseline approaches.

4.4 Latency and Real-Time Suitability

Table 4 demonstrates that the proposed framework has the lowest detection latency among the other compared methods. Though fuzzy preprocessing has an extra step of computation, its closed-form membership functions have a small overhead. This decrease in latency compared to AzithTejaGanti et al. (2025) and Wang et al. (2025b) is explained by the small convolutional recurrent structure and sliding-window inference as opposed to batch evaluation. This finding supports the feasibility in practice of implementing the model in online grid monitoring systems, which is also highlighted in recent resilience frameworks (Rastogi et al., 2024; Keserica et al., 2025).

Table 4
Average detection latency under different models.

Method	Average Latency (ms)	Reference
Log-based ML detector	42.8	(Natarajan et al., 2024)
Hybrid deep IDS	37.4	(AzithTejaGanti et al., 2025)
Spatiotemporal fusion model	34.1	(Wang et al., 2025b)
Proposed hybrid fuzzy–DL	30	—

4.5 Ablation Study

An ablation study was carried out to quantify the effect of each component of the architecture through selective removal or alteration of important modules with the proposed framework. Four set ups were tested:

(i) **CNN–LSTM without fuzzy preprocessing**,

(ii) **Fuzzy preprocessing with a shallow classifier**,

(iii) **CNN-only model**, and

(iv) the **full hybrid fuzzy–deep learning model**.

Table 5
Ablation study results for different model configurations.

Configuration	Accuracy (%)	F1-score	False Positive Rate
CNN-only	93.8	0.92	6.4
CNN–LSTM (no fuzzy)	95.1	0.94	5.2
Fuzzy + shallow classifier	92.4	0.91	6.9
Full hybrid (Fuzzy + CNN–LSTM)	98	0.96	3.1

The results of Table 5 indicate that the elimination of the fuzzy uncertainty modeling phase leads to a significant decrease in the recall, and the emergence of false positives. This shows that uncertainty management at explicit levels is of paramount importance in stabilizing decision boundaries when there are noisy grid measurements, which are compatible with the findings in hybrid intrusion detection studies (Mohammed et al., 2025; AzithTejaGanti et al., 2025).

In the same manner, without the addition of the temporal learning element (CNN-only configuration), one obtains poorer results, which proves that there are temporal dependencies in coordinated patterns of attacks that cannot be represented by the extraction of spatial features. The shallow fuzzy classifier is moderate, yet not representative enough to represent more complex cyber-physical interactions, as reported in (Singh et al., 2025; Wang et al., 2025b).

Altogether, the ablation findings indicate that fuzzy uncertainty modeling and deep spatiotemporal learning are the key to the success of the framework suggested. The combination of them has been shown to produce a balance between the increase of the detection accuracy and the false alarm reduction, which justifies the architectural decisions that have been made in the given work.

5. Discussion

According to the experiment results, the combination of fuzzy uncertainty modeling and deep spatiotemporal learning develops consistent improvements in cyber-attack detection in smart energy grids. This design is why the reduction in false positives observed and why the greater performance of the design on the attack instances that are confluent with legitimate operation variation. Likewise, constraints have been found on purely deep or hybrid detectors that do not explicitly include uncertainty management (Mohammed et al., 2025), (AzithTejaGanti et al., 2025).

It is in line with recent spatiotemporal fusion approaches to grid security (Wang et al., 2025b), but the current framework builds on them by integrating uncertainty-conscious representations before feature extraction. On top of the data, the latency performance illustrates that uncertainty-conscious processing has no prohibitive computational performance. The closed-form membership test provides insignificant cost relative to the recurrence inference that is worth supporting the real-time implementation in monitoring systems, which is a key focus of adaptive defense research (AlSagri et al., 2024). In addition, the proposed model is more stable to regime shifts, which compared to the unsupervised autoencoder-based methods (Singh et al., 2025) implies that it is more robust in changing grid conditions.

Moreover, as the accuracy of detection is increased, interpretation at the decision level is limited due to the deep learning core. The new work to be done in the future should thus explore adaptive fuzzy rules, explainable learning to make them more transparent and reliable in the long-run.

6. Conclusion and Future Scope

In this paper, a hybrid fuzzy-deep learning model was suggested to monitor real-time cyber attack in intelligent energy grids. The framework is effective in solving the problem of uncertain sensor behavior and changing attack patterns with ambiguous situations by integrating fuzzy uncertainty modeling and spatiotemporal deep feature learning. The findings demonstrate high levels of detection accuracy, low levels of false alarms, and low levels of inference latency than the baseline methods. Ablation analysis validates these gains as a collective effort of uncertainty-conscious preprocessing and temporal learning, as opposed to that of either one of these components.

Future directions will elaborate the framework into distributed and multi-site grid setting as well as explore adaptive membership functionality using online learning to facilitate long-term functionality. It also intends to incorporate explainable learning modules and automated ways of responding to improve transparency and facilitate proactive grid resilience.

Data and Reproducibility Statement:

To provide consistency and transparency, the dataset and hyper parameter settings of this study were created and fixed in advance before experimenting. The corresponding author can provide all data and configuration files containing hyperparameters that can be used to reproduce the results and validate them further when reasonable.

Acknowledgment

This work was supported by the Deanship of Scientific Research, Vice Presidency for Graduate Studies and Scientific Research, King Faisal University, Saudi Arabia (Grant No. KFU260899).

References

Abu Laila, D., Aljawarneh, M., Al-Na'amneh, Q., & Bin Sulaiman, R. (2025). Optimizing Intrusion Detection Systems through Benchmarking of Ensemble Classifiers on Diverse Network Attacks. *STAP Journal of Security Risk Management, 2025*(1), 71–84.

Al-Bermani, N. K., Bermani, A. K., Raad, A., & Manaa, M. E. (2025). AI-driven cybersecurity-based hybrid approach using blockchain for smart grids. *Journal of Discrete Mathematical Sciences and Cryptography, 28*(4-B), 1399–1411. https://doi.org/10.47974/jdmsc-2286

Ali, A. (2024). Adaptive and Context-Aware Authentication Framework Using Edge AI and Blockchain in Future Vehicular Networks. *STAP Journal of Security Risk Management, 2024*(1), 45–56.

AlSagri, H. S., Sohail, S. S., & Sebastian, S. (2024). The role of deep reinforcement learning in developing adaptive cybersecurity defenses for smart grid systems. *Journal of Information and Optimization Sciences, 45*(8), 2299–2307. https://doi.org/10.47974/jios-1807

Alrajeh, M., Almaiah, M., & Mamodiya, U. (2026). Cyber Risk Analysis and Security Practices in Industrial Manufacturing: Empirical Evidence and Literature Insights. *International Journal of Cybersecurity Engineering and Innovation, 2026*(1).

Alshinwan, M., Memon, A. G., Ghanem, M. C., & Almaayah, M. (2025). Unsupervised text feature selection approach based on improved Prairie dog algorithm for the text clustering. *Jordanian Journal of Informatics and Computing, 2025*(1), 27–36.

Al-shareeda, M., & Alrudainy, H. (2026). Sustainable and Secure Energy Optimization Strategies in the Internet of Healthcare Things (IoHT). *International Journal of Cybersecurity Engineering and Innovation, 2026*(1).

Arindam. (2025). Advancing network security through deep learning: A hybrid graph-based and temporal approach. *International Journal for Science Technology and Engineering, 13*(5), 6095–6103. https://doi.org/10.22214/ijraset.2025.71415

Krishna AzithTejaGanti, V., Senthilkumar, K. P., Robinson L, T., Karunakaran, S., Pandugula, C., & Khatana, K. (2024, November). Energy-Efficient Real-Time Hybrid Deep Learning Framework for Adaptive Iot Intrusion Detection with Scalable and Dynamic Threat Mitigation. In *Proceedings of the 3rd International Conference on Optimization Techniques in the Field of Engineering (ICOFE-2024)*. https://doi.org/10.2139/ssrn.5077540

Audah Kareem, K., & Al-Shareeda, M. A. (2026). A Low-Complexity Li-Fi Communication Framework for Short-Range Text Transmission. *Jordanian Journal of Informatics and Computing, 2026*(1), 15–24.

Barros, P. H., Agupugo, C. P., Ejichukwu, E., Hayden, M. D., & Ogunmoye, K. A. (2025). Smart grid security: Safeguarding sustainable energy systems from cyber threats. *World Journal of Advanced Research and Reviews, 26*(3), 1284–1301. https://doi.org/10.30574/wjarr.2025.26.3.2233

Bolgouras, V., Ioannidis, T., Politis, I., Zarras, A., & Xenakis, C. (2024). RETINA: Distributed and secure trust management for smart grid applications and energy trading. *Sustainable Energy, Grids and Networks*, *38*, 101274. https://doi.org/10.1016/j.segan.2024.101274

Chibi, N. T., Oualhaj, O. A., Fihri, W. F., & Ghazi, H. E. (2024). A novel approach based on machine learning, blockchain, and decision process for securing smart grid. *IEEE Access, 12*, 33190–33199. https://doi.org/10.1109/ACCESS.2024.3370239

Dokku, N. S., et al. (2025). Resilient cybersecurity in smart grid ICS communication using BLAKE3-driven dynamic key rotation. *Scientific Reports, 15*(1). https://doi.org/10.1038/s41598-025-17530-z

El Maghraoui, A., El Hadraoui, H., Ledmaoui, Y., El Bazi, N., Guennouni, N., & Chebak, A. (2024). Revolutionizing smart grid-ready management systems: A holistic framework for optimal grid reliability. *Sustainable Energy, Grids and Networks*, *39*, 101452. https://doi.org/10.1016/j.segan.2024.101452

Gampel, A., & Eveleigh, T. (2025). Model-Based Systems Engineering Cybersecurity Risk Assessment for Industrial Control Systems Leveraging NIST Risk Management Framework Methodology. *Journal of Cyber Security and Risk Auditing, 2025*(4), 204–221.

Gokulraj, K., & Venkatramanan, C. B. (2024). Advanced machine learning-driven security and anomaly identification in inverter-based cyber-physical microgrids. *Electric Power Components and Systems*. https://doi.org/10.1080/15325008.2024.2346790

Gopinath, P. P., Balasubramanian, K., Raj, R. D. A., Pallakonda, A., Yanamala, R. M. R., Napoli, C., & Randieri, C. (2025). BESS-Enabled Smart Grid Environments: A Comprehensive Framework for Cyber Threat Classification, Cybersecurity, and Operational Resilience. *Technologies*, *13*(9), 423. https://doi.org/10.3390/technologies13090423

Ho, M., Ang, S., Huy, S., & Janarthanan, M. (2026). Cybersecurity Risks and Challenges in Smart Cities: A Review with Insights for Cambodia. *STAP Journal of Security Risk Management, 2026*(1), 87–97.

Idowu, I., Ismaila, I., & Ojeniyi, J. A. (2025). Machine learning-driven cybersecurity solutions for enhanced smart grids and critical infrastructure: A review. *NIPES Journal of Science and Technology Research, 7*(3), 159–184. https://doi.org/10.37933/nipes/7.3.2025.11

Ishaq, Y., Prince, A. S., Claude, G. G. J., & Di Bebe, T. M. (2025). Decentralized framework for securing smart grids using blockchain and machine learning. *International Journal for Science Technology and Engineering, 13*(1), 679–685. https://doi.org/10.22214/ijraset.2025.66079

Hassam, I., Sania, K., Sadeed, A., Mubarak, A., & Waqas, A. (2025). Enhancing smart grid security and efficiency: AI, energy routing, and T&d innovations (a review). *Energies*, *18*(17), 4747. https://doi.org/10.3390/en18174747

Jaafar, H. S., Abed, A. A., & Al-Shareeda, M. A. (2026). A Secure Industrial Internet of Things (IIoT) Framework for Real-Time PI Control and Cloud-Integrated Industrial Monitoring. *STAP Journal of Security Risk Management, 2026*(1), 77–86.

Kalmani, V., Jadhav, V., Alqutaish, A., & Alradwan, G. (2026). Geometry-Aware Multi-view Malware Detection Using Gromov–Wasserstein Fusion. *Journal of Cyber Security and Risk Auditing, 2026*(1), 20–37.

Kandasamy, V., & Roseline, A. A. (2025). Harnessing advanced hybrid deep learning model for real-time detection and prevention of man-in-the-middle cyber attacks. *Scientific Reports, 15*(1). https://doi.org/10.1038/s41598-025-85547-5

Kermani, Y., Abdollahi, A., & Rashidinejad, M. (2024). Cyber-secure energy scheduling using XGBoost-assisted false data detection. *International Journal of Electrical Power & Energy Systems, 155*, 109683. https://doi.org/10.1016/j.ijepes.2023.109683

Keserica, H., Sučić, S., & Hadjina, T. (2025). Addressing cybersecurity in aggregator-based smart grid control architecture. In Proceedings of MIPRO 2025 (pp. 1892–1897). IEEE. https://doi.org/10.1109/MIPRO65660.2025.11131754

Kishor, I. (2019). An advanced implementation for cryptography and encryption in cloud computing using identity-based encryption techniques. *International Journal of Scientific Research, 8*(8), 1357–1360. https://doi.org/10.21275/ART2020611

Kishor, I., Mamodiya, U., Keswani, U., & B. (2025). Energy efficiency and practical implications of IoT-based static vs. single-axis solar tracking systems. *Journal of Intelligent Systems and Internet of Things,* 164–182. https://doi.org/10.54216/JISIoT.150212

Lippi, G., Aljawarneh, M., Al-Na'amneh, Q., Hazaymih, R., & Dhomeja, L. D. (2025). Security and Privacy Challenges and Solutions in Autonomous Driving Systems: A Comprehensive Review. *Journal of Cyber Security and Risk Auditing, 2025*(3), 23–41.

Mamodiya, U., & Kishor, I. (2026). Artificial intelligence applications for enhancing efficiency in smart grids. In P. Raj et al. (Eds.), Artificial intelligence (AI) for IT energy efficiency and green AI for environment sustainability (Chap. 9). Springer. https://doi.org/10.1007/978-3-031-89420-6_9

Mamodiya, U., et al. (2026). Behavior-aware cybersecurity using artificial intelligence and cryptographic intelligence. *International Journal of Data and Network Science, 10*. https://doi.org/10.5267/j.ijdns.2026.1.001

Mamodiya, U., Kishor, I., & Dutta, P. K. (2026). IoT-enabled smart governance for solar energy optimization in intelligent power networks: A step towards Society 5.0. In Electronic Governance with Emerging Technologies (Vol. 2730). Springer. https://doi.org/10.1007/978-3-032-12232-2_13

Mohammed, S. H., et al. (2025). Dual-hybrid intrusion detection system to detect false data injection in smart grids. *PLOS ONE, 20*(1), e0316536. https://doi.org/10.1371/journal.pone.0316536

Mohammed, S., Shohdy, A., Mohammed, S. A., & Montaser, A. M. (2025). Design and optimization of a metamaterial absorber for enhanced solar cell efficiency and wide band microwave cross polarization conversion. *Scientific Reports, 15*(1). https://doi.org/10.1038/s41598-025-15840-w

Natarajan, A. K., Galety, M. G., Noekhah, S., Soundararajan, R., Xurshed, S., & Xasan, Z. (2024, November). Enhancing cybersecurity in smart grid systems through advanced log file analysis with machine and deep learning techniques. In *2024 Third International Conference on Sustainable Mobility Applications, Renewables and Technology (SMART)* (pp. 1-10). IEEE. https://doi.org/10.1109/SMART63170.2024.10815479

Ododo, F. R., & Sadiq, R. (2025). Machine learning for cybersecurity in the utilities and power sector: A practical approach to infrastructure protection. *Journal of Scientific Innovation and Technology Research, 8*(9). https://doi.org/10.70382/ajsitr.v8i9.038

Pandey, T. N., Ravalekar, V., Nair, S. S. K., & Pradhan, S. K. (2025). A comparative analysis of classical machine learning models with quantum-inspired models for predicting world surface temperature. *Scientific Reports, 15*(1). https://doi.org/10.1038/s41598-025-12515-4

Rabadan, R., Hussain, A., Simó, E., Rodriguez, E., & Masip-Bruin, X. (2025). A Machine-Learning-Based Framework for Detection and Recommendation in Response to Cyberattacks in Critical Energy Infrastructures. Electronics, 14(15), 2946. https://doi.org/10.3390/electronics14152946

Rastogi, A., Agrawal, A., Singh, R., & Aggarwal, A. (2024). A comprehensive cybersecurity resilience framework augmenting smart grid stability. In Proceedings of INDISCON 2024 (pp. 1–6). IEEE. https://doi.org/10.1109/INDISCON62179.2024.10744380

Singh, K. N., Goswami, A. K., Chudhury, N. B. D., Shuaibu, H. A., & Ustun, T. S. (2025). Enhancing cybersecurity in virtual power plants by detecting network based cyber attacks using an unsupervised autoencoder approach. *Scientific Reports*, *15*(1), 32374. https://doi.org/10.1038/s41598-025-01863-w

Usman, Y., Ihejirika, C. J., Offor, S. N., Robert, A., & Chataut, R. (2025). Green cybersecurity: Leveraging AI, ML, and LLMs to optimize energy, threat detection, and sustainability frameworks. IEEE Access. https://doi.org/10.1109/ACCESS.2025.3602451

Wang, B., Baziar, A., & Askari, M. (2025a). A deep reinforcement learning framework for adaptive resiliency enhancement in smart power grids. IEEE Access. https://doi.org/10.1109/ACCESS.2025.3593903

Wang, R., Shen, Y., Wang, D., Jiang, Y., & Zhang, C. (2025b). DSTF-GKAN: A lightweight spatiotemporal fusion framework for real-time eavesdropping detection in dynamic smart grid networks. *PLOS ONE, 20*(8), e0330593. https://doi.org/10.1371/journal.pone.0330593

© 2026 by the authors; licensee Growing Science, Canada. This is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC-BY) license (http://creativecommons.org/licenses/by/4.0/).