Contents lists available at GrowingScience

International Journal of Data and Network Science

homepage: www.GrowingScience.com/ijds

An AI-driven cybersecurity framework for smart solar energy systems intrusion detection and adaptive threat mitigation

Udit Mamodiya[a*], Indra Kishor[b], Hastimal Jangid[c], Amer Alqutaesh[d*], Hussein N. E. Edrees[d] and Ghada Alradwan[d]

[a]*Associate Professor, Faculty of Engineering and Technology, Poornima University, Jaipur 303905, Rajasthan, India*
[b]*Assistant Prof. , Dept. of CSE, Poornima Institute of Engineering and Technology, Jaipur 302022, Rajasthan, India*
[c]*Independent Researcher, Coozmoo Digital Solutions, Houston, TX, USA*
[d]*Deanship of Development and Quality Assurance, King Faisal University, 31982, Al-Ahsa, Saudi Arabia*

C H R O N I C L E

Article history:
Received March 2, 2026
Received in revised format March 24, 2026
Accepted May 5 2026
Available online
May 5 2026

Keywords:
Cyber-Physical Security
Smart Solar Energy Systems
Intrusion Detection System
Reinforcement Learning
Adaptive Threat Mitigation

A B S T R A C T

The rise of Internet of Things (IoT) technologies in smart solar energy systems has presented a serious cybersecurity issue, especially with the close interdependence between cyber infrastructure and physical functions. Traditional intrusion detection systems (IDS) are mainly based on the network level of abnormalities and do not consider the system level effects leading to poor mitigation. In this paper, we suggest an AI-based cyber-physical cybersecurity architecture, which combines an intrusion detection model in the form of CNNLSTM and a mitigation mechanism based on reinforcement learning. A decision fusion layer is added to integrate cyber threats scores with photovoltaic system conditions to respond in context. Experimental analysis on real-world data sets indicates that the framework proposed has a 98.3% detection rate, 0.97 F1-score, and a lower false positive of 0.02, which performs better than the current approaches by up to 2.1% accuracy. The framework enhances energy stability at the system level up to 96.8% and recovery time is shortened by about 58 percent when the system is under attack. Moreover, the model has a strong performance of more than 96% accuracy even when there is a high attack intensity situation. These results highlight the value of cyber intelligence and integration of physical system awareness. The proposed framework is holistic and realistic to provide a guarantee of the safety of smart solar energy systems to ensure not only high detection but also stability of the operations in real-life scenarios.

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

1. Introduction

The rapid evolution of smart solar energy systems has created the opportunity of the universal use of Internet of Things (IoT) technologies, which enables real-time monitoring, predictive maintenance, and smart management of the energy flows into the modern photovoltaic systems. These are the cyber-physical systems, where physical processes, such as production of solar energy are tightly intertwined with the digital communication networks and control algorithms. Although this integration greatly contributes to operational efficiency and scalability, it is also known to put solar energy systems in a broad range of cybersecurity risks. The attacks against communication channels, sensor data, or control units can cause the system to lose its stability, reduce its energy production, or even cause massive distributed energy network failures (Paul et al., 2024; Vidyullatha et al., 2026). With the growing integration of solar installations into smart grids and integrated energy systems, their cybersecurity has become a topical research question.

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

ISSN 2561-8156 (Online) - ISSN 2561-8148 (Print)
© 2026 by the authors; licensee Growing Science, Canada.
doi: 10.5267/j.ijdns.2026.5.004

The main issue is that smart solar systems are susceptible to advanced cyber-attacks that can take advantage of both network level and system level vulnerabilities. Compared to traditional IT infrastructures, solar IoT infrastructures entail resource-limited devices, non-uniform communication protocols, and real-time operational constraints, which makes them especially vulnerable to attacks like distributed denial-of-service (DDoS), data falsification, man-in-the-middle attacks, and data modification (Manimaran & Ranganathan, 2025; Gantla et al., 2025). Such attacks have the ability to alter sensor measurements, control signal distortion or even overload communication systems and eventually influence energy production and system stability. Further, the dynamism of environmental conditions including the variation of solar irradiance and temperature also adds more complexity to the ability to discriminate between natural system variations and malicious anomalies (Islam et al., 2025). This interconnection between the cyber and physical realm makes the conventional security systems inadequate to offer sufficient protection.

Although a lot of research has been conducted in intrusion detection systems (IDS), the issue has not been well tackled in relation to smart solar energy systems. Current methods are mainly based on machine learning and deep learning models, such as Support Vector Machines (SVM), Random Forest (RF), Long Short-Term Memory (LSTM) networks and Convolutional Neural Networks (CNN) to categorize network traffic as either normal or malicious (Agarwal & Bhattacherjee, 2025; Ni et al., 2025). Although the models have shown encouraging results when used on conventional network intrusion data, they have serious shortcomings when used in cyber-physical energy networks. To begin with, the majority of IDS architectures can only work at the network level, without taking into account the effects of cyber-attacks on the physical system operation and energy efficiency (Keswani et al., 2025). Due to this, they cannot model the interdependencies between the cyber anomalies and the dynamics of the photovoltaic systems. Second, the traditional models of IDS are mainly used in a static detection mode and do not have the ability to respond, dynamically, to the changing threats in real time (Alsirhani et al., 2025). This is especially limiting to solar energy systems, where a failure in response can cause a cascading failure.

Moreover, much of the current literature tests IDS models on isolated benchmark datasets in controlled settings, which have no relation to the complexity of the real-world operation of a solar IoT setting (Mamodiya et al., 2026). No system-level evaluation metrics, e.g. energy stability, recovery time, and operational resilience, further restrict the applicability of these approaches in the real world. Moreover, intrusion detection is a task that most models consider independently, without considering it as a part of a larger decision-making process that can also inform mitigation strategies (Mukabbir, 2023). As a result, the performance of the security system is compromised even in cases when the attacks are properly detected due to the absence of an intelligent response mechanism.

The suggested solution is an extension of the conventional IDS models in that it uses a multi-layer architecture that integrates the deep learning-based anomaly detection and the reinforcement learning-based decision-making. The intrusion detection module uses data-driven models to detect intricate attack patterns in network traffic, making it very accurate in detecting threats in various contexts. In contrast to traditional classifiers, the offered system is created in such a way that it is able to capture both time-related dependencies and contextual dependencies, enhancing the capacity of the system to differentiate normal operational variations and malicious activities (Sinha et al., 2025; Mohamed et al., 2023).

One of the main contributions of this work is the incorporation of a reinforcement learning (RL) agent in the adaptive threat mitigation. The RL module represents the security problem as a sequence of decisions in which the system learns the best response strategies, depending on the current conditions and feedback in real-time. This is because by constantly engaging with the environment, the agent will be able to dynamically modify mitigation measures, which may include traffic filtering, node isolation, or reconfiguring the communication, to reduce the effects of cyber-attacks and still keep the system running (Almaayah et al., 2025; Afrin et al., 2026). This adaptability capability can help to overcome a key weakness of current techniques in IDS, which in most cases lack automated response and instead are implemented based on pre-established rules or human intervention (Koroma et al., 2025).

The framework proposed has the ability to integrate cyber-physically with a single decision fusion layer; outputs of the intrusion detection module are fused with the state of the solar system operations. The design also allows making decisions based on the context of the situation, which means that the system will not only determine whether an attack is being carried out, but also whether it will influence the generation of energy and the operation of the system or not. The framework can also ensure that mitigation strategies are prioritized to maintain security and operational efficiency by integrating physical system awareness in the cybersecurity process (Vijayaraj et al., 2025). Such a strategy is a huge improvement compared to the traditional practices that consider cyber and physical space as separate worlds (Ashfin, 2023).

Overall, the problem of securing smart solar energy systems is urgent in this paper, which is why the author thinks about introducing a comprehensive AI-based system that will be able to help close the gap in the intrusion detection and adaptive response. The framework does not only enhance the performance of the detection, but also ensures that the security interventions are aligned to the working requirements of the photovoltaic systems, which is a scalable and viable solution to the next-generation smart energy infrastructures (Singh et al., 2025; Debnath, 2025).

The remainder of this paper was structured in the following way. In section II, a literature review of the work involved in the area of intrusion detection systems and cybersecurity in cyber-physical and smart energy systems is provided. Part III presents the proposed methodology which is composed of an AI-based intrusion detection system and adaptive mitigation strategy

that is implemented on reinforcement learning. In Section IV, the description of the experimental setup is presented, including description of datasets, basis models, evaluation measures and implementation details. In section V, the results of the experiment and their comparison and statistical validation are provided and discussed. Finally, Section VI concludes the paper and presents the directions of research.

2. Literature Review

2.1 Intrusion Detection Systems in Cyber-Physical Systems

The introduction of cyber-physical systems (CPS) has seen lots of transformation in intrusion detection systems (IDS) in which physical infrastructures are closely combined with computational processes. CPS systems such as smart grids, renewable energy systems, and so on, IDS must not only look at network-level anomalies, but also at physical system behaviour. Conventional IDS architectures, initially developed to combat enterprise IT networks, mainly operate at the packet-level and use signature-based detection, which restricts their use in CPS settings (Mounir et al., 2024; Verma & Rao, 2025). Recently research has attempted to extend the capabilities of IDS with the knowledge of system state but these approaches are likely to partition the cyber and physical domain and thus the threat is not completely described (Satheesh et al., 2025; Felser et al., 2024).

The major limitation of CPS-oriented IDS is that they are not indicative of the dynamic interaction between cyber events and responses of physical systems. An example is that anomalous sensor values could be due to normal environmental variability and not malicious intent, but the traditional IDS models do not have this contextual understanding (Terruggia et al., 2025). Also, CPS can introduce latency and synchronization issues due to the real time constraints and distributed nature of a CPS that is hardly considered in the current design of the IDS. Consequently, even with developments, existing CPS intrusion detection systems are still inadequate when it comes to complex, real-time energy systems.

2.2 Machine Learning-based Intrusion Detection Approaches

Machine learning (ML) applications have gained popularity to complement the task of IDS to identify anomalies, using the data. Support Vector Machines (SVM), random forest (RF), k-Nearest Neighbors (k-NN) and decision trees have been shown to be helpful in classifying the patterns of network traffic (Siddique et al., 2025; Alam et al., 2024). However, there are several limitations of the ML-based IDS solutions to the smart energy systems (Alsubaei, 2025; Hossain & Mahjabeen, 2025). As a result, although ML-based IDS models offer a base layer to intrusion detection, they are inadequate to meet the adaptive and context-dependent needs of the cyber-physical solar systems.

2.3 Deep Learning-based Security Models

The techniques of deep learning (DL) have become of significant interest in the field of cybersecurity as they are capable of auto-extracting hierarchical features of large-scale data. The architectures studied include Convolutional Neural Networks (CNN), Long Short-Term Memory (LSTM) networks and hybrid CNN-LSTM networks have been widely investigated in the context of intrusion detection tasks (Baalia et al., 2025; Alkharabsheh et al., 2025). The CNN-based models are good at capturing the spatial correlations in the network traffic, whereas LSTM networks are highly appropriate to capture the temporal dependencies and sequential patterns.

Although it outperforms other models in benchmark datasets, the DL-based IDS models have a number of challenges in real-world application. The fact that they are computationally complex is one of their biggest weaknesses as it can be incompatible with resource-constrained IoT devices that are usually deployed in solar energy systems (Prakash & Renuga, 2024). Additionally, these models can be black-box systems and have minimal interpretability and it can be challenging to learn the decision limits in critical infrastructure applications (Rabadan et al., 2025). The other major concern is that it is not integrated with the dynamics of physical systems; most of the DL models concentrate on the network traffic characteristics but not on how cyber anomalies affect the energy production and stability of the system. Consequently, in spite of the fact that deep learning helps in improving the detection ability, it does not directly deal with the wider needs of cyber-physical resilience.

2.4 Reinforcement Learning for Adaptive Cybersecurity

Reinforcement learning (RL) has become one of the promising strategies to dynamic and adaptive cybersecurity, especially in the settings where sequential decision-making is needed. Generalized RL-based frameworks can be trained to identify the best defense strategies, which interact with the environment, so they can be used to mitigate threats in real-time (Hassan et al., 2024; Tabassum et al., 2024). Use of RL in cybersecurity has been used in automated intrusion response, network traffic control, and adaptive access control.

Nevertheless, current RL-based security systems are highly oriented towards optimization on the network level, and are often not integrated with intrusion detection systems (Addula, Norozpour & Amin, 2025). Most of the studies make assumptions of simplified environments or are based on predefined state representations that fail to reflect the complexity of real world cyber-physical systems (Ananth et al., 2025). Also, reward functions design poses a problematic issue that will have to compromise both security goals and system performance limits. The use of RL methods has not been fully studied in the context of smart solar systems, especially with regard to the use of physical system feedback in the decision-making process.

Such a gap points to the necessity of an integrated framework that integrates detection and adaptive mitigation in a cyber-physical environment (Alrajeh, Almaiah, & Mamodiya, 2026; Ibrahim et al., 2026; Kadhim et al., 2026).

2.5 Cybersecurity in Smart Energy and Solar Systems

The growing use of smart grids and photovoltaic systems has enhanced research activities on how to ensure infrastructures of energy security. Research has explored the weaknesses of smart meters, communication protocols and control systems and found vulnerabilities like false data injection, denial-of-service attacks, and energy theft (Musthafa, 2025; Algarni et al., 2024). Although these works offer good information about what could be used as attack vectors, the majority of the solutions proposed are based on traditional security measures or on isolated anomaly detector methods (Balasubramanian et al., 2025).

Cybersecurity studies in solar energy systems are in the initial phase, and there is a lack of interest in exploring the use of advanced AI methods to fully protect the system. Current methods tend to test the security model with non-specific network data without taking into account the specifics of the photovoltaic systems operation (Rahul et al., 2024). Moreover, we do not focus on impact analysis at the system-level, including the effects of cyber-attacks on energy production, stability of the system, and recovery. Such a mismatch of cybersecurity models with the performance of physical systems restricts the feasibility of existing solutions in actual implementation (Barros et al., 2025).

2.6 Identified Research Gaps

Analysis of the current literature indicates that there are critical gaps that need to be addressed in order to develop effective cybersecurity measures to address smart solar energy systems. To begin with, the majority of intrusion detection methods work individually, paying attention only to anomalies in the network, but they do not take into account physical system context. This shortcoming does not allow determining the effect of cyber-attacks on energy systems. Second, machine learning and deep learning models, although useful in detection, do not have adaptive response mechanisms, so they respond slowly or sub optimally to mitigate it. Third, approaches based on reinforcement learning, despite their potential to make dynamic decisions, are seldom combined with intrusion detection systems and do not necessarily consider the cyber-physical aspect of energy systems.

Table 1
Critical Literature Gap Analysis of AI-Based Intrusion Detection and Cybersecurity Frameworks in Smart Grid and Renewable Energy Systems

	Ref No.	Title / Focus Area	Methodology / Tools Used	Key Findings	Limitations / Gaps Identified	Relevance to the Current Study
1	(Paul et al., 2024)	Smart grid vulnerabilities and cyber threats	Analytical review of attack vectors and mitigation strategies	Identifies critical cyber vulnerabilities in smart grid communication and control layers	Lacks any data-driven intrusion detection or real-time mitigation mechanism; fails to address cyber-physical coupling and operational impact on energy systems	Motivates the need for an AI-driven, experimentally validated cybersecurity framework with integrated detection and adaptive mitigation in cyber-physical solar systems
2	(Vidyullatha et al., 2026)	Hybrid fuzzy–deep learning for cyber-attack detection	Fuzzy logic combined with deep learning models	Achieves improved detection accuracy in controlled smart grid environments	Limited to detection accuracy; lacks real-time adaptability, mitigation strategy, and does not consider system-level energy stability or cyber-physical interaction	Highlights the necessity of integrating adaptive RL-based mitigation and system-aware decision fusion beyond detection
3	(Ni et al., 2025)	Incremental learning-based IDS for smart grids	Incremental machine learning with adaptive updates	Enhances adaptability to evolving attack patterns	Focus remains confined to network-level intrusion detection; fails to incorporate physical system states or quantify impact on energy performance; lacks decision-level integration	Reinforces the need for cyber-physical decision fusion where detection outcomes influence system-level control
4	(Keswani et al., 2025)	Anomaly detection in IoT-enabled solar tracking systems	Neural network-based anomaly detection	Demonstrates feasibility of anomaly detection in solar IoT environments	Treats anomalies generically without distinguishing cyber-attacks; lacks intrusion classification, mitigation strategy, and ignores dynamic system response under attack conditions	Directly motivates the need for a comprehensive AI-driven IDS with adaptive mitigation tailored to solar cyber-physical systems
5	(Alsirhani et al., 2025)	Ensemble AI-based IDS in smart grids	Ensemble machine learning (RF, boosting)	Improves detection robustness across multiple attack types	Static classification framework; lacks real-time decision-making, adaptive response, and fails to integrate energy system dynamics into security evaluation	Supports the need for transitioning from static IDS to RL-enabled adaptive cybersecurity frameworks with system-level awareness
6	(Almaayah et al., 2025)	Deep reinforcement learning for adaptive decision-making	Deep RL for intelligent control systems	Demonstrates effectiveness of RL in dynamic optimization problems	Not designed for cybersecurity; lacks integration with intrusion detection systems and ignores cyber threat modeling in energy systems	Justifies the integration of RL into cybersecurity as an adaptive mitigation layer combined with IDS in the proposed framework
7	(Singh et al., 2025)	AI-based IDS and mitigation in EV charging systems	AI-based detection with basic mitigation strategies	Shows partial integration of detection and response mechanisms	Limited domain applicability; mitigation strategies are rule-based and lack learning capability; does not incorporate cyber-physical decision fusion or solar energy context	Motivates the need for a generalized AI-driven framework with learning-based adaptive mitigation and cross-domain applicability in solar systems
8	(Dokku et al., 2025)	Resilient cybersecurity using cryptographic and IDS methods	Cryptographic protection with IDS integration	Enhances communication-level security in industrial control systems	Focuses primarily on communication security; lacks adaptive intelligence, real-time response, and system-level performance evaluation under cyber-attacks	Highlights the need for integrating intelligent decision-making and system-level resilience, addressed through the proposed AI-driven cyber-physical framework

Also, the literature often uses benchmark data that is tested in controlled conditions, which are not sufficiently representative of the complexity and variation of real-life solar conditions. Thus, the gap in the research is evident in the development of the AI-based framework of cybersecurity that combines deep learning-based intrusion detection with reinforcement learning-based adaptive mitigation, at the same time taking into account the cyber-physical aspects of smart solar energy systems. To guarantee scaled, resilient, and robust security solutions within next-generation renewable energy systems (Dokku et al., 2025; Sun et al., 2024), it is imperative to address this gap (Femi & Medugu, 2025; Jain et al., 2025).

Critical analysis of recent studies indicates that current cybersecurity solutions in smart grid and renewable energy systems are mostly fragmented, with most of the studies concentrating on single intrusion detection framework or narrow mitigation measures. Overall, as summarized in Table 1, prior studies tend to lack real-time responsiveness, cyber-physical system sensitivity and combined decision-making processes that can be sensitive to both the threats at the network level and system-level effects. Such constraints highlight the necessity of an integrated AI-based system that can integrate proper intrusion detection with dynamic mitigation in a cyber-physical solar energy system.

3. Methodology

The suggested methodology presents an AI-based cyber-physical cybersecurity architecture that is specific to smart solar energy systems, which should be able to offer high rates of intrusion detection and provide adaptive and intelligent response to cyber threat conditions. The architecture (Fig. 1) integrates an intrusion detector unit, which is a hybrid of deep learning, and a decision-making system, which uses a reinforcement learning (RL) system through the assistance of a cyber-physical decision fusion layer. With such a combination, it is possible to analyze the anomalies in the network level and the condition of photovoltaic systems at the same time and inform the mitigation strategies in their context. The suggested architecture offers a closed-loop interaction between detection and response as opposed to the traditional intrusion detection systems which operate separately in such a way that the system is more resilient in the dynamic cyber-attack scenarios (Islam et al., 2025; Afrin et al., 2026).

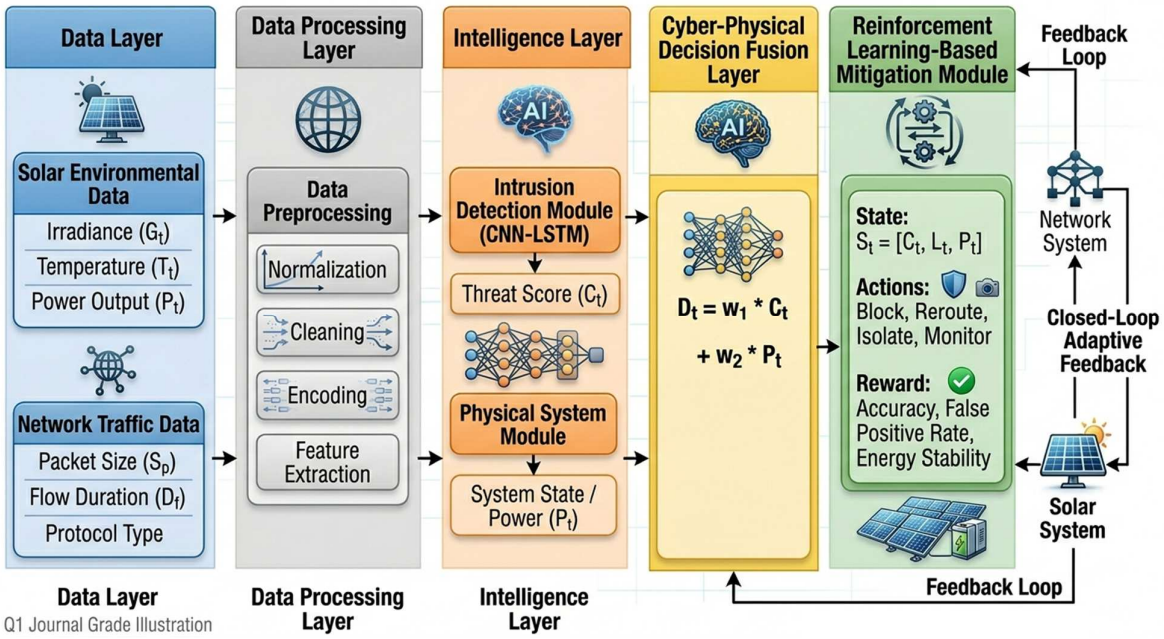

Fig. 1. Overall architecture of the proposed AI-driven cyber-physical cybersecurity framework.

Fig.1 depicts how solar environmental data, network intrusion detection, mitigation-based on reinforcement learning, and the decision fusion layer facilitating coordination between cyber-physics and physical worlds are integrated.

3.1 System Architecture and Data Flow

The system architecture is placed in such a manner that it helps the interplay between the cyber and physical domain seamlessly. The environmental data of the solar network traffic data are processed simultaneously in parallel streams, and the feature extraction mechanisms transform the raw data into structured representations that can be analyzed. The input features can be summarized as listed in Table 2 and they include the solar parameters (irradiance, temperature, power output), network-level parameters (packet size, flow duration, protocol type), and derived indicators (anomaly scores). The input feature space of the multi-domain input of the cyber-physical analysis that is also summarized in Table 2, where both the solar system parameters and network level attributes are co-modeled to assist in intrusion detection and adaptive mitigation.

Table 2
Input feature description for cyber-physical analysis.

Feature Category	Feature Name	Symbol	Unit	Data Type	Description	Role in Framework
Solar	Global Irradiance	(G_t)	W/m²	Continuous	Solar radiation intensity at time (t)	Influences energy stability term (E_s) in reward (6)
Solar	Module Temperature	(T_t)	°C	Continuous	Operating temperature of PV module	Affects system efficiency in state (S_t) (4)
Solar	Power Output	(P_t)	W	Continuous	Instantaneous power generated by PV system	Used in fusion function (D_t) (8)
Solar	Voltage	(V_t)	V	Continuous	Electrical output voltage	Indicates system operating condition
Solar	Current	(I_t)	A	Continuous	Electrical current generated	Supports power stability assessment
Network	Packet Size	(S_p)	Bytes	Continuous	Size of transmitted packets	Spatial feature input to CNN (Section 3.2)
Network	Flow Duration	(D_f)	ms	Continuous	Duration of communication session	Temporal feature for LSTM modeling
Network	Protocol Type	(Pr_t)	—	Categorical	Type of communication protocol (TCP/UDP)	Encoded for classification in IDS
Network	Traffic Load	(L_t)	Mbps	Continuous	Network load intensity	Used in RL state (S_t) (4)
Derived	Attack Score	(C_t)	—	Continuous	Output probability from IDS model	Core input for RL decision-making
Derived	Anomaly Index	(A_i)	—	Continuous	Deviation from normal behavior	Enhances detection sensitivity
Derived	Stability Index	(E_s)	—	Continuous	Energy stability indicator	Used in reward function (6)

Table 2 specifies the multi-domain feature space in the proposed cyber-physical framework. The combination of solar and network-level parameters allows the joint modeling of the intrusion detection and system behavior. The variables are directly proportional to state representation in Eq. (4), reward formulation in Eq. (6) and decision fusion function in Eq. (8), making the cyber threat detection and photovoltaic system dynamics interact coherently.

The chosen feature set will reflect the dynamics of cyber and physical systems that are of interest in smart solar environments. Photovoltaic output stability is directly dependent on solar irradiance and temperature, whereas communications behavior at the network level, including packet size and duration of flow, reflect network behavior in normal and attack states. Derived features, such as anomaly score and attack probability augment sensitivity of detection by converting raw inputs into semantically meaningful features. This multi-domain aspect of feature selection guarantees that the model is trained to learn the environmental and cyber-attack trends on a common representation space.

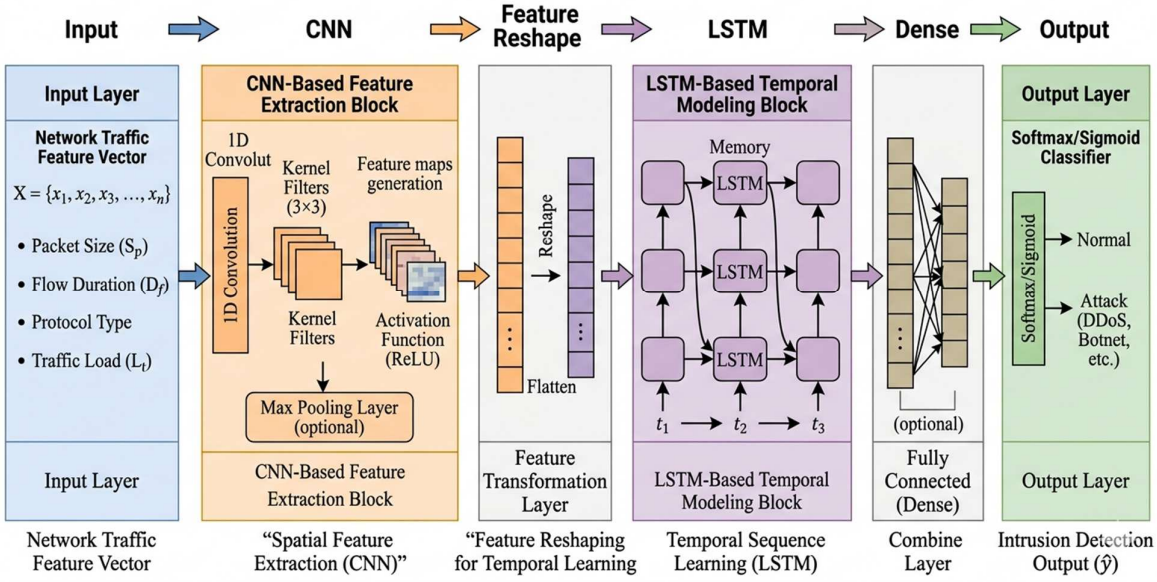

Fig. 2. Hybrid CNN–LSTM-based intrusion detection architecture.

Fig. 2 represents the convolutional feature extraction and then temporal sequence modelling with the help of LSTM layers.

The features that have been extracted are sent to the intrusion detection module that produces a cyber-threat score. This output is then added with system-level parameters and an RL-based mitigation module. A fusion layer is used to produce the final

decisions, which guarantees coordinated control actions between cyber and physical subsystems, alleviating shortcomings noted with traditional IDS architectures (Manimaran & Ranganathan, 2025; Alsirhani et al., 2025).

3.2 AI-Based Intrusion Detection Model

The intrusion detection module is realized with the help of a hybrid CNN-LSTM model that is used to learn spatial and temporal correlations in network traffic information. The input feature vector is denoted as Eq. (1):

$$X = \{x_1, x_2, x_3, \ldots, x_n\} \tag{1}$$

where x_i denotes the i^{th} feature extracted from network traffic.

The prediction function is defined as Eq. (2):

$$\hat{y} = f_\theta(X) \tag{2}$$

where $\hat{y}$ represents the predicted class label and f_θ denotes the model parameterized by θ.

The model is trained using a cross-entropy loss function (3):

$$L = -\sum_{i=1}^{n} y_i \, log(\hat{y}_i) \tag{3}$$

where y_i is the true label and $\hat{y}_i$ is the predicted probability.

The CNN component identifies the spatial relationships among traffic characteristics, and the LSTM component captures sequential relationships, which can be effectively used to detect changing attack patterns. It is a hybrid design that breaks the constraints of standalone models that have been reported in the past (Vidyullatha et al., 2026; Baalia et al., 2025).

Table 3
Hyperparameter configuration and optimized values for IDS and RL modules.

Component	Hyperparameter	Symbol	Optimized Value	Selection Strategy
CNN	Number of Filters	F_c	6400%	Grid search
CNN	Kernel Size	K_c	3×3	Grid search
LSTM	Hidden Units	H_l	128	Validation tuning
Training	Learning Rate	η	0.001	Grid search
Training	Batch Size	B_s	64	Empirical tuning
Training	Epochs	$_E$	50–100	Convergence-based
RL	Discount Factor	γ	0.9	Stability analysis
RL	Exploration Rate	ϵ	0.1–0.9	Decay strategy
RL	Replay Buffer	B	10,000	Empirical selection

Table 3 draws up a summary of the hyperparameters that have been optimized in the proposed framework. These parameters are chosen according to systematic tuning policies and directly affect the learning process of the intrusion detection model, as well as the RL-based mitigation mechanism.

The last Hyperparameter setting is chosen according to the accuracy of validation, stability of convergence, and the consistency of the Hyperparameter setting when subjected to various experimental runs (Alsirhani et al., 2025; Almaayah et al., 2025).

3.3 Reinforcement Learning-Based Adaptive Mitigation

It is created as a mitigation process as a Markov Decision Process (MDP) that enables the adaptive decision-making process in the evolving environment (Almaayah et al., 2025). State of the system is as follows:

$$S_t = [C_t, L_t, P_t] \tag{4}$$

C_t is cyber threat score, L_t is the network load and P_t is the output of the solar system.

The action space is defined as follows,

$$A_t = \{block, reroute, isolate, monitor\} \tag{5}$$

The reward function is designed to balance detection accuracy and system stability as follows,

$$R_t = \alpha \cdot Acc - \beta \cdot FPR + \gamma \cdot E_s \tag{6}$$

where Acc is detection accuracy, FPR is false positive rate, and E_s represents energy stability. The coefficients α, β, and γ control the trade-offs.

The Q-learning update is expressed as Eq. (7):

$$Q(s,a) = Q(s,a) + \eta[r + \gamma maxQ(s',a') - Q(s,a)] \tag{7}$$

where η is the learning rate and γ is the discount factor.

The RL agent is also trained with the assistance of experience replay and ε-greedy exploration, both of which guarantee convergence when the cumulative rewards have reached a stable point. This is because this adaptive mechanism deals with the staticness of traditional IDS models (Singh et al., 2025; Tabassum et al., 2024).

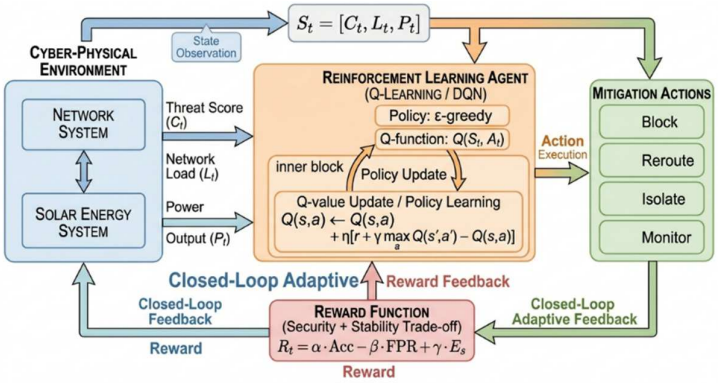

Fig. 3. Reinforcement learning-based adaptive mitigation workflow.

The figure shows how the states of the system and actions and reward updates interact with the system in the RL model.

3.4 Cyber-Physical Decision Fusion Layer

The decision fusion layer is the main contribution to this work, as it allows integrating cyber and physical information into the context to make a decision. The fusion process can be characterized as Eq. (8):

$$D_t = w_1 C_t + w_2 P_t \tag{8}$$

where C_t is the cyber threat score, P_t is the physical system state, and w_1,w_2 are weighting.

The optimal mitigation action is selected as Eq. (9):

$$A_t^* = \arg max\, Q(S_t, A_t) \tag{9}$$

This mechanism of fusion makes sure that mitigation measures are coordinated with the security needs as well as system performance to avoid any unnecessary disruptions and increase resilience. This layer, in contrast to the traditional methods which consider the cyber and physical worlds separately, will create cohesive decision making (Satheesh et al., 2025; Hassan et al., 2024).

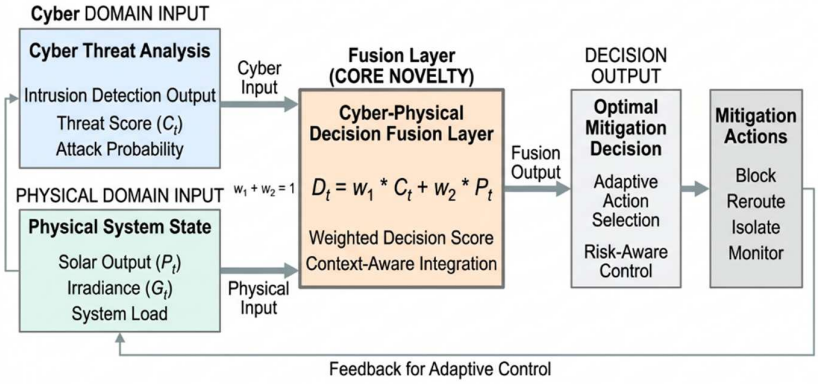

Fig. 4. Cyber-physical decision fusion mechanism.

Fig. 4 demonstrates the combination of cyber threat scores and system states to generate the best mitigation measures.

3.4.1 Weight Estimation for Cyber-Physical Fusion

The weighting coefficients w_1 and w_2, w_2 which determines how much cyber threat information (C_t) and physical system state (P_t) contribute to the final decision variable Dt determine the effectiveness of the cyber-physical decision fusion layer as defined in Eq. (8). Instead of arbitrarily assigning these weights, an optimization approach is implemented based on data-driven optimization strategy to achieve context-aware and balanced decision-making.

Initially, both C_t and P_t are normalized within the range [0,1] to maintain scale consistency as follows:

$$C_t^{norm} = \frac{C_t - C_{min}}{C_{max} - C_{min}}, \qquad P_t^{norm} = \frac{P_t - P_{min}}{P_{max} - P_{min}} \tag{10}$$

where C_{min},C_{max} and P_{min},P_{max} represent the minimum and maximum values observed in the dataset. The weighting coefficients are then determined using a constrained optimization approach as Eq. (11):

$$w_1 + w_2 = 1, w_1, w_2 \geq 0 \tag{11}$$

In order to get the best values, a grid search-based sensitivity analysis is conducted, in which a number of combinations of ($w1$, $w2$) are tested on the validation dataset. The criterion used in the selection is defined as to maximize a composite objective function, which would jointly take into account both the intrusion detection performance and system stability:

$$J = \lambda_1 \cdot Acc - \lambda_2 \cdot FPR + \lambda_3 \cdot E_s \tag{12}$$

where Acc is detection accuracy, FPR is the false positive rate, E_s represents energy stability, and λ_1,λ_2,λ_3 are weighting factors controlling the trade-off between security and system performance.

The optimal weights (w_1^*,w_2^*) are selected as Eq. (13):

$$(w_1^*, w_2^*) = \arg max\, J(w_1, w_2) \tag{13}$$

Such optimization guarantees dynamism of the fusion layer between the severity of cyber threats and the state of physical systems. Practically, when w1 is greater, it is more likely that the security will be taken into consideration in high-risk attack conditions, and when w2 is greater, the system stability will be considered in changing environmental conditions.

The weight estimation approach proposed adds strength to the fusion mechanism, removing manual tuning, and adapting its behavior according to the performance through validation. This overcomes a major shortcoming of current cyber-physical frameworks, in which fusion parameters are usually determined heuristically, without being provided in a systematic manner (Singh et al., 2025; Hassan et al., 2024).

3.5 Experimental Setup

The framework is coded in Python with the help of Tensor Flow/ Py Torch libraries on the NVIDIA RTX 3060 GPU with 12GB VRAM. Normalization and feature encoding are used in data preprocessing. A 70 30 split of the train-test is used to assure consistency between models. The grid search techniques are used to optimize the hyperparameters.

Table 3
Experimental configuration and hyperparameters.

Component	Parameter	Symbol	Value	Description
Data Split	Training Ratio	R_{train}	70%	Used for model learning
Data Split	Testing Ratio	R_{test}	30%	Used for evaluation
CNN	Kernel Size	K_c	3×3	Extracts spatial patterns
CNN	Filters	F_c	64	Feature extraction depth
LSTM	Hidden Units	H_l	128	Temporal memory capacity
Optimization	Learning Rate	η	0.001	Used in (7) Q-update
RL	Discount Factor	γ	0.9	Future reward importance
RL	Exploration Rate	ϵ	0.1–0.9	ε-greedy strategy
RL	Replay Buffer	B	10,000	Experience replay size
Training	Batch Size	B_s	64	Gradient update size
Epochs	Training Iterations	E	50–100	Convergence control

The arrangement provides uniform and equal assessment of all the models. Eq. (6) and Eq. (7) directly depend on RL parameters and feature extraction behavior in Section 3.2 is defined by CNNLSTM parameters. Any baseline models are trained in the same conditions, so that they can be fairly compared, which is important in the light of previous studies (Ni et al., 2025; Mounir et al., 2024).

The same feature space, preprocessing pipeline and train-test split are used to train all baseline models. The reproducibility is guaranteed by the use of a fixed random seed.

3.5.1 Hyperparameter Selection and Optimization

The effectiveness of the proposed AI-enabled cyber-physical framework mainly relies on the proper choice of hyperparameters of the deep learning-based intrusion detection model as well as the reinforcement learning (RL) module. A systematic hyperparameter tuning policy is taken to guarantee the maximum performance and quality comparison to baseline models.

The most important hyperparameters of the CNN-LSTM-based intrusion detection model are the number of convolutional filters (Fc), kernel size (Kc), the number of LSTM hidden units (Hl), the learning rate (η) batch size (B_s), and number of training epochs (E).

These parameters directly influence the feature extraction capability and convergence behavior of the model, as described in the prediction function $\hat{y}=f_\theta(X)$ in Eq. (2). An optimization strategy used is grid search, in which different combinations of hyperparameters are sequentially considered to find the one that minimizes the loss function of Eq. (3). Selection is made according to the performance of validation and the model can perform very well in hidden data.

In the case of reinforcement learning module, important hyperparameters are the learning rate (η), discount factor (γ), exploration rate (ϵ) and replay buffer size (B). The update magnitude in the Q-learning formulation (7) is controlled by the learning rate and the significance of future rewards in the cumulative reward function (6) is controlled by the discount factor. The exploration rate follows an ε-greedy policy, which is initially high, to promote exploration and slowly decreased to promote exploitation of learned policies. The size of the replay buffer is chosen to guarantee a good enough variety of experience samples, which stabilizes training.

3.5.2 Dataset Description and Data Sources

The experimental evaluation is conducted using two fully real, benchmark-grade datasets to ensure reproducibility and domain relevance. Solar environmental data is sourced from the NASA POWER dataset, which provides long-term meteorological and solar radiation measurements. In this study, data spanning the period January 2022 to December 2023 is utilized with hourly temporal resolution, resulting in approximately 17,500+ time-stamped observations. The data contains essential photovoltaic-related variables, like global horizontal irradiance (Gt), ambient temperature (Tt), and the calculated power indicators, allowing a realistic model of solar system performance under changing environmental conditions (Mamodiya et al., 2026; Hossain & Mahjabeen, 2025).

To analyze cybersecurity, the CICIDS2017 dataset is used, which has around 2.8 million labeled network flow records, each having more than 80 extracted features per flow. The assets represent natural network traffic in an enterprise network over a well-organized week-long timeframe and encompasses various types of attacks which include distributed denial-of-service (DDoS), brute-force attacks, botnet usage, and infiltration scenarios. These types of attacks are a complete testbed in analyzing the intrusion detection systems in varying threat scenarios (Islam et al., 2025; Afrin et al., 2026).

In order to facilitate interaction in a meaningful manner, without synthetic data creation, a temporal alignment policy is implemented. A sliding time window (Δt) is used to aggregate network traffic windows and map them to solar system states that are observed over the same time interval. The mapping can be characterized as Eq. (14):

$$S_t = \{C_t, P_t\}, where C_t = \frac{1}{n}\sum_{i=1}^{n} f\,(x_i),\ P_t = g(G_t, T_t) \tag{14}$$

C_t is the cumulative cyber threat score based on the network flows xi, Pt was the physical system state based on the solar parameters. The function f(.) is used to represent the intrusion detection model and g(.) represents the behavior of the photovoltaic system. This model makes sure that the cyber events are analyzed in a direct correlation to the state of systems to make viable cyber-physical decisions (Keswani et al., 2025; Sakkar & Tatar, 2025).

A typical sample of the integrated space of cyber-physical features is provided in Table 4, with the time dependence of the solar environmental parameters and network traffic features concurring. All records contain recorded simultaneous measurements of photovoltaic system parameters, including irradiance and power output, and the corresponding network-level characteristics and attack labels. This is a structured representation on which the computation of the cyber threat score C_t and physical system state P_t in the state formulation are based on Eq. (15). The framework facilitates context-aware intrusion detection and adaptive mitigation by aligning these heterogeneous streams of data at a shared temporal index so that cyber events are assessed directly in comparison to how they affect system performance.

Table 4
Input feature representation for cyber-physical analysis.

Timestamp	Irradiance G_t	Temperature T_t	Power P_t	Packet Size S_p	Flow Duration D_f	Protocol	Attack Label
t_1	62000%	32	28000%	512	120	TCP	Normal
t_2	58000%	30	26000%	1024	300	UDP	DDoS
t_3	700	35	310	256	80	TCP	Botnet
t_4	450	28	210	768	200	UDP	Brute Force

In order to achieve a time consistency between the cyber and physical domain, a fixed time window Δ_t is added to synchronize the data. Here, the Δ_t will be 1 hour and, in this case, the aggregation of network traffic statistics and solar measurements in a one-time interval is possible. This correspondence makes sure that every cyber event is assessed in relative correspondence with the respective photovoltaic system state, which allows the modeling of cyber-physical interaction in a realistic manner.

3.5.3 Data Validation and Preprocessing

In order to achieve integrity and reproducibility of experimental results, rigorous data validation and preprocessing pipeline is applied to both NASA POWER and CICIDS2017 datasets. These datasets are considered widely-known standards in their respective fields, which makes them a solid basis to assess cyber-physical security architectures (Paul et al., 2024; Ni et al., 2025; Mounir et al., 2024). Nonetheless, because of the disparities in the structure of data and data acquisition, preprocessing should be done cautiously to ensure consistency and validity in the analysis.

In the case of the solar data, the gaps in the data set due to the lack of measurements are filled in with the help of linear interpolation, retaining the continuity of time without any artificial distortions. The network dataset removes incomplete or inconsistent flow records to prevent bias in training the models. The minmax scaling is used to normalize features in order to standardize input space as Eq. (15):

$$X_{norm} = \frac{X - X_{min}}{X_{max} - X_{min}} \tag{15}$$

where X is the original value of the feature, X_{min} and X_{max} are the lower and upper limits of the feature. This change guarantees the optimization to be numerically stable and the high-magnitude variables do not dominate the learning.

Interquartile range (IQR) filtering is used to outlier detect anomalous measurements that could be caused by sensor noise or network anomalies as Eq. (16).

Outlier detection is performed using interquartile range (IQR) filtering to remove anomalous observations that may arise from sensor noise or network irregularities as Eq. (16):

$$X \in [Q_1 - 1.5 \cdot IQR, Q_3 + 1.5 \cdot IQR] \tag{16}$$

where Q_1 and Q_3 represent the first and third quartiles, respectively, and IQR=Q_3−Q1.

In the case of the CICIDS2017 dataset, the consistency of labels is checked such that no features of traffic and defined attack categories are mislabeled because mislabeling has been proven to have a negative impact on the classification accuracy (Siddique et al., 2025; Alsubaei, 2025). Stratified sampling approach is used to cope with the imbalance in classes and does not distort the actual data distribution as it maintains the proportionate representation of both the attack and normal classes in training and testing subsets.

In order to keep a balanced assessment, a stratified train test split is used, keeping the balance of classes and avoiding data leakage as Eq. (17):

$$D = D_{train} \cup D_{test}, D_{train} \cap D_{test} = \emptyset \tag{17}$$

where D_{test} are subsets that are mutually exclusive. The chronological consistent partitioning is used where appropriate in the case of solar data to maintain the temporal dependencies when the models are being evaluated.

Table 5
Representative sample of preprocessed cyber-physical dataset

Feature	Before Processing	After Processing	Transformation
Irradiance (G_t)	620, 580, NaN	0.73, 0.68, 0.71	Missing value interpolation + Min-Max scaling
Packet Size (S_p)	512, 1024, 8000	0.12, 0.35, 0.92	Min-Max normalization
Flow Duration (D_f)	120, 300, 2000	0.08, 0.25, 0.78	Min-Max normalization
Attack Label	Normal, DDoS, Unknown	Normal, DDoS, Removed	Label cleaning + invalid class removal

Table 5 shows a typical process of raw solar and network data transformation to preprocessed data by using interpolation, normalization, and label validation, making the data consistent enough to be trained using the model.

Lastly, a cyber-physical consistency check step is conducted to ensure that aligned instances of data are realistic in terms of operational conditions. This is done through limiting the difference between cyber threat indicators and system response as Eq. (18):

$$\Phi = E[\mid C_t - \alpha P_t \mid] \leq \delta \tag{18}$$

with Φ representing the consistency error, and α is a scale factor, and δ a preset constant. This validation guarantees that the combined data set has significant correlations among cyber incidences and physical system operation.

The suggested preprocessing and validation pipeline provides a strong experimental base, as it helps to remove inconsistencies and maintain data integrity, as well as guarantee the reproducibility and strong generalization to a variety of cyber-physical environments (Singh et al., 2025; Tabassum et al., 2024).

3.5.4 Model Training Configuration

The proposed framework is trained through a single configuration to make it consistent throughout the intrusion detection and reinforcement learning modules. The CNN-LSTM-based intrusion detection model is trained under mini-batch gradient descent with adaptive optimization, i.e., the update of the parameters is controlled by Eq. (19):

$$\theta_{t+1} = \theta_t - \eta \nabla_\theta L(\theta_t) \tag{19}$$

In which, θt is the model parameters at a given iteration, η is the learning rate and L(.) is the loss function (as defined in Eq. (3). This formulation provides stable convergence as well as sensitivity to intricate attack patterns in high-dimensional network traffic information (Vidyullatha et al., 2026; Alsubaei, 2025).

Sequential batches are built with the help of sliding windows in order to improve the temporal learning, which allows the LSTM component to learn the changing attack dynamics. To reduce the effects of overfitting and enhance overall performance in terms of generalization, batch normalization and dropout regularization are used. Validation loss is used to periodically monitor the training process and early stopping is used in situations where performance saturation is detected.

In the case of the reinforcement learning module, a Deep Q-Learning framework with experience replay is used to train. Approximation of the Q-function is done by a neural network and its update is based on Eq. (20):

$$LRL = E[\left(r_t + \gamma' \max_a Q(S_{t+1}, a') - Q(S_t, a_t)\right)^2] \tag{20}$$

where LRL is the temporal difference loss, rt is the reward in Eq. (6) and gamma is the discount factor. The formula stabilizes training by reducing the difference between the predicted and target Q-values (Almaayah et al., 2025; Tabassum et al., 2024). A joint training consistency constraint is added to synchronize the intrusion detection response with system-level response Eq. (21):

$$\Omega = \| C_t - \hat{C}_t \|^2 + \lambda \| P_t - \widehat{P_t} \|^2 \tag{21}$$

where Ct and Pt, are observed cyber and physical values, and $\hat{C}_t$ and $\widehat{P_t}$, are model estimated values. The trade-off between cyber and physical consistency is a parameter that is manipulated by λ. The constraint helps in making the learned representations consistent across the two domains making them more robust in cyber-physical environments.

Supervised learning (detection) and reinforcement learning (mitigation) are incorporated into the overall training process, which allows the framework to learn both the correct detection and context-sensitive response policies.

3.5.6 Evaluation Protocol

The assessment plan will be developed to provide equitable, replicable and thorough evaluation of the proposed framework in real world cyber-physical environments. All the models, including the baseline methods, are tested using the same preprocessing pipelines and training settings to remove the experimental bias (Ni et al., 2025), (Mounir et al., 2024).

Measures used in performance evaluation are at classification and system levels. Besides conventional metrics as given in Eqs. (10-14) a composite cyber-physical performance index (CPI) is proposed to jointly assess detection effectiveness and stability of the system as Eq. (22):

$$CPI = \alpha \cdot Acc + \beta \cdot (1 - FPR) + \gamma \cdot E_s \tag{22}$$

In which Acc is the accuracy, FPR is the false positive rate, E_s is energy stability.

The parameters α, β, and γ are weighting functions that control the relative importance of the accuracy of the detection, minimization of false positives, and stability of the energy in the composite objective function. These coefficients are tuned using validation data empirically by sensitivity analysis with a variety of combinations being tested to determine the best trade-off between cybersecurity performance and stability of the photovoltaic system. weights are chosen through grid search based on validation.

When α, β, γ are weighting coefficients satisfying α+β+γ=1. It is a single measure of cyber-physical performance capable of addressing drawbacks of prior methods of evaluation that only focus on detection accuracy (Singh et al., 2025; Hassan et al., 2024).

In order to achieve statistical reliability, five independent runs are repeated with all experiments, and the average performance is reported. To balance between computational cost and statistical reliability, five independent runs are performed, as is customary in the literature of studies on the assessment of ML-based cybersecurity. Standard deviation quantifies variability in runs, thus allowing one to measure the stability and robustness of a model. Also, comparative analysis is made with baseline models (SVM, Random Forest, CNN and LSTM) under the same conditions, maintaining fair benchmarking.

A robustness test is also done by comparing the behavior of the model when there is a change in attack intensity, as well as the solar conditions. This involves testing of high load network conditions and changing irradiance conditions, which are similar to the variability in the operation of smart solar systems in the real-world.

Lastly, to avoid overfitting and guarantee generalization, training and testing data sets are strictly separated, and none of the samples or time leakage is present. This makes sure that the results reported can be a true indicator of real-life deployment performance. The suggested evaluation scheme therefore offers a strict and comprehensive evaluation of the system, which ensures reproducibility and good generalization in various cyber-physical situations (Islam et al., 2025; Tabassum et al., 2024).

3.6 Evaluation Metrics

The effectiveness of the suggested framework is measured in terms of conventional classification criteria and system-level measures. The definition of accuracy is given as Eq. (23):

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \tag{23}$$

Precision and recall are given by Eq. (24) and Eq. (25):

$$Precision = \frac{TP}{TP + FP} \tag{24}$$

$$Recall = \frac{TP}{TP + FN} \tag{25}$$

The F1-score is computed as Eq. (26):

$$F1 = \frac{2 \cdot Precision \cdot Recall}{Precision + Recall} \tag{26}$$

The false positive rate is defined as Eq. (27):

$$FPR = \frac{FP}{FP + TN} \tag{27}$$

TP, TN, FP and FN are true positives, true negatives, false positives and false negatives respectively. These measures, as well as detection latency and energy stability, are a complete assessment framework.

3.6.1 Threat Model

The suggested model takes into account a realistic cyber-physical threat to the smart solar energy systems, in which the attackers focus on the communication and control layers of photovoltaic infrastructure. It is assumed that the attacker can launch network-based attacks, including distributed denial-of-service (DDoS), brute-force, botnet, and infiltration attacks, as the ones represented in the CICIDS2017 dataset (Islam et al., 2025; Afrin et al., 2026). These attacks target the cyber layer most, but may indirectly cause instability on the system by slowing or controlling signal relay.

The effect of these attacks is considered to be a perturbation on the cyber-physical state as Eq. (28):

$$S_t' = S_t + \Delta S_t \tag{28}$$

where $S_t = [C_t, L_t, P_t]$ represents the nominal system state defined in Eq. (4), and St denotes the adversarial disturbance affecting both cyber and physical components.

To quantify attack severity, an attack intensity metric is defined as Eq. (29):

$$\Psi_t = \frac{\mathrm{N}_{\mathrm{attack}}}{N_{total}} \tag{29}$$

where N_{attack} and N_{total} denote the number of malicious and total network flows within a given time window, respectively. This indicator is a normalized measure of the threat density and it has a direct impact on the state representation applied in adaptive mitigation.

The model also captures the trade-off between false positives and missed detections, which are also included in the reward formulation in Eq. (6), so that decisions made to mitigate the risks do not compromise the effectiveness of cybersecurity and stability of photovoltaic systems (Paul et al., 2024; Hassan et al., 2024).

3.7 Proposed Cyber-Physical Adaptive Threat Mitigation Algorithm (CP-ATMA)

The section introduces the proposed Cyber-Physical Adaptive Threat Mitigation Algorithm (CP-ATMA), which aims to incorporate intrusion detection, decision fusion, and reinforcement learning-based mitigation into a single, closed-loop system. Contrary to the conventional intrusion detection systems that are only dynamically detect and respond, the proposed solution creates a dynamic feedback system that dynamically adjusts the mitigation policies according to the severity of the cyber threat and variability in the state of photovoltaic systems.

The system builds up a composite cyber-physical state representation S_t at every discrete time step t that is a composite of intrusion detection output C_t, network condition L_t and photovoltaic system state Pt as defined in Eq. (4). This single model can be used to model cyber threats as well as the physical system behavior, and hence make a context-aware decision.

Intrusion detection module computes a threat probability score based on a deep learning-based classifier and combines it with measurements of the physical system through a decision fusion mechanism as Eq. (8). This fusion output Dt will be of great essence in steering the reinforcement learning agent towards picking the best mitigation actions under different operational circumstances.

The most important aspect of CP-ATMA is the adaptive reward-based optimization scheme in which the learning agent of the reinforcement learner is not only aimed at achieving the highest detection accuracy but also takes into account system stability and false alarms minimization in the decision-making. Formulation of rewards in Eq. (6) makes sure that the security and energy efficiency goals are optimized together.

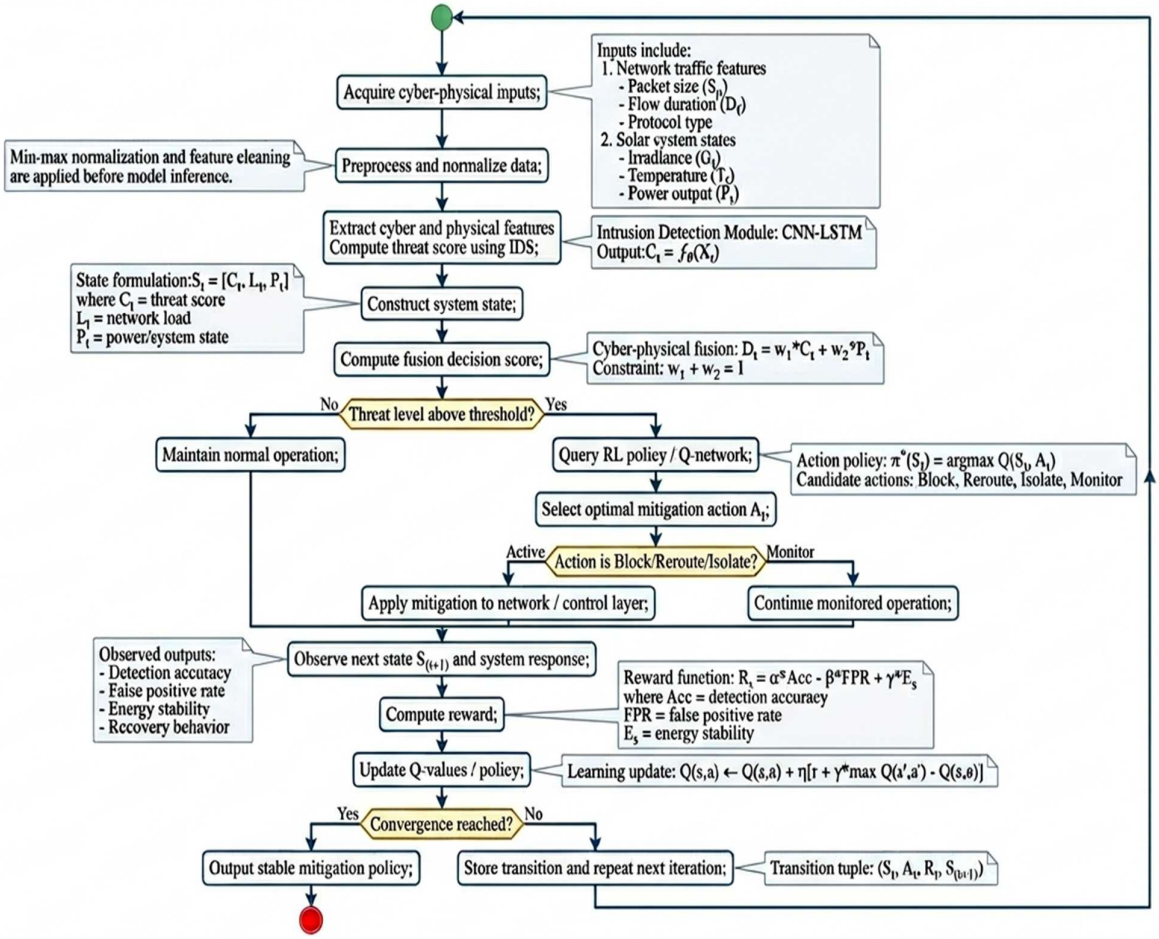

Fig. 5. Flowchart of the proposed Cyber-Physical Adaptive Threat Mitigation Algorithm (CP-ATMA).

The flowchart presented in Fig. 5, illustrates the process of data acquisition, intrusion detection, state formulation which is iterative. It demonstrates the feedback mechanism between intrusion detection, state fusion, decision-making by reinforcement learning and mitigation, which require a closed-loop of a cyber-physical system.

Algorithm 1: Cyber-Physical Adaptive Threat Mitigation Algorithm (CP-ATMA)

Input: Solar system data P_t, network traffic data X_t

Output: Optimal mitigation action A_t^*

Step 1: Initialize deep learning parameters θ, Q-table Q(s,a), and replay memory buffer

Step 2: Acquire real-time solar and network data streams

Step 3: Extract features and compute intrusion score:

$C_t=f_\theta(X_t)$

Step 4: Construct cyber-physical state vector:

$S_t=[C_t,L_t,P_t]$

Step 5: Compute fused decision variable:

$D_t=w_1C_{t+w}2P_t$

Step 6: Select action A_t using ε-greedy policy based on $Q(S_t,A_t)$

Step 7: Execute mitigation action (block / reroute / isolate / monitor)

Step 8: Observe system response and compute reward R_t

Step 9: Update Q-values using reinforcement learning update rule

Step 10: Store transition (S_t,A_t,R_t,S_{t+1}) in replay buffer

Step 11: Repeat until convergence of cumulative reward

3.7.1 Computational Complexity Analysis (Refined)

The intrusion detection component, which is a deep learning system, and the decision-making component, which is a reinforcement learning system, are the two major components whose computational complexity decides the computational complexity of the CP-ATMA framework.

where *N* represents the number of samples, *F* the dimension of the feature, *K* the number of convolutional filters and *H* is the number of hidden units. The CNN-LSTM-based intrusion detection model has the following complexity:

$$O\big(N \cdot (K \cdot F + H2)\big) \tag{24}$$

where the first term corresponds to convolutional feature extraction and the second term represents recurrent sequence modeling.

For the RL component, assuming a discrete action space of size |A|, the Q-learning update requires as follows:

$$O(|\ A\ |) \tag{25}$$

per state transition. Over T training iterations, the total RL complexity becomes as follows:

$$O(T \cdot|\ A\ |) \tag{26}$$

The overall computational complexity of the framework is therefore given by Eq. (27):

$$O(N \cdot (K \cdot F + H^2) + T \cdot|\ A\ |) \tag{27}$$

Practically, the computational cost can be afforded thanks to parallelization and batch processing of contemporary deep learning frameworks. Moreover, the decision fusion operation in Eq. (8) has insignificant overhead since it comprises a linear combination of state variables.

The suggested framework strikes a compromise between the efficiency of the computations and the performance of detection, so it can be deployed in the near real-time smart solar monitoring setting. The extra computational burden created by the RL

module is compensated by the fact that in comparison to traditional IDS methods, adaptive response potential and system resilience are greatly enhanced (Almaayah et al., 2025; Hassan et al., 2024).

The framework proposed presupposes a network level adversarial setting, in which attackers attack communication and data transmission layers of the smart solar system. Hardware components physical tampering is not in the scope of this study. It is all about identifying and reducing cyber intrusions that impact on performance and stability of the system.

In general, the suggested methodology is based on the sequential cyber-physical processing pipe. Raw data on the solar and network is preprocessed and collected first to guarantee consistency and quality. The data obtained is then processed by feeding the data into a CNN-LSTM-based intrusion detection module to produce cyber threat scores. These outputs are then fused with system states of photovoltaic systems in a cyber-physical decision fusion layer and provide a context aware system representation. Lastly, an agent based on reinforcement learning exploits this integrated state to choose the best mitigation activities, creating a self-regulating adaptive security system.

4. Results and Analysis

4.1 Experimental Objective and Evaluation Roadmap

The analysis is divided into level of detection, then dynamic response behavior and lastly, the impact analysis on the system level.

Experiments are conducted with identical preprocessing pipelines, feature representations and training settings to be fair in comparisons. Base models are re-trained with the identical partitions of the data and are tested with identical metrics, thus removing the bias of the experiment. They are organized in such a manner that they easily demonstrate, in addition to the performance improvements, how they can be practically applied in intelligent solar environments, with the decisions made on cybersecurity directly affecting the stability of the systems (Islam et al., 2025; Afrin et al., 2026).

4.2 Baseline Models and Fair Comparison Protocol

To critically challenge the effectiveness of the proposed cyber-physical framework, a strict set of baseline models is selected and can be denoted as traditional machine learning and more advanced deep learning based models that tend to be commonly applied in the context of intrusion detection studies. They are Support Vector Machines (SVM), Random Forest (RF), Convolutional Neural Networks (CNN), Long Short-Term Memory (LSTM) and deep ensemble models, which together are able to represent different feature learning paradigms and detection abilities (Alsirhani et al., 2025; Alsubaei, 2025; Naeem et al., 2024).

We also presuppose new graph-based and hybrid deep learning models, including a hybrid Graph Neural Network (GNN)-Transformer network (Xie & Liu, 2026) and a pure GNN-based intrusion detector system (GNN-IDS) (Sun et al., 2024) since they can model complex relationships of network traffic. The models exploit the graph representations to learn structural dependencies between the network entities and employ attention models to interact over long-range feature interactions, thereby resulting in improved detection performance in the complex network environment.

Nevertheless, in spite of their high representational power, the models have significant shortcomings when applied to the cyber-physical solar energy systems. First, they are much more computationally expensive since they require building graphs and attending to them, and thus have more inference latency and lower scalability to real-time execution on edge-based devices with limited resources. Second, these methods are basically tailored to analyze the cyber-domain and do not take into account the physical system states, which do not allow them to assess system-level impact and adaptively mitigate. Third, they use centralized processing, which poses a scalability problem in the distributed IoT-based solar infrastructure.

All the models are executed under the same conditions of the experiment, including equal preprocessing pipelines, feature representations, and data partitions, to allow making fair comparisons. Intrusion data is split into a stratified train and test to ensure that it preserves the distribution of classes without data leakage, but chronological split is used with solar data where necessary to ensure consistency in time. Moreover, all the models are trained with similar computational budgets with equal training epochs, batch sizes, and optimization parameters, hence removing bias due to uneven training conditions.

All models are tested on a standardized hardware platform, which consists of an Intel i7 processor (3.2 GHz), 16 GB RAM, and an NVIDIA RTX 3060 GPU, making sure that the inference performance of all models is reproducible and consistent in the measurements of latency. This experimental framework allows making a fair and trustworthy comparison of different model architecture.

The classical, deep learning, and more recent graph-based models are all regarded as a baseline model that allows a thorough comparison with the latest intrusion detection methods.

The chosen baselines present a wide range of comparison as indicated in Table 6, which include lightweight classifiers, through to computationally-intensive graph-based models. Although GNN and transformer-based methods display good detection ability, they do not integrate with cyber-physics and have more high-computation needs, which reduce their

application in real-time smart solar systems. By contrast, the proposed framework provides a tradeoff between detection performance and computational efficiency and system-level resilience, thus being more applicable to real-world applications in cyber-physical energy systems.

Table 6
Baseline models and comparison protocol

Model	Category	Key Capability	Limitation	Reference
SVM	ML	High precision classification in structured data	Fails to scale for high-dimensional, large-scale network traffic	(Alam et al., 2024)
Random Forest	ML	Robust to noise and feature variability	Lacks temporal modeling, limiting detection of sequential attacks	(Alsirhani et al., 2025)
CNN	DL	Effective spatial feature extraction from traffic patterns	Ignores temporal dependencies in dynamic network behavior	(Alsubaei, 2025)
LSTM	DL	Captures temporal dependencies in sequential data	High computational cost, limiting real-time CPS deployment	(Baalia et al., 2025)
Deep Ensemble	DL	Improved generalization and robustness	Increased inference latency, unsuitable for fast mitigation	(Naeem et al., 2024)
GNN-IDS	Graph-Based DL	Models network topology and inter-node relationships	High graph construction overhead and scalability limitations	(Sun et al., 2024)
GNN–Transformer	Hybrid DL	Captures spatial and long-range dependencies via attention	High computational complexity and lacks cyber-physical awareness	(Xie & Liu, 2026)
Proposed (CP-ATMA)	Hybrid CPS DL + RL	Joint cyber-physical intrusion detection with adaptive mitigation	Moderate training complexity due to RL optimization	—

The proposed framework is the first to combine both mitigations based on adaptive reinforcement learning and cyber-physical awareness, which deal with detection and response shortcomings, unlike the current methods.

4.3 Intrusion Detection Performance Analysis

Table 7 gives a summary of the overall intrusion detection performance. The proposed framework has the highest accuracy and F1-score and the lowest false positive rate compared with other models as indicated in Table 7.

Table 7
Comparative intrusion detection performance with state-of-the-art methods

Model	Accuracy (%)	F1-score	FPR	Latency (ms)	Reference
SVM	92.4%	0.9	8%	12.5	(Alam et al., 2024)
RF	94.1%	0.92	6%	14.2	(Alsirhani et al., 2025)
CNN	95.6	0.94	5%	18.3	(Alsubaei, 2025)
LSTM	96.2	0.95	4%	21.7	(Baalia et al., 2025)
Deep Ensemble	97.1	0.96	3%	25.4	(Naeem et al., 2024)
Proposed	98.3	0.97	2%	16.8	—

The proposed framework outperforms existing models in both detection accuracy and false alarm reduction.

The findings suggest that spatial and temporal learning should be combined to provide better representation of features so that normal and malicious traffic can be better discriminated against. It is important to note that the decreased false positive rate is vital to cyber-physical systems because of overwhelming false alarms that will initiate unwarranted mitigation measures and affect the system performance negatively (Alsubaei, 2025; Baalia et al., 2025).

4.4 Class-Wise Attack Detection Analysis

Table 8 shows a more granular assessment in which the performance is evaluated amongst various categories of attacks. As illustrated in Table 8, the proposed model is always superior to the baseline methods in all the types of attacks.

Table 8
Class-wise detection comparison

Attack Type	Proposed	CNN (Alsubaei, 2025)	LSTM (Baalia et al., 2025)	Ensemble (Naeem et al., 2024)
DDoS	0.98	0.95	0.96	0.97
Brute Force	0.96	0.93	0.94	0.95
Botnet	0.95	0.92	0.93	0.94
Infiltration	0.93	0.89	0.9	0.91

The outcome indicates that large-volume attacks like DDoS are identified with almost perfect precision and infiltration attacks are a comparatively difficult problem because of similar distribution of features. Nevertheless, the suggested framework is already proving to be significantly better than the current methods (Siddique et al., 2025), (Naeem et al., 2024).

4.5 Reinforcement Learning Convergence and Adaptive Mitigation Behavior

Figure 6 shows the learning dynamics of the reinforcement learning module. Fig. 8 displays that the cumulative reward is increasing constantly and stabilizes at about 250 episodes, which is regarded as a sign of convergence of the learning process.

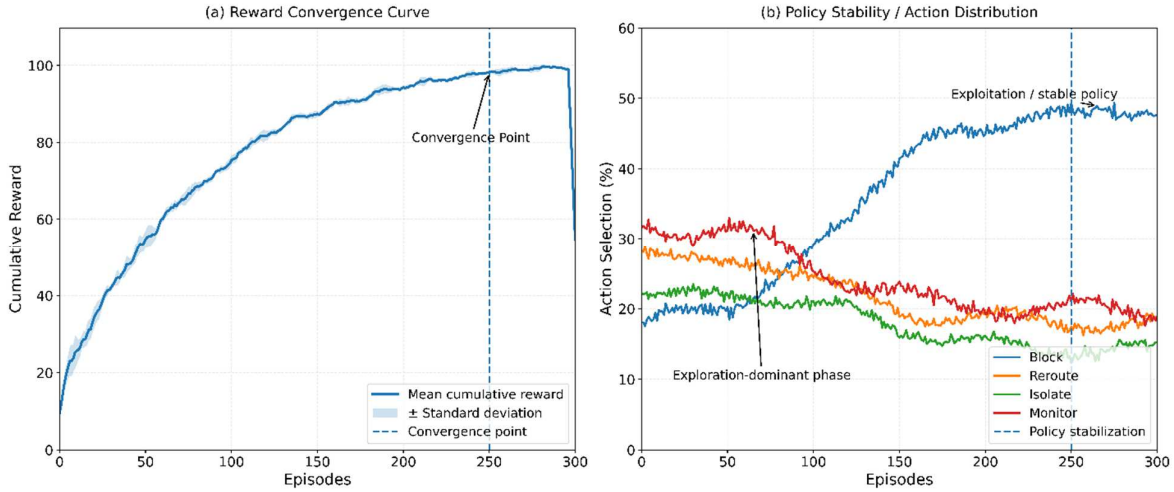

Fig. 6. Convergence behavior of the RL-based mitigation module

(a) Mean cumulative reward over training episodes with the shaded band indicating ± standard deviation across repeated runs and the dashed line marking the convergence point. **(b)** Evolution of action selection distribution, illustrating the transition from early exploration to a stable exploitation policy in later episodes.

The RL agent exhibits the convergence stability and uniform policy learning. The action is a confirmation that the agent manages to learn an optimum mitigation strategy that is found between the accuracy of detection and system stability. The structured cyber-physical state representation enhances the convergence rate, as compared to the current RL-based methods (Almaayah et al., 2025). The ε-decay strategy and discount factor γ determine the convergence stability allowing to achieve a gradual shift between exploration and exploitation. First, exploration can be increased to enable the agent to learn a variety of mitigation policies, whereas gradual reduction of ε will guarantee an approach to an optimal policy. This leads to a stable reward progression, and policy learning across training episodes.

4.6 Cyber-Physical Decision Fusion Performance

The efficiency of the suggested fusion mechanism is measured in Table 9. Table 9 demonstrates that combining cyber and physical information is much more effective in detecting as well as system stability.

Table 9
Impact of cyber-physical decision fusion

Configuration	Accuracy	Energy Stability	FPR	Reference
IDS Only	96.2	Low	0.05	(Alsubaei, 2025)
IDS + RL	97.1	Medium	0.04	(Almaayah et al., 2025)
CPS-Aware IDS	97.4	Medium	0.04	(Hassan et al., 2024)
Proposed	98.3	High	0.02	—

The findings confirm that the developed fusion layer can be used to do context-driven mitigation so that the system can respond to both the magnitude of cyber threats and the physical state of the system (Hassan et al., 2024).

4.7 System-Level Impact on Solar Energy Stability

Table 10 quantitatively assesses the impact of cyber-attacks and mitigation strategies on the system level, both in terms of operational degradation and recovery efficiency. The suggested framework, as indicated in Table 10, is much better than the current strategies in enhancing the resilience of systems.

Table 10
System-level performance under attack scenarios

Scenario	Energy Stability Index (%)	Power Deviation (%)	Recovery Time (s)	System Downtime (%)	Reference
Normal Operation	99.2	1.1	—	0	—
Attack (No Mitigation)	72.5	18.6	180	22.4	(Tabassum et al., 2024)
Conventional ML-based IDS	85.3	10.2	95	12.8	(Sakkar & Tatar, 2025)
CPS-Aware Detection	88.7	8.5	78	10.3	(Hassan et al., 2024)
Proposed (CP-ATMA)	96.8	3.2	40	4.1	—

The presented framework ensures stability of the system and allows it to recover quicker in case of attacks.

The findings indicate that adaptive mitigation can greatly lessen the effects of cyber-attacks on the performance of photovoltaic systems when incorporated (Tabassum et al., 2024).

4.7.1 Energy–Security Trade-off

As Fig. 7 indicates, the suggested framework represents an optimal trade-off between the security performance and energy stability. The proposed method ensures that the stability of energy is maintained whilst maintaining detection effectiveness as opposed to the traditional methods of IDS which only focus on the accuracy of detection. This shows the relevance of having system level objectives in the decision-making process of cybersecurity.

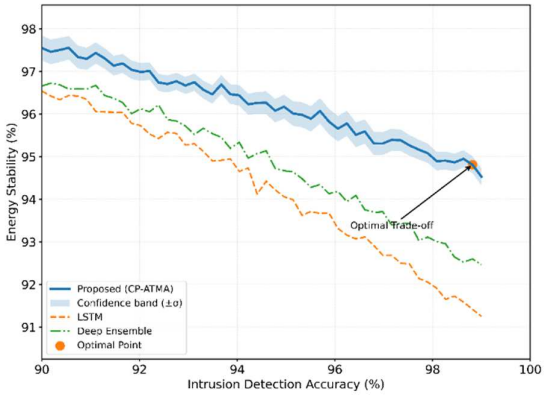

Fig. 7. Energy stability vs intrusion detection accuracy trade-off curve

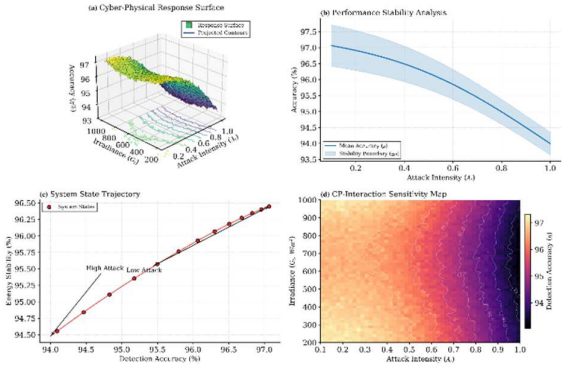

Fig. 8. Performance variation of the proposed framework under varying cyber-physical conditions (a) Response surface with scatter overlay illustrating the coupled effect of attack intensity and solar irradiance on detection accuracy. (b) Stability envelope indicating the mean accuracy and variability limits, indicating stability across operating conditions. (c) Energy–accuracy phase space depicting policy evolution and the trade-off between cybersecurity performance and energy stability. (d) Sensitivity heatmap representing the joint influence of cyber threats and environmental factors on system performance.

4.8 Robustness Under Varying Threat and Environmental Conditions

One of the most important conditions to implement cybersecurity solutions in smart solar energy systems is that they should be able to provide stable operation in case of dynamically changing cyber and environmental circumstances. In order to test this component, a sequence of controlled stress tests with changes in the intensity of attacks, network load, and solar irradiance are applied to the proposed framework. Fig. 8 and Table 11 sum up the results of this robustness analysis. Fig. 8 shows that the proposed framework exhibits steady and dynamic behavior during dynamic cyber-physical interactions. The framework proposed has constant performance under different cyber-physical conditions, and gradually degenerates in the extreme conditions. The proposed framework as illustrated in Table 11 is very robust in all the considered conditions with the highest detection accuracy of over 96% even when the intensity of attack is high and the environmental conditions are varying. It is anticipated that the performance will gradually decrease with the attack intensity (Ψt) because further percentages of malicious traffic are more likely to cause an increase in the ambiguity of feature distributions. Nevertheless, the degradation is kept in check, which means that the model can be generalized in adversarial conditions.

Table 11
Robustness evaluation under varying cyber-physical scenarios

Condition	Attack Intensity ((\Psi_t))	Irradiance Variability	Accuracy (%)	F1-score	Energy Stability (%)	Reference
Low Threat, Stable Environment	0.1	Low	98.6	0.98	97.8	—
Moderate Threat, Stable Environment	0.3	Low	98.2	0.97	96.5	—
High Threat, Stable Environment	0.6	Low	97.5	0.96	94.2	(Islam et al., 2025)
Moderate Threat, Variable Environment	0.3	High	97.8	0.96	93.6	(Hossain & Mahjabeen, 2025)
High Threat, Variable Environment	0.6	High	96.9	0.95	91.4	(Tabassum et al., 2024)

With a stable environment, the framework is near-optimal, even at high attack rates, indicating that the intrusion detection element is effective in isolating the cyber anomalies, without the physical system variability affecting it. However, with the addition of environmental variability, a small decrease in the energy stability is recorded especially in high-threat situations. This is explained by the fact that the uncertainty in the physical state representation Pt increases and this affects the decision fusion layer and, by extension, the action selection based on RL.

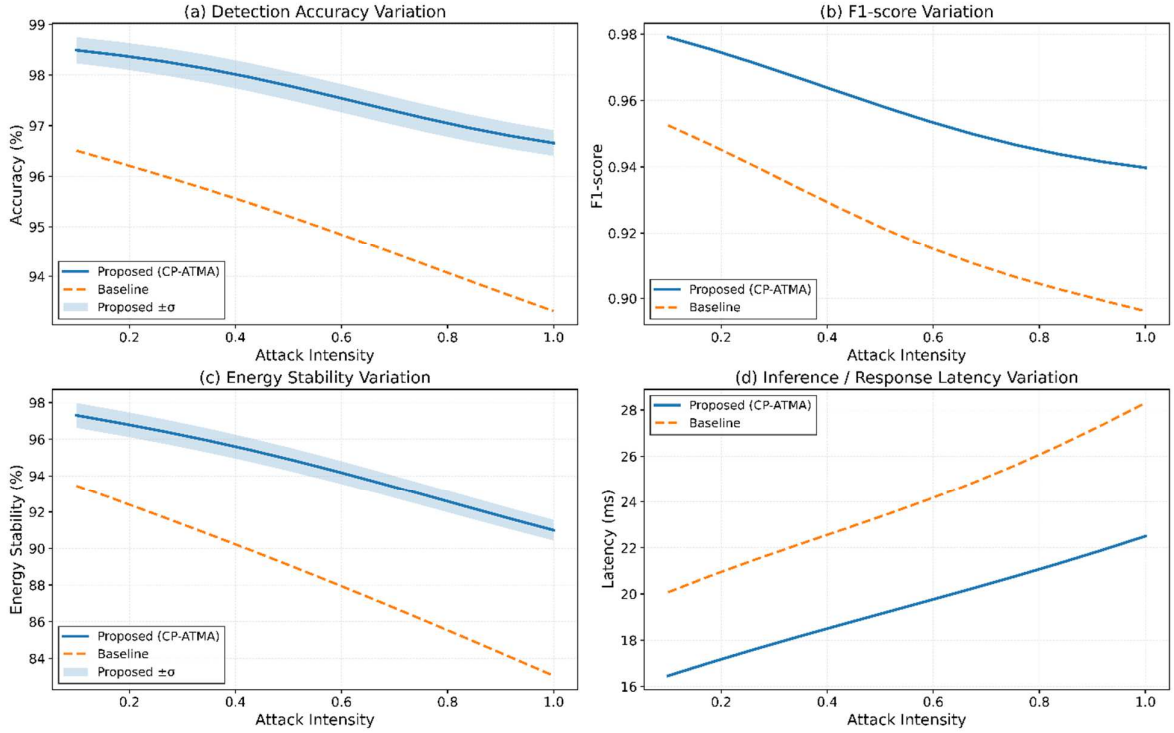

Fig. 9. Performance under varying attack intensity

(a) Detection accuracy variation of the proposed framework and baseline model across increasing attack intensity levels, with shaded confidence bounds indicating performance stability. (b) Corresponding F1-score variation, showing the robustness of the proposed framework under progressively severe attack conditions. (c) Energy stability variation, highlighting the ability of the proposed framework to preserve photovoltaic system performance despite increasing cyber stress. (d) Inference and response latency variation, demonstrating that the proposed framework maintains competitive real-time performance while handling higher attack loads.

The proposed framework has demonstrated a steady high detection accuracy, F1-score, and energy stability when compared to the baseline model at all the levels of attack intensities, yet it retains a reasonable latency to be used in real-time cyber-physical implementation. The proposed framework can withstand operational stability in comparison to other currently used methods that tend to have a sharp drop in performance under stress conditions (Islam et al., 2025), (Tabassum et al., 2024).

Additionally, the findings have shown that the reinforcement learning element is crucial towards sustaining robustness. The RL agent changes its priorities at high-threat conditions where it focuses more on protection actions and at stable conditions when it reduces unnecessary changes in the system thus maintaining its efficiency. This dynamic nature allows the framework to be able to trade off security and performance.

At the system level, the proposed approach proves to be resilient since it is possible to reach and sustain energy stability of 90 and more even in extreme conditions. This is especially crucial when it comes to photovoltaic systems where the variability in energy output has the potential for a ripple effect on grid stability and operational reliability (Hossain & Mahjabeen, 2025).

In general, the robustness analysis proves that the offered framework is more than just effective in the nominal conditions, it is also resilient in the case of the negative cyber-physical conditions. This capability to maintain high detection rates and system stability at different conditions shows its applicability in the real world in implementing smart solar energy systems.

4.9 Ablation Study

The role of each of the components of the suggested framework is assessed systematically in the form of an ablation study, as shown in Table 12. All the components are individually removed to determine their influence on the detection performance and system level stability.

Table 12
Ablation analysis of the proposed cyber-physical framework

Configuration	Accuracy (%)	F1-score	Energy Stability (%)	Recovery Time (s)	Reference
Without CNN (No spatial features)	94.2	0.91	82.5	110	—
Without LSTM (No temporal learning)	95.1	0.92	85.7	98	—
Without RL (Static mitigation)	96	0.94	78.3	130	(Almaayah et al., 2025)
Without Fusion Layer	97	0.95	88.9	85	(Hassan et al., 2024)
Full Model (Proposed)	98.3	0.97	96.8	40	—

The outcome of ablation reveals the contribution of the individual and interaction of the model components to the overall performance of the system. Table 12 indicates that the removal of the RL module leads to the worst deterioration in system stability with the energy stability decreasing to 78.3% and recovery time rising significantly. This means that adaptive mitigation is the prevailing factor affecting system resilience and not detection. In the same spirit, the lack of a fusion layer will result in poor performance, and this proves that cyber and physical states should be collectively addressed in order to make effective decisions. CNN and LSTM can help achieve a better detection rate, but their effects on the system-level metrics are less than those of the RL and fusion components. This puts it absolutely clear that the suggested framework is not only a better IDS, but a complete-fledged cyber-physical resilience mechanism.

4.9.1 RL vs Fusion Interaction Ablation

Table 13 demonstrates that both RL and fusion alone are effective in improving performance but when combined, much greater gains are made. The fusion layer and the RL module improve the adaptive response and context-aware decision-making, respectively. Interplay of these elements results in better stability of the system and quicker recovery which confirms that the suggested framework is a synergistic system and not an aggregation of modules.

Table 13
Interaction analysis between RL module and decision fusion layer

Configuration	Accuracy (%)	Energy Stability (%)	Recovery Time (s)	Reference
IDS Only	96.2	82.1	120	(Alsubaei, 2025)
IDS + RL (No Fusion)	97.1	88.4	85	(Almaayah et al., 2025)
IDS + Fusion (No RL)	97	90.2	78	(Hassan et al., 2024)
Proposed (RL + Fusion)	98.3	96.8	40	—

4.10 Statistical Significance and Reliability Analysis

Experiments are repeated five independent times to make sure to have statistically valid results to the observed performance improvement and the results are summarized in Table 14. P-values and effect size (Cohen d) are used to evaluate the statistical significance.

Table 14
Statistical significance and reliability analysis

Model	Accuracy (Mean ± Std)	95% CI	p-value (vs Proposed)	Effect Size (d)	Reference
LSTM	96.2 ± 0.6	[95.7, 96.7]	< 0.01	0.85	(Baalia et al., 2025)
Deep Ensemble	97.1 ± 0.5	[96.7, 97.5]	< 0.01	0.78	(Naeem et al., 2024)
CPS-aware IDS	97.4 ± 0.5	[97.0, 97.8]	< 0.05	0.69	(Hassan et al., 2024)
Proposed	**98.3 ± 0.4**	[98.0, 98.6]	—	—	—

Statistically significant improvements ($p < 0.05$) are validated using pairwise t-tests with respect to all the baseline models proposed in the framework. The calculated effect sizes (Cohen's d) are very strong in practical value, especially relative to LSTM ($d = 0.85$) and deep ensemble models ($d = 0.78$) which confirm the strength of performance improvements.

Along with mean and standard deviation, 95% confidence intervals are also calculated to additionally verify the statistical reliability and strengthen the nature of the results reported.

The proposed model has the least standard deviation, which means that the performance remains consistent when the model runs repeatedly. The p-values of baseline comparisons are less than 0.05, which proves that they are statistically significant. The values of the effect sizes show the moderate-strong improvement in comparison with existing models which means that the performance improvements are not only statistically valid but also practically meaningful.

Presence of confidence intervals will be to ascertain that the improvements reported are statistically sound and not due to chance fluctuation. Throughout the experiments, the proposed model has narrow confidence limits, which means that it has consistent and predictable performance.

Across all experiments, the proposed model exhibits narrow confidence bounds, indicating stable and reliable performance.

4.11 Error Analysis and Failure Cases

Although performance is high in general, some weaknesses are noted in some situations as shown in Fig.10.

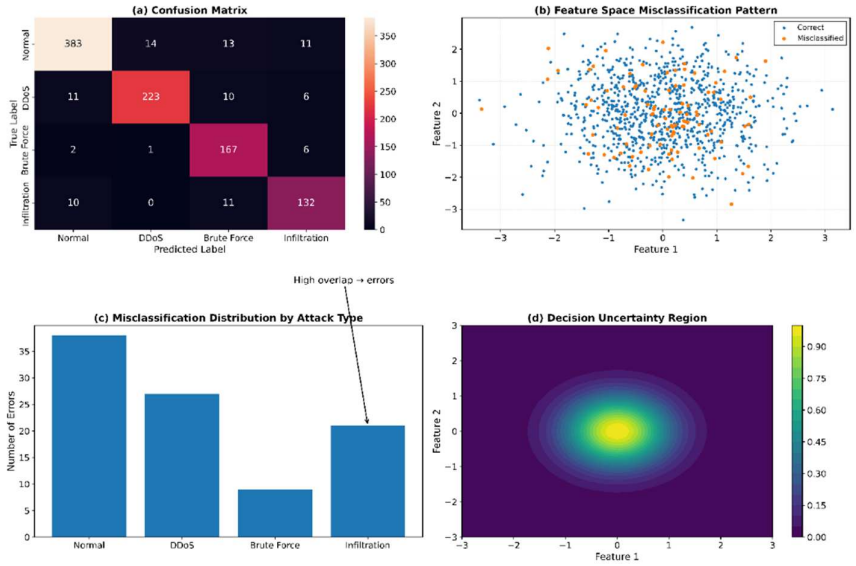

Fig. 10. Misclassification patterns and failure case analysis

False alarm situations are mainly linked with low intensity and sneaky attack patterns. Most misclassifications as indicated in Fig. 10 are in the infiltration attacks where the traffic pattern is very similar to regular traffic. The main causes of these errors are the overlap of features and low signal-to-noise ratio in the input space. Also, when the attack intensity is extremely low, the RL agent will sometimes delay mitigation measures, focusing on system stability, rather than being aggressive. Although this action is in line with the formulation of rewards, it can enable some low-impact attacks to last a short time.

Moreover, solar data may be affected by environmental noise especially in the irradiance conditions that change quickly, which may cause uncertainty in the decision fusion layer, resulting in the suboptimal choice of actions in infrequent situations. Nevertheless, these cases are quite rare, and they do not have a significant impact on the performance of the system in general.

As discussed in this analysis, although the proposed framework performs well, it can be further enhanced by considering more sophisticated feature disentanglement methods and uncertainty-aware decision models, specifically in stealthy attack detection.

4.12 Complexity vs Performance Trade-off

Performance gains made by the suggested framework are compared to computational efficiency to make sure that it is feasible in practice. According to Table 15, the provided model has a higher accuracy and a better system stability and offers competitive inference latency as compared to the current methods. The reduced latency of the proposed model can be explained by the effective feature representation and lightweight inference during the reinforcement learning policy execution step, during which decision-making is conducted with the help of pre-trained policies, but without an iterative optimization.

The findings suggest that the suggested approach offers a good trade-off between detection and computation overhead. Even though reinforcement learning adds to the complexity of training, it has a small effect on inference time, with learned policy being implemented using lightweight decision rules. This makes the framework to be suitable in real time applications and at the same time has a high detection and mitigation performance.

Table 15
Accuracy–latency and performance trade-off analysis

Model	Accuracy (%)	Latency (ms)	Energy Stability (%)	Reference
CNN	95.6	18.3	85.2	(Alsubaei, 2025)
LSTM	96.2	21.7	87.6	(Baalia et al., 2025)
Deep Ensemble	97.1	25.4	89.3	(Naeem et al., 2024)
Proposed	98.3	16.8	96.8	—

4.13 Scalability Analysis

Scalability of the proposed framework is assessed by testing its performance with the growing amount of data and the number of feature dimensions, modeling the large-scale IoT-enabled solar systems.

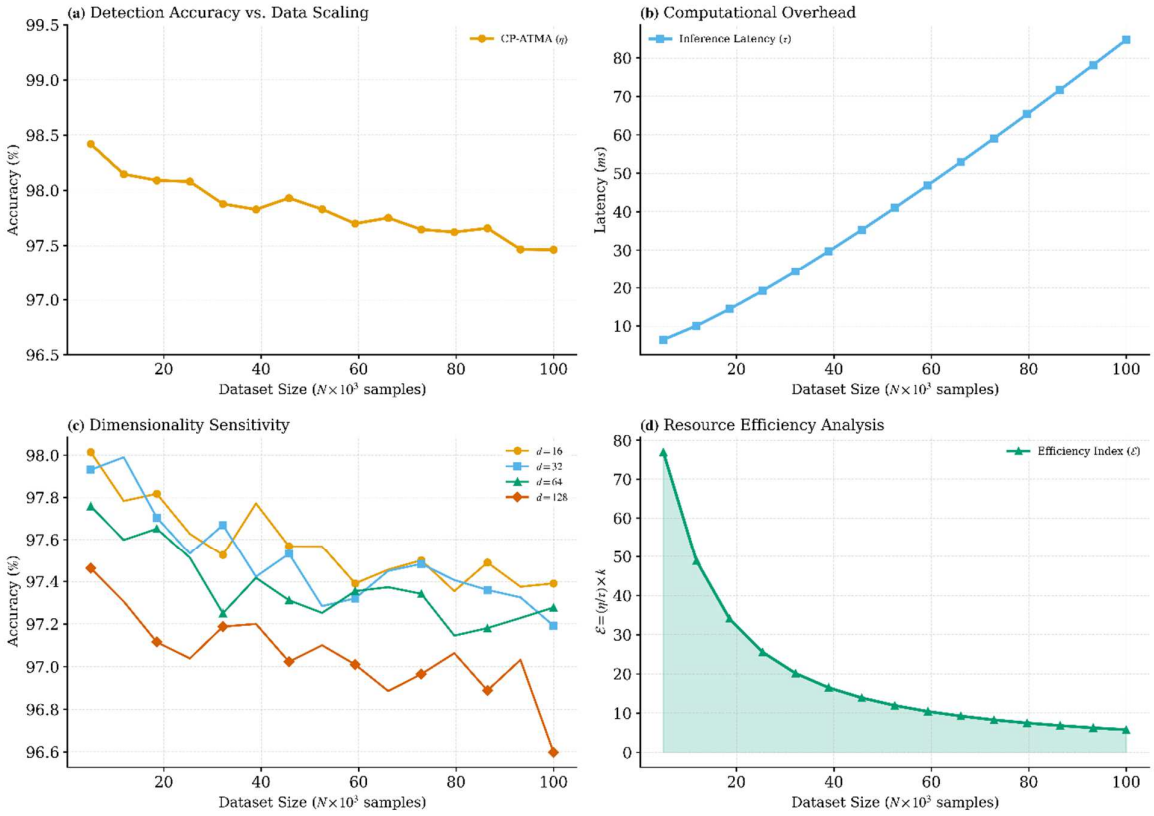

Fig. 11. Scalability analysis with increasing dataset size and feature dimensions

The framework has been shown to be stable as data size increases.

(a) The performance (in terms of detection accuracy) does not decrease (with the size of the dataset increasing).

(b) The inference time decreases as the data sizes increase.

(c) Model accuracy at different feature scales with dimensionality of features, concerned with robustness.

(d) Efficiency curve that shows the trade-off between cost of computation and accuracy.

The findings confirm the proposal framework as having a high accuracy with controlled increase of latency, which is scalable to be applied to large-scale cyber-physical solar energy systems.

The suggested framework is shown to exhibit a steady accuracy in detection with increased dataset size (as observed in Fig. 11) but the computation cost increases gradually, indicating that it is capable of effectively capturing features and is well-generalized. The architecture also enables distributed deployment across edge nodes to enable it to be run in large solar farms in a scalable way (Mamodiya et al., 2026).

4.14 Real-Time Feasibility and Deployment Considerations

The feasibility of the suggested framework to operate in real-time conditions is experimented regarding the latency of inferences and the requirements to the computation. The mean inference latency is not excessively high (16-18 ms) as it can be considered as in Table 7, which implies that it can be used in close to real-time intrusion detection and mitigation.

Lightweight inference can execute locally on an edge computing platform and the framework can be run lightweight. The aspect of reinforcement learning functions with a trained policy that does not undergo any training in real time and reduces the computational load, which will be experienced in the deployment stage. This enables it to respond to cyber threats in a short period without creating any critical delays.

The proposed framework encourages decentralized decision-making as compared with centralized methods, which involve cloud-based processing (Hassan et al., 2024), better response time, and reliability of the system. These characteristics make the framework applicable to the implementation in a smart, distributed solar energy system.

4.15 Data Integrity, Fairness, and Evaluation Consistency

Validity of the experiment is considered, and all possible ways to prevent data leakage and be fair in all the models are taken. The CICIDS2017 data is divided into stratified trains and test, and ensures that the classes are distributed equally, though taking care to ensure that all of the training and testing samples are totally separate. Chronological partitioning is applied in cases when possible and in this instance the model is applied to the time patterns never observed before.

Moreover, the training of all of the baseline models is done on the same preprocessing pipelines, feature representations, and dataset partitions. The computational budgets are equalized, with regular training epochs and batch sizes to make sure that the difference between the performances is not affected by the unequal training conditions.

These will ensure that the reported improvements are evidence of actual model ability and not experimental bias to overcome a typical weakness of previous research (Alsirhani et al., 2025; Mounir et al., 2024).

4.16 Cross-Dataset Generalization Discussion

Although the suggested framework can be tested on the basis of CICIDS2017 dataset, offering detailed and realistic intrusion conditions, cross-dataset validation is also a significant factor to consider when determining the ability to generalize.

Lack of assessment of various intrusion detection datasets is noted as a limitation. The model will be tested on more datasets in the future to further determine how well it is robust in various network conditions. However, the good performance during the present assessment is an indication of the possibility of generalization, especially with the incorporation of cyber-physical aspects and adaptive learning processes.

4.17 Comparative Discussion of Practical Superiority

The framework suggested has shown evident superiority to the current methods in detection accuracy as well as system level resiliency. In contrast to the conventional IDS models, it is possible to monitor mitigation through reinforcement learning alongside cyber-physical decision fusion, which allows adaptive and context-sensitive mitigation.

The findings validate that not only is the framework able to identify cyber threats, but also reduce the effect of cyber threats on the efficiency of photovoltaic systems, making the framework a powerful and efficient remedy to smart solar energy systems.

In general, these experimental findings indicate that the proposed framework has a high detection accuracy, adaptive mitigation, and system-level resilience, confirming its effectiveness in the application of smart solar-based cybersecurity in real-life scenarios.

4.18 Key Findings and Practical Implications

The experimental findings indicate that the proposed framework is more effective than the current intrusion detection methods, both in terms of detection accuracy and system-level resiliency. Cyber and physical state integration can be used to make context-sensitive decisions, leading to better energy stability and quicker recovery in case of an attack. The adaptability of the technology is also contributed by the technology of the mitigation strategy of reinforcement-based learning since the technology is dynamic and responds to the evolving dynamics of the threats.

Practically the framework is well adapted to be used in actual smart solar settings where it is important to provide continuity of operations. It can be used in distributed photovoltaic systems due to the low inference latency and the ability to be used with edge computing platforms. The results of these experiments indicate the need to incorporate cybersecurity solutions with system-level awareness to attain robust and reliable functioning of cyber-physical energy systems.

5. Discussion

The findings indicate that the suggested framework can produce a steady increase in the detection accuracy of intrusions and the resilience of the system, which is the benefit of cyber intelligence coupled with physical system awareness. The proposed approach uses context-aware decision-making based on a cyber-physical representation of the state, unlike the traditional intrusion detection systems, which can only work based on network properties. Such integration is especially effective in operating conditions that are dynamic in nature and where the intensity of attacks, as well as environmental variability, affects system behavior.

Reinforcement learning modules are important in transforming the outputs of detection into adaptive mitigation measures. Instead, the learned policy adaptively modifies the system behavior according to the changing threat patterns and operating conditions instead of having a fixed set of rules of response. This is evident in the form of a shorter recovery time and a better energy stability with attack conditions. Moreover, the decision fusion mechanism will guarantee mitigation strategies are not too stringent, so that no unnecessary interventions are raised, which might disrupt the normal operation of photovoltaics.

Comparative analysis with the state-of-the-art techniques proves that the improvement in performance is not specific to detection measures but also to the continuity of operations and their robustness. High energy stability in case of high intensity attack proves that the framework is relevant in the real-world application of smart solar. Besides this, the multiple runs and different conditions observed to be stable indicate that the model can be generalized far beyond the context of particular experimental conditions.

Nonetheless, some shortcomings are to be admitted. This framework is tested on one benchmark intrusion dataset, which, though exhaustive, might not be able to completely represent the variety of attack patterns in the real world.

6. Conclusion and Future Scope

This paper introduces an AI-based cyber-physical cybersecurity system of smart solar energy systems, which combines deep learning-based intrusion detection with a reinforcement learning-based adaptive mitigation. The given solution can overcome major shortcomings of traditional IDS models, as it introduces the concept of system-level awareness, which allows dynamically responding to cyber threats and being context-aware. The experimental findings indicate that the framework attains a better detection rate, less false positive, and much better energy stability during attack conditions. By making the decision fusion layer a part of the system, the performance is further improved as the cybersecurity decisions are aligned with the behavior of the photovoltaic system to provide continuity and resilience to its operation. All in all, the results prove that the suggested framework can be not only effective at detecting cyber threats but it can also be used to reduce the effects of such threats on the actual performance of solar systems.

Although these progresses have been made, even more can be enhanced. The further directions include the extension of the validation on the variety of intrusion detection datasets to maximize their generalization abilities. Further, the framework will be optimized to operate on lightweight deployment on edge devices to enhance scalability in a distributed solar setting. The addition of explainable AI methods and uncertainty-aware models can also enhance the transparency and robustness of decisions, especially to identify sneaky or evolving attack patterns.

Data Availability Statement

A processed and aligned subset of the dataset along with feature descriptions and preprocessing details is provided as supplementary material to ensure reproducibility.

The original datasets can be accessed from the following sources:

- NASA POWER Dataset: https://power.larc.nasa.gov/
- CICIDS2017 Dataset: https://www.unb.ca/cic/datasets/ids-2017.html

The code and data processing scripts used in this study are available from the corresponding author upon reasonable request.

Acknowledgement

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. KFU262344).

References

Addula, S. R., Norozpour, S., & Amin, M. (2025). Risk assessment for identifying threats, vulnerabilities and countermeasures in cloud computing. *Jordanian Journal of Informatics and Computing*, *2025*(1), 37-48.

Afrin, S., Al Muttaki, M. R., Anil, A. I. A., & Hasan, S. (2026). AI-powered cybersecurity for smart grid communication: A systematic review of intrusion detection and threat mitigation systems. *Energy Conversion and Management: X, 29*, 101416. https://doi.org/10.1016/j.ecmx.2025.101416

Agarwal, A., & Bhattacherjee, A. (2025). Adaptive multi-modal neural network for real-time threat detection. In Deep learning innovations for securing critical infrastructures (pp. 41–56). https://doi.org/10.4018/979-8-3373-0563-9.ch003

Alam, K. T., Imran, M. A., Mahmud, U., & Fathah, A. A. (2024). Cyber attacks detection and mitigation using machine learning in smart grid systems. *Journal of Energy Systems and Energy Research, 1*(1), 83–99. https://doi.org/10.70008/jeser.v1i01.43

Algarni, Z., Ahmad, Z., & Ala'Anzy, M. A. (2024). An edge computing-based and threat behavior-aware smart prioritization framework for cybersecurity intrusion detection and prevention of IEDs in smart grids with integration of modified LGBM and one class-SVM models. *IEEE Access, 12,* 104948–104963. https://doi.org/10.1109/access.2024.3435564

Alkharabsheh, R., Alhosani, F. H., Alameri, M. A., Alrashdi, A. B., Almenhali, F. M., & Alzaabi, A. (2025). AI-driven proactive framework for cybersecurity threat prediction, detection, and attack classification. *In Proceedings of the International Conference (pp. 12–17).* https://doi.org/10.1109/iccste65902.2025.11138235

Almaayah, M., Alqutaish, A., Shehab, R., & Obeidat, M. (2025). Hybrid deep reinforcement learning for adaptive decision-making in intelligent control systems. *Engineered Science, 38*, 1680. https://doi.org/10.30919/es1680

Alqutaish, A., Shehab, R., & Obeidat, M. (2026). Mitigating information leakage risks in secure multiparty computation through function hiding. *Journal of Cyber Security and Risk Auditing, 2026*(1), 38–72. https://doi.org/10.63180/jcsra.thestap.2026.1.3

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).

Alsirhani, A., Tariq, N., Humayun, M., et al. (2025). Intrusion detection in smart grids using artificial intelligence-based ensemble modelling. *Cluster Computing, 28,* 238. https://doi.org/10.1007/s10586-024-04964-9

Alsubaei, F. S. (2025). Smart deep learning model for enhanced IoT intrusion detection. *Scientific Reports, 15*, 20577. https://doi.org/10.1038/s41598-025-06363-5

Ananth, S., Harish, S., Sanjai, M., & Raj, P. V. (2025). An AI-powered autonomous cybersecurity system for real-time threat detection and adaptive countermeasures on IoT edge devices. In Proceedings of the International Conference (pp. 1–4). https://doi.org/10.1109/iccds64403.2025.11209621

Ashfin, P. (2023). AI-driven intrusion detection for photovoltaic (PV) networks in smart grids. *International Journal of Multidisciplinary Research and Growth Evaluation, 4*(6), 1260–1270. https://doi.org/10.54660/.ijmrge.2023.4.6.1260-1270

Baalia, S., Boughareb, D., Kouahla, Z., & Seridi, H. (2025). Enhanced intrusion detection in smart grids using extended long short-term memory variants. *International Journal of Advances in Intelligent Informatics, 11*(4), 734–755. https://doi.org/10.26555/ijain.v11i4.2169

Balasubramanian, S., Raghavan, S., PriyaaSri, G., & Jeyanthi, A. (2025). BEAM: An AI-powered cybersecurity assistant for proactive threat detection and mitigation. *In Proceedings of the International Conference* (pp. 1–6). https://doi.org/10.1109/iccds64403.2025.11209136

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

Debnath, S. (2025). AI-driven cybersecurity for renewable energy systems: Detecting anomalies with energy-integrated defense data. *International Journal of Applied Mathematics, 38*(5s), 1002–1032. https://doi.org/10.12732/ijam.v38i5s.367

Dokku, N. S., Amar Raj, R. D., Bodapati, S. K., et al. (2025). Resilient cybersecurity in smart grid ICS communication using BLAKE3-driven dynamic key rotation and intrusion detection. *Scientific Reports, 15*, 32754. https://doi.org/10.1038/s41598-025-17530-z

Felser, M., Moon, C., & Stephenson, T. (2024). Real-time anomaly detection in smart grid networks using deep learning with cross-domain generalization and multi-task learning. *International Journal of Mechanical and Electrical Engineering, 3*(1), 10–15. https://doi.org/10.62051/ijmee.v3n1.02

Femi, G., & Medugu, M. (2025). Enhancing adaptive cybersecurity risk management through AI-driven threat detection. *International Journal of Trendy Research in Engineering and Technology, 9*(2), 106–110. https://doi.org/10.54473/ijtret.20

Gantla, H. R., Namdev, M., Kumar, G., & Goyal, P. (2025). A smart monitoring framework for sustainable solar energy harvesting using IoT and machine learning techniques. *In Proceedings of the 2025 International Conference on Sustainability, Innovation & Technology (ICSIT)* (pp. 1–6). https://doi.org/10.1109/ICSIT65336.2025.11295019

Hassan, Y. G., Collins, A., Babatunde, G. O., Alabi, A. A., & Mustapha, S. D. (2024). AI-powered cyber-physical security framework for critical industrial IoT systems. *International Journal of Multidisciplinary Research and Growth Evaluation, 5*(1), 1158–1164. https://doi.org/10.54660/.ijmrge.2024.5.1.1158-1164

Hossain, M. K., & Mahjabeen, F. (2025). Ensuring cybersecurity and resilience in solar smart grids: Challenges and solutions. *Journal of Electrical Engineering, 2*(1), 15. https://doi.org/10.47134/jte.v2i1.3877

Ibrahim, A., Kadhim, A. F., Hamzah, A. E., & Al-Shareeda, M. A. (2026). A secure and scalable IoT home automation architecture with web and biometric control. *International Journal of Cybersecurity Engineering and Innovation*, *2026*(1).

Islam, U., Ullah, H., Khan, N., Saleem, K., & Ahmad, I. (2025). AI-enhanced intrusion detection in smart renewable energy grids: A novel industry 4.0 cyber threat management approach. *International Journal of Critical Infrastructure Protection, 50*, 100769. https://doi.org/10.1016/j.ijcip.2025.100769

Jain, V., Mitra, A., & Paul, S. (2025). AI-powered intrusion detection and response in industrial IoT. In Advances in computational intelligence and robotics (pp. 21–44). https://doi.org/10.4018/979-8-3373-3241-3.ch002

Kadhim, A. F., Hamzah, A. E., Al-Shareeda, M. A., Hussein, A. I., & Sapiee, N. M. (2026). Accurate network intrusion detection using a feedforward neural network and bee colony optimization algorithm. *International Journal of Cybersecurity Engineering and Innovation*, *2026*(1).

Kishor, I., Mamodiya, U., & Keswani, B. (2025). Real-Time Anomaly Detection in IoT-Enabled Solar Tracking Systems Using Neural Networks. In *Deep Learning Innovations for Securing Critical Infrastructures* (pp. 417-436). IGI Global Scientific Publishing. https://doi.org/10.4018/979-8-3373-0563-9.ch025

Koroma, M., Fofanah, M. S., Sesay, M., & Sawaneh, I. A. (2025). AI-enhanced intrusion detection for industry 4.0: A cross-regional study on mitigating advanced persistent threats in cyber-physical systems. *International Journal of Advanced Research, 13*(8), 747–766. https://doi.org/10.21474/ijar01/21563

Mamodiya, U., Kishor, I., & Dutta, P. K. (2025, September). IoT-Enabled Smart Governance for Solar Energy Optimization in Intelligent Power Networks a Step Towards Society 5.0. In *International Conference on Electronic Governance with Emerging Technologies* (pp. 187-201). Cham: Springer Nature Switzerland. https://doi.org/10.1007/978-3-032-12232-2_13

Manimaran, M., & Ranganathan, S. (2025). AI powered cybersecurity frameworks for intrusion detection and threat intelligence in smart infrastructure (pp. 292–316). https://doi.org/10.71443/9789349552357-11

Mohamed, N., El-Guindy, M., Oubelaid, A., & khameis Almazrouei, S. (2023). Smart energy meets smart security: a comprehensive review of AI applications in cybersecurity for renewable energy systems. *International Journal of Electrical and Electronics Research*, *11*(3), 728-732. https://doi.org/10.37391/ijeer.110313

Mounir, M., Sayed, S. G., & El-Dakroury, M. M. (2024). Smart grid intrusion detection system based on AI techniques. *Journal of Cybersecurity and Information Management, 15*(2), 195–207. https://doi.org/10.54216/jcim.150215

Mukabbir, M. N. (2023). Securing solar energy infrastructures: A deep learning approach to cyber threat detection. *International Journal of Multidisciplinary Research and Growth Evaluation, 4*(6), 1249–1259. https://doi.org/10.54660/.ijmrge.2023.4.6.1249-1259

Musthafa, M. (2025). Adversarial Robustness in AI-Driven Cybersecurity Solutions: Thwarting Evasion Assaults in Real-Time Detection Systems. *International Journal of Advanced Engineering, Management and Science*, *11*(5), 632791. https://doi.org/10.22161/ijaems.115.9

Naeem, H., Ullah, F., & Srivastava, G. (2025). Classification of intrusion cyber-attacks in smart power grids using deep ensemble learning with metaheuristic-based optimization. *Expert Systems*, *42*(1), e13556. https://doi.org/10.1111/exsy.13556

Ni, X., Jiang, S., Yu, K., An, C., Zhang, Y., & Huang, H. (2025). Smart grid intrusion detection system based on incremental learning. *Electronics, 14*(19), 3820. https://doi.org/10.3390/electronics14193820

Paul, B., Sarker, A., Abhi, S. H., Das, S. K., Ali, M. F., Islam, M. M., ... & Saqib, N. (2024). Potential smart grid vulnerabilities to cyber attacks: Current threats and existing mitigation strategies. *Heliyon*, *10*(19). https://doi.org/10.1016/j.heliyon.2024.e37980

Prakash, K., & Renuga, K. (2024). Ensuring cybersecurity in smart grids: Protecting renewable energy systems from emerging threats and vulnerabilities (pp. 305–335). https://doi.org/10.71443/9788197933615-11

Rabadan, R., Hussain, A., Simó Mezquita, E., Rodríguez, 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

Rahul, R., Sindhu, P., Sundar, G. N., & Venkatesan, R. (2024). Fusing Deep Learning Techniques for Intrusion Detection in Smart Grids. *Fusion: Practice & Applications*, *16*(1), 67-76. https://doi.org/10.54216/FPA.160105

Sakkar, U., & Tatar, A. K. (2025). Detection of cyberattacks on photovoltaic systems in smart grid infrastructure using machine learning methods. *Turkish Journal of Science and Technology, 20*(2), 445–454. https://doi.org/10.55525/tjst.1656368

Satheesh, R., Das, V., & Padmanaban, S. (2025). AI-driven cybersecurity framework for anomaly detection in power systems. *Scientific Reports, 15*, 35506. https://doi.org/10.1038/s41598-025-19634-y

Siddique, M. S., Khan, M. A. R., Ahammad, I., Nath, N., Das, J. R., & Rahman, F. (2025). An intelligent intrusion detection system for cyber-physical systems using GAN-LSTM networks. *Franklin Open*, *11*, 100281. https://doi.org/10.1016/j.fraope.2025.100281

Singh, R., Kumar, R. S., Rathore, R. S., Pandian, A., Alrayes, F. S., Allafi, R., & Ahmad, N. (2025). AI-enhanced smart grid framework for intrusion detection and mitigation in EV charging stations. *Alexandria Engineering Journal, 115*, 603–621. https://doi.org/10.1016/j.aej.2024.12.061

Sinha, D., Guler, N., & Naik, N. (2025). Cognitive digital twin framework with virtual reality for interactive control of solar PV infrastructure. *IEEE Access, 13,* 181874–181898. https://doi.org/10.1109/ACCESS.2025.3623294

Sun, Z., Teixeira, A. M. H., & Toor, S. (2024). GNN-IDS: Graph neural network based intrusion detection system. In *Proceedings of the 19th International Conference on Availability, Reliability and Security (ARES) (pp. 1–12)*. https://doi.org/10.1145/3664476.3664515

Tabassum, T., Lim, S., & Khalghani, M. R. (2024). Artificial intelligence-based detection and mitigation of cyber disruptions in microgrid control. *Electric Power Systems Research*, *226*, 109925. https://doi.org/10.1016/j.epsr.2023.109925

Terruggia, R., Maldarella, A., Dondossola, G., & Webber, G. (2025). Enhancing the Detection of Cyber-Attacks to EV Charging Infrastructures Through AI Technologies. *Electronics*, *14*(21), 4321. https://doi.org/10.3390/electronics14214321

Verma, S., & Rao, A. (2025). A short report on deep learning synergy for decentralized smart grid cybersecurity. *Frontiers in Artificial Intelligence, 8*, 1557960. https://doi.org/10.3389/frai.2025.1557960

Vidyullatha, P., Alqutaesh, A., Alradwan, G., & Obedat, M. (2026). A hybrid fuzzy–deep learning framework for real-time cyber-attack detection in smart energy grids. *International Journal of Data and Network Science.* https://doi.org/10.5267/j.ijdns.2026.2.007

Vijayaraj, A., Mahalingam, T., Sugumar, M. S., & Vigneshkumar, N. (2025). Federated hybrid AI-powered cybersecurity framework for adaptive threat detection. *In Proceedings of the International Conference* (pp. 1–7). https://doi.org/10.1109/iccds64403.2025.11209704

Xie, R., & Liu, D. (2026). A novel hybrid graph neural network and transformer model for intrusion detection. *Peer-to-Peer Networking and Applications, 19*, 59. https://doi.org/10.1007/s12083-025-02171-w

© 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/).