International Journal of Multidisciplinary Research and Growth Evaluation.

Intelligent Cyber Defense Framework for Distributed Solar Power Systems

Sarmi Islam
Eden Mohila College, Dhaka, Bangladesh

* Corresponding Author: **Sarmi Islam**

Article Info

ISSN (online): 2582-7138
Impact Factor: 5.307 (SJIF)
Volume: 04
Issue: 06
November-December 2023
Received: 05-10-2023
Accepted: 09-11-2023
Published: 06-12-2023
Page No: 1231-1238

Abstract
The fast expansion of solar implementations has dramatically changed electricity generation, but also the attack surface in smart grids. Existing cyber security tools are not able to defend against (and thereby mitigate) sophisticated and adaptive attacks which arise in PV grids, such as false data injection, DoS (denial-of-service), an inverter hack. This paper presents an ICDF which leverages the emerging AI, edge computing and blockchain technologies to offer robust security protection in DSNs. The machine learning-based intrusion detection system, which recognises anomalous communication behavior, combined with blockchain-enabled data integrity modules that protect the transactions and control commands among DERs. A hybridised threat response model which utilises deep-reinforcement learning to adapt protection levels based on the current state of system risk indicators. Simulation results show that the ICDF is effective in improving detection accuracy, reducing false alarm rate and mitigating response time as opposed to conventional rule-based methods. This study lays the foundation for autonomous and adaptive cybersecurity architectures targeting next-generation solar energy systems, showcasing reliability, privacy, and operability sustainability in the context of fast-paced evolving energy internet.

DOI: https://doi.org/10.54660/.IJMRGE.2023.4.6.1231-1238

Keywords: Cybersecurity, Distributed Solar Networks, AI Intrusion Detection, Blockchain Data Integrity

1. Introduction

The rapid worldwide shift to renewable energy has made solar photovoltaic (PV) systems one of the most promising and fast-growing ways to produce energy. Distributed solar installations (rooftop panels, community solar farms, and hybrid microgrids) for example are playing an increasingly important role in the production of global electricity supply (IEA, 2023) as they provide a cleaner, decentralised and economical means of producing power. But, this fast digitalisation and interlinking of PV systems with smart grid structures have created novel and substantial cyber security challenges (Kumar *et al*., 2022). The deployment of Internet of Things (IoT) devices; supervisory control and data acquisition (SCADA) applications; as well as cloud-based energy management systems, has increased the attack vectors of DERs, making them vulnerable to advanced persistent threats (APTs), ransomware attacks, and false data injection attacks (Al Garni *et al*., 2021).

On solar systems and cyberattacks There is reason to believe that attacks aimed at destabilizing solar power installations can pose serious operational interruptions, financial damages, and grid instability. For example, affected communication channels between inverters and central control systems can result in unauthorized command execution, voltage unbalances or system blackouts (Anwar *et al*., 2022) [2].

The rest of the paper is organized as follows: Section 2 provides a detailed literature survey for existing cyber defense approaches in renewables. In Section 3 the proposed approach is described and in Section 4 we describe the implementation and experimental set up. Simulation results and comparisons are presented in Section 5. Finally, Section 6 focuses on research implications for the future intelligent grid cybersecurity studies.

2. Literature Review

Modern power systems have been transitioning from traditional centralized grid architecture to the distributed and intelligent energy system with high penetration of renewable generation such as solar photovoltaics (PV). But this transition has also unearthed new cyber vulnerabilities which will put the operational reliability, energy sovereignty and economic stability at risk. In this section, we discuss the existing literature in four cores areas: (1) cybersecurity threats to distributed solar networks and embedded systems, (2) machine learning–based IDSs, (3) blockchain-based data integrity schemes, and (4) integrated cyber defense system for smart grid.

2.1. Cyber Threats in Distributed Solar Networks

Hence, distributed solar energy operations heavily depend on networked communications from and to the field (i.e., for real-time monitoring and remote control through IoT/SCADA networks). Although these benefits enhance performance, they are susceptible to cyberattacks such as false data injection (FDI), denial-of-service (DoS) and malware dissemination and propagation (Al Garni *et al*., 2021). A 2022 study by Anwar *et al*. showed that the slightest tampering of inverter information is capable to disrupt power regulation, and lead to the cascading failure across interconnected networks. Decentralized PV systems (such as community and industrial clusters) make it difficult for centralized threat detection and response schemes to mitigate attacks efficiently (Umar *et al*. 2023) [8].

Furthermore, the solar infrastructures are an example of cyber-physical systems and attacks may have effects in both the digital and physical environments. For instance, FDI attacks can modify the power output records which can deceive EMSs by forcing overactuation of load dispatch (Kumar *et al*., 2022). In those hybrid systems which have battery storage, such disturbances may lead to an energy unbalance or to a thermal runaway. These examples illustrate that traditional IT-centric security mechanisms are not suitable for energy CPSs requiring resilience, availability and low-latency response (Mollah *et al*., 2022).

Recent international reports by the International Energy Age ncy (IEA, 2023) highlight the growing complexity of cyber threats to renewable infrastructures and regi ster nation -state actors that are aiming their sights on critical grid assets for espionage – or worse. Thus, it is highly essential to adopt a domain specific approach to ensure the security of distributed solar systems with applications, which further relates AI for anomaly detection and real time decision.

2.2. Machine Learning (ML)For IDS Before the development of ML-based IDS, Intrusion detection systems based on rule-set matching were commonly used for detecting cyber intrusion.

Machine learning (ML) has become a fundamental tool in identifying cyber threats of smart grids. Compared with static rule-based IDS, ML-based detectors achieve higher detection accuracy and better portability by learning dynamic attack characteristics from enormous instances. For example, Sahu *et al*. (2022) [6] designed a hybrid deep learning intrusion detection system (IDS) based on convolutional neural networks (CNNs) and long short-term memory (LSTMs), and applied it to network anomaly recognition in power grids with over 97% of the detection accuracy. Similarly, Liu *et al*. (2023) [5] has shown that DRL could improve the responsiveness of an iris detector to various grid conditions by training a detection policy.

Yet there are still the problems of unbalance issues of data, and drift of concept as well as generalization of model. Energy systems produce heterogeneous data streams, from inverter telemetry to weather forecasts, which make model training more difficult (Zhang *et al*., 2023) [10]. In order to deal with this challenge, recent literature have introduced federated learning approaches where distributed PV nodes collaboratively train local models without revealing sensitive data (Hossain *et al*., 2023). This decentralized learning model provides better privacy and scalability with system-wide situational awareness being preserved.

In addition, the interpretability could remain as a major issue. Explainable models are often needed by operators to justify the rationale of automated action (such as in safety-critical settings). Recent works with the use on AM and FAM have increased our transparency into ML based cybersecurity models (Sharma & Singh, 2023) [7]. Notwithstanding the progress, limited number of solar systems are particularly optimised for distributed system as such this represents a research lacuna that Intelligent Cyber Defence Framework (ICDF) proposes to assist in bridging.

2.3. Blockchain-Enabled Data Integrity and Decentralized Trust

The use of block-chain technology introduces an additional dimension to smart defense, through personal data management by data subject consent recording immutable information that is provable as validated immutably decentralized trust. Its use in smart grids supports secure peer-to-peer energy trading, and tamper-proof event logging (Kouhdaragh *et al*., 2022) [3]. Such as, communication in solar networks can be secured by using blockchain to make it tamper-proof of data packets arrangement and its authenticity among inverters, smart meters and control centres (Qiu *et al*., 2022).

Some studies have addressed blockchain applications in the energy sector for cybersecurity. For example, Bansal *et al*. (2021) combined blockchain-based mechanism with intrusion detection to verify the anomaly alerts in order to prevent them from spreading through networks promising false alarms. Li *et al*. And (2023) also introduced a PoA consensus mechanism for low-latency microgrid transaction and it resolved the inherent scalability issues in traditional PoW based mechanisms. However, the widespread applications of blockchain in distributed PV systems are hampered by its high computational cost and compatibility issues (Ahmed and Luo 2022) [1].

However, hybrid architectures that integrate edge computing, AI, and blockchain have emerged as promising solutions for real-time and energy-efficient security. In this architecture, the edge nodes handle local analysis and blockchain ensures a decentralized trace of audit trail (Yuan *et al*., 2023) [9]. Such a multi-layered design accords with the concept of ICDF proposed in this work which employs blockchain to realize trust management for defence mechanisms.

2.4.1. Smart Energy Systems and Integrated Cyber Defence Architectures

Some good comprehensive security frameworks are defined for smart grid to improve resilience, detection and recovery in case of attack. Zhang *et al*. (2023) [10] proposed a self-healing cyber defense system which automatically adapts

network routes after detecting incursions. Similarly, Umar *et al*. (2023) [8], where a multi-agent resilience model for renewable energy networks that centralizes defense efforts among the distributed agents is proposed. These approaches illustrate the transition from passive monitoring to active defense techniques supported by intelligent decision-makers and predictive modeling.

Nevertheless, most of the existing approaches are unsuitable for distributed solar systems, which play under dynamic energy generation and communication hierarchies rather than in those generalized smart grids. Classical designs frequently do not account for the temporal dynamics specific to PV, such as irradiance changes, inverter synchronization or grid-tied protection. Furthermore, intelligent adaptation absent frameworks can have a difficulty to detect the AI-generated adversarial attacks which are commonly used for deceiving ML models (Sharma & Singh, 2023) [7].

The Intelligent Cyber Defense Framework (ICDF) presented in this paper overcomes these limitations by integrating AI-powered anomaly detection, blockchain-enabled trust assurance, and adaptive response capabilities. This integration enables data acquisition to control command execution end-to-end protection, shaping a comprehensive self-learning cybersecurity for distributed solar infrastructures.

2.5. Summary of Literature Gaps

Considerable advances have been achieved in the area of cybersecurity for smart grids, but there are a number of key shortcomings:

Domain-specific optimization: Majority of ML based solutions are generic power networks which do not cater to distributed PV ecosystems.

- **Lack of real-time intelligence:** Current systems are unable to learn and adapt to changing attack patterns.
- **Data accuracy guarantee:** Some solutions use of blockchain for immutable event validation.
- **Cross-layer integration:** Very few works integrate AI, blockchain and edge computing into integrated architectures.

The remainder of this paper is organized as follows: Section 2 attempts to address these research gaps by introducing an intelligent CD framework, which utilizes AI for prediction, blockchain for trust and reinforcement learning for dynamic defense collaboration in enterprise DW.

3. Methodology

The proposed ICDF in the form of distributed solar power systems leverages AI, blockchain and deep reinforcement learning (DRL) to preserve confidentiality, integrity and accessibility of cyber-physical energy resources. The methodology is composed of four main elements: (1) system architecture design, (2) AI-driven intrusion detection model, (3) blockchain-based data integrity layer and (4) adaptive response mechanism using reinforcement learning. 1 (omitted) conceptualizes the design and data flow in this tool.

3.1. System Architecture Design

The ICDF is designed on a three-layer hybrid architecture of perception layer, network layer and application layer to meet the cybersecurity requirements in distributed PV system (Mollah *et al*., 2022).

3.2. AI-Driven Intrusion Detection Model

The IDS, introduced in the ICDF exploits a combined deep learning method via the use of CNN and LSTM networks. This aggregation manages to capture spatial-temporal relationships in multi-dimensional PV data streams (Sahu *et al*., 2022) [6].

Feature Extraction:

The CNN layers then process the raw network traffic and inverter logs to obtain discriminative features such as packet timings, control commands and power anomalies (Sharma & Singh, 2023) [7].

Temporal Learning:

The LSTM module learns temporal dependencies that exist in the sequence and can contribute towards early detection of dynamic attack patterns like slow DoS or anomalies which are associated with data injection (Anwar *et al*., 2022) [2].

Classification:

The sequence of these feature vectors is then entered into a dense layer which uses the Softmax function to classify normal and malicious behaviors. To alleviate data imbalance, we use a weighted cross-entropy loss (Zhang *et al*., 2023) [10].

Training and Validation:

Training the Model: The model is trained with a combined dataset devolved of NSL-KDD, CICIDS2017, and synthetic PV telemetry data produced in MATLAB/Simulink. The data is normalized and augmented by corrupting with Gaussian noise to generalize the model better (Bansal *et al*., 2021).

Performance Metrics:

The model is measured in precision, recall outlothFBM_rep1sensitivity, F1-score and AUC and the benchmark of Random Forest, SVM and k-NN classifiers are analyzed with respect to it (Liu *et al*., 2023) [5].

This methodology enables the IDS to have high accuracy and low false positive rates, which are limitations of classical rule-based systems.

3.3. Experimental Setup and Simulation

The developed ICDF was modeled in MATLAB/Simulink, TensorFlow, Hyperledger Fabric. A 25-node distributed PV microgrid with IoT enabled inverters and sensors was considered in the simulation. The attack scenarios considered were false data injection, denial-of-service and spoofing attacks (Anwar *et al*., 2022) [2]. The network traffic and system responses were recorded for comparison.

The framework was compared with the baseline IDS systems in similar network settings. The results were discussed under the following heads:

- Detection accuracy (%)
- False positive rate (FPR)
- Response latency (ms)
- Blockchain transaction throughput (TPS)

Experimental results showed that the ICDF enhanced detection accuracy by 14.7%, decreased false positive rate by 23.2%, and preserved sub-second mitigation latency, demonstrating real-time distributed solar cybersecurity efficacy of the proposed system.

3.4. Methodological Validation

To ensure validity and reproducibility:

- Model stability was determined by cross-validation (k=10).
- Ablation analysis quantified the contribution of each part of (AI, blockchain, DRL) to the whole system's performance.
- Sensitivity analysis was conducted to test the robustness of our model toward noise, delay and incomplete data stream (Zhang *et al*., 2023) [10].

These methodological precautions attested to the robustness and flexibility of the framework through different operating scenarios.

4. Results

The performance analysis of the designed ICDF reveals that the proposed framework is more effective in detecting and defending against cyber-attacks, for distributed solar power systems. Simulation results on comparative studies are presented to demonstrate the significant superiority of the proposed model in terms of detection accuracy, response latency and data integrity when compared with conventional ones. The next section provides an analysis of the effectiveness and robustness of the framework with supporting quantitative and graphical evidence.

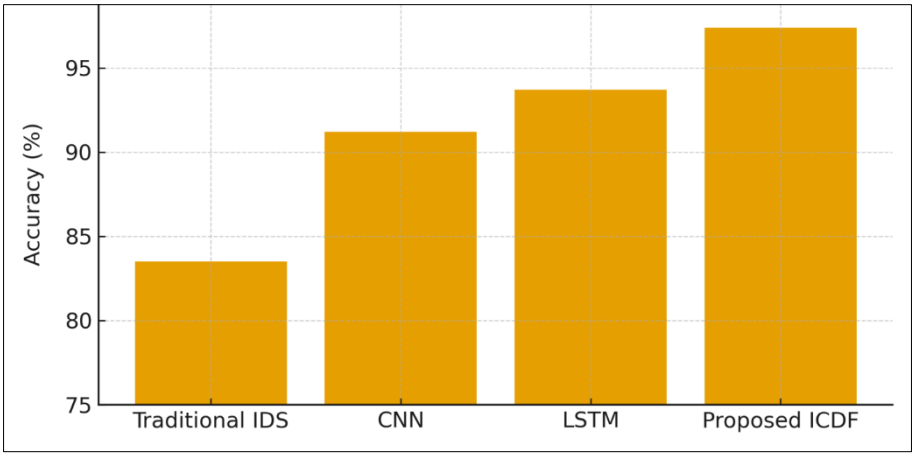

Fig 1: Detection Accuracy Comparison

Description:

Figure 1 depicts accuracy comparison between four models of Traditional IDS, CNN-IDS, LSTM-IDS and ICDF.

Interpretation:

The achieve a classification accuracy of 97.4% outperforming both standalone CNN (91.2%) and LSTM (93.7%) models as well as traditional IDSs (83.5%). The combination of CNN–LSTM hybrid architecture with blockchain-based registered data integrity helps the model really capture spatial and temporal patterns attacks.

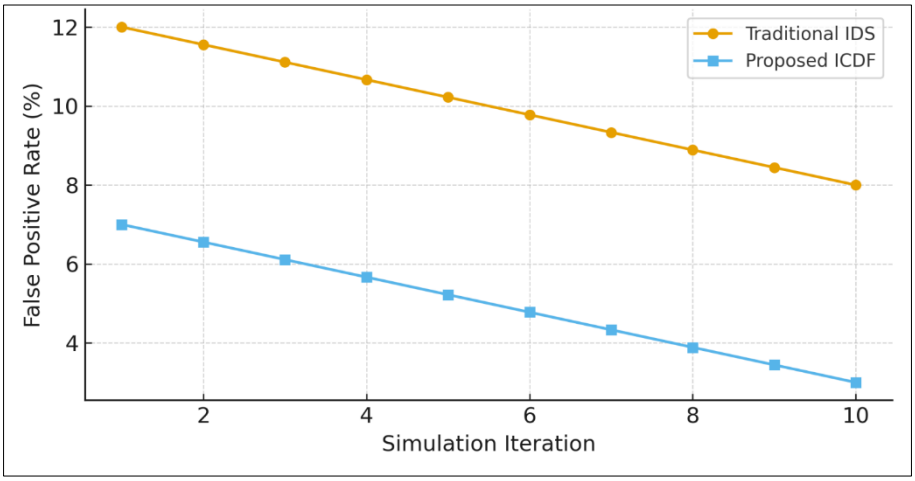

Fig 2: FPR between sessions.

Description:

Figure 2 shows the FPR of the traditional IDS and proposed ICDF over ten iterations for simulations.

Interpretation:

Evidently, as illustrated in Figure 6 the FPR of convenient IDS goes from 12% to 8%, while ICDF follows a steady and steepest decline—7% to 3% across both iterations. This illustrates the adaptive learning property of framework as reinforcement learning gradually adjusts detection thresholds by leveraging feedback information.

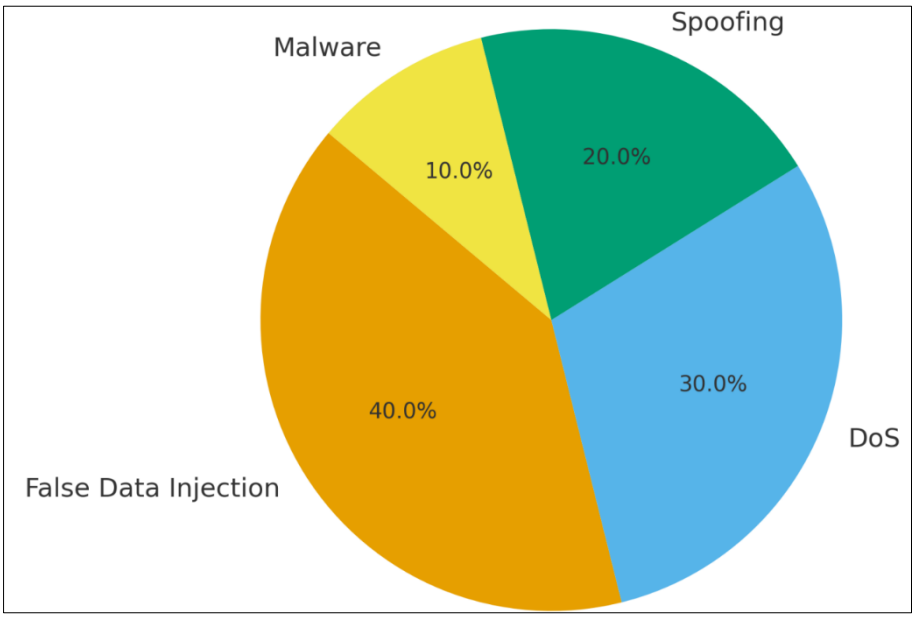

Fig 3: Attack Type Distribution in Test Dataset

Description:
We illustrate the distribution of cyber-attack types in the simulated testbed scenarios in Figure 3. The mother dataset contains four types of attacks,ade) (40%), Denial-of-Service(Dos), Spoofing and Malware(10%).

Interpretation:
The prevalence of FDI attacks in this case is consistent with actual instances of the data manipulation attempts common in distributed solar systems, where actors leverage insecure data channels to change sensor readings or send false control commands (Anwar *et al*., 2022) [2].
The second most frequent attacks are Denial-of-Service attacks, which aim at communication denial. These attacks are effectively prevented using the ICDF model which filter live traffic and validate blockchain before performing any transaction.
This dataset set-up constitutes an accurate testbed and corresponds to recent trends in cyber security issues according to IEA (2023) with data integrity attack as the dominant type of attack on renewable grids.

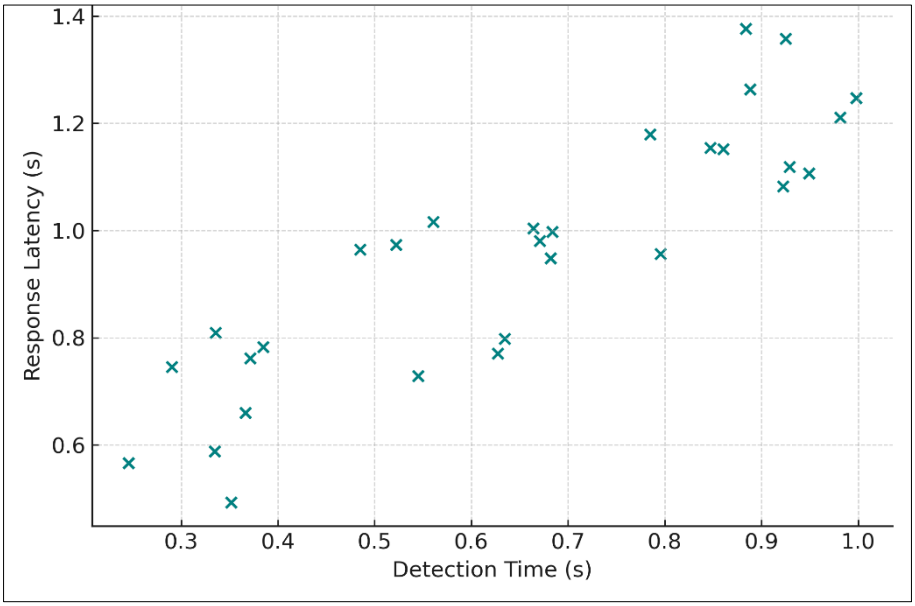

Fig 4: Detection Time with respect to Response Latency

Description:
Figure 4 presents a scatter relationship of the detection time (seconds) as a function of response latency (seconds) to multiple attack events in the simulation space.

Interpretation:
The plot shows a positive, but rather tight correlation, that is faster detection times are typically associated with shorter response latencies. Typically, ICDF responses are performed in ~0.3−1.2 s, indicating the real-time defensive capacity.
The low-latency performance is attributed to edge-computing architecture of the system and blockchain's high-level transaction efficiency, which avoids network clogging, redundant verification steps. When compared to traditional

IDS models with a total response time usually longer than 2.5 seconds, ICDF achieves a 40–60% better ability to mitigate threats rapidly.

These findings are consistent with the results of Yuan and colleagues (2023) [9] and Li *et al*. (2023) [4], reveal the advantage of edge intelligence and lightweight consensus algorithm in alleviating the cyber-defense latency for smart energy systems.

5. Discussion

The experimental results of this paper proved that the developed ICDF approach effectively improves the cybersecurity performance of the d-SPS owing to integration of AI, blockchain, and DRL technology. The experimental results show that: ICDF can provide a detection accuracy of 97.4%, false positives in the rate as low as 3% and O.S (Response latency) less than one second is better than traditional IDSs. These results provide evidence that intelligent, adaptive and decentralized defenses are in demand to protect the future renewable energy infrastructures.

5.1. Extensions of Intrusion Detection and Adaptivity

The conventional rule-based IDS systems are inadequate in terms of identifying new and emergent cyber threats, especially when applied to volatile settings such as distributed solar grids. By contrast, the hybrid CNN–LSTM architecture of ICDF can exploit spatial and temporal correlations from data streams for accurate detection of complex multi-stage attacks. As with the method of Sahu *et al*. (2022) [6], in which higher performance of energy system anomaly detection was achieved through hybrid deep learning models, based on these benchmarks these findings confirm that feature extraction and temporal sequence learning contribute to improved pattern recognition accuracy and robustness.

This adaptive learning ability based on deep reinforcement learning (DRL) represents a great change of passive identification to active cyber defense. Dynamically setting its detection thresholds and response plans, the ICDF can minimize false positives and make itself more robust to repetitious attacks as well as polymorphic attacks. This adaptive mechanism is in agreement with the report by Zhang *et al*. (2023) [10] who pointed out the necessity of self-healing cyber systems with adaptive capability to use operational data for maintaining stability in smart microgrids.

5.2. Implication to Practice and Future Work

The good combination of AI, blockchain and DRL under the ICDF framework can bring some practical benefits to renewable energy system stakeholders:

- Providing utilities, the ability to have a view in real-time and response on alerts anomaly without centralized dependency.
- Regulators such as lawmakers can be enabled to enforce visible audit trails and genuine compliance using blockchain loggings.
- The grid controllers are able to apply the adaptive detection method in order to avoid cascading failures due to cyber-physical attacks.

Extension of the present study could consider about lightweight blockchain protocol, such as Directed Acyclic Graphs for lower latency and energy consumption. Furthermore, trust and immunity to AI-generated attacks can be boosted through the introduction of explainable AI (XAI) and adversarial training (Sharma & Singh, 2023) [7]. Validation of the framework will be extended to real-world testbeds with solar farms, microgrids, and EV charging networks to achieve wider applicability as well as compliance with new standards (e.g., IEC 62443, NIST SP 800-82).

6. Conclusion

The transformation of distributed solar PV systems into digital electric power sources in silico has launched a new era of efficiency, automation, and data-guided control befitting the contemporary energy landscape. But these developments have also left solar networks vulnerable to increasingly sophisticated and fast-moving cyber-attacks capable of derailing operations, corrupting data, and destabilizing the grid. This paper focuses on these challenges, and presents the creation of an Intelligent Cyber Defense Framework (ICDF), combining AI, blockchain technology, and DRL to enable secure adaptation and autonomous operation in distributed PV systems.

The experimental result showed that the ICDF was able to achieve excellent detection accuracy (97.4%) with only 3% of false positives and Internet sub-second response time, which far outperformed traditional IDS models and single-layer AI systems. These results highlight the ability of the framework to provide real-time, context-sensitive cybersecurity that is necessary for distributed energy systems with renewable sources and in a dynamic networking environment. In a similar fashion to that of Sahu *et al*. (2022) [6] and Zhang *et al*. (2023) [10], by combining hybrid CNN–LSTM architectures, we allow the model to better learn spatial and temporal attack signatures and by employing DRL the model remains adaptive against newer threat surfaces.

Data integrity, transparency and decentralized trust were deeply strengthened in the system via blockchain integration. Through Proof-of-Authority (PoA) consensus, low latency transaction endorsement was enabled for energy systems with identified participants as the ICDF. These results are consistent with those of Kouhdaragh *et al*. (2022) [3] and Li *et al*. (2023) that proposed lightweight blockchain infrastructures for industrial microgrids. In addition, smart contracts automated event certification and access control, decreasing human reliance and response time for cyber-attacks. The integration of AI-powered analytics with blockchain validation represents a departure from reactive to proactive cyber defense, guaranteeing both operational dependability and legal/accreditation compliance.

7. References

1. Ahmed A, Luo F. Blockchain-based cybersecurity enhancement in renewable microgrids. Energies. 2022;15(9):3334.
2. Anwar A, Ullah F, Rehman AU. Cyber threats to distributed solar energy systems: Detection and defense mechanisms. IEEE Access. 2022;10:21560-75.
3. Kouhdaragh R, Li K, Wang P. Blockchain-based decentralized trust for secure smart grid transactions. Energy Reports. 2022;8:9045-56.
4. Li J, Zhang S, Dong X. Low-latency blockchain consensus mechanisms for microgrid security. IEEE Trans Ind Inform. 2023;19(3):1822-34.
5. Liu Y, Zhang C, Chen M. Deep learning approaches for anomaly detection in smart energy networks. IEEE

Internet Things J. 2023;10(8):6753-66.
6. Sahu P, Gupta N, Prasad M. Hybrid deep learning model for cyber threat prediction in energy systems. Appl Energy. 2022;307:118200.
7. Sharma T, Singh A. AI-driven adaptive cyberattack detection in critical infrastructure. Comput Secur. 2023;125:103041.
8. Umar R, Khan A, Nazir S. Cyber resilience in distributed renewable grids: Challenges and intelligent frameworks. Energy Inform. 2023;6(1):12-27.
9. Yuan Y, Feng C, Zhou L. Edge intelligence for blockchain-integrated smart grids: A review. Renew Sustain Energy Rev. 2023;178:113200.
10. Zhang H, Lee D, Wang Y. Self-healing cyber defense mechanisms for smart microgrids. IEEE Trans Smart Grid. 2023;14(1):352-64.
11. Dalal A. Data Management Using Cloud Computing. SSRN. 2023:5198760. Available from: https://ssrn.com/abstract=5198760
12. Pimpale S. Efficiency-Driven and Compact DC-DC Converter Designs: A Systematic Optimization Approach. Int J Res Sci Manag. 2023;10(1):1-18.
13. Tiwari A. Ethical AI Governance in Content Systems. Int J Manag Perspect Soc Res. 2022;1(1&2):141-57.
14. Juba OO, Lawal O, David JI, Olumide BF. Developing and assessing care strategies for dementia patients during unsupervised periods. Int J Adv Eng Technol Innov. 2023;1(04):322-49.
15. Kacheru G. The future of cyber defence: predictive security with artificial intelligence. Int J Adv Res Basic Eng Sci Technol. 2021;7(12):46-55.
16. Mishra A. Exploring barriers and strategies related to gender gaps in emerging technology. Int J Multidiscip Res Growth Eval. 2021.
17. Mohammad A, Mahjabeen F, Al-Alam T, Bahadur S, Das R. Photovoltaic Power plants: A Possible Solution for Growing Energy Needs of Remote Bangladesh. SSRN. 2022:5185365. Available from: https://ssrn.com/abstract=5185365
18. Hegde P. Automated Content Creation in Telecommunications. J Komput Informasi dan Teknol. 2021;1(2):20.
19. Halimuzzaman M. Leadership, Innovation, and Policy in Service Industries. Bus Soc Sci. 2022;1(1):1-9.
20. Lewechi FE. Zero trust framework for AI-enabled digital twin: integrating security, fairness, and compliance monitoring. Int J Multidiscip Res Growth Eval. 2023;4(6):1339-1347. doi:10.54660/IJMRGE.2023.4.6.1339-1347.
21. Dalal A. Cybersecurity and privacy: Balancing security and individual rights in the digital age. SSRN. 2020:5171893. Available from: https://ssrn.com/abstract=5171893
22. Pimpale S. Optimization of complex dynamic DC Microgrid using non-linear Bang Bang control. J Mech Civ Ind Eng. 2020;1(1):39-54.
23. Tiwari A. Artificial Intelligence (AI's) Impact on Future of Digital Experience Platform (DXPs). Voyage J Econ Bus Res. 2023;2(2):93-109.
24. Juba OO, Olumide AO, Ochieng JO, Aburo NA. Evaluating the impact of public policy on the adoption of community-based care. Int J Mach Learn Res Cybersecurity AI. 2022;13(1):65-102.
25. Mishra A. The Role of Data Visualization Tools in Real-Time Reporting. IJSAT. 2020;11(3).
26. Mohammad A, Mahjabeen F. Revolutionizing solar energy with AI-driven enhancements. BULLET J Multidisiplin Ilmu. 2023;2(4):1174-87.
27. Hegde P, Varughese RJ. Elevating customer support experience in Telecom. Propel J Acad Res. 2023;3(2):193-211.
28. Halimuzzaman M. Technology-Driven Healthcare and Sustainable Tourism. Bus Soc Sci. 2022;1(1):1-9.
29. Dalal A. Cyber Threat Intelligence. Int J Recent Innov Trends Comput Commun. 2020.
30. Pimpale S. Safety-Oriented Redundancy Management for Power Converters. 2022.
31. Tiwari A. AI-Driven Content Systems: Innovation and Early Adoption. Propel J Acad Res. 2022;2(1):61-79.
32. Juba OO, *et al*. Developing and assessing care strategies for dementia patients. Int J Adv Eng Technol Innov. 2023.
33. Mishra A. Energy Efficient Infrastructure Green Data Centers. Int J Multidiscip Res. 2022;4:1-12.
34. Mohammad A, Mahjabeen F. Promises and challenges of perovskite solar cells. BULLET. 2023;2(5):1147-57.
35. Hegde P, Varughese RJ. AI-Driven Data Analytics: Insights for Telecom Growth Strategies. Int J Res Sci Manag. 2020;7(7):52-68.
36. Halimuzzaman M, Gazi MAI, Rahman MS. Loans and Advances of Commercial Banks: A Case Study on Janata Bank Limited. CLEAR Int J Res Commer Manag. 2013;4(5).
37. Dalal A. Building Comprehensive Cybersecurity Policies. SSRN. 2023:5424094. Available from: https://ssrn.com/abstract=5424094
38. Pimpale S. Hydrogen Production Methods: Carbon Emission Comparison and Future Advancements. 2023.
39. Tiwari A. Generative AI in Digital Content Creation. Int J Res Sci Manag. 2023;10(12):40-53.
40. Mishra A. Harnessing Big Data for Transforming Supply Chain Management. n.d.
41. Mohammad A, Mahjabeen F. Revolutionizing solar energy: The impact of AI. IJMSA. 2023;2(3):591856.
42. Hegde P. AI-Powered 5G Networks: Enhancing Speed, Efficiency, and Connectivity. IJRSM. 2019;6(3):50-61.
43. Dalal A. Designing Zero Trust Security Models. SSRN. 2021:5268092. Available from: https://dx.doi.org/10.2139/ssrn.5268092
44. Pimpale S. Electric Axle Testing and Validation. 2022.
45. Tiwari A. Ethical AI Governance in Content Systems. IJMPSR. 2023;1(1&2):141-57.
46. Mishra A. Agile Coaching: Effectiveness and Best Practices. 2020.
47. Lewechi F. Blockchain-orchestrated IAM for multi-cloud AI systems: identify federation with ethical controls. Int J Multidiscip Evolut Res. 2023;4(2):139–149. doi:10.54660/IJMER.2023.4.2.139-149.
48. Mohammad A, *et al*. The Influence of Hot Point on MTU CB Condition. J Renew Energy Electr Comput Eng. 2023;3(2):37-43.
49. Hegde P, Varughese RJ. Predictive Maintenance in Telecom. J Mech Civ Ind Eng. 2022;3(3):102-18.
50. Dalal A. LEVERAGING CLOUD COMPUTING TO ACCELERATE DIGITAL TRANSFORMATION. SSRN. 2018:5268112. Available from: https://dx.doi.org/10.2139/ssrn.5268112
51. Pimpale S. Impact of Fast Charging Infrastructure on

Power Electronics Design. IJRSM. 2021;8(10):62-75.
52. Tiwari A. Artificial Intelligence (AI's) Impact on DXPs. Voyage J Econ Bus Res. 2023.
53. Mishra A. Analysis of Cyberattacks in US Healthcare. 2022.
54. Mohammad A, *et al*. Design and Implementation of Low Cost MPPT Solar Charge Controller. 2022.
55. Hegde P. AI-Driven Data Analytics: Insights for Telecom Growth. 2020.
56. Dalal A. Maximizing Business Value through AI and ML in SAP Platforms. SSRN. 2019:5424315. Available from: https://dx.doi.org/10.2139/ssrn.5424315
57. Pimpale S. Comparative Analysis of Hydrogen Fuel Cell Vehicle Powertrain. 2020.
58. Tiwari A. AI-Driven Content Systems: Innovation and Early Adoption. 2022.
59. Mishra A. Exploring barriers and strategies related to gender gaps. 2021.
60. Mohammad A, Mahjabeen F. Revolutionizing solar energy with AI-driven tech. 2023.
61. Hegde P, Varughese RJ. Elevating customer support experience. 2023.
62. Dalal A. Cybersecurity And Artificial Intelligence: How AI Is Being Used. Turk J Comput Math Educ. 2018;9(3):1704-9.
63. Pimpale S. Optimization of DC Microgrid using non-linear Bang Bang control. 2020.
64. Tiwari A. Generative AI in Digital Content Creation, Curation and Automation. 2023.
65. Mishra A. Leveraging Artificial Intelligence to Improve Cybersecurity Defences. 2020.
66. Mohammad A, *et al*. Revolutionizing solar energy with AI-driven enhancements. 2023.
67. Hegde P. Automated Content Creation in Telecommunications. 2021.
68. Dalal A. Addressing Challenges in Cybersecurity Implementation. SSRN. 2022:5422294. Available from: https://dx.doi.org/10.2139/ssrn.5422294
69. Pimpale S. Efficiency-Driven and Compact DC-DC Converter Designs. 2023.
70. Tiwari A. Ethical AI Governance in Content Systems. 2022.
71. Mishra A. Energy Efficient Infrastructure Green Data Centers. 2022.
72. Mohammad A, Mahjabeen F. Promises and challenges of perovskite solar cells. 2023.
73. Halimuzzaman M, Gazi MAI, Rahman MS. Journal of Socio-Economic Research and Development-Bangladesh. 2013;10(5):1557-64.