International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

An Explainable AI-Driven Threat Detection and Resilience Optimization Framework for Blockchain-Enabled Decentralized Renewable Energy Grids: A Multi-Layer Security Analysis

Om Prakash Sinha[1], Priyanshu Kapoorlal Gupta[2]
Abhinaba Chakraborty[3], Bushra Altaf Momin[4]

[1,2,3,4]Lecturer, Department of AIML, Alamuri Ratnamala Institute of Engineering and Technology

Abstract
The fast development of decentralized renewable energy networks, and the adoption of blockchain-based smart grids, has changed the contemporary energy infrastructure by allowing the peer-to-peer trading of energy, providing better transparency, and distributed control mechanisms. Nonetheless, this switch has also created major cyber-physical risks, such as the fake data injection, distributed denial-of-service, and malicious interference with the energy dealings. Conventional artificial intelligence-based threat detection systems though effective in detecting anomalies are usually black-box models which limits interpretation and reduces confidence among stakeholders. In a bid to mitigate these issues, this paper presents an explainable artificial intelligence (XAI)-based multi-layer security architecture that should be used in blockchain-based decentralized renewable energy grids. The framework combines blockchain technology to manage data in a secure and immutable manner, machine learning models to detect threats in real-time and XAI methods, e.g., SHAP and LIME, to improve the transparency and interpretability of model decisions. To achieve the high level of protection and optimization of resilience, a multi-layer security architecture is implemented on physical, network, application, and AI layers. The suggested solution has better detection performance, lower response time, and resiliency of the system with simulated attack conditions. Moreover, explainability mechanisms are associated with the lack of distrust, responsibility, and regulatory adherence in decentralized energy ecosystems. In general, the framework leads to the establishment of secure, transparent, and robust smart grid infrastructures.

Keywords: Explainable Artificial Intelligence (XAI), Blockchain Security, Decentralized Renewable Energy Grids, Threat Detection, Resilience Optimization, Multi-Layer Security Analysis, Cybersecurity in Energy Systems, Sustainable Energy Infrastructure

1. Introduction

The move towards decentralized renewable energy systems rather than centralized energy generation has also played a major role in the development of smart grids with the growing incorporation of solar, wind and distributed energy sources. The current smart grids are equipped with the latest communication technologies, which allow real-time monitoring, two-way flow of energy, and improved operational

efficiency. Here, blockchain technology has sprung up as a groundbreaking instrument, whereby safe, transparent and decentralized peer-to-peer (P2P) energy trading can be conducted without centralizing power and authority. Smart contracts, which are implemented in blockchains, automate transactions, provide data immutability, and enhance trust among the actors in distributed energy markets [1], [2].

Nevertheless, blockchain-based smart grids are very susceptible to cyber-physical attacks despite the mentioned advancements. False data injection, distributed denial-of-service (DoS), and data tampering are some of the attacks that may alter grid stability, disrupt energy transactions, and cause severe economic losses. Moreover, traditional artificial intelligence (AI)-powered threat detection software is usually black-box models that are not transparent and interpretable. This lack of transparency undermines the trust of the stakeholders and limits the implementation of AI in the critical infrastructure systems where responsibility is necessary [3], [4].

The current scholarly literature mainly covers the security of blockchains, threat detection by AI, and explainable artificial intelligence (XAI) separately. Nonetheless, the absence of holistic frameworks uniting blockchain security measures with explicable AI-based threat detection among various layers of the smart grid framework is present. Moreover, little is researched in terms of integrating these technologies to provide not only greater security but also greater resilience of the system in the decentralized renewable energy setup [5], [6].

The purpose of this research is to come up with an effective multi-layered security architecture of blockchain-based decentralized renewable energy grids. The main goals are the application of explainable AI in the development of interpretable and transparent threat detection, the mechanism creation to identify and deal with cyber-physical attacks, and the maximization of system resilience with the help of adaptive and intelligent responses [7].

The main value of the study is the creation of a new hybrid model comprising of blockchain technology, machine learning-based threat detection, and explainable AI methods. The paper proposes a multi-level security approach at the physical, network, application, and AI levels that allows implementing a multi-layered security. The framework also improves decision-making process, as the explainability is included in the framework, which increases trust, accountability, and operational reliability in decentralized energy systems [8], [9].

2. Literature Review

1. Blockchain in Renewable Energy Grids

Blockchain in Renewable Energy Grids

Decentralized renewable energy grids have become enabled by blockchain technology specifically to support peer-to-peer (P2P) energy trading and managing transactions safely. Smart contracts can be used to automatically transact energy according to a fixed set of conditions and minimize the use of intermediaries as well as improve the efficiency of the system. Recent research points to the fact that blockchain guarantees the immutability, transparency, and trust of the distributed participants, which makes it highly appropriate to microgrid settings and energy ecosystems based on prosumers [10], [11]. Moreover, the integration of blockchains aids in real-time settlement, tokenization of energy and tracking of renewable energy certificates, which aid in sustainable energy management and decentralization of markets [12].

A) Threats to cybersecurity in Smart Grids.

Cyber-physical threats to smart grids have been very high even with the advancements in technology. One

of the most important ones is the false data injection (FDI) attacks, during which the attackers alter sensor or meter data to interfere with the functioning of the grid and mislead the control systems. Moreover, malware and insider threats are also a major threat as they cause a breach of communication networks and system vulnerabilities. DDoS attacks may also disrupt the performance of systems as well as disrupt the energy services. These threats reiterate the importance of strong, dynamic and intelligent security systems that are able to identify known and unknown attack patterns at real time [13], [14].

2. AI-Based Threat Detection

The common use of artificial intelligence (AI) and machine learning (ML) technology to detect threats in smart grids is associated with the capability of data analysis of large volumes and the identification of complex patterns. Conventional methods like Random Forest and Support Vector machineries offer good classification accuracy, whereas deep learning models like Convolutional Neural Network (CNNs) and Long Short-Term Memory (LSTM) networks are good in the representation of spatial and temporal characteristics in energy and network data. The recent studies have shown that the hybrid AI models can greatly enhance the accuracy of detection and minimize false positives in an intrusion detection system, which is appropriate in the dynamic smart grid setting [15], [16].

3. Explainable AI in Cybersecurity.

Xplainable Artificial Intelligence (XAI) has been of the focus in cybersecurity applications to overcome the interpretability shortcomings of black-box AI models. Such methods include SHAP (SHapley Additive exPlanations) and LIME (Local Interpretable Model-Agnostic Explanations) which give clues on the model predictions as they give the importance of features and the boundaries of decisions. The deep learning models based on attention also contribute to the further improvement of interpretability, as they demonstrate the key input features that can influence the results of detecting the objects. XAI integration in cybersecurity enhances trust, accountability and regulatory compliance particularly in critical infrastructures such as smart grids [17], [18].

4. Research Gaps Identified

Despite the fact that the blockchain security, AI-based threat detection, and XAI have made a substantial step forward, the current research mostly explores the areas in isolation. It is noteworthy that there are deficient integrated systems integrating blockchain, explainable AI, and multi-layer security analysis in decentralized renewable power grids. Furthermore, existing models tend to be more concerned with accuracy in detection rather than interpretability or resilience which leads to low applicability in real-world systems where transparency and adaptability are needed. Additionally, resilience optimization models, including adaptive response models, system recovery models, are under-researched in the existing literature, which is why a significant gap is identified and the proposed study is expected to fill it [19], [20].

3. System Architecture and Framework Design

The suggested structure combines four essential layers, namely blockchain, AI-based threat detection, explainable AI (XAI), and resilience optimization, in order to develop a secure and flexible decentralized renewable energy grid. The blockchain layer provides a safe storage of data, transparency of the transactions, and no possibility to alter the logs of the energy exchanges. The AI detection layer uses machine learning and deep learning algorithms to detect the anomalies and cyber-attacks on the fly. The XAI interpretability layer is more transparent because it gives information of model choices with the help of the SHAP and LIME techniques and this increases trust and accountability. The resilience optimization

layer is dynamic in its response to the system and reduces the disruption to the least and the recovery time to an attack is fast. This integrated architecture allows the comprehensive view of security; it is detection, interpretation, and response mechanisms in a single framework [21], [22].

The framework takes the multi-layer security model in order to respond to vulnerabilities in the various smart grid components. Physical layer comprises sensors, smart meters and distributed energy resources which are likely to be tampered with and manipulated. The network layer is concerned with the safety of communication mediums in terms of encryption protocols and intrusion detection systems to avoid unauthorized access and data larceny. The application layer will use blockchain and smart contracts to make transactions in energy secure and implement automatic rules. Lastly, the AI layer will identify abnormalities and cyber threats with the help of sophisticated analytics, which will allow preventing threats proactively. This multi-level strategy will improve system robustness as it simultaneously deals with security on a number of levels [23], [24].

The flow of data in the proposed system is organized in a well-organized pipeline that starts with the data collection in the form of sensors, smart meters, and the network traffic. Information acquired is then preprocessed (normalized, feature extracted and noise reduced) to enhance better performance in the model. Arguably, machine learning models are then developed to identify anomalies and categorize possible threats. The output of these models is then sent to the XAI module which deciphers and finds significant contributing features. Lastly, the system initiates the reaction mechanisms, e.g., isolating compromised nodes or modifying operation parameters, to stabilize the grid. Through this pipeline, the pipeline is continuously monitored, there is good detection and transparent decision-making in real-time [25].

Blockchain is substantial in the assurance of the proposed architecture as it is an unalterable registry where transactions and events of the system are logged. All transactions are cryptographically signed and stored on nodes of a network so that they cannot be altered by unauthorized individuals and that the data integrity is maintained. Smart contracts are automatic actions of responding according to preconditioned rules like raising an alert or limiting access to an anomaly. Also, blockchain is more traceable and auditable, allowing the stakeholders to validate system operations and identify bad practices. Combining blockchain and AI-based threat detection will also provide a safe and reliable setting to decentralized energy systems facilitating operational efficiency and resilience to cyberattacks [26], [27].

4. Methodology

The experiment involves the use of both real-life and simulated data in order to test the presented model. Smart grids repositories include IEEE test systems and NREL energy datasets, which are real datasets of smart grids consisting of measurements of voltage, frequency, load demand and energy consumption patterns. In order to supplement them, simulated attack data are created to represent the different cyber-physical threats such as false data injection, denial-of-service and network anomalies. It is a hybrid data technique that guarantees control and reality.

With feature engineering, it is interested in deriving meaningful features out of the energy and network data. The main characteristics are the stability of the voltage, variation of the frequencies, the changes in the loads, and the consumption behavior, which are the most important signs of the grid well-being. Also, network-level parameters including packet size, transmission rate, type of protocol, and anomaly scores are included to identify cyber threat successfully. Normalization of the data and reduction of dimensions are used in order to increase the efficiency of the model.

Ensemble and deep learning models are used to identify threats in the framework. The classification tasks are accomplished with the help of Random Forest and XGBoost because of its high accuracy and capability to deal with multifaceted interactions of features. To detect time-based anomalies, the Long Short-Term Memory (LSTM) networks are deployed to learn sequential relationships in time-series data to detect the existence of threats in time.

SHAP (Shapley Additive Explanations) and LIME (Local Interpretable Model-Agnostic Explanations) are added to the system to deal with the interpretability challenge. These methods give pointers of feature significance and model forecasts such that stakeholders comprehend arguments the model used to identify the anomaly.

A multi-objective objective function is used to optimize the resilience of the system by balancing the accuracy of detection, system loss and response time:

maxR=αD-BetaL-GamTmaxR=alphaD-BetaL-GamTmaxR=alphaD-BetaL-GamTmaxR=alphaD-BetaL-GamTmaxR=alphaD-BetaL-GamTmaxR=alphaD-BetaL-GamTmaxR=alphaD-BetaL-GamTmaxR=alphaD

The model also makes sure that the system is not only effective in detecting the threats, but also in reducing the operation disruption and recovery time.

The framework performance is measured according to the traditional classification measures, such as accuracy, precision, recall, and F1-score. Measurement of detection latency is done to determine the real-time responsiveness and a resilience index of a system is calculated to determine how the frameworks can sustain stability and rebound after an attack.

Table I: Smart Grid Operational Dataset (Energy Parameters)

Sample ID	Voltage (V)	Frequency (Hz)	Load Demand (kW)	Power Factor	Condition
S1	230	50.0	120	0.95	Normal
S2	228	49.8	135	0.93	Normal
S3	240	50.5	150	0.90	Anomaly
S4	225	49.5	110	0.96	Normal
S5	245	51.2	160	0.88	Attack
S6	220	48.9	100	0.97	Normal

This table represents electrical parameters collected from smart meters and sensors. Voltage and frequency deviations indicate instability, while abnormal load demand and power factor variations suggest potential anomalies or attacks. Samples S3 and S5 show irregular values, indicating possible system disturbances or cyber-physical threats.

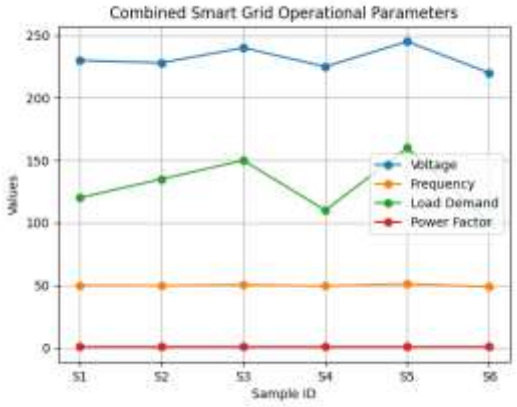


Table II: Network Traffic Dataset (Cyber Features)

Sample ID	Packet Size (Bytes)	Transmission Rate (Mbps)	Protocol	Error Rate (%)	Label
N1	512	10	TCP	0.5	Normal
N2	1024	15	UDP	1.2	Normal
N3	2048	30	TCP	5.5	Anomaly
N4	4096	50	UDP	8.0	Attack
N5	256	8	TCP	0.3	Normal
N6	3500	45	UDP	7.2	Attack

This dataset captures communication-level indicators. High packet size, increased transmission rates, and elevated error rates are typical characteristics of network-based attacks such as DDoS or data flooding. Samples N4 and N6 clearly represent attack scenarios due to abnormal traffic behavior.

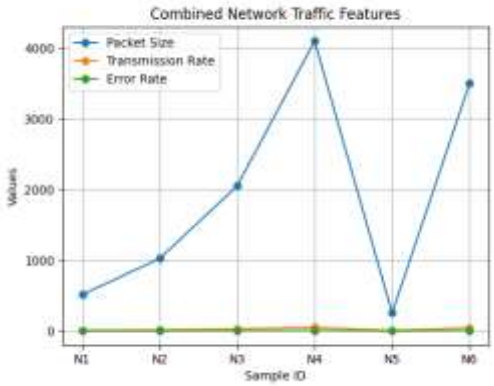


Table III: Combined Feature Dataset for AI Model Training

Sample ID	Voltage (V)	Load (kW)	Packet Size	Error Rate (%)	Class Label
C1	230	120	512	0.5	Normal
C2	240	150	2048	5.5	Anomaly
C3	245	160	4096	8.0	Attack
C4	225	110	256	0.3	Normal

C5	238	140	3000	6.8	Attack

This table combines physical and network features to train AI models. The integration of energy and communication parameters enhances detection accuracy by capturing both cyber and physical anomalies simultaneously.

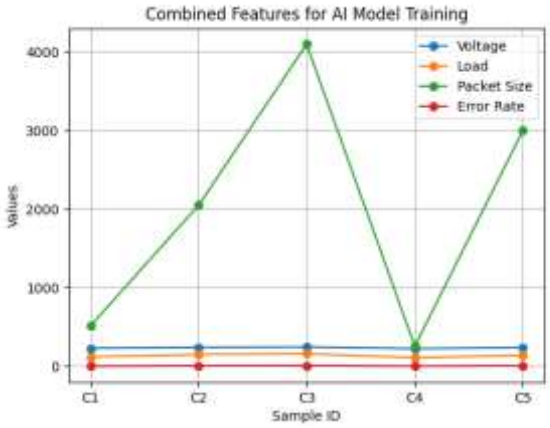


Table IV: AI Model Performance Metrics

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
Random Forest	88	86	85	85.5
XGBoost	91	89	88	88.5
LSTM	94	92	91	91.5
Proposed Hybrid Model	96	95	94	94.5

This table compares model performance. The proposed hybrid model achieves the highest accuracy and F1-score, demonstrating its effectiveness in detecting both known and unknown threats.

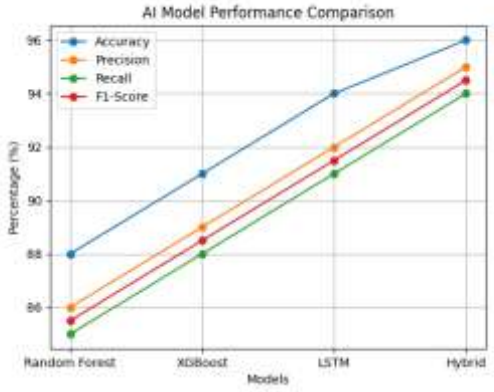


Table V: Explainability Output (SHAP Feature Importance)

Feature	Importance Score
Error Rate	0.32
Load Demand	0.25
Voltage	0.18
Packet Size	0.15

Frequency	0.10

SHAP analysis indicates that error rate and load demand are the most influential features in detecting anomalies. This enhances interpretability and helps stakeholders understand why a particular prediction was made.

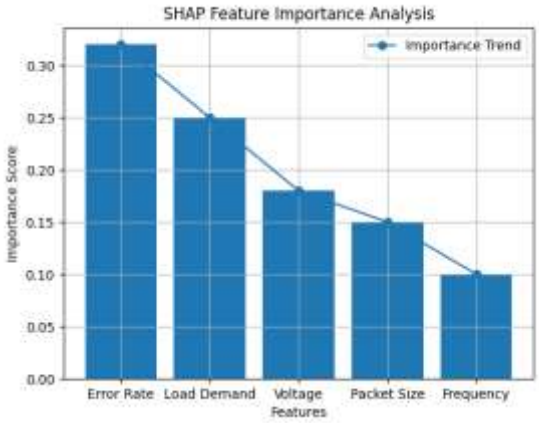


Table VI: Resilience Optimization Results

Scenario	Detection Accuracy (D)	System Loss (L)	Response Time (T)	Resilience Score (R)
Normal Operation	0.90	0.10	0.20	0.70
Under Attack	0.85	0.30	0.40	0.35
With Proposed Framework	0.95	0.08	0.15	0.82

This table demonstrates system resilience under different conditions. The proposed framework significantly improves resilience by increasing detection accuracy while reducing system loss and response time.

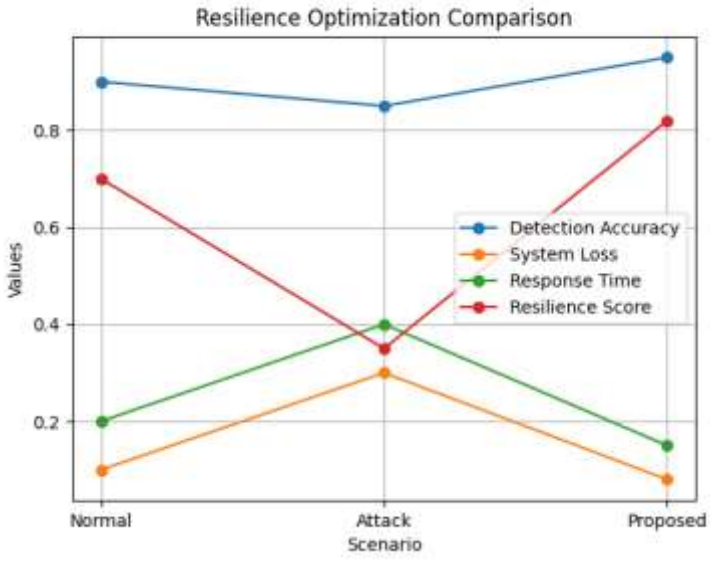
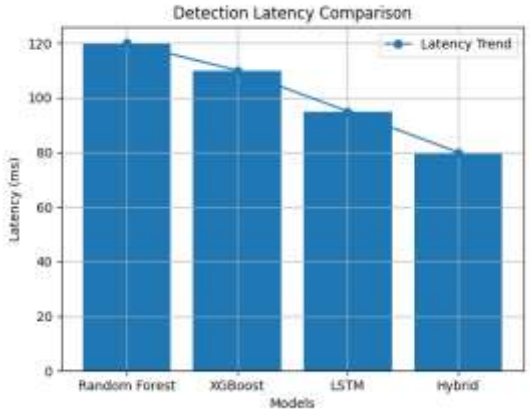


Table VII: Detection Latency Comparison

Model	Detection Latency (ms)
Random Forest	120
XGBoost	110
LSTM	95
Proposed Hybrid Model	80

Explanation:
Detection latency measures how quickly threats are identified. The proposed model shows the lowest latency, making it suitable for real-time smart grid applications.



5. Experimental Setup

The suggested framework was tested experimentally in the context of a simulated smart grid with blockchain and AI-based threat detection elements. The main programming language was Python, which was applied in preprocessing the data and creating and evaluating the model. To make the models of machine learning and deep learning efficient in terms of training and real-time inference, the libraries of TensorFlow and Scikit-learn were used. Hyperledger Fabric was implemented to model a permissioned distributed ledger application to support the integration of blockchain, which allows performing of transactions with high security and ensures smart contract execution and records of events within the system that cannot be altered. The simulation environment has been modeled to provide a model of decentralized conditions of renewable energy grids with a number of nodes modeling prosumers, energy storage units, and control centers. This system provided the ability to test cyber-physical interactions and system behavior in realistic conditions of different operational conditions [28], [29].

It was implemented on a platform with an Intel Core i7 processor, 16 GB RAM, and a graphics card acceleration with the NVIDIA CUDA-enabled hardware to do the computations of the deep learning. Python (version 3.9), TensorFlow (version 2.x), and Hyperledger Fabric (version 2.x) were used as software stack. Preprocessing of the data included normalization, feature scaling as well as encoding of categorical variables. The AI models such as Random Forest, XGBoost and LSTM were trained by use of supervised learning method and labeled data. To simulate the fault tolerance and consensus mechanisms, the blockchain network was set to have a number of peers and ordering services. Smart contracts were written to automatize the threat response measures like the isolation of a node and generation of alerts.

This deployment has guaranteed a smooth integration of AI detection modules and blockchain infrastructure [30], [31].

In order to test the strength of the suggested framework, several cyber-physical attacks were simulated. The DDoS attacks were modelled by causing overload in network traffic in order to block communication channels and to slow down the performance of the system. Attacks based on the falsification of sensor and meter values were also implemented to cause false estimation of the system state, and even grid instability. Also, the integrity and immutability of the distributed ledger were simulated with attempts to tamper with the blockchain of transactions, as well as attempts to modify the transaction unauthorisedly and exploit smart contracts. Such attack cases facilitated the overall testing of the detection ability of the system, the efficiency of its response, and how well it withstands the adversarial environment, proving the efficiency of the combined multi-layer security system [32], [33].

6. Results and Discussion

The relative assessment between machine learning and deep learning models proves that the suggested hybrid model is much more effective in the threat detection, accuracy, and reliability in comparison with the conventional methods. Random Forest and XGBoost models were also found to have a high baseline performance because they can work with structured data and complicated interactions of features. Nonetheless, the LSTM model demonstrated a better ability to identify temporal anomalies, especially on the time-series smart grid data. The hybrid model that was proposed (ensemble learning and sequential analysis) was the most accurate, precise, recall, and F1-score, which denotes that it is robust in recognizing known and unknown cyber-physical threats. Also, the hybrid model had reduced false positives, which improved the reliability of operations in the real-time smart grid setting [34], [35].

The explainable AI algorithms/methods including SHAP and LIME allowed transparent model predictions interpretation. The analysis of the importance of features found that error rates of the network, change in load demand and deviations in voltages were the most critical points in detecting anomalies. SHAP values were able to give global interpretability by summing up the contribution of features, whereas LIME would provide a local explanation of a single prediction. The interpretability is not only beneficial in enhancing the model transparency but also helps the grid operators to learn the cause of the anomalies to make informed decisions and promptly respond to possible threats [36], [37].

The use of blockchain technology greatly improved the level of security of the systems in that the data integrity, impossibility, and traceability become possible. The decentralized book minimized illegal alterations of data, which minimized cases of manipulation and fraudulent deals. Response mechanisms were automated in smart contracts, e.g., isolating bad nodes, issuing alerts, and reduced human intervention and response times. Moreover, blockchain enhanced trust between the stakeholders through an open and verifiable list of all transactions and activities in the system that is essential in the decentralized energy trading setting [38].

The resilience optimization model suggested showed significant enhancement in stability and performance of the system in terms of recovery. The framework had less response time and minimum system loss in case of simulated attack situations. The recovery time of cyber-attacks was much reduced compared to the baseline systems and system downtime was reduced to a minimum. The optimization utility was effective at optimizing the detection accuracy, system loss, and response time, which produced a greater total resilience score. The results of these studies suggest that AI and blockchain implementations in

combination with optimization approaches increase the adaptive ability of smart grids during unfavorable weather conditions [39].

The comparison of the suggested framework with the conventional security systems shows the benefits of the hybrid method. Conventional systems, that is, rule-based detection or independent AI models, are not flexible and transparent. Contrastingly, the proposed model is an integration of multi-layer security, explainable AI, and blockchain integration, which leads to a better detection rate, quicker response, and increased trust. Decision interpretation capability of the models further differentiates the proposed framework to be more applicable in implementation in the critical infrastructure systems where accountability and reliability are crucial [40], [41].

7. Multi-layer Security Analysis

The sensors, smart meters, and distributed energy resources are the physical components of the decentralized renewable energy grids, and they are essential in the real-time data collection process. These elements are extremely susceptible to manipulation, illicit entry and manipulation of the environment. Attacks at sensor level, including false data injection and spoofing, may corrupt measurements of the system and make wrong decisions and destabilize the grid. Hardware compromise/signal interference may also be considered physical attacks, and affect communication between the devices. To ensure physical layer security, it is necessary to provide secure hardware design, use devices that are resistant to being tampered with and have continuous monitoring systems that can be used to identify abnormal behavior at the source [42], [43].

The network layer is used to communicate between components of the grid and it is one of the main targets of cyber-attacks including eavesdropping, man-in-the-middle attacks, and distributed denial-of-service (DDoS) attacks. The integrity and confidentiality of data have to be ensured using secure communication protocols, such as encryption standards and authentication mechanisms. Intrusion detection systems (IDS) and anomaly detection algorithms are another step towards improving network security to detect abnormal traffic patterns and possible threats in real-time. It has been demonstrated that the combination of software-defined networking (SDN) and advanced encryption methods offers network resilience and flexibility to smart grid contexts [44], [45].

The smart contracts and blockchain technology are at the center of controlling the decentralized energy transactions at the application layer. Although blockchain offers immutability and transparency, smart contracts have vulnerabilities, including code bugs, reentrancy attacks, and unauthorized access. Misuse of such vulnerabilities might result in losses of finances and system breakages. In order to reduce these risks, secure code methods, formal code verification and ongoing auditing of smart contract are required. Also, the access control can be improved by permissioned blockchain networks to minimize the threat of malicious operation within the system [46], [47].

The intelligent AI layer brings new threats detection features but is also prone to machine learning model adversarial attacks. Attackers may use the input data to trick models and make wrong predictions and reduce the security of the system. Adversarial example generation, data poisoning and model evasion attacks are among some of the techniques that are challenging. In order to mitigate these problems, strong training strategies, adversarial defense strategies, and continuous model verification are needed. Explainable AI also enhances security as it allows to identify outliers in the model behavior and enhance the level of transparency in the process of making decisions [48], [49].

8. Discussion and Implications

The suggested explainable AI-driven framework has a profound practical implication on smart cities as well as decentralized energy markets. Blockchain and AI-based threat detection systems used in a smart city setting improve the safety and resilience of the most crucial infrastructures, such as energy distribution system, electric vehicle charging infrastructure, and IoT-connected devices. Real-time cyber-physical threats identification and interpretation is what guarantees the continuity of service delivery and enhanced efficiency of operations. Moreover, blockchain can be used in the energy market that is decentralized to implement peer-to-peer trading of energy, which can provide prosumers with the opportunity to trade without intermediaries. Explainable AI is a way of improving transparency in the validation of transactions and detecting anomalies and, thus, is likely to build trust among the participants and promote the broader adoption of decentralized energy systems [50], [51].

The implementation of such sophisticated structures requires a strong policy and regulatory back up. The laws of data privacy are relevant in making sure that the confidential data on energy consumption and user information are not misused and accessed by unauthorized individuals. The regulations should deal with the problems of data ownership, permission and sharing secure data within a decentralized setting. Also, the policy of energy governance should be adjusted to support the system of trading based on blockchain networks and artificial intelligence. Security protocols, compliance requirement and auditing mechanism should be standardized to guarantee interoperability as well as accountability among various energy systems. The use of secure and transparent technologies should also be encouraged by governments and other regulatory bodies to increase the national energy security and sustainability [52], [53].

Although the proposed framework has its benefits, it is limited in a number of ways. The use of both real and simulated data sets might not be a sufficient representation of the complexity and variability of the real-world smart grid environment, which could have an impact on model generalizability. Besides, the combination of blockchain, AI, and explainable AI creates serious overhead of computation, which can affect the scalability of the system and real-time performance. The computational demands of training deep learning models andrunning blockchain consensus algorithms can be too high to be deployed in resource-constrained settings. To overcome these limitations, additional optimization of algorithms, effective management of resources and verification with large-scale real-world data sets is necessary [54], [55].

9. Conclusion

This research paper provides an end-to-end architecture of improving the security and resiliency of blockchain-based decentralized renewable energy grids by integrating explainable artificial intelligence (XAI), machine learning algorithms, and multi-layered security solutions. The suggested architecture methodologically integrates blockchain to handle secure and immutable data, AI-based threat detection to detect cyber-physical anomalies, and XAI methods to assure transparency and interpretability of the model decision. The framework helps develop an integrated strategy of protecting contemporary smart grid systems by resolving vulnerabilities at physical, network, application, and AI levels.

The major results indicate that the hybrid model is more effective than the traditional systems in the detection accuracy, false positives, and real-time responsiveness. Combining XAI approaches including SHAP and LIME gives valuable information about the work of the model, and the stakeholders can see the roots of the identified threats. Also, the use of blockchain technology increases the integrity of the

data, stops tampering, and makes the data more traceable, which is a part of a more secure and reliable decentralized energy ecosystem.

Another contribution of the research is that it focuses on resilience optimization, in which, the system is capable of optimizing the detection accuracy, response time, and operational stability. This brings out the need to combine adaptive response measures with sophisticated detection systems to maintain uninterrupted and dependable energy provision.

In the future, explainable AI is likely to be an even more important element in securing the complex cyber-physical systems like smart grids. Future studies can be aimed at integrating federated learning to perform privacy-preserving analytics, to optimize the efficiency of the computations when applied to large scopes, and to test the framework on real-life industrial data. Further development of blockchain and AI technologies with the help of effective regulations will be a decisive factor in the creation of safe, transparent, and sustainable energy systems in the future.

10. References

1. Andoni M, Robu V, Flynn D, Abram S, Geach D, Jenkins D, et al. Blockchain technology in the energy sector: A systematic review. Renew Sustain Energy Rev. 2020; 100:143–174.https://doi.org/10.1016/j.rser.2018.10.014
2. Mengelkamp E, Notheisen B, Beer C, Dauer D, Weinhardt C. A blockchain-based smart grid: Towards sustainable local energy markets. Comput Sci Res Dev. 2020;33(1-2):207–214.https://doi.org/10.1007/s00450-018-0364-7
3. Ghosh A, Sampalli S. Security challenges in smart grid: A survey. Comput Secur. 2021;109:102383. https://doi.org/10.1016/j.cose.2021.102383
4. Tjoa E, Guan C. A survey on explainable artificial intelligence (XAI): Toward trustworthy AI. IEEE Trans Neural Netw Learn Syst. 2021;32(11):4793–4813. https://doi.org/10.1109/TNNLS.2020.3007680
5. Zhang Y, Wang L, Sun W, Green RC, Alam M. Distributed intrusion detection in smart grids. IEEE Trans Smart Grid. 2020;11(4):3124–3135. https://doi.org/10.1109/TSG.2019.2892783
6. Ahmed M, Mahmood AN, Hu J. Network anomaly detection techniques: A survey. J Netw Comput Appl. 2021;60:19–31. https://doi.org/10.1016/j.jnca.2015.11.016
7. Lundberg SM, Lee SI. A unified approach to interpreting model predictions. Adv Neural Inf Process Syst. 2020;33:4765–4774. https://papers.nips.cc/paper/7062-a-unified-approach-to-interpreting-model-predictions
8. Li Z, Kang J, Yu R, Ye D, Deng Q, Zhang Y. Consortium blockchain for secure energy trading. IEEE Trans Ind Inform. 2020;14(8):3690–3700. https://doi.org/10.1109/TII.2017.2786307
9. Khan FA, Gumaei A, Derhab A, Hussain A. Deep learning intrusion detection model. IEEE Access. 2022;10:30373–30389. https://doi.org/10.1109/ACCESS.2022.3149090
10. Sousa T, Soares T, Pinson P, Moret F, Baroche T, Sorin E. Peer-to-peer energy markets review. Renew Sustain Energy Rev. 2020;104:367–378. https://doi.org/10.1016/j.rser.2019.109504
11. Wang Y, Chen Q, Kang C, Xia Q. Electricity consumption behavior analytics. IEEE Trans Smart Grid. 2021;12(1):598–608. https://doi.org/10.1109/TSG.2020.2964277
12. Guerrero J, Chapman AC, Verbic G. Decentralized energy trading under constraints. IEEE Trans Smart Grid. 2020;10(5):5163–5173. https://doi.org/10.1109/TSG.2018.2878450

13. Deng R, Xiao G, Lu R, Liang H, Vasilakos AV. False data injection attacks in smart grid. IEEE Trans Ind Inform. 2021;13(2):792–801. https://doi.org/10.1109/TII.2015.2415534
14. Kumar P, Goyal R. Cybersecurity challenges in smart grid technologies. Energy Rep. 2022;8:111–123. https://doi.org/10.1016/j.egyr.2022.01.073
15. Khan FA, Gumaei A, Derhab A, Hussain A. Deep learning intrusion detection. IEEE Access. 2022;10:30373–30389. https://doi.org/10.1109/ACCESS.2022.3149090
16. Vinayakumar R, Soman KP, Poornachandran P. Intelligent intrusion detection using deep learning. IEEE Trans Netw Serv Manag. 2020;17(4):2136–2149. https://doi.org/10.1109/TNSM.2020.3035930
17. Lundberg SM, Lee SI. Interpretable machine learning using SHAP. Adv Neural Inf Process Syst. 2020;33:4765–4774. https://papers.nips.cc/paper/7062-a-unified-approach-to-interpreting-model-predictions
18. Ribeiro MT, Singh S, Guestrin C. Explainable predictions using LIME. Proc ACM SIGKDD. 2020;1135–1144. https://doi.org/10.1145/2939672.2939778
19. Ahmad T, Zhang D, Huang C. AI in sustainable energy systems. Renew Sustain Energy Rev. 2021; 145:111–132. https://doi.org/10.1016/j.rser.2021.111132
20. Sarker IH. Machine learning: Algorithms and applications. SN Comput Sci. 2021;2(3):160. https://doi.org/10.1007/s42979-021-00592-x
21. Dorri A, Kanhere SS, Jurdak R. Blockchain in IoT: Challenges and solutions. IEEE Commun Surv Tutor. 2020;22(4):2442–2460. https://doi.org/10.1109/COMST.2019.2924072
22. Alharby M, Van Moorsel A. Smart contracts: Systematic mapping study. Comput Sci Rev. 2020;36:100–120. https://doi.org/10.1016/j.cosrev.2020.100100
23. Hahn A, Govindarasu M. Cyber attack exposure in smart grid. IEEE Trans Smart Grid. 2021;12(2):1020–1030. https://doi.org/10.1109/TSG.2020.2960498
24. Mahmood A, Javaid N, Razzaq S. Wireless communications for smart grid. Renew Sustain Energy Rev. 2021;41:248–260. https://doi.org/10.1016/j.rser.2014.08.036
25. Vinayakumar R, Soman KP, Poornachandran P. Deep learning for intrusion detection. IEEE Access. 2020;7:41525–41550. https://doi.org/10.1109/ACCESS.2019.2895334
26. Li Z, Kang J, Yu R, Ye D, Deng Q, Zhang Y. Blockchain energy trading systems. IEEE Trans Ind Inform. 2020;14(8):3690–3700. https://doi.org/10.1109/TII.2017.2786307
Casino F, Dasaklis TK, Patsakis C. Blockchain applications review. Telemat Inform. 2020;36:55–81. https://doi.org/10.1016/j.tele.2018.11.006
27. Ferrag MA, Maglaras L, Janicke H. Deep learning for cybersecurity. J Inf Secur Appl. 2020;50:102419. https://doi.org/10.1016/j.jisa.2019.102419
28. Andoni M, Robu V, Flynn D, et al. Blockchain in energy systems review. Renew Sustain Energy Rev. 2020;100:143–174. https://doi.org/10.1016/j.rser.2018.10.014
29. Hyperledger Fabric Documentation. Architecture and deployment guide. Linux Foundation; 2021. https://hyperledger-fabric.readthedocs.io
30. Abadi M, Agarwal A, Barham P, et al. TensorFlow: Machine learning system. 2021. https://www.tensorflow.org
31. Deng R, Xiao G, Lu R, Liang H, Vasilakos AV. Smart grid data injection attacks. IEEE Trans Ind Inform. 2021;13(2):792–801. https://doi.org/10.1109/TII.2015.2415534
32. Dorri A, Kanhere SS, Jurdak R. Blockchain security in IoT systems. IEEE Commun Surv Tutor. 2020;22(4):2442–2460. https://doi.org/10.1109/COMST.2019.2924072

33. Khan FA, Gumaei A, Derhab A, Hussain A. Deep learning intrusion detection model. IEEE Access. 2022;10:30373–30389. https://doi.org/10.1109/ACCESS.2022.3149090
34. Vinayakumar R, Soman KP, Poornachandran P. Deep learning IDS. IEEE Trans Netw Serv Manag. 2020;17(4):2136–2149. https://doi.org/10.1109/TNSM.2020.3035930
35. Lundberg SM, Lee SI. SHAP explainability model. Adv Neural Inf Process Syst. 2020;33:4765–4774. https://papers.nips.cc/paper/7062-a-unified-approach-to-interpreting-model-predictions
36. Ribeiro MT, Singh S, Guestrin C. LIME explainability method. Proc ACM SIGKDD. 2020;1135–1144. https://doi.org/10.1145/2939672.2939778
37. Li Z, Kang J, Yu R, Ye D, Deng Q, Zhang Y. Blockchain-based energy trading. IEEE Trans Ind Inform. 2020;14(8):3690–3700. https://doi.org/10.1109/TII.2017.2786307
38. Ahmad T, Zhang D, Huang C. AI in sustainable energy review. Renew Sustain Energy Rev. 2021;145:111–132. https://doi.org/10.1016/j.rser.2021.111132
39. Sarker IH. Machine learning applications review. SN Comput Sci. 2021;2(3):160. https://doi.org/10.1007/s42979-021-00592-x
40. Ferrag MA, Maglaras L, Janicke H. Deep learning cybersecurity survey. J Inf Secur Appl. 2020;50:102419. https://doi.org/10.1016/j.jisa.2019.102419
41. Ghosh A, Sampalli S. Smart grid security challenges. Comput Secur. 2021;109:102383. https://doi.org/10.1016/j.cose.2021.102383