Cyber-Security Enabled Smart Controller for Grid-Connected Microgrid

Abdul Samad
Computer Science & Engineering
Presidency University
Bengaluru, India
abdul.20221cse0121@presidencyuniversity.in

Siddique Ali Khan
Computer Science & Engineering
Presidency University
Bengaluru, India
siddique.20221cse0048@presidencyuniversity.in

Mohammed Anzal A
Computer Science & Engineering
Presidency University
Bengaluru, India
mohammed.20221cse0026@presidencyuniversity.in

Dr. Manju More E,
Associate Professor
Computer Science & Engineering
Presidency University
Bengaluru, India
manju.me@presidencyuniversity.in

***Abstract*— Grid-connected microgrids have become a critical component of modern power systems, providing improved reliability and seamless integration of renewable energy sources. Due to increased reliance on cyberspace systems, microgrids and their connection to the central grid suffer from a range of cyber perils: Data Injection, Denial of Service, or Man in the Middle. There is more to these systematic attacks, but all in all, it's a threat to the grid's balance alongside its economic and operational efficiency. This paper concerns the design of a multi-function smart controller which has at its core cyber perimeter defenses, and military-grade elliptic curve cryptography for isolated communication in conjunction with blockchain for real-time immutable audit trails, and an advanced detection layer for cyber subsystem real-time perimeter isolation. Additionally, a dashboard provides operators with real-time monitoring and control capabilities. This system's uniqueness lies in its ability to combine several cybersecurity technologies into one seamless system, which optimizes real-time processing on microgrid controllers and balances system performance with security.**

***Keywords*— Microgrid security, Elliptic Curve Cryptography, Anomaly Detection, Smart Grid, Cyber-Physical Systems**

I. Introduction

The continued development of power systems into smart grids and the integration of distributed energy resources have microgrids being considered as multifunctional elements of contemporary electrical architectures [1], [2]. These systems support local generation, storage and distribution of energy which can operate in both grid connected and islanded configurations. The integration of information and communication technologies (ICT) that enable such capabilities also bring along substantial cybersecurity risks[3].

The culmination of multiple cyber devices such as smart meters, sensors, controllers, and interfaces, as well as network devices, makes microgrids easily vulnerable to cyber-attacks. Unlike traditional networks, these networks are not entirely centralized, making them easy targets. They are also more prone to cyber-physical attacks due to the nature of their connectivity, which equally threatens the availability and service continuity of the physical system. Microgrid attacks, as per recent studies, carry the risk of impacting network stability and social security, which completely endangers the public.

Man-in-the-middle virtual attacks intercept and manipulate the control and monitor channels of a conversation [5] and insert malicious data within. These attacks within microgrids draw alarms because of the critical data communications within the microgrid system and the reliance on wireless technologies. MITM attacks can operate on data, contributing to system instability because they can manipulate the data's confidentiality and data integrity at the same time.

Denial of Service (DoS) aims at crushing the communicational and computational capabilities of the microgrid control system [9] including routers and switches. These attacks are capable of lowering processing capabilities by flooding the communication networks and thus, the isolation of the control functions can be interrupted and control coordination of dispersed energy resources is seriously compromised undermining the system.

False Data Injection (FDI) attacks represent one of the most significant threats to microgrid operations [14] – [16]. The attacks mislead system operators and automated controllers by actively manipulating control signals or sensor measurements. Careful planning enables attackers to design FDI attacks that bypass traditional bad data detection mechanisms. These attackers remain within operational limits and slowly diminish system performance.

The outcomes of existing microgrid cybersecurity solutions stem from isolating and trying to solve each attack vector individually, and/or implementing countermeasures in isolation. Most approaches still don't tackle set objectives of balance between operational efficiency and real-time requirements of microgrid systems, which is why optimal system performance is rarely accomplished. Almost all focus is placed on system performance, or system security.

The aim of this paper is to counter the misconceptions and shortcomings of integrated approaches which combine multiple, and often divergent, attack vector focus points. There are agile countermeasures to every attack vector. These include advanced microgrid-focused platforms for cryptography, distributed ledgers, and intelligent anomaly detection. With this approach, we address both preventive and detective architectural security simultaneously.

II. Literature Review

In recent years, allocating research in to the problems posed by microgrid system security has proven the use of a multi-layered approach for the architectural defense domain offers significant advantages. This chapter analyses existing literature on the use of microgrids protected by cryptography, blockchain, and resilient control strategies as well as the work on blockchain-based anomaly detection.

Ayele et al. [4] have thoroughly analyzed the implementation of ECC in smart grid communications and proved the computational and key size efficiency of elliptic curve cryptography over classical RSA-based systems. Their work proved that ECC can provide the same levels of security while significantly alleviating the processing burden, thereby making it a prime candidate for resource-scarce microgrid devices. However, the implementation was a static key distribution system and did not deal with the dynamic key management needed in real time for control systems.

Ahmed et al. [6] studied the incorporation of blockchain technology in logging and auditing in energy systems and proposed the use of a distributed ledger for storing energy transactions and system events in an immutable way. Their framework shows the ease of accountability and improved transparency on energy trading systems, however, the framework lacks attention on the needs of real-time control systems as well as the integration with legacy microgrid infrastructure. Their blockchain system's limited scalability is a primary concern with large microgrid implementations.

Liu et al. [9] studied the implications that DoS attacks have on load frequency control in smart grids and developed mathematical models for analyzing the effects of communication failures on the stability of the system. These models analyzed the effects of DoS attacks aimed on the strategically weak operational times and how they impact the power system's stability.

Wang et al. [12] address cyber-resilient control strategies for hybrid microgrids with a focus on detection and suppression of multi-target coordinated attacks on several system components at a microlevel. Each of these scenarios was modeled within a game-theoretic frame, and optimal strategies were constructed. While one could extract very useful results on the dynamics of attack–defense from such a theoretical approach, the practicality of such defense forms and the real-time need for such a model did not seem to receive much attention.

Distributed control for frame forming in AC microgrids under cyberattacks with resilience features was developed by Marasini and Qu [17], who brought forth the idea of virtual anchors for stabilizing an attacked system at the inverter level. Still, there were severe restrictions on the attack. With the concealment of the control-suppressed layer, mitigation of the FDI and DoS attacks was achieved. More holistic attack–defense strategies were not formulated within that model, though it did achieve positive easing of the austerity of control system complexes.

Recent literature on hybrid machine learning approaches to cyberattack detection and mitigation in microgrids has shown promising results [9], [10], [11]. These methods typically combine multiple algorithms such as logistic regression, Long Short-Term Memory (LSTM) networks, and support vector machines to achieve improved detection accuracy and reduced false positive rates. The hybrid approach lets systems adjust to a variety of attacks and operational scenarios while still being computationally efficient enough to be real-time applicable.

Even with the progress that has been made, the literature has serious gaps. Most modern strategies treat each problem with regard to an individual security problem in isolation, poorly describing the complicated relations between different attacking methods and defense techniques.

To bridge the gaps outlined above, this research aims to devise an all-encompassing cybersecurity framework. It aims to integrate ECC encryption, blockchain logging, and distributed hybrid anomaly detection, collaboratively, for microgrid systems. This approach works around the weaknesses of the existing solutions and tackles practical integration issues pertinent to microgrid systems.

III. Methodology

The cybersecurity-enabled smart controller integrates multiple security technologies within a unified framework designed to protect grid-connected microgrids against cyber-attacks. The combination of logging, threat detection, secure communication, and real-time monitoring of the system architecture, allows for secure monitoring operated at the highest efficiency possible.

A. System Architecture Overview

The entire system is made up of five core components. These components include the cyber-attack simulation environment, ECC encryption module, hyper anomaly detection system, lightweight blockchain logging framework, and the monitoring dashboard. These components work together to provide end-to-end security coverage for microgrid operations.

The cyber-physical interface layer manages the flow of information between the physical components of the microgrid and the cybersecurity controller. It relies on validated data and secure communication frameworks to control the data integrity among the sensors, control systems, and actuators. Each element of the integrated security systems relies on the processing and control core to provide coordinated cyber processing functions and responses to the detected threats.

B. ECC Encryption Implementation

The Elliptic Curve Cryptography module provides secure communication channels between microgrid components using optimized algorithms suitable for real-time applications. The ECC implementation [3] utilizes the NIST P 256 curve, which provides 128-bit security equivalent with minimal computational overhead compared to traditional RSA-based systems. The elliptic curve used is defined as:

$$E: y^2 \equiv x^3 + ax + b \bmod p \qquad (1)$$

with the constraint

$$4a^3 + 27b^2 \neq 0 mod p \quad (2)$$

where p is a large prime, a and $b$are curve parameters, and G is the generator point of order n.

The key management system implements dynamic key generation and distribution protocols to ensure forward secrecy and prevent compromise propagation. A private key d is randomly generated, and the corresponding public key is computed as:

$$d \in [1, n-1], Q = dG \quad (3)$$

where d represents the private key, and Q the associated public key.

For secure session establishment, the Elliptic Curve Diffie–Hellman (ECDH) protocol is employed.

Two entities $A$and $B$with key pairs (d_A, Q_A) and (d_B, Q_B), respectively, derive a common shared secret S:

$$S = d_A Q_B = d_B Q_A = d_A d_B G \quad (4)$$

ensuring that only the legitimate parties can compute the same session key.

Message authentication employs the Elliptic Curve Digital Signature Algorithm (ECDSA) to ensure data integrity and non-repudiation.

For a message m, a random nonce k is selected, and the signature pair (r, s) is generated as:

$$r = (kG)_x mod n \quad (5)$$

$$s = k^{(-1)}(h(m) + rd) mod n \quad (6)$$

where $h(m)$ is the hash of the message.

All control messages and obtained measurements utilize private and public keys on both ends of verification. Only the sender signs the documents, while the recipients check the signatures against the sender's public key. This technique protects against any attempts that try to change important control information, and proves the existence of a MITM interception.

C. Hybrid Anomaly Detection System

The hybrid anomaly detection system combines threshold-based monitoring with machine learning algorithms to identify malicious activities with high accuracy and low false positive rates [9] . The system operates in two stages: initial screening using statistical thresholds and comprehensive analysis using trained machine learning models.

The threshold component of the system operates and monitors the values such as the voltage of the system, frequency shifts, inter-module power loss, and the latency of inter-module communications. These thresholds are set to represent the standard operational window and the regulated range. When such measurements are obtained, the system sets alerts and initiates machine-learning driven secondary analyses of the sample set.

The machine learning systems incorporate LSTM Networks together with logistic regression for predictive analytics of time series data. The LSTM Networks learn training data associated with the normal behavior of the system so as to identify and flag temporal anomalies within time series data. Subsequently, Logistic regression helps in the rapid classification of distinct events and the individual parameter deviations. This approach allows the machine learning systems to identify both gradual and abrupt attacks. The data used to train the machine learning models stems from extensive complex simulations that contain normal situations as well as attack patterns. The training data comprises the full scope of cyber-physical systems. FDI attacks of particular magnitude and duration, MITM attacks data attacks of varying upload and deletion strategies, and various DoS attacks that target different communication channels.

D. Lightweight Blockchain Logging

The framework integrates a permissioned distributed ledger which is specifically optimized for microgrid application scale and is kept in a secured system that is free from tampering. All authentication attempts, anomalies, control actions, and modifications to system configurations in the secure system are recorded.

The implementation of blockchains applies a lightweight consensus protocol and is optimized for low-latency application scope. Instead of the proof-of-work algorithms, the system uses a Practical Byzantine Fault Tolerance (pBFT) consensus protocol, which ensures confirmation of transactions without sacrificing security guarantees.

Every node in the blockchain is part of the consensus and the new block creation process and stores a local version of the distributed ledger. The blocks, which contain timestamps, transaction hashes, signatures, and Merkle tree roots, provide high-speed verification of the data and assurance of integrity.

E. Dashboard Interface

The monitoring and control dashboard provides the system operator a detailed interface to track and respond to microgrid security status and any associated threats. The use of Simulink to implement dashboard performance allows appropriate response time and operational environments. The dashboard's primary function is to track security measures in real-time and displays metrics on the status of encryption, system anomalies, blockchain sync, and overall system health.

The use of charts and graphs allows operators to conduct retrospective examinations and identify security anomalies as well as understand the trends. Operators are able to confirm, counter, and supervise system security changes using the alert management functions in a timely manner.

IV. Implementation Plan

The approach taken to incorporate the cybersecurity features within the controller is to work systematically through internal phases to lower the risk factors and systematically validate all parts of the solution. The development is broken down into five phases, with each step, each with set goals, timelines, outputs, and divided metrics to evaluate progress.

A. Environment Setup and Initial Configuration - Phase 1

This stage focused on the setting up of virtual environments needed for wireless cyber-attack, cyber kill chain, and attack surface development within the attack emulation lifecycle.

These environments were constructed and set up using MATLAB and Simulink, and relevant toolboxes designed for

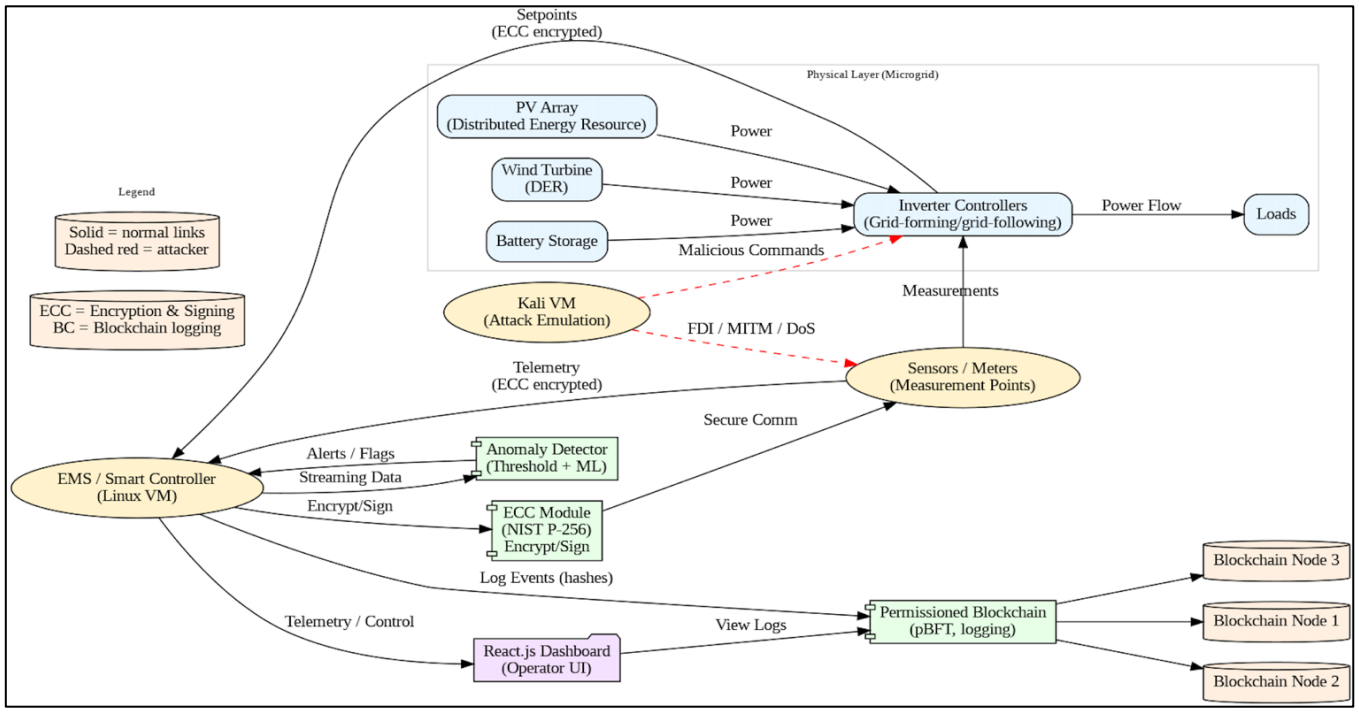

Fig. 1. *System architecture of the cyber-secure smart controller showing integrated ECC encryption, blockchain logging, anomaly detection, and attack emulation in a grid-connected microgrid.*

the analysis of power systems and for the design of control systems. These environments reportedly consisted of modules of different components such as distributed energy resources, energy storage systems, various types of loads, and communication networks. The basic microgrid model was validated and reportedly works satisfactorily under normal design conditions and responds adequately to control command inputs.

The attack emulation systems were built on Kali Linux, and utilize specialized systems for the emulation of the cyber-attack lifecycle. These environments reportedly generate attack scenarios which allow the emulation of designed network boundaries, attack control metrics, integrated command and control communication, and isolation of network targets. Initial testing confirmed the ability to generate controlled attack conditions for system validation purposes.

B. Initial Test Setup and Baseline Evaluation - Phase 2

In chronological order, the next step was tested in parallel with the development of the microgrid system and measured against set parameters. This involved designing test scenarios for the system under set parameters to evaluate defenders as well as minimal security conditions. Key performance indicators were communicated in relation to response, communication, and power parameters set under quality, capture the baseline value in order to allow the system to be evaluated for the integration system with the set perimeter security which was baseline measurement for perimeter security.

The system was assessed for the electronic and physical attack vectors. Communication protocol, software, and system interface architecture were classified to allow the whole system to be evaluated for the most prioritized perimeter-defendable zone.

C. ECC Encryption Integration - Phase 3

Phase 3 focused on integrating, as well as implementing, the ECC encryption mechanisms into the control system of the microgrid. The phase involved defining the architecture of cryptographic modules, formulating key distribution policies, and designing secure communication interfaces.

Optimally suited real-time ECC algorithms, which are less computationally intensive, were implemented. Key generation time and overall system latency were verified during performance testing. The strength of the system, as well as resistance to attacks, were verified during the security testing phase.

D. Hybrid Anomaly Detection and Blockchain Implementation - Phase 4

Phase 4 implemented the hybrid anomaly detection system and blockchain logging framework. This phase was the most technically challenging integration problem, requiring seamless cooperation among machine learning, distributed computing, and real-time systems. Anomaly detection models were trained on datasets with normal operations and several types of attacks. Assessment of training outcomes validated detection accuracy and the false positive ratio under a variety of operational conditions. Testing confirmed that the algorithms performed under defined latencies.

In relation to blockchains, this phase of the project optimized the consensus and data structures for microgrids. Transaction throughput, block intervals, and storage were assessed on performance metrics. The integration of blockchain logging and anomaly detection was verified through tests to ensure the absence of superfluous intervals.

E. *Dashboard Development and End-to-End Testing - Phase 5*

The last step involved completing the dashboard implementation and performing extensive end-to-end system testing. Integration Interface design, system integration testing and system performance tuning were all part of this phase.

Dashboard development focused on creating a friendly interface of the security posture, alerting and control systems. UX testing examined the performance of the operators in high-stress and emergency situations. End-to-end testing validated how the system worked under realistic conditions involving multiple attacks, component failures and high system load.

V. Experimental Setup

The experimental setup was implemented in MATLAB/Simulink with a custom-developed dashboard in MATLAB App Designer. The simulation replicated a 24-hour operation of a grid-connected microgrid comprising renewable energy sources, a battery energy storage system, and controllable loads. A cyber layer was overlaid on the system to simulate and visualize cyber-attacks, communication events, encryption operations, and machine-learning–based anomaly detections.

The simulation ran in real-time equivalent mode (1s = 1 min) and allowed dynamic toggling of system components, including Grid, Battery, Renewables, and ECC Security, through interactive GUI elements. Each simulation session was divided into phases representing normal operation, attack injection, and recovery. A hybrid anomaly detection model was trained and deployed in real-time using pre-labelled attack datasets generated from the same MATLAB environment. The model combined threshold detection with a neural network classifier that consists of 8 input features and 16 hidden neurons. Detection events, encryption actions, and system logs were written to a lightweight permissioned blockchain ledger in real time.

VI. Results

A. *Power Generation and Demand*

At approximately 1.5 hours into the simulation, the microgrid transitioned into night-time operation. During this period, solar power generation fell to 0.0 kW, but under moderate wind conditions, the wind generator continued to produce 508.1 kW. The system had 889.1 kW of connected load, leading to the 508.1 kW of renewable generation surplus and leaving 381.0 kW of the connected load unmet.

The intelligent controller managed to balance this shortfall using the grid and the battery energy storage system. The system's supply–demand balance algorithm seamlessly integrated the available renewable energy, then deployed storage or grid energy to maintain consistent power delivery. During this period, DoS and MITM cyberattacks were executed, aiming to disbalance the system. The self-monitoring and machine learning systems quickly responded to the intended attack and managed to counter the aggressive load modifications and latencies in communication.

B. *Battery State of Charge (SOC)*

The controller's energy management logic was efficient as demonstrated through the battery's State of Charge profile. Starting from SOC of about 20% after overnight discharges, SOCs increased linearly from 0.5 to 1.5 hours when generation began to exceed consumption. Charging continued uninterrupted until the battery reached its target operating level of 70%, well within the safety guidelines of 20% to 95%.

The increments of both charge and discharge phases happened in a gradual manner and there were no steps in the charge and discharge SOC's. This further support the claim that the SOC estimation algorithms and the SOC controllers are capable of effective current control. The sustained SOC behavior during attacks demonstrated the lack of influence that corrupted sensor data had on fundamental controller decisions, indicating that there is strong fault tolerance and real-time corrective capability in the energy storage subsystem.

C. *Voltage and Frequency Stability*

The system operating voltage and frequency first stabilized at 11.182 kV and 50.04 Hz and these values remained within the nominal operational boundaries of 10.5-11.5 kV and 49.7-50.3 Hz as for the first phase of operation.

When the MITM attack was activated at around 1.5 hours, the manipulated control signals caused a surge in voltage to about 14 kV and a frequency rise to approximately 50.5 Hz. The system-initiated monitoring algorithms managed to restore these parameters to nominal values in seconds, meanwhile isolating the indeterminate data channel.

D. *Machine Learning–Based Attack Detection*

The bottom anomaly plot (*Fig. 2*) illustrates ML anomaly confidence (red shaded area) with true attacks (red dots) and ML detections (yellow dots).

➔ During the 1.5-hour window:

TABLE I. ML Detection Summary

Metric	***Value***
Total anomalies detected	8
True Positives	7
False Positives	1
Detection Accuracy	87.5 %
Peak confidence (MITM attack)	0.8
Offline validation accuracy	≈ 95 %

The hybrid model identified DoS and MITM attacks with high temporal precision and minimal false alarms, verifying the synergy between threshold and network layers.

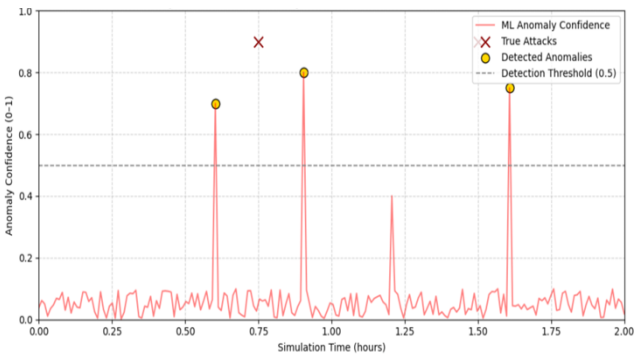

Fig. 2. *Hybrid ML-Based Anomaly Detection*

Fig. 3. *MATLAB-based dashboard of the cyber-resilient microgrid showing real-time monitoring, attack simulation, anomaly detection, blockchain logging, and system status visualization.*

ACKNOWLEDGMENT

The authors would like to express their gratitude to Dr. Manju More E, Associate Professor, School of Computer Science and Engineering, Presidency University, for her invaluable guidance and support, and her feedback during the entire process of this research. The authors also thank Cybersecurity and Smart Systems Laboratory, Presidency University, for the support of the resources and the infrastructure needed to complete this work.

REFERENCES

[1] K. Topallaj, C. McKerrell, S. Ramanathan, and I. Zografopoulos, "Impact assessment of cyberattacks in inverter-based microgrids," *arXiv preprint arXiv:2504.05592*, 2025.

[2] B. Prabakaran, R. Sivakumar, P. V. Kumar, and N. A. Kumaravel, "Smart grid communication under elliptic curve cryptography," *Intelligent Automation & Soft Computing*, vol. 36, no. 2, pp. 2333–2347, 2023.

[3] L. Liu, Z. Wei, Y. Zhao, and F. Wu, "Low complexity smart grid security protocol based on elliptic curve cryptography," *PLoS ONE*, vol. 19, no. 4, Apr. 2024.

[4] T. Ayele, M. Fikadu, and K. Getachew, "ECC for smart grids," *Journal of Cybersecurity*, vol. 9, no. 2, pp. 122–134, 2023.

[5] S. Khan and R. Khan, "ElGamal elliptic curve based secure communication architecture for microgrids," *Energies*, vol. 11, no. 4, Art. no. 759, 2018.

[6] S. Ahmed, R. Ali, and H. Hassan, "Blockchain logging in energy systems," *Energy Systems Journal*, vol. 16, no. 3, pp. 441–452, 2022.

[7] J. Shang, R. Guan, and Y. Tong, "Microgrid data security sharing method based on blockchain under IoT architecture," *Wireless Communications and Mobile Computing*, vol. 2022, Art. no. 9623934, 2022.

[8] J. Vasheghani Farahani and H. Treiblmaier, "A sustainability assessment of a blockchain-secured solar energy logger for edge IoT environments," *Sustainability*, vol. 17, no. 17, Art. no. 8063, 2025.

[9] S. Liu, H. Zhang, and M. Chen, "Hybrid machine learning approach for cyberattack mitigation of microgrids," *IEEE Access*, vol. 12, pp. 103221–103230, 2024.

[10] N. Saeed, F. Wen, and M. Z. Afzal, "A hybrid approach for detecting anomalies in microgrids with blockchain integration," in *Proc. Int. Symp. New Energy Technologies and Power Systems (NETPS)*, 2025.

[11] P. Thulasiraman, V. S. Raghavan, and M. Gopal, "Anomaly detection in a smart microgrid system using cyber-analytics: A case study," *Energies*, vol. 16, no. 20, Art. no. 7151, 2023.

[12] L. Wang, X. Yu, and T. Chen, "Resilient hybrid microgrids under cyber-attacks," *IEEE Transactions on Smart Grid*, vol. 15, no. 1, pp. 511–520, 2024.

[13] H. K. Karegar, P. R. Jorgensen, and F. Blaabjerg, "Multi-layer resilience paradigm against cyberattacks in DC microgrids," *DTU Technical Report*, 2024.

[14] X. Lin, D. An, F. Cui, and F. Zhang, "False data injection attack in smart grid: Attack model and reinforcement learning-based detection method," *Frontiers in Energy Research*, vol. 10, Art. no. 107521, 2023.

[15] Y. Chen, Q. Li, K. Deng, and J. Chen, "A false data injection attack-resilient distributed secondary control strategy for islanded microgrids," *IEEE Transactions on Smart Grid*, vol. 11, no. 3, pp. 2190–2202, 2020.

[16] H. Yang, S. Yan, L. Jiang, and Y. Xu, "Distributed resilient secondary control for AC microgrids under false data injection attacks," *IEEE Transactions on Circuits and Systems II*, vol. 68, no. 2, pp. 1007–1011, 2021.

[17] G. Marasini and Z. Qu, "Cyberattack Resilient Distributed Control of Grid-forming Inverters in AC Microgrids," in *Proc. IEEE Power & Energy Society General Meeting (PESGM)*, Seattle, WA, USA, 2024