# 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's 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.***

***This paper presents a multifunction smart controller with cyber defenses based on Elliptic Curve Cryptography (ECC) for real-time secure communications, lightweight blockchains for immutable audit logs, and integrated hybrid anomaly detection for real-time cyber-physical system defenses.***

***The advantages of ECC, in this case, include the establishment of low-latency secure communication. Blockchain provides operational integrity, real-time data, and traceability. The proposed hybrid model improves the accuracy and reliability of detecting intruder systems and other malfunctions in operational cyber-physical systems. Additionally, a React.js-based 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 (ECC), Blockchain, 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. These systems support local generation, storage and distribution of energy which can operate in both grid connected and islanded configurations. The integration of advanced information and communication technologies (ICT) that enable such capabilities also bring along substantial cybersecurity risks.

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.

False Data Injection (FDI) attacks represent one of the most significant threats to microgrid operations. 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.

Denial of Service (DoS) aims at crushing the communicational and computational capabilities of the microgrid control system 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. Microgrids control systems are subject to real-time operations, hence they are easily vulnerable to DoS attacks due to their strict latency requirements.

Man-in-the-middle virtual attacks intercept and manipulate the control and monitor channels of a conversation 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.

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. We integrate agile countermeasures for each attack vector, including advanced cryptography, distributed ledger technology, and intelligent anomaly detection within microgrid systems dedicated platforms. This layered defense model ensures resilience by addressing both preventive and detective security requirements simultaneously.

## II. Literature Review

The cybersecurity challenges in microgrid systems have attracted significant research attention in recent years, with various approaches proposed to address specific aspects of the security landscape. This section reviews relevant work in the areas of cryptographic protection, blockchain applications, anomaly detection, and resilient control strategies for microgrids.

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.

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 [18], 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. 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.

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.

This research highlighted the importance of implementing robust communication protection mechanisms and developing attack-resilient control strategies.

Despite the advancements made, the literature still possesses deep shortcomings. Most current approaches treat each security problem in isolation, poorly addressing the complicated relations among various attacking techniques and defense methodologies. The integration of microgrid technologies and the architecture of real time multilevel grid systems is pioneering and substantially incomplete. Furthermore, issues regarding computation and communication latency, and overall system reliability, are, far too frequently, excluded from the solutions presented.

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 incorporates existing solutions' shortcomings while addressing real-world implementation challenges for 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 of course, real-time monitoring of the system architecture, allows for secure monitoring operated at the highest efficiency possible.

### *A. System Architecture Overview*

The overall system architecture consists of five primary components. These components include the cyber-attack simulation environment, ECC encryption module, hyper anomaly detection system, lightweight blockchain logging framework, and the monitoring dashboard that utilizes React.js. 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

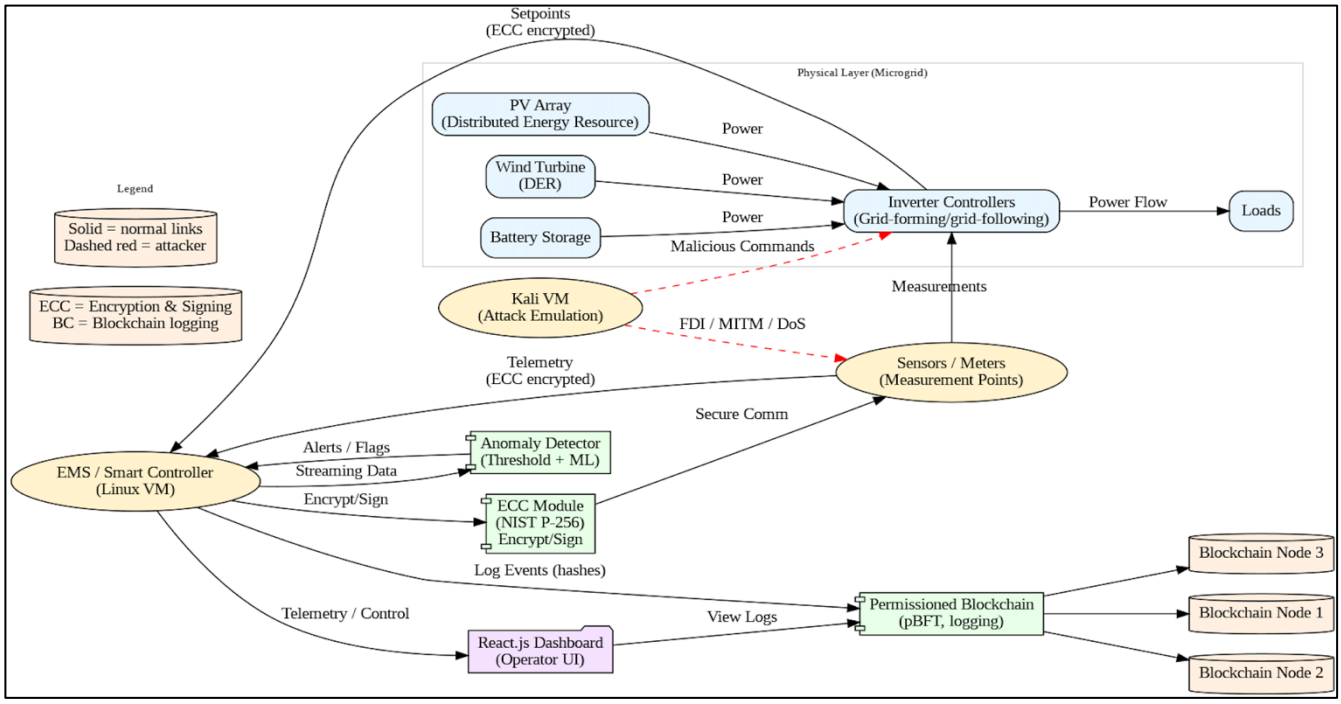


Fig. 1. *System architecture for the Cyber-Security Enabled Smart Controller*

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 the 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 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:

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

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. 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 component employs a hybrid architecture combining Long Short-Term Memory (LSTM) networks and logistic regression algorithms. LSTM networks are trained to model normal system behavior patterns and detect temporal anomalies in time-series data. Logistic

regression provides rapid classification of discrete events and parameter deviations. The hybrid approach enables the system to detect both gradual attacks that evolve over time and sudden anomalous events.

Training data for the machine learning models is generated using comprehensive simulation scenarios that include normal operational conditions and various attack patterns. The training dataset encompasses FDI attacks with different magnitude and duration characteristics, DoS attacks targeting various communication channels, and MITM attacks with different data manipulation strategies.

### *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 rapid 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. React.js 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 React.js 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 interactive charts and graphs allows operators to conduct retrospective examinations and identify security anomalies as well as understand the trends. Alert management functions permit operators to acknowledge, respond to, and monitor security alterations in a timely manner. User authentication and access allow only certain people to view critical security control and information, defending sensitive information from unwarranted scrutiny. Under security policies, a user's operational role and clearance are the only reasons to exercise the restrictions of set actions.

### *F. Integration and Coordination*

The operational framework manages the interactions among all components of the system and ensures their effectiveness under different operational scenarios. Using adaptive algorithms, the system manages security-performance trade-offs by adjusting security levels based on prevailing threat conditions and operational needs.

Mechanisms of real-time coordination guarantee that security measures do not conflict with essential control functions and do not destabilize the system.

## 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.

Phases 1 and 2 have been completed, covering environment setup, initial configuration, and vulnerability assessment. Phases 3, 4, and 5 covering ECC encryption integration, hybrid anomaly detection with blockchain implementation, and dashboard development with end-to-end testing are currently planned and will be executed in subsequent stages.

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 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 will focus on integrating, as well as implementing, the ECC encryption mechanisms into the control system of the microgrid. The phase involves 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, will be implemented. Key generation time and overall system latency will be verified during performance testing. The strength of the system, as well as resistance to attacks, will be verified during the security testing phase.

Integration testing will focus on the performance of the encrypted communication links, taking into consideration diverse operational scenarios which comprise high data volume, network congestion, and component outages. Validation will test if the messages can be authenticated, data can be controlled, and real-time performance requirements can be sustained.

### D. Hybrid Anomaly Detection and Blockchain Implementation – Phase 4

Phase 4 will implement the hybrid anomaly detection system and blockchain logging framework. This phase is the most technically challenging integration problem, requiring seamless cooperation among machine learning, distributed computing, and real-time systems.

Anomaly detection models will be trained on datasets with normal operations and several types of attacks. Assessment of training outcomes will validate detection accuracy and the false positive ratio under a variety of operational conditions. Testing will confirm the algorithms perform under defined latencies.

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

### E. Dashboard Development and End-to-End Testing – Phase 5

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

Dashboard development will focus on creating a friendly interface of the security posture, alerting and control systems. UX testing will examine the performance of the operators in high-stress and emergency situations.

End-to-end testing will validate how the system works for a realistic conditions scenario of multiple attacks, component failures and high system load. Performance tuning will resolve any performance issues and system integration issues uncovered to ensure the system works at the optimum.

## V. Expected Outcomes

### A. Enhanced Security Resilience

The integrated security framework is expected to enhance security systems and rationalize and improve the attack detection and response process. The varied layers of ECC encryption coupled to blockchain and hybrid anomaly detection creates multiple layers for the attacker. The resulting attack will therefore be more expensive and more difficult to perform.

The ECC encryption implementation is expected to provide secure communication with encryption/decryption times under 1 millisecond for typical message sizes, ensuring that security enhancements do not compromise real-time control requirements. The lightweight nature of elliptic curve algorithms enables deployment on resource-constrained embedded systems commonly used in microgrid applications.

### B. Tamper-Proof Operational Logging

The use of blockchains as a logging system allows for microgrid operations to be more open and accountable. Any critical event which has a security relevance is recorded in a distributed ledger. This allows for the complete audit and forensic review which is needed after a security event.

The target block generation in the consensus mechanism is lightweight and aims to be under ten seconds. The mechanism also aims to have Byzantine fault tolerance of at least one third of the nodes participating. This means that the system can be in real-time logging in of security without adding any major delays to the operations.

### C. Improved Operational Awareness

The React.js dashboard gives operators visibility and offers real-time responses to threat mitigation within the system's internal security posture. With the help of many data sources, the intuitive dashboard helps in offering better situational awareness as well as decision making in the event of a security incident.

Security operators can make use of tactics to analyze system security data in order to monitor emergence trends, patterns and concealed correlations. This improved awareness feature enables proactive security management and proactive threat hunting.

### D. Performance Considerations

The system we propose has been designed to minimize the overhead of security enhancements through optimization of proposed algorithms, even though designed systems generally entail some computational and communication overhead. From the preliminary analysis we have conducted, the computational overhead has been established to be below 5% for the available processing capacity of microgrid controllers.

Overhead communication has been established through the use of fast cryptographic procedures and optimized blockchain protocols. Under normal operational conditions, the anticipated increase to the security mechanisms is below 15%, which is a downward estimation of the typical communication capacity margins.

TABLE I. PERFORMANCE METRICS

| *Metric* | *Target / acceptable level* |
|---|---|
| ECC overhead (enc/dec) | <1 ms per message |
| Blockchain block time | <10 s for write-confirmation |
| Detection latency | <2 s from data arrival |
| Anomaly detection accuracy | >90% (target) |
| False positive rate | <5% (target) |

### *E. Performance Considerations*

The security framework is expected to provide economic benefits through reduced risk of successful cyber-attacks and improved operational reliability. The cost of implementing the proposed security measures is substantially lower than the potential economic impact of successful attacks on critical microgrid infrastructure.

## VI. CONCLUSION & FUTURE WORK

This document describes a smart controller for microgrids integrated with technologies in cybersecurity and blockchain to record and control system performance in real-time and optimize its operation with microgrids. The focus remains on addressing vulnerabilities and performance issues simultaneously, a feature absent from most proposed solutions. This system utilizes Elliptic Curve Cryptography, lightweight blockchain logging, and hybrid anomaly detection systems.

This proposed system is unique in embedding these features in a single and real-time distributed system. Moreover, in contrast to competing systems that address distinct and individual security issues with no coordination, this framework integrates and defends against multiple approaches, while managing stringent performance which is typical from power system operations.

Low latency is obtained from the provided ECC as the Elliptic Curve Cryptography implementation bridges latency gaps with real-time control meshed systems. In addition, hybrid anomaly detection utilizes the most effective features from alarm systems responsive to intrusion detection and learns from agnostic system models, which comprise real-time feature detection systems. Everything works seamlessly as the system performance remains uncompromised. The blockchain framework is tamper-proof to promote audit capabilities as well as protective documentation.


## 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 guidance, encouragement, and insightful feedback throughout the course of this research.


## 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] E. Drayer and T. Routtenberg, “Detection of false data injection attacks in smart grids based on graph signal processing,” *arXiv preprint arXiv:1810.04894*, 2018.

[16] 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.

[17] 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.

[18] 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