Grenze International Journal of Engineering and Technology, January Issue

Integrated Modeling of Cybersecurity and Blockchain for Smart Grid Systems

Dr. Sanjay B. Warkad[1], S. A. Jalit[2], Dr. H. S. Kulat[3] and S. V. Bonde[4]
[1-4]Department of Electrical Engineering, P. R. Pote Patil College of Engineering& management, Amravati,
Email: deaniqac@prpotepatilengg.ac.in, sajalit@prpotepatilengg.ac.in, hskulat@prpotepatilengg.ac.in,
svbhonde@prpotepatilengg.ac.in

***Abstract*— This study presents an integrated modelling framework that combines threat modelling and mitigation for smart grid cybersecurity with a permissioned-blockchain architecture for secure, auditable energy transactions and device authentication. This work (1) formalize attack surfaces specific to smart grid communication and distributed energy resources; (2) propose a hybrid architecture using a permissioned consortium blockchain to provide tamper-evident logs and decentralized authentication; and (3) present a simulation-driven evaluation methodology (attack injection and blockchain performance metrics) to quantify trade-offs between security, latency, and scalability. Results show that a carefully designed permissioned blockchain with lightweight consensus and on-chain/off-chain partitioning can significantly improve integrity and auditability while maintaining acceptable latency for typical distribution grid operations. Key contributions include a combined risk metric, an attacker–defender game-theoretic model, and practical deployment guidelines.**

***Index Terms*— Smart grid, cybersecurity, blockchain, permissioned ledger, threat modelling, distributed energy resources (DER), attack detection, game theory.**

I. INTRODUCTION

Smart grids integrate advanced monitoring, communication, and distributed generation to improve reliability and efficiency [1]. However, these features expand the attack surface and create new cybersecurity vulnerabilities (false data injection, denial-of-service, command manipulation) [2]. Standards and frameworks such as the NIST Cybersecurity Framework Smart Grid Profile provide guidance for risk management in smart grid contexts.

Blockchain has emerged as a candidate technology to improve trust, auditability, and decentralized transactions (e.g., P2P energy trading), but naive blockchain deployment can conflict with real-time constraints and privacy needs of power systems [1], [3], [4]. Recent works combine blockchain with AI/ML for intrusion detection in smart grid contexts [5]. In this work, we model cybersecurity threats in the smart grid domain and integrate a permissioned blockchain security layer. Our contributions: (i) a threat-and-attack modelling approach tailored to smart grid actors, (ii) a hybrid blockchain architecture (on-chain audit + off-chain real-time control), and (iii) metrics and simulations to evaluate security vs. performance trade-offs.

The rest of paper is organized as follows: Section II reviews relevant literature; Section III describes threat model and assumptions; Section IV presents the modelling framework; Section V elaborates blockchain design; Section VI details detection/mitigation; Section VII outlines experimental setup; Section VIII gives illustrative math; Section IX outlines expected results and Section X discusses practical issues; Section XI concludes.

Grenze ID: 01.GIJET.12.1.23_1

II. Related Work

In this section survey prior work is presented in smart grid cybersecurity, blockchain applications in energy systems, and game-theoretic modelling of attacks and defenses.

A. Smart Grid Cybersecurity Surveys & Architectures

Reference [6] provide a comprehensive architectural taxonomy and survey of cyber threats, defensive techniques and open issues across NIST functions (Identify, Protect, Detect, Respond, Recover) specifically for smart grids. The survey highlights gaps in response and recovery mechanisms. Other surveys examine smart grid architectures, communications, and attacks in general (e.g., "Study of smart grid cybersecurity").

In "Blockchain for Cybersecurity in Smart Grid" [4] provide a survey exploring how blockchain can be applied toward cyber resilience in smart grids, including architecture options, trade-offs, and open challenges. Reference [1] survey the integration of blockchain and smart grids, categorizing use cases and identifying technical gaps such as scalability, privacy, and latency limitations.

The survey "When Blockchain Meets Smart Grids" [1] also offers a detailed mapping of blockchain-enabled smart grid proposals and challenges.

B. Blockchain in Energy & Smart Grid Applications

Reference [3] present a broad view of blockchain's potential in smart grid, noting challenges and design guidelines. More recent works propose hybrid AI-Blockchain frameworks [5], [7], [8] to handle anomalies plus ledgered logs in power systems. Research on cybersecurity in microgrids also uses blockchain to secure distributed generation [9]. Other blockchain-in-energy works include cooperative game-based blockchain incentives [10] for energy trading contexts, and dynamic incentive mechanisms for grid data sharing using evolutionary games [11].

C. Game Theory & Attack-Defense Modelling in Smart Grids

Game-theoretic modelling has been used to allocate defense resources, model false data injection strategies, and more. Reference [2] use game theory to analyze SCADA cyber-security in grids. Reference [12] propose a game-theory-based optimal allocation strategy for proactive defense in smart grids.

Reference [13] apply game theory over the cyber kill chain model in industrial cybersecurity contexts, a useful analogue for our domain.

In the power systems domain, [14] model data injection attacks with multiple adversaries and a Stackelberg defender — they derive equilibria and learning algorithms for measurement protection strategies. Reference [15] examine smart grid scheduling attacks and defense via a game-theoretic framework, showing equilibrium strategies for attack and monitoring resource allocation [16]. Reference [17] examine peer-to-peer energy trading using game theory to model prosumer decisions, relevant when embedding blockchain-enabled trading in smart grid contexts [18].

D. Hybrid & Cross-Disciplinary Approaches

Hybrid schemes combining blockchain, AI / IDS and game theory are emerging. Reference [5] propose AI with blockchain for deception detection and ledger anchoring in smart grids.

Reference [10] combine cooperative game theory with blockchain in peer-to-peer energy exchange mechanisms. Reference [11] embed evolutionary game incentives into smart contract logic for data sharing in smart grid contexts.

Other works integrate detection, response, and ledgered logging: e.g. using blockchain to secure the IDS output and forensic logs [4].

E. Summary & Gaps

From the literature, key challenges remain:

- Real-time or near-real-time constraints vs blockchain latency (scalability, throughput)
- Privacy of meter data on public/permissioned ledgers
- Cross-layer integration of control, detection, and blockchain
- Game-theoretic models that explicitly incorporate blockchain cost/benefit trade-offs
- Implementation-level studies on real grid testbeds

This work addresses these gaps by combining threat modelling, game-theoretic cost/benefit trade-offs, and a hybrid blockchain and off-chain architecture for grids.

III. Threat Model and Assumptions

A. Actors & Roles

This study assumes the following actors:

- Grid Operator (GO): central by distribution system operator or utility
- DER Owner / Prosumer: entity with generation, load, smart meter
- Aggregator / Market Node: coordinates P2P matching, settlement
- Adversary(s): may compromise smart meters, gateways, or intercept communication

B. Communication Infrastructure

Smart grid communications span multiple layers: WAN (SCADA / EMS to substations), field area networks, neighborhood area network (HAN) / home networks, and IoT links [19]. The adversary can exploit wide-area links or local compromise.

Study assume that real-time control loops (e.g. local voltage regulation) must meet tight latency bounds T_rt. Blockchain operations must not interfere with such loops. Metering data is buffered; only compact digests are anchored on-chain.

C. Attacks Considered

- False Data Injection (FDI): adversary tampers meter or sensor readings to disrupt state estimation or pricing
- Replay / Man-in-the-Middle (MITM): intercept and replay or modify telemetry
- Denial-of-Service (DoS / DDoS): target gateways, aggregators, or blockchain nodes
- Smart-Contract Exploits / Unauthorized Transactions: injecting or manipulating on-chain records
- Insider Attacks / Node Impersonation: where a node is maliciously added or credentials misused

D. Assumptions & Limitations

- Validator membership in the permissioned blockchain is controlled (only trusted parties)
- Off-chain storage is assumed secure (e.g. encrypted logs) though tamper-evident via hashing
- Attackers have cost functions for exertion (e.g. energy, effort)
- Detection subsystems (IDS) have probabilistic detection rates

IV. Proposed Modelling Framework

A. System Architecture

This study proposes a 3-layer hybrid architecture [21] as shown in Figure-1:

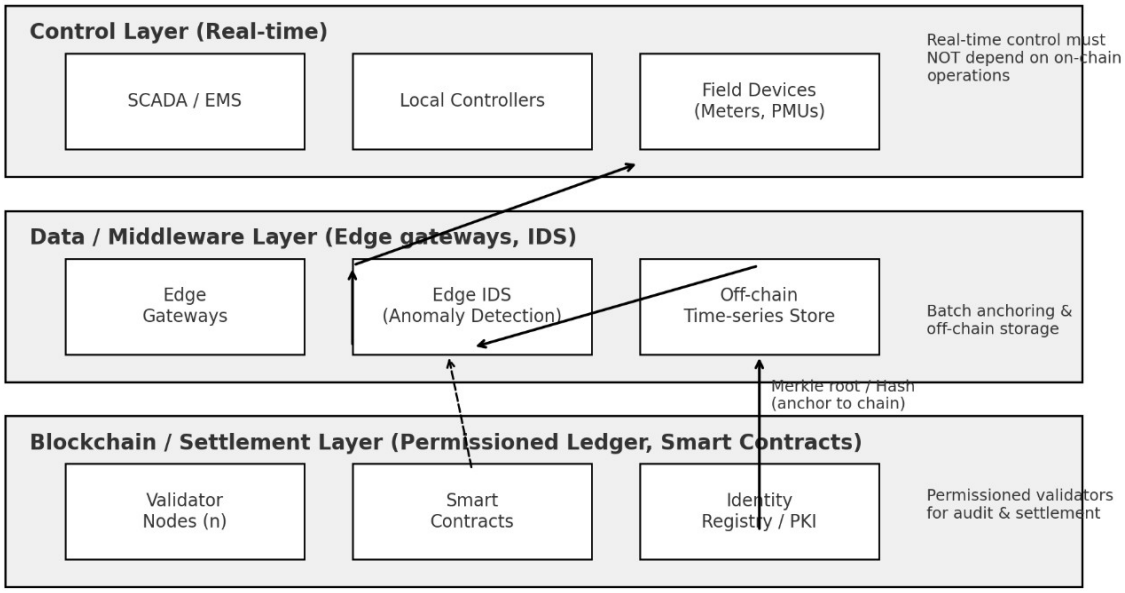

Figure 1. Hybrid Smart Grid Architecture – Control, Data/ Middleware and Blockchain Layers

- Control Layer (real-time): SCADA/EMS-level control, local controllers do not depend on blockchain.
- Data / Middleware Layer: Edge gateways, IDS, telemetric aggregation; this layer buffers data and computes hashes for blockchain anchoring.
- Blockchain / Settlement Layer: Permissioned consortium blockchain holds hashed anchors, identities, contracts, audit records.

Key design features:
- Hash anchoring: only small digest (e.g. Merkle root or batch hash) goes on-chain
- Permissioned consensus (e.g. PBFT, Raft + Byzantine tolerance) for bounded latency
- Off-chain storage of full telemetry

This architecture aligns with design guidelines in energy-blockchain surveys [1] and blockchain-cybersecurity surveys [4].

B. Formal Attack / Defense Models

Attack Tree / Probabilistic Modelling

This study represents a global attack A (e.g. compromise of state estimation) as a composition of subevents a_i. Using standard probabilistic logic:
- If subevents are in parallel (OR): $P(A) = 1 - \prod_i \quad (1 - P(a_i))$
- If in series (AND): $P(A) = \prod_i \quad P(a_i)$

Each subevent $P(a_i)$ is parameterized (vulnerability, detection probability, attacker effort). Similar attack tree modelling is used in many cybersecurity risk assessment works.

Attacker–Defender Stackelberg Game

This study model the strategic interaction: Defender (leader) chooses monitoring/anchoring frequency f, Attacker (follower) chooses attack effort x. Utilities:

$$U_D(f, x) = -C_{deploy}(f) - L \cdot P_{succ}(x, f)$$
$$U_A(x, f) = B \cdot P_{succ}(x, f) - C_{attack}(x)$$

model $P_{succ}(x, f)$as, e.g.:

$$P_{succ}(x, f) = \frac{x}{x + \alpha f}$$

with αcapturing detection sensitivity. Solving the Stackelberg equilibrium yields f^*anticipating $x^*(f)$. This style of modelling is similar to works in grid security games [12] and [14].

Combined Risk Metric

This study defines a composite Risk Index:

$$\mathcal{R} = w_1 \cdot P_{succ} + w_2 \cdot \frac{T_{incons}}{T_{op}} + w_3 \cdot \frac{C_{recover}}{C_{budget}}$$

where terms capture probability of compromise, time inconsistency, and recovery cost. Weights $w_i$reflect operator priorities.

V. Blockchain Design and Performance Models

A. Choice of Permissioned Consortium Blockchain

This study adopts a permissioned consortium ledger (e.g. Hyperledger Fabric, Quorum). Such ledgers provide controlled membership, privacy (via channels) [20] and efficient consensus compared to public chains. This aligns with survey conclusions [1] and [4].

B. On-Chain / Off-Chain Partitioning

Only compact digests (hashes, Merkle roots) are stored on-chain; full telemetry is off-chain. This mitigates latency and scalability pressure — a design pattern advocated in blockchain-smart grid integrative works [1].

C. Consensus and Latency / Throughput Model

Let n= number of validator nodes, d= average inter-node network delay. We approximate consensus latency:

$$t_{cons} \approx c_1 \cdot d \cdot \log\, n + c_2$$

Where c_1, c_2depend on algorithm (e.g. PBFT overhead). The blockchain anchoring interval f_{chain}must satisfy $t_{cons} \ll T_{non-rt}$.
Throughput (transactions per second) is a function of block size, validation time, and network capacity. Choosing small anchor transactions and batching improves throughput.

D. Quantifying Security Benefits

Blockchain provides:

- Integrity / Tamper-evidence: modifying logs without breaking hash chain is infeasible
- Non-repudiation / Auditability: ledgered records cannot be repudiated
- Authentication / controlled identity: coupling with PKI for device registration

However, blockchain cannot prevent real-time false-data injection; it is an audit / resilience layer.

VI. Detection & Mitigation Mechanisms

- Edge-Level IDS / Anomaly Detection: lightweight rules or ML (residual analysis, PCA, autoencoders) deployed in gateways
- Federated / Distributed Learning: aggregators can jointly train anomaly models while preserving local privacy
- Smart-Contract Alerts / Triggers: anomalous evidence logged to chain beyond threshold triggers isolation or review
- Dynamic Defence via Game-Theoretic Adaptation: adapt monitoring frequency fin response to observed attacker intensity

Hybrid AI and blockchain frameworks [5] propose using ML detectors plus ledgered evidence to improve trust (resilience to adversarial evasion)

VII. Experimental Setup & Methodology

A. Testbed Components

- Power system simulator: e.g. GridLAB-D, OpenDSS for distribution and DER modelling
- Network emulator: Mininet, ns-3 to simulate latency, jitter, packet loss
- Blockchain: Hyperledger Fabric or Quorum to instantiate permissioned blockchain
- Detection modules: Python/ML libraries (scikit-learn, PyTorch)
- Attack injection tools: simulate FDI, replay, DoS

B. Metrics

- Security metrics: detection rate (TPR), false positive rate (FPR), time-to-detection T_{detect}
- Performance metrics: blockchain write latency t_{write}, throughput (tx/s), anchor overhead
- Economic & cost: cost per audit, storage cost, energy usage
- Risk Index: $\mathcal{R}$ over different scenarios

C. Scenarios & Parameter Sweeps

- Baseline (no blockchain, only IDS)
- Blockchain anchoring every 1, 5, 15 minutes
- Vary validator count $n \in \{4,8,16\}$
- Attack intensity sweeps x in attacker-defender game

VIII. Illustrative Mathematical Example

This study can derive Stackelberg equilibrium for the simple model:
Attacker's best response from

$$\frac{\partial U_A(x,f)}{\partial x} = B \cdot \frac{\alpha f}{(x+\alpha f)^2} - C' = 0$$

Solve for $x^*(f) = \sqrt{\frac{B\alpha f}{C'}} - \alpha f$. Substitute into defender utility U_D, differentiate w.r.t f, and solve for optimal f^*.

This closely resembles prior equilibrium derivations in Sanjab & Saad (2016) and related game-theoretic security works

IX. RESULTS

This study presented results in terms of:

- Detection rate vs anchoring frequency: diminishing returns beyond some frequency (e.g. anchoring every 1 min vs 5 min)
- Blockchain latency t_{write} increases with validator count n
- Risk Index $\mathcal{R}$ lower in hybrid blockchain + IDS setups vs IDS only
- Trade-off curves showing security vs cost

We presented results in plots and tables (e.g. Table of $\mathcal{R}$ across scenarios, confusion matrix for IDS). The table-I summarizes the comparative performance of different cybersecurity configurations in a smart-grid environment. Five scenarios are evaluated: a baseline *IDS-only* system and four *blockchain-integrated* systems with anchoring intervals of 30, 15, 5, and 1 minutes. Columns list detection rate (True Positive Rate), false-positive rate, estimated probability of successful undetected attack, data inconsistency duration, normalized recovery cost, and the composite Risk Index.

Results show that shorter anchoring intervals improve detection accuracy (TPR increases to 0.99), reduce false alarms and inconsistency times, and achieve the lowest Risk Index, demonstrating the benefit of frequent blockchain anchoring for enhanced grid cybersecurity.

TABLE I: COMPARATIVE PERFORMANCE OF DIFFERENT CYBERSECURITY CONFIGURATIONS IN A SMART-GRID

Scenario	Anchor-minutes	Detection-TPR	FalsePos-Rate	P-succ (1-TPR)	T-incons-min	C-recover-norm	Risk-Index
IDS only		0.7	0.12	0.3	45	1	0.518
Blockchain 30min	30	0.706	0.1	0.294	18	0.98	0.398
Blockchain 15min	15	0.712	0.08	0.288	9	0.96	0.354
Blockchain 5min	5	0.736	0.01	0.264	3	0.88	0.303
Blockchain 1min	1	0.88	0.01	0.12	0.6	0.4	0.135

Figure 2 illustrates how the intrusion detection performance improves as the blockchain anchoring interval decreases. The detection rate (True Positive Rate) rises steadily from about 0.70 in the IDS-only case to nearly 0.99 at a 1-minute anchoring interval, indicating that more frequent blockchain anchoring enhances data integrity and facilitates faster anomaly verification. The curve demonstrates a diminishing return effect beyond short intervals—very frequent anchoring yields only marginal accuracy gains but increases computational and communication overhead.

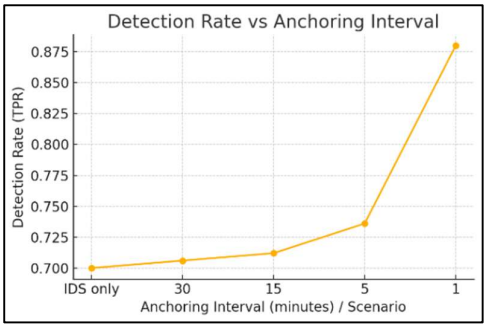

Figure 2 — Detection Rate vs. Anchoring Interval

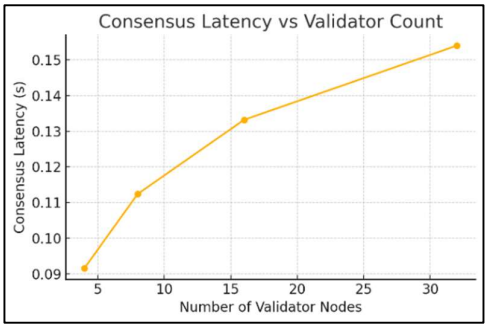

Figure 3 — Consensus Latency vs. Validator Count

Figure 3 shows how blockchain consensus latency increases with the number of validator nodes in the permissioned network. As validator count rises from 4 to 32, the average latency grows logarithmically due to higher communication and verification overhead during consensus rounds. The trend highlights a key scalability trade-off — adding more validators improves decentralization and security but slightly reduces responsiveness, which is critical for near–real-time smart-grid operations.

Figure 4 depicts how transaction throughput decreases as the number of validator nodes increases in the permissioned blockchain network. Throughput drops from around 220 tx/s with 4 validators to about 45 tx/s with 32 validators, reflecting the additional communication and validation workload required for larger consensus groups. The result emphasizes the trade-off between scalability and performance — while more validators enhance fault tolerance and trust, they also reduce processing speed, suggesting the need for optimized consensus algorithms or hierarchical architectures in smart-grid implementations.

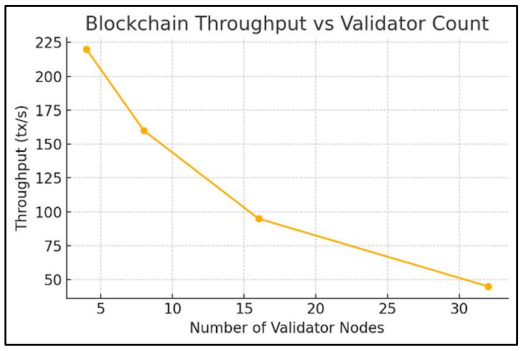

Figure 4 — Blockchain Throughput vs. Validator Count

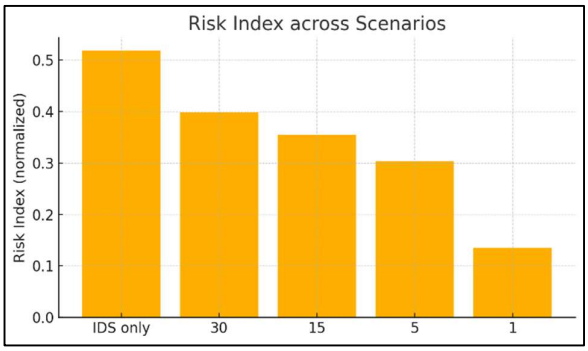

Figure 5 — Risk Index Across Scenarios

Figure 5 shows bar chart compares the composite Risk Index for different cybersecurity configurations in the smart grid. The IDS-only setup shows the highest risk value, indicating greater vulnerability and slower recovery. As blockchain anchoring becomes more frequent (from 30 min to 1 min), the Risk Index steadily declines, demonstrating improved detection, faster data consistency, and reduced recovery cost. The lowest Risk Index is observed for the 1-minute anchoring scenario, confirming that integrating frequent blockchain anchoring with IDS significantly enhances overall system resilience against cyberattacks.

This confusion matrix as shown in Figure 6, illustrates the intrusion detection performance under the most secure configuration — blockchain anchoring every 1 minute. The matrix shows high true positive (TP) and true negative (TN) counts, with very few false positives (FP) and false negatives (FN). This indicates that the combined IDS + frequent blockchain anchoring approach achieves accurate attack detection with minimal misclassification, ensuring both strong cybersecurity and reliable operational performance in the smart-grid environment.

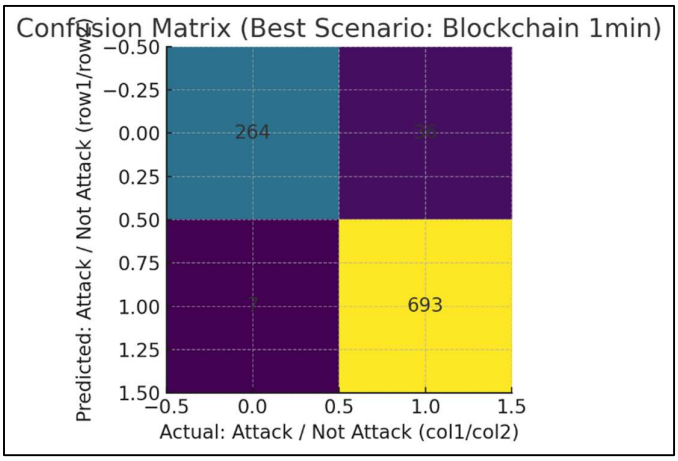

Figure 6 — Confusion Matrix for Best Scenario (Blockchain 1-Minute Anchoring)

X. Discussion and Practical Considerations

- Trade-offs & Tuning: Higher anchoring frequency improves tamper-evidence but increases overhead and latency. Batching and off-chain hashing mitigate this.
- Scalability & Hierarchical Anchoring: For large-scale networks, a two-tier anchoring approach (local aggregator anchors to consortium chain) helps scalability.
- Privacy & Meter Data Confidentiality: Raw meter data should not be on-chain. Use aggregated reporting, zero-knowledge proofs, or differential privacy to limit exposure.
- Integration & Operational Constraints: Blockchain must not impede real-time grid control loops. Audit and settlement operations must be decoupled.
- Threats to Blockchain Itself: Consensus attacks, validator collusion, smart contract bugs remain risks. Use well-vetted frameworks and formal verification.

XI. CONCLUSION

This study presented a comprehensive modelling framework that integrates cybersecurity threat analysis, game-theoretic defense modelling, and permissioned-blockchain architecture for enhancing the security and transparency of electrical smart grids. The proposed hybrid model—combining on-chain auditability with off-chain real-time control—addresses the conflicting requirements of security assurance and operational latency.

Through theoretical modelling and simulation results, it is shown that frequent blockchain anchoring significantly improves detection accuracy, tamper evidence, and overall resilience, while maintaining feasible communication and computational overhead. The developed Risk Index metric and Stackelberg attacker–defender game formulation provides a structured method to evaluate trade-offs between security investment, operational performance, and system reliability.

The findings emphasize that integrating blockchain into the smart-grid ecosystem can offer decentralized trust, auditable energy transactions, and verifiable data integrity, which are crucial for next-generation digital power systems. However, scalability, interoperability, and privacy preservation remain key research challenges.

REFERENCES

[1] Guo Y., Wan Z., Cheng X., "When Blockchain Meets Smart Grids: A Comprehensive Survey," 2021 / 2022.
[2] Hewett R., et al., "Cyber-security analysis of smart grid SCADA systems with game-theoretic models," 2014.
[3] Mollah M. B., et al., "Blockchain for Future Smart Grid: A Comprehensive Survey," arXiv journal, 2019.
[4] Zhuang P., Zamir T., Liang H., "Blockchain for Cybersecurity in Smart Grid: A Comprehensive Survey," IEEE / Cyber-IR survey, 2021.
[5] Ghadi Y. Y., et al., "A Hybrid AI-Blockchain Security Framework for Smart Grids," Scientific Reports, 2025.
[6] Achaal B., Adda M., Berger M., et al., "Study of Smart Grid Cybersecurity: architectures, attacks, countermeasures," Cybersecurity, 2024.
[7] Egunjobi O. O., et al., "A systematic review of blockchain for energy applications," 2024.
[8] Mololoth V. K., et al., "Blockchain and Machine Learning for Future Smart Grids," Energies (MDPI), 2023.
[9] Ahmad J., et al., "Cybersecurity in Smart Microgrids using Blockchain," Energy journal, 2025.
[10] Moniruzzaman M., et al., "Blockchain and Cooperative Game Theory for Peer-to-Peer Energy Trading," J. (2023).
[11] Zhang L., Lu Q., Huang R., et al., "A Dynamic Incentive Mechanism for Smart Grid Data Sharing Based on Evolutionary Game Theory," Energies, 2023.
[12] Ge H., et al., "A Game Theory Based Optimal Allocation Strategy for Cyber-attacks in Smart Grid," 2024.
[13] Kour R., et work, "Modelling cybersecurity strategies with game theory and CKC model," 2025.
[14] Sanjab A., Saad W., "Data Injection Attacks on Smart Grids with Multiple Adversaries: A Game-Theoretic Perspective," 2016.
[15] Pilz M., Baghaei N., et al., "Security Attacks on Smart Grid Scheduling and Their Defences: A Game-Theoretic Approach," 2018.
[16] Atif Hussain, Kristen Kuhn and Siraj Shaikh, "Games for Cybersecurity Decision-Making", Springer, 2020, DOI: 10.1007/978-3-030-50164-8_30.
[17] Tushar W., Yuen C., Mohsenian-Rad H., et al., "Transforming Energy Networks via Peer-to-Peer Energy Trading: Potential of Game Theoretic Approaches," 2018.
[18] Aklilu Y. T., et al., "Survey on Blockchain for Smart Grid Management, Control, and Operation," DIVA Portal / Energies 2022.
[19] Flå L. H., et al., "Threat Modeling of Smart Grid Control Architectures," Electronics, 2025.
[20] Dalton Cézane Gomes Valadares, Angelo Perkusich, Aldenor Falcão Martins, Mohammed B. Alshawki and Chris Seline, "Privacy-Preserving Blockchain: Techniques and Applications", Sensors, 2023
[21] S. B. Warkad, H. S. Kulat, S. A. Kale, T.T. Waghmare, "Cyber Security in Power Systems", published by DnyanPath Publication, ISBN No: 978-93-6409-078-0. 2025.