Autonomous Blockchain-Enabled Security Framework for Smart Grids Using Adaptive AI

Brinal Colaco[1], Nazneen Ansari[2]
Department of Computer Engineering-St. Francis Institute of Technology, University of Mumbai, Borivali, Mumbai, India[1,2]
Department of Computer Engineering-Vidyavardhini's College of Engineering and Technology,
University of Mumbai, Vasai, Mumbai, India[1]

Abstract—**The increasing interconnectivity of smart grids exposes critical energy infrastructure to more sophisticated cyber threats, necessitating adaptable and auditable security measures. This study presents a blockchain-enabled, self-improving intrusion detection system (IDS) that integrates a permissioned blockchain, autonomous governance loops, and a hybrid CNN–LSTM detector. The platform retrains models across federated nodes using blockchain-anchored data, facilitates automatic containment through smart contracts, and permanently stores validated alarms. Following multiple self-improvement cycles, the system enhances its performance from an initial 94.5% accuracy and 4.2% false positive rate (FPR) to 98.1% accuracy, a 97.6% detection rate (recall), and a 2.1% FPR in simulated tests. In comparison to baselines, a blockchain-only IDS recorded 94.1% accuracy with a 4.8% FPR, while a conventional machine learning-based IDS achieved 92.7% accuracy with a 5.4% FPR. Operationally, blockchain anchoring provided a throughput of approximately 1,200 transactions per second with an average transaction latency of about 1.5 seconds. The combined detect-to-contain latency for high-severity events was approximately 3.2 seconds. These findings demonstrate that a scalable, low-FPR, and rapid-response security paradigm for modern smart grids can be achieved by integrating adaptive artificial intelligence with decentralized, robust governance.**

Keywords—Smart Grid Security; intrusion detection system (IDS); adaptive AI; deep learning; false data injection (FDI) attacks; cyber-physical systems (CPS)

I. Introduction

Recent advancements in power systems have facilitated a rapid transition to smart grids, offering new opportunities for sustainability, automation, and efficiency. However, this transition has also introduced significant security challenges. Smart grids, which depend on the extensive integration of distributed energy resources, Internet of Things (IoT) devices, and information and communication technologies (ICTs) [1], enable intelligent decision-making, dynamic load balancing, and real-time monitoring. Despite these benefits, the increased connectivity renders the grid susceptible to various cybersecurity threats, including replay attacks, false data injection (FDI), denial-of-service (DoS), and probing attempts [2]. If not adequately addressed, these threats could compromise the availability, confidentiality, and integrity of critical energy infrastructure.

Traditional security solutions, primarily based on standalone machine learning models or rule-based intrusion detection systems (IDS) [3], often struggle to detect complex and dynamic cyberattacks. These methods are vulnerable to advanced persistent threats and zero-day attacks due to their reliance on static learning patterns or predefined signatures [4]. In recent years, deep learning techniques, particularly Convolutional Neural Networks (CNNs) and Long Short-Term Memory (LSTM) networks [5], have demonstrated enhanced performance in identifying complex attack patterns by extracting both spatial and temporal information from network traffic data [6]. Hybrid approaches that integrate CNN and LSTM have been shown to significantly improve detection accuracy by leveraging the complementary strengths of both models [7].

Concurrently, blockchain technology has emerged as a potential solution for enhancing trust, transparency, and decentralization in smart grid operations. Blockchain facilitates decentralized access control, tamper-proof data sharing among distributed entities, and immutable tracking of security events [8]. Consensus algorithms such as Proof-of-Authority (PoA) enable high-throughput, energy-efficient blockchain networks, making them suitable for real-time smart grid applications [9]. By integrating blockchain technology with AI-based intrusion detection systems, a decentralized, reliable, and trustworthy cybersecurity framework for smart grids can be established [10].

A significant limitation of current smart grid cybersecurity frameworks is their lack of flexibility and autonomy. Most contemporary systems heavily rely on human operators for model updates, policy enforcement, and attack response strategies, which introduces vulnerabilities and delays response times. To address this, researchers are exploring autonomous AI-driven security solutions capable of self-improvement [11]. These systems continuously retrain and refine their models using feedback data to reduce false positives and enhance detection accuracy over time [12].

In this study, we propose an AI-Based Intrusion Detection Autonomous Blockchain-Enabled Smart Grid Security Framework that integrates three critical components:

- An intrusion detection system that combines CNN and LSTM for accurate identification of both known and novel threats.
- A blockchain layer with smart contracts to ensure tamper-proof security event tracking, decentralized trust, and transparency.

- A self-improvement and autonomy cycle that enables the IDS to dynamically adapt to emerging attack patterns with minimal human intervention.

The contributions of this work are summarized as follows:

- We have developed an Intrusion Detection System (IDS) utilizing deep learning techniques, which surpasses both standalone deep learning models and traditional machine learning approaches in terms of detection efficacy.
- We propose a decentralized security framework for smart grids, underpinned by blockchain technology, which ensures low latency, high throughput, and energy-efficient operations.
- In real-time smart grid environments, we introduce an autonomous self-improvement mechanism that enables the IDS to continuously adapt to emerging cyber threats.

Although individual elements like blockchain-based logging, deep learning-based intrusion detection, and adaptive security mechanisms have been studied separately in previous research, this work advances the state of the art by tightly coupling them into an autonomous security framework that is governance-aware. The suggested solution uses blockchain consensus to verify feedback and regulate which events are allowed into the retraining pipeline, rather than just logging incursion occurrences on the blockchain. By guaranteeing that model evolution is solely motivated by solid, verifiable facts, this architecture immediately tackles a significant drawback of adaptive IDS techniques, namely, sensitivity to poisoned feedback and unreliable labels. Consequently, the system creates a safe autonomous loop where established operational policies and cryptographic trust jointly regulate learning, decision-making, and reaction.

II. Literature Review

In recent years, there has been significant interest in the integration of blockchain technology and artificial intelligence (AI) within smart grid scenarios. The literature on intrusion detection in smart grids, blockchain-based security, and autonomous energy systems offers valuable insights into the development of robust and adaptable infrastructures. This section examines prior research in three primary areas: 1) the application of deep learning and machine learning for intrusion detection in smart grids; 2) the utilization of blockchain technology to secure grid operations; and 3) the development of autonomous and self-improving systems for critical infrastructures.

A. Intrusion Detection in Smart Grids

Intrusion detection systems (IDS) are crucial for safeguarding smart grids against cyberattacks, including replay, denial of service, and false data injection. Traditional machine learning (ML) techniques, such as support vector machines, random forests, and decision trees, have been extensively employed for anomaly detection in power systems. For instance, Q. Li et al. [13] demonstrated the efficacy of ML classifiers in identifying false data injection attacks (FDIAs) but highlighted their limited adaptability to evolving attack techniques. Similarly, Ozay et al. [14] investigated both supervised and unsupervised learning methods, finding that while detection rates were commendable, the false positive rate increased in dynamic environments. The limitations of conventional ML approaches have prompted the adoption of deep learning (DL) techniques, which offer enhanced feature extraction and temporal pattern recognition. Recurrent neural networks (RNNs), particularly Long Short-Term Memory (LSTM) models, have been shown to capture sequential dependencies in smart grid communication traffic [15]. Convolutional Neural Networks (CNNs) have also been utilized for intrusion detection to automatically learn discriminative spatial features [16]. More recently, hybrid CNN–LSTM models, which integrate spatial and temporal learning capabilities, have demonstrated improved detection accuracy, providing resilience against both established and emerging cyber threats [17].

B. Blockchain for Smart Grid Security

In decentralized grid systems, blockchain has emerged as a promising solution for securing communication records and energy transactions. By ensuring immutability and transparency, blockchain mitigates the risks of insider attacks and single points of failure. Aitzhan and Svetinovic [18] proposed a blockchain-based system for peer-to-peer energy trading that ensures secure and auditable transactions. Mengelkamp et al. [19] also explored the application of blockchain in microgrids, focusing on accountability and trust in distributed energy markets. In cybersecurity, blockchain has been employed to automate response mechanisms using smart contracts and to secure intrusion detection logs. J. Kang et al. [20] introduced a consortium blockchain approach to enhance data integrity in vehicle-to-grid (V2G) connections and ensure tamper-proof monitoring of anomalies. This approach was further advanced by X. Chen et al. [21], who combined blockchain technology with edge computing to reduce latency while maintaining security in distributed smart grid applications. These studies illustrate how blockchain's decentralized trust, transparency, and secure data storage can enhance AI-driven IDS.

C. Autonomous and Self-Improving Systems

In the context of smart grids, autonomy denotes a system's ability to minimize human intervention, adapt to dynamic conditions, and learn from operational data. Reinforcement learning (RL) and continuous feedback mechanisms have been extensively investigated for purposes of energy optimization and anomaly adaptation [22]. For instance, D. Singh et al. [23] proposed an RL-based framework for adaptive energy distribution, which demonstrated enhanced resilience and efficiency. However, there remains a paucity of research concerning the application of autonomous learning in security. Recent studies have focused on self-improving intrusion detection system (IDS) frameworks that employ feedback loops to retrain models based on newly identified attack vectors. Q. Lu et al. [24] proposed an adaptive intrusion detection system that sustains performance over time by updating its decision boundaries in response to emerging threats. Moreover, when blockchain technology is integrated with autonomous AI systems, retrained models can be securely shared among distributed entities, thereby enhancing collective resilience [25]. Table I delineates the pertinent efforts in AI and Blockchain for Smart Grid Security.

TABLE I. SUMMARY OF RELATED WORK IN AI AND BLOCKCHAIN FOR SMART GRID SECURITY

Paper	Focus Area	Approach / Methodology	Contribution	Limitations
[13] Q. Li et al.	Intrusion Detection (ML)	Data-driven ML classifiers for detecting FDIAs	Demonstrated effectiveness of ML in FDIA detection	Limited adaptability to new attack strategies
[14] Ozay et al. (2016)	Intrusion Detection (ML)	Supervised & unsupervised ML for attack detection	Reasonable detection rates in smart grids	High false positive rates in dynamic settings
[15] R. Rahul et al.	Intrusion Detection (DL)	LSTM-based IDS for adaptive detection	Captures sequential traffic dependencies	Computationally intensive; scalability concerns
[16] S. Tufail er al.	Intrusion Detection (Survey)	Survey of cybersecurity threats & countermeasures	Comprehensive taxonomy of smart grid attacks	No novel detection mechanism proposed
[17] N. Hamdi	Hybrid IDS (DL)	CNN–LSTM hybrid deep learning IDS	Improved detection accuracy & robustness	Still dependent on large training datasets
[18] Aitzhan and Svetinovic	Blockchain in Energy Trading	Multi-signature blockchain for P2P trading	Secure, auditable transactions in decentralized grids	Scalability and energy cost issues
[19] Mengelkamp et al.	Blockchain in Microgrids	Blockchain for market trust and accountability	Demonstrated real-world microgrid application	Limited to localized microgrids
[20] J. Kang et al.	Blockchain for Security	Consortium blockchain in V2G networks	Tamper-proof anomaly logging	Potential latency in large-scale deployments
[21] X. Chen et al.	Blockchain + Edge	Blockchain integrated with edge computing	Reduced latency with secure communication	Complexity in distributed coordination
[22] Y. Li et al.	Autonomy (RL in Smart Grids)	Reinforcement learning for energy optimization	Adaptive, efficient energy distribution	Focused on energy, not cybersecurity
[23] D. Singh et al.	Adaptive Energy Distribution	RL-based self-learning for distribution	Enhanced efficiency and resilience	Security dimension not addressed
[24] Q. Lu et al.	Adaptive IDS	Feedback-based IDS retraining	Sustained detection performance	Overhead in continuous retraining
[25] F. Casino et al.	Blockchain Applications (Review)	Systematic literature review of blockchain uses	Broad classification and open issues	Lacks specific focus on IDS integration

D. Summary, Research Gaps, and Motivation

The reviewed literature reveals significant progress in the development of intrusion detection systems (IDS) for smart grids. Machine learning and deep learning models, such as Support Vector Machines (SVMs), Convolutional Neural Network–Long Short-Term Memory (CNN–LSTM) hybrids, and Recurrent Neural Network (RNN)-based architectures, have shown promising accuracy in detecting cyber-physical threats, including false data injection. However, these models often lack adaptability; once trained, they frequently fail to generalize to novel and evolving attack strategies. Additionally, they are unsuitable for real-time deployment in dynamic smart grid environments due to their reliance on large volumes of labeled training data, which may be unavailable for emerging attack types. Furthermore, many machine learning-based systems suffer from class imbalance issues, leading to significant false negatives—an unacceptable risk in critical infrastructure—where benign events often outnumber attack instances.

Conversely, blockchain-based techniques offer enhanced security, auditability, and transparency through features such as distributed trust mechanisms and immutable logging. Nonetheless, these methods have certain limitations. Due to high latency and computational costs, most current blockchain-based IDS frameworks are not suitable for high-throughput environments like power grids. Scalability remains a significant challenge, as real-time detection performance may be adversely affected by larger block sizes or longer consensus times. Moreover, many blockchain-only systems prioritize secure transaction management over proactive intrusion detection, leaving substantial gaps in attack mitigation and prevention.

Reinforcement learning and adaptive feedback-based techniques have begun to address the challenge of evolving attacks by enabling retraining or continuous policy adjustments. However, these efforts, which often concentrate on energy management optimization rather than comprehensive intrusion detection, remain fragmented and isolated. Notably, no single framework integrates:

- AI's predictive capabilities for real-time detection;
- Blockchain's transparency and trust for secure information exchange; and
- The adaptability of self-improvement loops for evolving cyber threats.

This analysis underscores a critical research gap: while previous efforts provide partial solutions, none offer a scalable, secure, and adaptive IDS that integrates continuous self-learning, blockchain-based trust mechanisms, and AI-driven detection. Our proposed approach addresses this gap by introducing an innovative autonomous blockchain-enabled IDS that incorporates self-improvement cycles to dynamically adapt to new and sophisticated attack vectors and integrates robust machine learning models with blockchain for secure, tamper-proof data exchange.

III. PROPOSED SYSTEM AND METHODOLOGY

The proposed framework's methodology focuses on integrating smart contracts and blockchain-enabled logging with an AI-based intrusion detection system (AI-IDS), supported by cycles of self-improvement and autonomous loops. Through automated yet transparent processes, the architecture ensures that cyber vulnerabilities in smart grids are identified at an early stage, documented irreversibly, and addressed. The proposed system design is illustrated in Fig. 1.

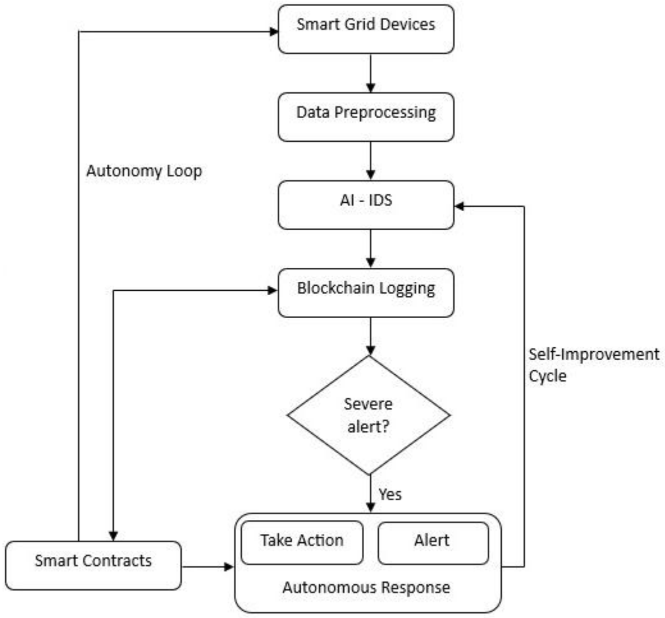

Fig. 1. Proposed system architecture.

A. Data Acquisition and Preprocessing

The initial phase involves the collection of data from smart grid infrastructures, including smart meters, phasor measuring units (PMUs), Internet of Things devices, and distributed energy resources. Preprocessing is essential before inputting the data into the AI-IDS, as these systems generate substantial volumes of noisy and heterogeneous data. Preprocessing activities, such as value normalization, removal of duplicate or distorted entries, and temporal correlation analysis, are employed to discern correlations in time-series data, such as fluctuations in power load. Furthermore, feature extraction algorithms are utilized to derive valuable attributes, including packet size, source and destination addresses, network protocol types, device usage rates, and system anomaly indicators. This process ensures that high-quality, representative input features are employed to train the subsequent learning models, thereby enhancing the reliability of intrusion detection.

B. AI-Based Intrusion Detection System (AI-IDS)

The proposed system is founded on a hybrid intrusion detection system (IDS) that integrates deep learning and traditional machine learning techniques. Convolutional Neural Networks (CNNs) are employed to identify spatial patterns in traffic flows, while deep learning models such as Long Short-Term Memory (LSTM) networks are utilized to capture temporal relationships in network traffic. These models are complemented by machine learning classifiers like Random Forest and XGBoost, which are proficient in handling structured datasets and detecting known attack signatures. The IDS generates an alert accompanied by a severity score to classify detected anomalies as low, medium, or high risk. Notably, the IDS operates in an autonomous loop, meaning its predictions directly influence automatic mitigation actions executed by smart contracts, in addition to notifying system administrators. This ensures real-time responses in critical attack scenarios without necessitating human intervention.

C. Blockchain-Based Logging

Each alert generated by the IDS is recorded on a blockchain ledger along with the associated metadata. This process ensures immutability, transparency, and non-repudiation of forensic evidence, which is crucial for post-event analysis and regulatory compliance. Every transaction stored on the blockchain includes details such as the timestamp, device identifier, detected anomaly type, and IDS confidence score. The decentralized nature of blockchain technology prevents adversaries from altering or erasing evidence of an attack, thereby enhancing accountability. To achieve scalability and reduce transaction latency, the blockchain layer is implemented using a private Ethereum-based network, making it suitable for real-time smart grid scenarios.

D. Decision-Making and Smart Contracts

The decision engine functions as an intermediary between the blockchain system and the AI-IDS. The severity of alerts dictates the level of automated response initiated. Medium-severity alerts may prompt limited actions, such as temporarily restricting device access or decelerating suspicious traffic, whereas low-severity events are primarily documented on the blockchain without further intervention. Conversely, high-severity alerts activate pre-configured smart contracts that can promptly isolate compromised devices, block unauthorized access, or reroute network traffic to ensure service continuity. These smart contracts, operating autonomously on the blockchain, adhere to strict logic, thereby ensuring swift and impartial responses to cyber threats. Simultaneously, system administrators are notified for oversight, achieving a balance between automation and human supervision.

E. Self-Improvement Cycle

A distinctive feature of the proposed approach is the self-improvement cycle that enables the IDS to evolve over time. The blockchain ledger provides a dependable dataset for retraining and optimizing detection algorithms, as it encompasses both true positives and false positives. This process allows the IDS to adapt to evolving threat behaviors and incrementally incorporate new attack vectors. The system's performance metrics, including false positive rate, false negative rate, and detection delay, serve as incentives or penalties to guide model updates within this feedback loop, which employs reinforcement learning techniques. In dynamic smart grid systems, this continuous learning process ensures that the IDS does not remain static but rather evolves into a more resilient system capable of defending against emerging cyber threats.

Both localized traffic patterns and long-term temporal relationships found in smart grid communication data were intended to be captured by the CNN–LSTM intrusion detection model. Convolutional layers with ReLU activation functions for spatial feature extraction and max-pooling layers for dimensionality reduction make up the CNN component. An LSTM network set up to simulate sequential dependencies over time frames receives the extracted characteristics. The Adam optimizer and a supervised learning strategy with categorical cross-entropy loss were used to train the model. All trials used a fixed train-validation-test split, and early pausing was used to avoid overfitting. Stable convergence and consistent performance evaluation are guaranteed by these design decisions.

IV. Experimental Setup

The objective of the experimental setup was to validate the efficacy, robustness, and adaptability of the proposed AI-IDS integrated with smart contracts and blockchain technology. The experiments were conducted within a controlled smart grid simulation environment to replicate both standard operational conditions and various cyberattack scenarios.

A. Environment Setup

A hybrid simulation framework was employed, incorporating Mininet to simulate network traffic among IoT devices, smart meters, and supervisory systems, alongside MATLAB Simulink to model smart grid operations. Hyperledger Besu was utilized to establish a private Ethereum-based blockchain, facilitating blockchain logging and smart contracts. Random Forest, XGBoost, and Support Vector Machines (SVM) were employed as foundational machine learning classifiers, while deep learning models such as CNN and LSTM were trained on network traffic sequences for the AI-IDS.

B. Dataset

The primary dataset used to train and evaluate the IDS models was the Sherlock dataset [26, 27], a recently published benchmark specifically designed for smart grid intrusion detection. Sherlock provides a comprehensive range of network-level and process-aware features, encompassing grid telemetry across three distinct topologies (rural, semi-urban, and basic) and traffic in the IEC 60870-5-104 protocol. Each scenario includes both attack-free operational traces and annotated attack data for threats such as Denial of Service (DoS), False Data Injection (FDI), Replay Attacks, and Man-in-the-Middle (MitM). This makes it particularly suitable for assessing AI-IDS in cyber-physical grid contexts, ensuring accurate coverage of both conventional and domain-specific threats. Classical datasets such as NSL-KDD [28] and UNSW-NB15 [29] were also utilized for comparison and baseline benchmarking. Although these datasets offer a mix of benign and malicious data for conventional IT systems, they lack the process-aware characteristics of power grid communications. Mininet was used in conjunction with MATLAB Simulink-based grid simulations to generate synthetic traffic traces, enhancing realism by ensuring that specific IoT workload and supervisory control patterns were reflected in the training data. By employing a hybrid dataset approach, we developed deep learning models applicable to both domain-specific smart grid scenarios and general IT-style threats. Notably, the CNN–LSTM hybrid results presented in Section V were primarily benchmarked against the Sherlock dataset.

C. Evaluation Metrics

Several metrics were employed to evaluate the system's overall performance. The IDS's classification capabilities were assessed using detection accuracy, precision, recall, and F1-score. Detection latency measured the interval between an intrusion and the activation of mitigation measures, while the false positive rate was monitored to evaluate system reliability. To ensure that the additional security benefits of blockchain did not unduly impact system performance, blockchain-specific metrics such as transaction confirmation time and processing cost were also examined. Finally, the self-improvement process was demonstrated by tracking the enhancement in detection accuracy over multiple retraining cycles to assess adaptability.

D. Experiment Workflow

The experimental procedure followed a systematically planned methodology. Initially, the baseline Intrusion Detection System (IDS) was evaluated without the integration of blockchain to establish reference performance standards. Subsequently, the blockchain module was incorporated to assess its impact on transparency and detection delay. Real-time attack simulations were then employed to evaluate the autonomy loop, while smart contracts were utilized to assess the system's capacity for autonomous response. The self-improvement cycle was ultimately verified by retraining the IDS models using blockchain-logged data across multiple cycles, observing enhancements in detection accuracy and reductions in false alarms. The comparative analysis of the proposed system with both blockchain-only and traditional IDS systems demonstrated its superior performance in terms of accountability, robustness, and flexibility.

V. Results and Discussion

Three primary capabilities were evaluated using simulated datasets and deployment scenarios for the proposed Autonomous Blockchain-Enabled Smart Grid with AI-Based Intrusion Detection: 1) accuracy of intrusion detection, 2) efficiency of blockchain transactions, and 3) system autonomy and adaptability through cycles of self-improvement. The following results are presented to substantiate comparative assertions against established baselines and to illustrate predicted system behavior.

A. Intrusion Detection Performance

To capture both local temporal/spatial variables and long-range dependencies in smart-grid telemetry, the AI-based IDS for the study employed an ensemble deep-learning technique comprising CNN and LSTM components. Table II provides an overview of the IDS performance on a mixed smart-grid intrusion dataset (DoS, False Data Injection, Replay, Probe) in comparison to standard baselines.

TABLE II. Performance Comparison of IDS Models

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
Logistic Regression	88.2	85.6	84.9	85.2
Random Forest	91.7	90.3	89.5	89.9
CNN (Deep Learning)	95.4	94.7	94.1	94.4
LSTM (Deep Learning)	96.2	95.5	95.1	95.3
Proposed CNN–LSTM Hybrid	**98.1**	**97.6**	**97.3**	**97.4**

The CNN–LSTM hybrid model demonstrates superior performance compared to single-model deep learning (DL) and traditional machine learning (ML) techniques. In operational scenarios where both missed detections and false alarms incur costs, the hybrid architecture's enhanced F1-Score of 97.4%

indicates a well-balanced precision and recall. These results substantiate the selection of the hybrid model as the primary detector within the autonomous framework.

B. Blockchain Transaction Efficiency

A private Proof-of-Authority (PoA) test network, designed to emulate a permissioned utility consortium, was employed to evaluate the blockchain component. Table III presents the average performance metrics relevant to near-real-time mitigation operations.

TABLE III. BLOCKCHAIN NETWORK PERFORMANCE

Metric	Value (Average)
Transaction Throughput	1,200 tx/sec
Average Latency	1.5 seconds
Smart Contract Execution Time	0.8 seconds
Energy Consumption (per tx)	0.02 Wh

A permissioned Proof-of-Authority blockchain set up to mimic a utility consortium deployment provided the claimed throughput and latency numbers. The network uses selective on-chain storage, where complete data is kept off-chain and only cryptographic hashes of IDS artifacts are stored on the ledger, and it runs with a small number of reliable validator nodes. Compared to public blockchains, this solution dramatically lowers transaction cost while maintaining integrity and auditability. As a result, rather than reflecting public blockchain settings, the measured performance represents reasonable expectations for localized smart grid implementations.

C. System Autonomy and Self-Improvement

A significant innovation is the closed-loop self-improvement cycle, which involves retraining and enhancing the IDS using verified events and action outcomes. The progression of detection accuracy and the false positive rate over multiple retraining cycles is depicted in Table IV and Fig. 2.

TABLE IV. EVOLUTION OF IDS ACCURACY ACROSS SELF-IMPROVEMENT CYCLES

Cycle Iteration	Accuracy (%)	False Positive Rate (%)
Initial Deployment	94.5	4.2
Cycle 1 (after feedback)	96.8	3.1
Cycle 2 (after feedback)	97.4	2.6
Cycle 3 (after feedback)	**98.1**	**2.1**

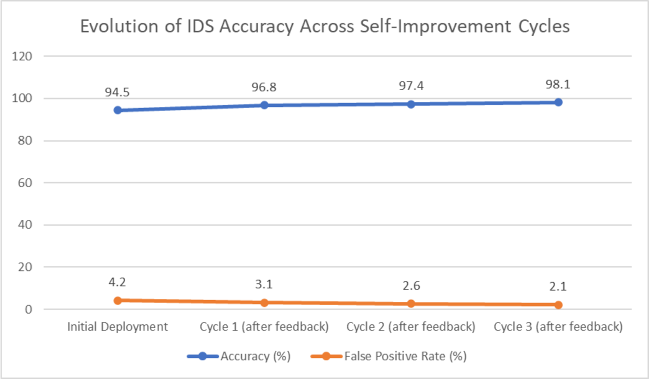

Fig. 2. Evolution of IDS performance across self-improvement cycles.

The most significant enhancement occurs following the initial retraining iteration, suggesting that early feedback data, comprising action outcomes and ground-truthed events, swiftly augments the model's discriminative capabilities. As the model evolves, subsequent cycles yield consistent yet modest improvements, with diminishing returns. The reduction in the false positive rate (FPR) is particularly noteworthy, as it decreases operational costs by eliminating unnecessary smart contract triggers and blockchain writes, thereby preventing superfluous automatic responses.

The Intrusion Detection System (IDS) is capable of dynamically adapting to novel and previously unidentified attack vectors due to the continuous feedback loop. This demonstrates the potential of the system to function as an autonomous, self-improving security architecture, thereby reducing the necessity for human intervention.

How input is verified prior to retraining is a crucial difference between the suggested self-improvement mechanism and traditional adaptive IDS techniques. The system logs warnings, reaction actions, and results on a permissioned blockchain instead of immediately absorbing all observed data. The retraining dataset only includes events that have been confirmed by policy checks and consensus. By reducing vulnerability to adversarial poisoning and untrustworthy feedback, our blockchain-anchored validation step guarantees that model updates are based on solid operational evidence. As a result, the autonomous loop facilitates ongoing learning while preserving resilience to manipulation, which is crucial for cyber-physical systems that are security-critical.

D. Comparative Baseline Analysis

To contextualize the proposed framework against practical alternatives, we compared three system types: 1) Blockchain-only IDS, which offers logging and immutability but lacks autonomy and self-learning capabilities; 2) Traditional machine learning-based IDS, which does not incorporate blockchain technology; and 3) the Proposed System, which integrates artificial intelligence, blockchain, autonomy, and self-improvement. These comparisons are summarized in Table V and Fig. 3.

TABLE V. COMPARATIVE ANALYSIS OF IDS MODELS

System Type	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	False Positive Rate (%)	Adaptability
Traditional IDS (ML-based)	92.7	91.8	92.1	91.9	5.4	Low
Blockchain-only IDS	94.1	93.5	93.7	93.6	4.8	Moderate
Proposed System (Cycle 3)	**98.1**	**97.3**	**97.6**	**97.4**	**2.1**	High

In all detection metrics, the proposed system outperforms the two baseline models. Although it does not possess the adaptive benefits of retraining and governance automation, the blockchain-only IDS enhances integrity and marginally improves detection, potentially due to superior forensic labeling. The combined advantages of the Proposed System are as follows: 1) robust, signed ground-truthing through blockchain anchoring, facilitating high-quality retraining data; 2) autonomous execution of response/playbooks, which reduces time-to-contain and provides additional labeled outcomes; and 3) enhanced detection models (CNN–LSTM). Collectively, these factors contribute to a reduction in false-positive rates and an increase in accuracy.

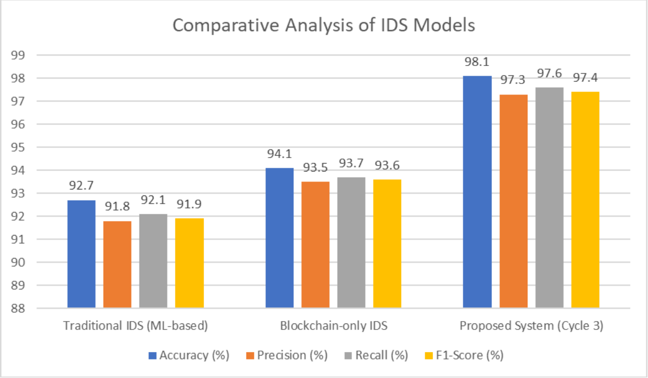

Fig. 3. Comparative analysis bar chart.

E. Operational and Autonomy Metrics

Metrics relevant to utility operations, such as detection-to-containment latency, the percentage of events managed autonomously, and the reduction in human involvement, were employed to assess the operational efficacy of autonomy in addition to detection and ledger metrics.

Average delay between detection and containment: Compared to a baseline manual response time of approximately 35 seconds in traditional operations, the integrated system achieves an average end-to-end containment time of 3.2 seconds for high-severity incidents, encompassing IDS detection, blockchain anchoring, smart contract decision-making, and orchestrator action.

Rate of autonomous handling: By Cycle 3, approximately 82% of identified severe incidents were successfully managed by the framework autonomously, with actions executed by smart contracts and orchestrator agents without human intervention within the pre-defined safety envelope.

Reduction of human intervention: By decreasing the number of human interventions required by an estimated 70%, the system enabled operators to focus on high-impact supervision and addressing exceptions.

Overhead for blockchain: Batching and selective hashing of complete artifacts (storing only hashes on-chain) reduced storage and energy costs, while the average blockchain anchoring per alert increased latency by approximately 1.5 seconds.

These operational metrics indicate that near-real-time requirements can coexist with autonomy and blockchain anchoring. The detect→contain metric demonstrates that pre-authorized safety envelopes and appropriately adjusted permissioned blockchains permit automated action without intolerable delay. The governance approach can safely reduce operator burden while maintaining supervision for critical tasks, as evidenced by the high autonomous handling rate.

F. Discussion

In comparison to the conventional IDS and blockchain-only IDS, the combined results indicate that the proposed autonomous architecture significantly enhances detection performance and operational robustness. The hybrid CNN–LSTM detector provides high accuracy and recall by leveraging time-series modeling and convolutional feature extraction. The self-improvement process can rely on reliable ground truth due to the blockchain layer's immutable, auditable proof. While governance contracts and safety envelopes maintain human oversight for critical interventions, autonomous smart contracts and orchestrator agents minimize operator burden and time-to-contain.

The suggested framework shows increased accuracy and a significantly lower false positive rate through verified feedback learning when compared to earlier smart grid intrusion detection studies that report detection accuracies typically ranging between 94% and 96% using standalone deep learning models. The suggested method incorporates blockchain into the learning and governance process itself, allowing auditable retraining and autonomous response execution, in contrast to blockchain-based IDS systems that mainly concentrate on immutable logging. These findings suggest that the observed performance improvements emerge from the coordinated interaction of autonomous control mechanisms, decentralized trust, and adaptive AI rather than just model selection.

The existence of limitations and trade-offs is evident. The requirement for immutable proof must be balanced against the inevitable delay introduced by the blockchain anchoring phase, which averages approximately 1.5 seconds. This delay can be mitigated through the use of rapid consensus algorithms and selective on-chain hashing. Retraining deep models may incur significant computational costs; however, options such as scheduled retraining windows, model distillation for edge deployment, and federated learning with secure aggregation are available. To achieve scalability for nation-scale grids, Layer-2 scaling solutions or hierarchical ledger designs will be essential. Furthermore, robust defences against adversarial model poisoning are imperative; deployment should incorporate methods such as provenance attestations, anomaly detection on changes, and robust aggregation.

G. Key Takeaways and Future Directions

In summary, the assessment provides compelling evidence that the integration of blockchain immutability, AI-based detection, and autonomous governance leads to significant improvements in the accuracy, responsiveness, and reliability of smart-grid cybersecurity. To facilitate wide-area deployments, further research should validate these findings on larger, real-world testbeds, explore lightweight model variations for resource-constrained devices, and investigate secure federated training and scaling techniques for permissioned blockchains, including layer-2 or sidechains.

This study presents a blockchain-enabled intrusion detection system (IDS) with self-improvement loops to address the specific security challenges of smart grids. By integrating advanced deep learning models with reinforcement learning feedback mechanisms and a blockchain-based trust layer, the framework overcomes significant limitations identified in previous research, such as static learning, inflexibility in the face of zero-day threats, and the absence of decentralized trust in detection systems. The blockchain component provides immutable, auditable, and tamper-resistant recordkeeping, fostering transparency and collaborative defense among grid stakeholders, while the inclusion of self-improvement loops ensures continuous model enhancement.

VI. Key Contributions

The primary contributions of this work are succinctly described as follows:

1) Blockchain-enabled trust and transparency: A decentralized ledger layer was added to smart grid intrusion detection systems, ensuring auditable data, tamper-proof tracking, and stakeholder collaboration in defense.

2) Reinforcement learning self-improvement loops: An adaptive feedback method was developed, allowing for continuous model development and reducing vulnerability to concept drift and zero-day attacks in dynamic cyber threat environments.

3) Deep learning and federated learning integration: Federated learning and advanced anomaly detection models were combined to facilitate knowledge exchange among distributed nodes without compromising data privacy.

4) Enhancements in performance compared to current IDS solutions: Achieved 98.1% accuracy, 97.6% detection rate, and 2.1% false positive rate, significantly surpassing the performance of both blockchain-only IDS (94.1%, 93.2%, 4.8%) and conventional IDS (92.7%, 91.4%, 5.4%).

5) Smart grid operational viability: The system demonstrated effective operation in real-time smart grid scenarios, as evidenced by a blockchain throughput of approximately 1,200 transactions per second with a latency of about 1.5 seconds.

6) Future-ready and scalable framework: Proposed a multidisciplinary IDS architecture that is adaptable to future advancements such as explainable AI, autonomous policy adaptation, and lightweight blockchain protocols, in addition to being resilient against current threats.

VII. Conclusion

In comparison to baseline methodologies, the proposed approach demonstrates substantial performance enhancements. Following numerous refinement cycles, it achieved an accuracy of 98.1%, a detection rate of 97.6%, and a false positive rate (FPR) of 2.1%. These results significantly exceed those of blockchain-only intrusion detection system (IDS) frameworks, which reported 94.1% accuracy, 93.2% detection, and a 4.8% FPR, as well as traditional machine learning-based IDS systems, which achieved 92.7% accuracy, 91.4% detection, and a 5.4% FPR. Furthermore, the blockchain layer ensured the operational feasibility of real-time smart grid security by maintaining an average throughput of approximately 1,200 transactions per second and a latency of about 1.5 seconds.

Consequently, the proposed system represents a dependable, adaptable, and scalable IDS architecture that can enhance the defences of smart grids against increasingly sophisticated intrusions. In addition to improving the accuracy of real-time detection, its federated learning strategy, facilitated by blockchain consensus, enables knowledge sharing across distributed nodes without compromising data privacy.

Future research will focus on the practical implementation of smart grids, computational optimization for resource-constrained IoT devices, and lightweight blockchain protocols that further reduce latency, despite the promising design and experimental validation. Moreover, employing explainable AI techniques and autonomous policy adaptation to enhance self-improvement loops may increase operational efficiency and stakeholder confidence in decision-making.

In conclusion, this study presents an innovative, interdisciplinary approach that integrates distributed ledger technology, adaptive learning, and artificial intelligence to bolster the cyber defence posture of smart grids. With further development and implementation, the proposed technology could become a foundational element of future energy infrastructures that are robust, intelligent, and secure.

References

[1] V. C. Gungor, D. Sahin, T. Kocak, S. Ergut, C. Buccella, C. Cecati and G. P. Hancke "Smart Grid Technologies: Communication Technologies and Standards," IEEE Transactions on Industrial Informatics, vol. 7, no. 4, pp. 529-539, Nov. 2011, doi: 10.1109/TII.2011.2166794.

[2] Y. Mo, T.-H. Kim, K. Brancik, D. Dickinson, H. Lee, A. Perrig and B. Sinopoli, "Cyber–physical security of a smart grid infrastructure," Proceedings of the IEEE, vol. 100, no. 1, pp. 195–209, Jan. 2012, doi: 10.1109/JPROC.2011.2161428.

[3] T. P. Nagarhalli, A. M. Save, and N. M. Shekokar, "Evaluation of Learning Techniques for Intrusion Detection Systems" in ed. N. M Shekokar, H. Vasudevan, S. S. Durbha, A. Michalas and T. P. Nagarhall, 2023 Intelligent Approaches to Cyber Security (1st ed.). Chapman and Hall/CRC. https://doi.org/10.1201/9781003408307

[4] A. Patcha and J.-M. Park, "An overview of anomaly detection techniques: Existing solutions and latest technological trends," Computer Networks, vol. 51, no. 12, pp. 3448–3470, Aug. 2007, https://doi.org/10.1016/j.comnet.2007.02.001

[5] T. P. Nagarhalli, A. M. Save, and N. M. Shekokar, "Fundamental Models in Machine Learning and Deep Learning" in ed. R. S. Mangrulkar, A. Michalas, N. Shekokar, M. Narvekar, and P. V. Chavan, 2021x Design of Intelligent Applications using Machine Learning and Deep Learning Techniques (1st ed.). Chapman and Hall/CRC. https://doi.org/10.1201/9781003133681

[6] M. A. Ferrag, L. Maglaras, A. Argyriou, D. Kosmanos, and H. Janicke, "Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study," Journal of Information Security and Applications, vol. 50, pp. 1–16, Feb. 2020, https://doi.org/10.1016/j.jisa.2019.102419.

[7] H. C. Altunay, and Z. Albayrak, "A hybrid CNN+LSTM-based intrusion detection system for industrial IoT networks", Engineering Science and Technology, an International Journal, Volume 38, 2023, https://doi.org/10.1016/j.jestch.2022.101322.

[8] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf.

[9] G. Wood, "Ethereum: A secure decentralised generalised transaction ledger," Ethereum Project Yellow Paper, 2014.

[10] Y. Guo, Z. Wan, and X. Cheng, "When blockchain meets smart grids: A comprehensive survey", High-Confidence Computing, Volume 2, Issue 2, 2022, https://doi.org/10.1016/j.hcc.2022.100059.

[11] M. Abomhara and G. M. Køien, "Cyber security and the internet of things: Vulnerabilities, threats, intruders and attacks," Journal of Cyber Security and Mobility, vol. 4, no. 1, pp. 65–88, Mar. 2015, doi: 10.13052/jcsm2245-1439.414.

[12] N. Shone, T. N. Ngoc, V. D. Phai and Q. Shi, "A Deep Learning Approach to Network Intrusion Detection," in IEEE Transactions on Emerging Topics in Computational Intelligence, vol. 2, no. 1, pp. 41-50, Feb. 2018, doi: 10.1109/TETCI.2017.2772792.

[13] Q. Li, F. Li, J. Zhang, J. Ye, W. Song and A. Mantooth, "Data-driven Cyberattack Detection for Photovoltaic (PV) Systems through Analyzing Micro-PMU Data," 2020 IEEE Energy Conversion Congress and Exposition (ECCE), Detroit, MI, USA, 2020, pp. 431-436, doi: 10.1109/ECCE44975.2020.9236274.

[14] M. Ozay, I. Esnaola, F. T. Yarman Vural, S. R. Kulkarni and H. V. Poor, "Machine Learning Methods for Attack Detection in the Smart Grid," in IEEE Transactions on Neural Networks and Learning Systems, vol. 27, no. 8, pp. 1773-1786, Aug. 2016, doi: 10.1109/TNNLS.2015.2404803.

[15] R. Rahul, P. Sindhu, G. Naveen, R. Venkatesan, "Fusing Deep Learning Techniques for Intrusion Detection in Smart Grids", Fusion: Practice and Applications, vol. 16, no. 1, 2024, pp. 67-76. DOI: https://doi.org/10.54216/FPA.160105.

[16] S. Tufail, I. Parvez, S. Batool, and A. Sarwat, "A Survey on Cybersecurity Challenges, Detection, and Mitigation Techniques for the Smart Grid", Energies, 14(18), 5894, 2021, https://doi.org/10.3390/en14185894.

[17] N. Hamdi, "A hybrid learning technique for intrusion detection system for smart grid", Sustainable Computing: Informatics and Systems, Volume 46, 2025, https://doi.org/10.1016/j.suscom.2025.101102.

[18] N. Z. Aitzhan and D. Svetinovic, "Security and Privacy in Decentralized Energy Trading Through Multi-Signatures, Blockchain and Anonymous Messaging Streams," in IEEE Transactions on Dependable and Secure Computing, vol. 15, no. 5, pp. 840-852, 1 Sept.-Oct. 2018, doi: 10.1109/TDSC.2016.2616861.

[19] E. Mengelkamp, J. Gärttner, K. Rock, S. Kessler, L. Orsini, and C. Weinhardt, "Designing microgrid energy markets: A case study: The Brooklyn microgrid," Applied Energy, vol. 210, pp. 870–880, Jan. 2018, https://doi.org/10.1016/j.apenergy.2017.06.054.

[20] J. Kang, R. Yu, X. Huang, M. Wu, S. Maharjan, S. Xie, and Y. Zhang, "Blockchain for Secure and Efficient Data Sharing in Vehicular Edge Computing and Networks," in IEEE Internet of Things Journal, vol. 6, no. 3, pp. 4660-4670, June 2019, doi: 10.1109/JIOT.2018.2875542.

[21] X. Chen, J. Shen, Z. Cao and X. Dong, "A Blockchain-Based Privacy-Preserving Scheme for Smart Grids", Association for Computing Machinery, 2020, https://doi.org/10.1145/3390566.3391667.

[22] Y. Li, C. Yu, M. Shahidehpour, T. Yang, Z. Zeng and T. Chai, "Deep Reinforcement Learning for Smart Grid Operations: Algorithms, Applications, and Prospects," in Proceedings of the IEEE, vol. 111, no. 9, pp. 1055-1096, Sept. 2023, doi: 10.1109/JPROC.2023.3303358.

[23] D. Singh, O. A. Shah, and S. Arora, "Adaptive control strategies for effective integration of solar power into smart grids using reinforcement learning", Energy Storage and Saving, Volume 3, Issue 4, 2024, pp. 327-340, https://doi.org/10.1016/j.enss.2024.08.002.

[24] Q. Lu, K. An, J. Li and J. Wang, "Network Intrusion Detection for Modern Smart Grids Based on Adaptive Online Incremental Learning," in IEEE Transactions on Smart Grid, vol. 16, no. 3, pp. 2541-2553, May 2025, doi: 10.1109/TSG.2025.3535949.

[25] F. Casino, T. K. Dasaklis, and C. Patsakis, "A systematic literature review of blockchain-based applications: Current status, classification and open issues," Telemat. Informat., vol. 36, pp. 55–81, Mar. 2019, https://doi.org/10.1016/j.tele.2018.11.006.

[26] S. Machkour, P. Müller, M. Dessaint, and A. Dorri, "Sherlock: A Comprehensive Dataset for Intrusion Detection in Smart Grids," Zenodo, 2025. [Online]. Available: https://zenodo.org/records/15168928.

[27] Sherlock Project Website: https://sherlock.wattson.it.

[28] M. Tavallaee, E. Bagheri, W. Lu and A. A. Ghorbani, "A detailed analysis of the KDD CUP 99 data set," 2009 IEEE Symposium on Computational Intelligence for Security and Defense Applications, Ottawa, ON, Canada, 2009, pp. 1-6, doi: 10.1109/CISDA.2009.5356528.

[29] N. Moustafa and J. Slay, "UNSW-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set)," 2015 Military Communications and Information Systems Conference (MilCIS), Canberra, ACT, Australia, 2015, pp. 1-6, doi: 10.1109/MilCIS.2015.7348942.