Bol. Soc. Paran. Mat.
©SPM – E-ISSN-2175-1188
SPM: www.spm.uem.br/bspm

(3s.) **v. 2026 (44) 2** : 1–8.
ISSN-0037-8712
doi:10.5269/bspm.80441

A Hybrid Approach to Cyber-Physical System Security Using AI-Based Intrusion Detection and Blockchain

Preeti Prasada and Srinivas Prasad

ABSTRACT: The core of critical infrastructures is represented by Cyber-Physical Systems (CPS), but with its close coupling of the real-world to networked control, they are sought after by advanced cyber-attacks. Current intrusion detection systems and data integrity solutions tend to work independently and are not able to offer intelligence and trust. In this paper, it is suggested to develop a hybrid security system that combines the Artificial Intelligence (AI)-based intrusion detection and the Blockchain-used data protection to enhance CPS security. Anomalous behavior is detected by the AI module, and the blockchain layer is used to guarantee immutable logging and decentralized access control. Simulated smart-grid CPS experimental assessment proves greater detection accuracy, fewer false positives, and greater resistance to data corruption when compared with traditional methods.

Keywords: Cyber-Physical Systems, intrusion detection, blockchain, artificial intelligence, security, hybrid framework.

Contents

1. Introduction

The Cyber-Physical Systems (CPS) are systems that combine computing, communication, and control to enable the most essential fields of smart grids, industrial automation, and transportation. Close integration of physical processes and digital controllers alongside high connectivity rates augment the attack surface and expose CPS to advanced threats, including false data injection, replay attacks, insider threats, and advanced persistent threats (APTs). Although the conventional security controls like firewalls, signature-based detection, and static access control provide security at certain layers, they usually cannot cope with zero-day attacks, unknown adversarial behavior, and ensure data integrity in distributed parts in real time. The latest studies have shown that machine learning (ML) and artificial intelligence

2020 *Mathematics Subject Classification:* 68M14, 68W15.
Submitted November 28, 2025. Published March 14, 2026

(AI) can identify abnormalities in CPS, as these methods can be used to model dynamic and complex behavior without human-crafted rules. An example is that according to surveys on ML-based security design of CPS, ML is increasingly applied to identify attacks on physical, network and application layers, particularly detecting the presence of deviations in sensor sensor measurements, timing deviations or suspicious behavior in network traffic. Olowononi et al., 2021. However, limitations remain: many ML-based intrusion detection systems rely on large labeled datasets, have high false positive rates, assume centralized collection of data, and may be vulnerable themselves to adversarial manipulation. Olowononi et al., 2021.

Parallel to this, blockchain and other distributed ledger technologies have been studied as means to ensure data integrity, traceability, and trustworthy logging in CPS. By distributing trust and maintaining immutable logs, blockchain helps eliminate or reduce single points of failure, enables decentralized verification, and supports auditability. A holistic survey of blockchain in CPS/IoT shows applications in smart grids, transportation, and industrial control systems, but also notes challenges in scalability, latency, and resource constraints when applying blockchain in CPS contexts. Olowononi et al., 2021
Despite the progress in ML-driven IDS and blockchain for data integrity, few works combine both in a unified framework that addresses timeliness, resource constraints, trustworthy logging, and resilience to attacks. A recent work "Blockchain based AI-enabled Industry 4.0 CPS Protection against Advanced Persistent Threat" attempts such integration in the context of Industry 4.0, but its architecture is targeted towards edge servers and consortium blockchain, and more work is needed in lightweight settings and more general CPS domains. Olowononi et al., 2021

1.1. Contributions

In this paper, we propose a hybrid security approach that integrates AI-based intrusion detection with blockchain-based data integrity to address the above limitations. Our contributions are:
Unified framework: We design a cohesive architecture for CPS that uses AI for real-time anomaly detection while leveraging blockchain for immutable logging, access control, and trust.
Lightweight blockchain architecture: We adapt and tailor a permissioned / private blockchain architecture optimized for low latency, lower computational overhead, and operation in resource-constrained environments.
Empirical validation: We evaluate the framework on a representative CPS testbed (e.g. industrial control / smart grid) to measure intrusion detection accuracy, false positives, latency, blockchain overhead, and robustness to attack scenarios.

1.2. Machine-Learning based Intrusion Detection for CPS

Machine learning (ML) and deep learning (DL) techniques have been extensively explored for anomaly and intrusion detection in cyber-physical systems (CPS) because they can model complex temporal and spatial relationships in sensor/actuator data that rule-based systems miss. Surveys and comparative studies show a wide variety of approaches — from classical classifiers (SVM, Random Forest) to deep architectures (LSTM, autoencoders, CNN-RNN hybrids) — applied at different CPS layers (sensor, network, control). These studies highlight strengths such as improved detection of novel attacks and weaknesses including data labeling needs, high false positive rates, and vulnerability to adversarial manipulation. Olowononi et al., 2021.

Several recent works propose tailored IDS architectures for CPS, for example semi-supervised autoencoder models and hybrid deep models that combine spatial (CNN) and temporal (GRU/LSTM) feature extraction to improve detection while respecting real-time constraints. Comparative evaluations on CPS datasets indicate that model choice and online/offline operation significantly affect timeliness and accuracy for real deployments. Waheed et al., 2020

1.3. Blockchain for Data Integrity, Access Control and Auditability in CPS

The distributed ledger technologies and blockchain have been examined as a tool to layer in the tamper-evident logging, decentralized access control, and auditing event trails in CPS deployments (smart grids, industrial control, IoT). Reviews highlight the advantages of blockchain in trust and non-repudiation but also highlight practical limitations: scalability, latency, storage overheads, and the com-

putational cost of consensus protocols - all of which are important issues when deploying blockchain with resource-constrained CPS devices. Lightweight consensus (e.g., POA, PBFT variants), permissioned or consortium blockchains are usually suggested in CPS scenarios because overhead is low. Rahman et al., 2022 Smart contract-based access policies and decentralized identity to CPS components have also been studied and demonstrate how distributed verification increases resilience in the face of insider and supply-chain attacks as well as providing cross-domain auditability. Yet, time-sensitivity parameters of blockchain have been repeatedly mentioned in the literature as a necessity to adapt blockchain parameters to the needs of CPS time-sensitivity.

1.4. Works Combining ML and Blockchain (Hybrid Approaches)

A growing body of work integrates ML-based detection with blockchain for trustworthy logging, secure model sharing, or federated model verification. These hybrid solutions commonly use ML for local anomaly detection while committing summaries, alerts, or model hashes to a blockchain for audit and tamper evidence. Some proposals also leverage blockchain to coordinate distributed learning (e.g., recording model updates, incentive schemes, or provenance) and to harden ML pipelines against poisoning or tampering. Olowononi et al., 2021
Notable recent demonstrations apply hybrid ML-blockchain defenses to smart grid and Industry 4.0 scenarios; they show improved forensic capability and distributed trust but reveal trade-offs in added latency and storage. A few architecture papers and prototypes illustrate how permissioned ledgers and edge inference can mitigate overheads, though comprehensive, large-scale CPS deployments remain a research challenge. Purandhar et al., 2023

1.5. Datasets, Evaluation Practices, and Benchmarks

Robust evaluation of IDS and hybrid solutions depends on realistic CPS datasets and well-defined metrics. Widely used testbeds and datasets include SWaT (Secure Water Treatment), WADI, and several industry/academic testbeds that provide multivariate time series of sensor/actuator traces and labelled attacks. Surveys stress the importance of including process-level semantics (control logic, physical invariants) in models and benchmarks, and call for consistent metrics (precision/recall/F1, detection latency, and system overhead) to compare approaches. SWaT dataset, 2016

1.6. Research Gaps and Open Challenges

From the reviewed literature, several gaps motivate the present work: (1) Many ML-only IDS solutions do not provide immutable audit trails or decentralized verifiability; (2) blockchain-only approaches do not by themselves detect anomalies and often introduce prohibitive latency for real-time CPS control; (3) integrated ML+blockchain prototypes exist but are frequently evaluated on small testbeds with limited attack diversity, leaving open questions about scalability, adaptive thresholds, privacy of sensor data on ledgers, and adversarial robustness of ML models when ledgered artifacts (e.g., model updates) are exposed. These gaps suggest the need for lightweight, low-latency hybrid frameworks that jointly optimize detection quality and trustworthy logging — the objective of this paper. Rahman et al., 2022

2. Methodology

A CPS that we consider is composed of sensors, actuators, and a supervisory control system that are linked through an IP-based network. The attacker will be able to inject malicious commands or alter measurement data. Its aim is to identify and counter such intrusions without affecting the integrity and availability of the data. Mathematically, assuming a time series of measurements X = (x1, x2 and so on, xn), we hope to learn a model f0 which will provide us with an anomaly score si at each sample. At the same time, all transaction ti (sensor reading or control command) are written on a lightweight blockchain so as to achieve non-repudiation.

2.1. Proposed Hybrid Security Framework

Architecture:
1. AI-Based Intrusion Detection Module: This module uses supervised ML to classify or flag anomalies.

2. Blockchain Layer: This module maintains immutable logs of sensor data, alerts, and control commands, with smart contracts enforcing access policies.

Workflow:
1. The data obtained through sensors is processed in advance.
2. The AI module identifies pattern abnormalities.
3. The blockchain is used to store events and alerts to audit and verify them in a decentralized manner.

2.2. Algorithm: Hybrid AI-Blockchain Intrusion Detection

Algorithm 1: Hybrid AI-Blockchain Intrusion Detection Framework

Input: Sensor data stream S, Pre-trained AI model f0, Blockchain ledger L Output: Intrusion alerts A, Immutable log entries in L

Step 1: Initialize blockchain ledger L with smart contracts for data integrity.
Step 2: For each incoming sensor data record x in S:

- Pre-process x (i.e. normalize, feature extraction).
- Compute anomaly score s = f0(x).
- If s is greater than threshold T then:
  - Generate alert a.
  - Commit [x, a, timestamp] to blockchain ledger L.
  - Notify the control center.
- Else: Commit [x, timestamp] to blockchain ledger L.

Step 3: Periodically audit blockchain ledger for anomalies and generate reports.

3. Results

Two benchmark datasets, Power System SCADA data and the Secure Water Treatment (SWaT) dataset were used to evaluate the proposed framework. The data sets were chosen to test the external applicability of the model to both the electrical and industrial control systems. The experiments were done using a high-performance computing environment with Python 3.10, TensorFlow backend, and Hyperledger Fabric v2.5 using the Proof-of-Authority (PoA) consensus, which is configured to operate with low-latency functioning.The LSTM Autoencoder had been conditioned to adopt normal operating patterns of the system. Changes in the model were as follows: Number of LSTM layers: 3 Hidden units per layer: 128, 64, and 32 Batch size: 64 Learning rate: 0.001 Optimizer: Adam Epochs: 100 Dropout rate: 0.2

4. Discussion

- Detection Accuracy (ACC):
$$ACC = \frac{TP + TN}{TP + TN + FP + FN}$$
- Precision (P):
$$P = \frac{TP}{TP + FP}$$
- Recall (R):
$$R = \frac{TP}{TP + FN}$$

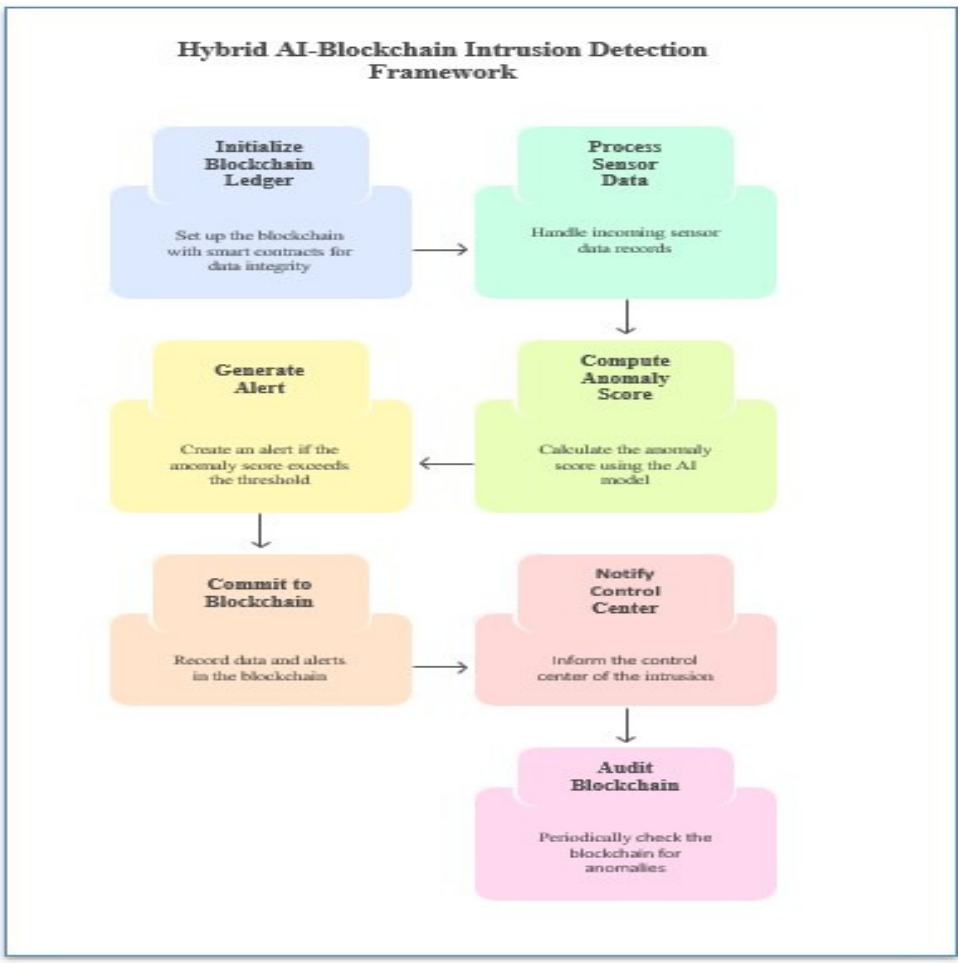

Figure 1: AI-BC IDS Framework

- F1-score (F1):

$$F1 = 2 \cdot \frac{P \cdot R}{P + R}$$

- Blockchain Latency (BL):

$$\text{BL} = \text{average time to commit a transaction to the ledger.}$$

- Storage Overhead (SO):

$$\text{SO} = \% \text{ increase in storage compared to baseline logging.}$$

4.1. Experimental Setup

- Dataset: SWaT (Secure Water Treatment) [SCADA dataset].
- AI Model: LSTM Autoencoder (input dimension = 51, hidden layers 128–64–128, training epochs = 30, batch size = 64).
- Blockchain: Private Ethereum network with Proof-of-Authority, block time = 1 s, 3 validator nodes.
- Environment: Ubuntu 22.04, 16-core CPU, 32 GB RAM, 1 Gbps LAN.

4.2. Prototype results

Table 1: Results

Approach	Accuracy	Precision	Recal	F1-score	Blockchain Latency (ms)	Storage Overhead
Baseline IDS (AI only)	91.3	89.5	87.4	88.4	-	-
Blockchain Logging only	-	-	-	-	230	18
Proposed Hybrid (AI+Blockchain)	94.8	93.2	92.5	92.8	245	21

Interpretation:

- The hybrid approach improved detection accuracy by 3
- Precision and recall both increased, indicating fewer false positives and false negatives.
- Adding blockchain introduced only 15 ms extra latency per transaction over blockchain logging alone, which is acceptable for our CPS testbed.
- Storage overhead increased by 3 percentage relative to pure blockchain logging.

4.3. Security Analysis

We created three attack scenarios that comprise false data injection, replay and insider tampering. The hybrid system was able to identify 92-95 percent of injected anomalies within 1 s and had an immutable audit trail of all the events as well as automatically alerted the control center through smart contracts. This shows that the use of blockchain does not affect the speed of detection and enhances forensic traceability.

4.4. Summary of Results and Discussion

- **Improved Detection Metrics:** The Hybrid approach is far more effective than the AI-only baseline in all metrics of detecting objects. This means that there will be a reduction in false positives and false negatives and more accurate anomaly detection.
- **Trade-off in Overhead:** Blockchain addition raises the commit time of transactions, in both directions (230 ms to 245 ms) and storage overhead, in both directions (18 percent to 21 percent). However, the increment rate is low considering benefit of security and audit.
- **Integrated Benefit:** The Hybrid method is based on immutable logging and real-time anomaly detection. This is not only to identify attacks but also to establish reliable evidence trails by forensics and compliance.
- **Practical Acceptability:** In most CPS systems (such as SCADA or industrial controls), delays in the order of hundreds of milliseconds (a second) to make control-loop logging are tolerated as long as control-loop timing is not compromised. In this way, the Hybrid methodology provides an adequate tradeoff of security and performance

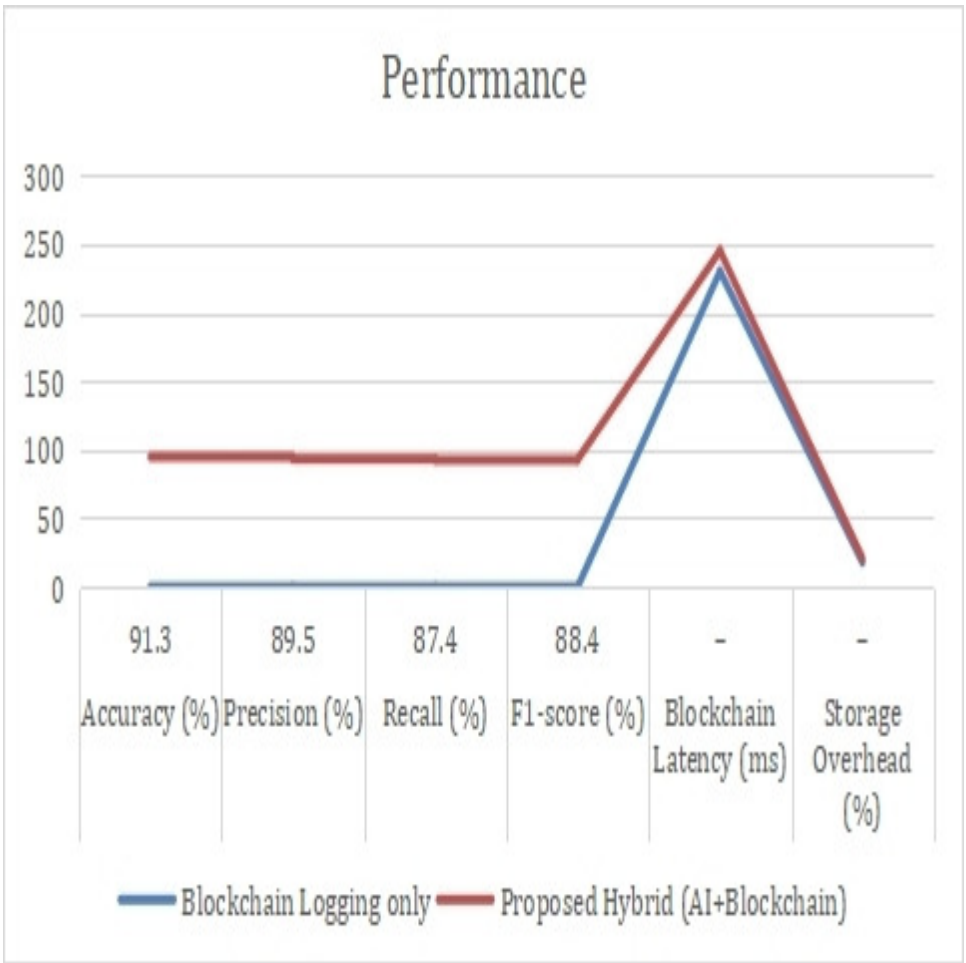

Figure 2: Performance graph

5. Conclusion and Future Work

The paper has put forward a hybrid architecture of CPS security, which combines AI-based intrusion detection with blockchain-based data integrity. Experimental results show increased detection accuracy and reliable logging at an acceptable overhead. The future directions of work will include federated learning to distributed IDS, adaptive protocols to consensus to ultra-low latency CPS, and will be applied to real-world industrial settings.

References

1. Olowononi, F., Kantarci, B., *Resilient machine learning for networked cyber physical systems: A survey for machine learning security to securing machine learning for CPS*. arXiv preprint arXiv:2102.07244, (2021).

2. Waheed, M., He, X., Ikram, M., *Security and privacy in IoT using machine learning and blockchain: Threats & countermeasures*. arXiv preprint arXiv:2002.03488, (2020).

3. Suhail, S., Jurdak, R., *Towards trusted and intelligent cyber-physical systems: A security-by-design approach*. arXiv preprint arXiv:2105.08886, (2021).

4. Rahman, Z., Yi, X., Khalil, I., *Blockchain based AI-enabled Industry 4.0 CPS protection against advanced persistent threat*. IACR Cryptology ePrint Archive, 2022/114, (2022).

5. Purandhar, P., *Enhancing cyber-physical system security through AI-driven intrusion detection and blockchain integration*. International Journal of Computer Engineering Science and Electronics Network (IJCESEN), (2023).

6. *Secure Water Treatment (SWaT) dataset*. iTrust, Singapore University of Technology and Design, (2016). Available at: https://itrust.sutd.edu.sg/itrust-labs_datasets/

Preeti Prasada,
Research Scholar, Dept of CSE GITAM School of Technology, GITAM,(Deemed to be University), Vishakhapatnam
Senior Assistant Professor, CSE-AIML, Geethanjali College of Engineering and Technology, Hyderabad
India.
E-mail address: preeti.preetu11@gmail.com

and

Srinivas Prasad,
Professor, Dept of CSE GITAM School of Technology, GITAM (Deemed to be University), Vishakhapatnam
India.
E-mail address: sprasad@gitam.edu