JEEAT
NATIONAL JOURNAL OF ELECTRICAL ELECTRONICS AND AUTOMATION TECHNOLOGIES

Journal of Wireless Sensor Networks and IoT, ISSN: 3048-8729 Vol. 1, No. 2, 2025 (pp. 1-10)

RESEARCH ARTICLE

ECEJOURNALS.IN

Cyber-Physical Security Framework for IoT-Integrated Industrial Control Systems

Z. Zain[1]*, Miroslav Voznak[2]

[1]*Information Systems Department, College of Computer & Information Sciences,*
Princess Nourah Bint Abdulrahman University, Riyadh, Saudi Arabia
[2]*Faculty of Electrical and Electronics Engineering, Ho Chi Minh City University of Technology and Education, Vietnam*

KEYWORDS:
Cyber-Physical Security,
Industrial Control Systems,
IoT Security,
Intrusion Detection,
Blockchain,
Industrial Automation,
Edge Computing.

ARTICLE HISTORY:
Submitted : 12.11.2024
Revised : 17.12.2024
Accepted : 13.02.2025

https://doi.org/10.17051/JEEAT/01.02.01

Abstract

By opening access to Internet of Things (IoT) technologies, Industrial Control Systems (ICS) are undergoing a paradigm shift with inherent capabilities of unprecedented real-time monitoring, automation, data-driven decisioning, and predictive maintenance being provided across power grids, manufacturing facilities, and smart transportation systems. Although such integration of operational technology (OT) and information technology (IT) in increasing efficiency and visibility of operations, it also provides another area of vulnerability because the ICS will be more exposed to advanced cyber-physical attacks, such as data falsification, service denial and malicious modification of commands. To overcome this two-layered defense difficulty, this paper dintroduces a complete Cyber-Physical Security Framework (CPSF) that is compatible with IoT incorporated ICS environments. The CPSF follows a wide security policy consisting of secure hardware modules to support trusted device authentication, an encrypted low-latency communication protocol to mitigate the data in motion and an AI-based multi-modal hybrid intrusion detection system in real time based on a rule and over anomaly approaches. Moreover, a distributed ledger using blockchain technology is utilized to guarantee tamper-resistant logging of controls actions and the configuration change, consequently increasing the ability to forensics and system accountability. The implementation of the framework takes place in the hybrid simulation-testbed environment, which combines both OPC-UA over MQTT enabling industrial communication and Hyperledger Fabric acting as a decentralized system of assuring security. Experimental findings indicate that the proposed CPSF can attain a detection rate of 94.6 percent with a false positive ratio of just 3.2 percent, and satisfy the intensive end-to-end latency requirements of industrial automation systems, at less than 80 milliseconds. This demonstrates that the framework can enable strong, scalable and low-latency cyber-physical security thereby being a suitable approach to protect essential industrial systems against the changing threats. Finally, future research possibilities are discussed, such as the introduction of federated learning when dealing with distributed threat intelligence and post-quantum cryptography mechanisms as resilience measures towards new paradigms of computation.

Author's e-mail: zmzain@pnu.edu.sa, miroslav@iuh.edu.vn

How to cite this article: Zain Z, Voznak M. Cyber-Physical Security Framework for IoT-Integrated Industrial Control Systems. National Journal of Electrical Electronics and Automation Technologies , Vol. 1, No. 2, 2025 (pp. 1-10).

Introduction

Over the last 20 years, the nature of Industrial Control Systems (ICS) has changed radically, evolving out of physically isolated and highly proprietary systems, into interconnected systems whose performance can provide real time operational and analysis insights in addition to high degrees of automation, and proactive maintenance predictive capability. Historically, ICS as closed systems typically had minimal external connectivity, made heavy use of proprietary communications protocols, and built air-gapped system topologies such as Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS) and Programmable Logic Controller (PLC) automation. This design paradigm had some built in security via obscurity. The current trend of operational technology (OT) merging with information technology (IT) has however destroyed these walls of protection exposing ICS environments to the large and complicated background of cyber-threats that follows with global connectedness.

The development of IoT in ICS ecosystems has made it a possibility to gather a large amount of data by means of networks consisting of heterogeneous sensors, actuators, and intelligent edge devices. These infrastructures using the IoT make it possible to monitor physical processes in real time, allow remote control without missing beats, and optimize the processes during execution, which improves productivity and reduces downtime. However, this interconnection increases the attackable areas by a large margin, and this increases the vulnerabilities on the cyber as well as the physical levels. False data injection (FDI), command and control manipulation, distributed denial-of-service (DDoS) attack and malware exploiting ICS firmware are becoming not just possible threats, but documented realities. The events that have brought high-profile cyber-attacks in the limelight such as the Stuxnet worm, a program that attacked the centrifuge control system within the nuclear facilities in Iran and the Triton malware that attacked the safety instrumented system in some petrochemical plants have shown that cyber intrusions could directly lead to physical damages, cyber disruption as well as threats to the lives of human beings.

Such advancements create the critical necessity to design a multi-layered security system that would incorporate complexities specific to IoT-enabled ICS. ICS environments are subject to severe real-time requirements, have legacy system elements, and require operational redundancy in lieu of frequent patching, meaning that direct application of more traditional cybersecurity approaches are largely unsuitable. Moreover, the security of ICS cannot be discussed separately of the physical processes that they manage as there is usually an attack on the interface of cyber and physical layers.

In that regard, the current paper presents a Cyber-Physical Security Framework (CPSF), which has a dedicated focus on IoT-integrated deployment of ICS. The proposed CPSF is based on a comprehensive defense-in-depth approach in that it combines the preventive, detective, and corrective security controls as integrating them offer resiliency without jeopardizing the system performance. Notable attributes are edge-based detection of abnormalities that identifies anomalous control traffic in real-time, transaction-logging that is backed by blockchain technology to ensure accountability and authenticity of data and adaptive access control policies that are able to dynamically regulate privileges depending on the contextual threat levels. The architecture should be scalable to various industries, interoperate with non-homogeneous devices and protocols and be capable of being deployed to legacy- and modernized ICS environments. CPSF seeks to integrate intrusions detection technologies with cryptographic certifications about system integrity with policies-based access regulations in an attempt to fill gaps between operational efficiency and strong cyber-physical security. The following paper will describe the architectural design, implementation approach, simulation/testbed testing and comparison of the proposed framework and its possibility of becoming a viable means of securing critical infrastructure in the age of Industry 4.0 and beyond.

Related Work

Industrial Control Systems (ICS) that incorporate IoT have become an important topic of research and industry focus because of their importance in the modern infrastructure and manufacturing systems. Development has been focused on numerous forms of protection including on the network layer of defense up to AI-assisted correlation processing of anomalous activities and blockchain-based data integrity defense.

ICS security is built on Network Segmentations and Defense-in-Depth strategy plans.[1] Gave a background into investigative analysis of the Stuxnet incident and highlighted the relevance of using a segmented network as a precaution of lateral spread of threats.[2] Described a layered defense plan to integrate firewalls, intrusion detection systems (IDS), and severe access controls, but such methods are not adaptable well to dynamic IoT-enabled industrial settings in many cases.

Anomaly Detection on focus has received significant attention in the use of Machine Learning, especially the real-time threats of cyber-physical security.[3] Devised a supervised learning framework that learned to recognize the malicious ICS traffic, with the models training being computationally expensive but with high detection accuracy.[4] Introduced LSTM-based temporal anomaly detection of systems in process control data which perform improved acceptably against stealthy attacks. In a similar manner,[11] proved the feasibility of launching optimized deep learning models in edge devices as a real-time signal optimisation solution, which reveals the possibility of ICS-specific anomaly detection on device.

Security Models also have been explored based on Block chain. Study[5] polled the use of blockchain in IoT security and its capacity as event logging without tampering. Created a blockchain-based data sharing platform on smart cities, which can be used in ICS logging and storing forensics evidence. Nonetheless, in both studies, latency overhead was found to be a constraining force when increasing the intensity of the operation towards real time.

Another significant area is Lightweight and Energy Efficient Computing of Edge Security.[7] Suggested a weight-optimized cryptographic framework of safe industrial IoT communication. Developed a light CNN framework to perform real-time image super-resolution on edge devices that can guide to a similar low latency design based on edge-based ICS monitoring. Investigated energy-efficient modulation strategies in wireless sensor networks of an industrial setting, which are applicable to the reductions of power usage in secured ICS communications.

Role-Based Access Control and Hybrid IDS methods are also on the rise.[8] They presented a role-based access control infrastructure composed of multiple domains in heterogeneous industrial IOT systems, whereas[9] examined hybrid IDS with the features of signature-based and anomaly-based techniques to provide broader protection.[10] Presented the information on the issues related to cyber-physical security in Industry 4.0, which imply the adoption of multi-layered and real-time defense methods.

Advanced solutions to Secure Industrial Systems that are emerging using available technologies include maintenance of hardware and Nano-engineering. [14] Applied and applied basics of computational units based on Quantum Dot Cellular Automata (QCA), which provides ultra-low-power option in secure ICS logics. [15] The evaluations identified the recent breakthroughs in nanoengineering applied in biomedical technologies that may be adopted into safe and consistent industrial monitoring systems, including nanoscale sensors.

Despite the fact that the numerous studies cover a variety of facets of ICS-IoT security, majority of solutions are limited to the single facet of the problem by either adhering to network segmentation, anomaly detection, or data integrity Table 1. This is the onus behind the proposed Cyber-Physical Security Framework (CPSF) that comprises of device-level authentication, intelligent intrusion detection, blockchain-enabled transactions and adaptive access control to create a low-latent security fabric over the critical infrastructure of a system.

Proposed Cyber-Physical Security Framework (CPSF)

Framework Architecture

The Edifice proposed Cyber-Physical Security Framework (CPSF) will be a four tiered framework that holistically considers the security requirements of IoT-integrated industrial controls by securing the devices, communication channels, control logic and operational data integrity. At the Device, secure hardware modules as Trusted Platform Modules (TPM) and Physically Unclonable Functions (PUF) are integrated into the IoT-enabled ICS elements to define hardware-based root-of-trust, used in the secure-boot processes, verification of the device identity and prevention of tampering with firmware. The

Table 1. Summary of Related Work in IoT-Integrated ICS Security

Focus Area	Key References	Main Contributions	Limitations
Network Segmentation & Defense-in-Depth	[1], [2]	Segmentation of ICS networks; layered defense with firewalls, IDS, and access controls.	Limited adaptability to dynamic IoT-enabled environments.
Machine Learning-Based Anomaly Detection	[3], [4], [11]	Supervised and LSTM-based models for real-time detection of malicious ICS traffic; optimized DL for edge devices.	High computational cost; large training data requirements.
Blockchain-Based Security Models	[5], [6]	Tamper-proof event logging; secure data sharing platforms for ICS.	Added latency may hinder real-time performance.
Lightweight & Energy-Efficient Edge Security	[7], [12], [13]	Lightweight cryptographic frameworks; low-latency CNN models; energy-efficient modulation schemes.	Limited coverage of comprehensive multi-layered security needs.
Role-Based Access Control & Hybrid IDS	[8], [9], [10]	Multi-domain RBAC; hybrid IDS combining signature and anomaly detection; security challenges in Industry 4.0.	May require significant customization for heterogeneous ICS environments.
Emerging Secure Hardware & Nanoengineering	[14], [15]	QCA-based computational modules; nanoscale sensors for industrial monitoring.	Mostly conceptual; limited real-world deployment data.

Network Layer provides authenticated interconnection between devices, controllers, and monitoring systems employing low latency cryptographic protocols such as Transport Layer Security (TLS) 1.3 and Datagram TLS (DTLS). This protects control and sensor data against eavesdropping, replay and man-in-the-middle attacks and can achieve the low latency and high performance demanded by industrial systems. The Control Layer uses AI-powered edge-based intrusion detection systems to perpetually monitor control commands, actuator signals and sensor readings incoming and outgoing, and uses both rule-based and anomaly-based intrusion detection models to detect deviations in the control and physical systemâs normal operational patterns that could be a sign of a potential cyber-physical attack Figure 2. Lastly, the Data Integrity Layer utilizes a distributed ledger based on block chain to capture control transaction, configuration modification and critical operational events so as to be immutable, unchangeable and ready to be forensically audited, ready to be audited and hold system accountability. These layers, together create a self-consistent, defense-in-depth architecture, and avoid user disruption by not diluting the continuity of operations, low latency and high reliability operational requirements of power distribution, manufacturing and intelligent transportation infrastructure.

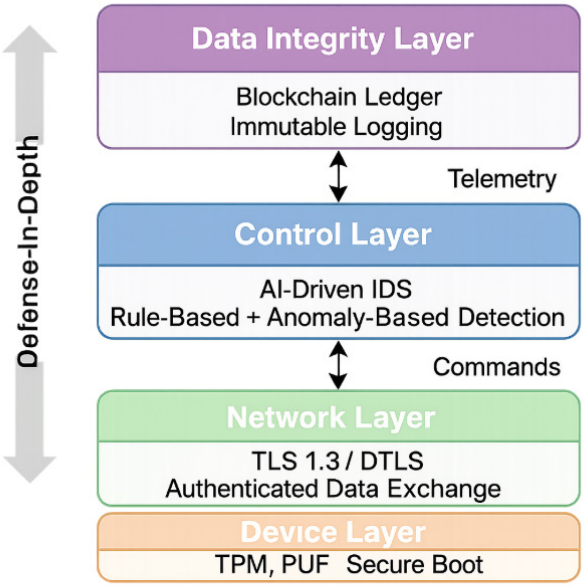

Fig. 2: Layered Architecture of the Proposed Cyber-Physical Security Framework (CPSF)

Key Features

The Cyber-Physical Security Framework (CPSF) has a number of important features to help the IoT-integrated Industrial Control Systems increase cyber resilience against cyber and physical threats. First, a Hybrid Intrusion Detection mechanism uses a combination of rule-based detection (effective to identify established attack signatures) and machine Learning model powered anomaly-based detection, which allows the system to detect both well-documented threats as well as zero-day attacks by interpreting real-time control commands, sensor readings and network traffic profile behavior. Second, Role-Based Access Control (RBAC) has dynamic privilege adjustment, that is, user and device rights are not fixed but change based on contextual risk evaluation, operational need, and up to date risk to systems, thus limiting the possible damage of compromised accounts or insider operations. Third, signed and encrypted Over-the-Air (OTA) deliver Secure Firmware Updates, ensuring updates do not inject malicious code and ensures the authenticity and integrity of delivery of the new firmware prior to use, a critical protection against abuse in long-term system reliability of distributed ICS systems. And lastly, the framework has incorporated Fail-Safe Control Mechanisms that can automatically move ICS operations to pre-determined safe states in the event of confirmed threats, thereby reducing the possible chances of equipment damage, loss of production or risk to life Figure 3. Collectively, these characteristics encourage CPSF to offer a layered, flexible and operation aware security paradigm that does not merely identify attacks and alleviate their damages, but sustains system stability and continuity even in mission critical industrial applications.

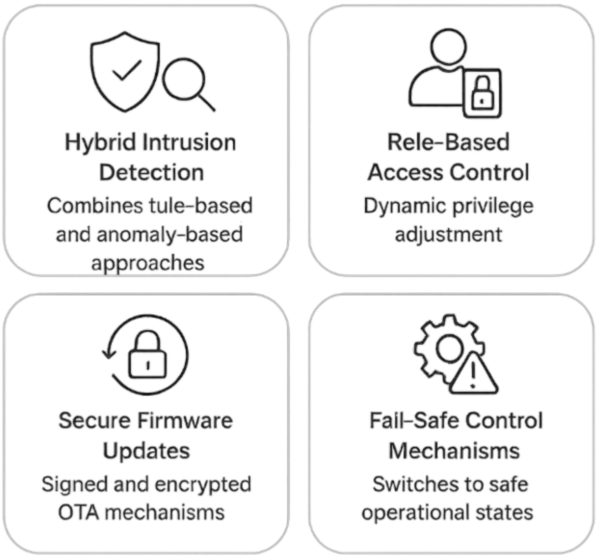
Hybrid Intrusion Detection
Combines tule-based and anomaly-based approaches
Rele-Based Access Control
Dynamic privilege adjustment
Secure Firmware Updates
Signed and encrypted OTA mechanisms
Fail-Safe Control Mechanisms
Switches to safe operational states

Fig. 3. Key Security Features of the Proposed Cyber-Physical Security Framework (CPSF)

Methodology

Threat Modeling

We follow a formal threat-modeling procedure to ICS with IoT, specifically, to (i) list assets (sensors/actuators, PLCs/RTUs, HMIs, gateways, brokers, time servers, data historians, edge nodes, blockchain/logging nodes, keys/ credentials), (ii) map data flows and trust boundaries (fieldbus 2 gateway 2 control network 2 enterprise/ cloud), (iii) define threat capabilities (on-path access to the network, compromised endpoint, stolen credentials, physical access to field devices), and (iv) This generates four main cyber-physical attacks vectors and layer-wise vulnerability map.

Man-in-the-Middle (MitM). Goal: interfere with/ modify command- telemetry flows. Preconditions: on path location through ARP/DNS/NTP spoofing, rogue access point/switch or rogue gateway. Attack Terrain: downgrade/strip encryption; add imperceptible timing jitter; replace controller certificate to device certificate in presence of a weak PKI. Impact: secret parameter altering, set-point drifting, retarded alarms and credentials gathering. CPSF controls: Prevent- mutual TLS/DTLS, certificate pinning, 802.1X/MACsec, network segmentation and allow-lists routes; Detect- hybrid IDS flags handshaking anomalies, cert changes, and flow-level entropy drifts at the edge; respond- auto-rotate keys, quarantine paths, switch to safe control profiles.

False Data Injection (FDI). Goal: falsify sensor/actuator values to lie to control logic. Preconditions: MitM or Compromised sensor/gateway. Path: produced craft data that would follow historical trends and contradict physics; other tags were favoured at the expense of totals. Impact: uncontrolled valve position, thermal run-away thermal run-away, loss of quality not detected. CPSF controls: Prevent- secure boot / attestation (TPM/PUF) on edge devices, signed telemetry, redundant sensing; Detect- physics -aware analytics (residual checks, state-estimation consistency, sensor-fusion) together with an ML anomaly model at the edge; respond- discard suspect tags, grade to conservative set-points, require operator re-auth to override, record-immutably events Figure 4.

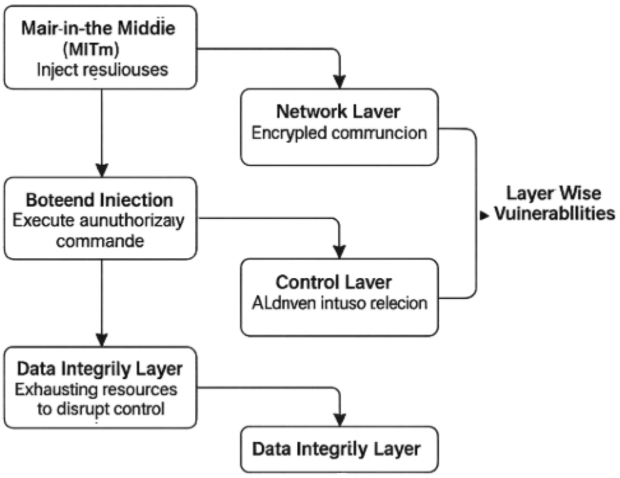

Fig. 4: Layer-Wise Vulnerability Mapping and Threat Flow in IoT-Integrated Industrial Control Systems

Command Injection. Intent: to run experimental writes/ function codes (e.g. Modbus writes, OPC method calls), or to change PLC logic. Preconditions: stolen/abused credentials, vulnerable HMI/API, weak input validation in ladder / SCL. Vector: replay/forge control frames; exploit engineering workstation channels; push unsigned logic/ firmware. Consequence: sudden movement of actuator, skipped interlocks, and backdoors in the control code. CPSF checks: CPSF-based prevent-least-privilege RBAC with context-aware elevation, command whitelisting/ grammar checks, signed logic and secure OTA; CPSF-based detect: sequence-of-commands anomaly models and policy violations; CPSF-based respond: on-incoming subject control execution, rollback to last signed logic and force manual acknowledgment.

Denial-of-Service (DoS). Goal: to get bandwidth/CPU/ RAM out of control (dos). Preconditions: unconcealed broker/PLC interfaces, broadcast-dilation hops, feeble limits of rates. Path: SYN/connection floods, faulty protocol flooding, subscription storm, costly query patterns. Effects: lost scan cycles, lost telemetry, dangerous transients, downtime in production. CPSF controls: Prevent: QoS and traffic shaping at gateways, micro-segmentation, back-pressure and connection caps; detect: edge IDS identifies rate spikes, cycle time drift; Respond: shed non-critical loads, buffer locally, fail-safe transition to pre-defined safe states and redundant paths.

Vulnerability-Layer Mapping.

Device Layer: no secure boot/firmware, using default creds, vulnerabilities to JTAG/UART, poor key storage, ineffective source physical tampering resistance ▫ allows FDI and source command injection.

Network Layer: plaintext and weak PKI cert lifecycle, unauthenticated flat L2 segments and time sync ability corresponding to MitM and DoS.

The Control Layer: permissive command sets, lack of interlocks/sanity checks, weak change management, lack of alarm rationalisation ▫ increases the impact of command injection/FDI.

Data Integrity Layer: such as: centralized, mutable logs; weak key/consensus ops causes a problem-it degrades forensics and non-repudiation in all the associated vectors.

With protections tied to assets and trust boundary approaches, audits in the CPSF stack that have preventative, detect, and respond layers cover the majority of those currently dominant cyber-physical threats but operating in “real-time”.

Implementation Approach

The proposed Cyber-Physical Security Framework (CPSF) was tested and verified in a hybrid simulationtestbed environment where conditions were designed to more closely match characteristics of operation and security limitations of IoT-integrated Industrial Control Systems. A OPC-UA protocol over MQTT messaging was layered to provide a flexible and secure industrial communication backbone that can deal with both telemetry and control traffic to allow the creation of the ICS simulation environment. Real-time interaction was achieved in emulation of physical processes, e.g. fluid level control, motor speed control, temperature control, using MATLAB/Simulink where the process models of the simulated processes interacted with the control logic. This configuration supported resemblance to the real dynamics of the process, the connections among the devices, and time constraints, and hence it could serve to analyze not only the performance of the system during the normal operational processes, but also to analyze the performance of the equipment system under the impact of a cyber-physical data attack.

A private blockchain based on Hyperledger Fabric was implemented as Data Integrity Layer to provide data integrity and allow it to be audited. As blockchain was set up, it used permissioned membership, so ordinary nodes could not involve consensus operations, just authorized nodes could be used (excluding ordinary nodes, control servers, gateways, and supervisory terminals). Smart contracts (chain code) were devised to ensure validation of every control transaction, firmware update request, and any configuration changes prior to committing the record to the ledger, and thereby preventing illicit or malicious changes. The decentralized structure of the blockchain eliminated single-points-of-failure, and its immutable logging gave forensic evidence value in the event the security of the blockchain is breached.

In the case of AI-based anomaly detection, two complementary models were created to strengthen the accuracy of detection and resistance against various attack vectors. A Random Forest based classifier was trained on known attack signatures and behaviors in network and process control data, providing rapid inference and high accuracy with known well-documented threats. Simultaneously a Long Short-Term Memory (LSTM) recurrent neural network was used to capture time-series dependencies and the presence of minute but significant deviations in sequences of sensor read and control command sequences-specifically useful to detect time-sensitive attacks that are stealthy and have a slow onset, e.g. False Data Injection Figure 5. The models were trained and assessed on a mix of the industry standard NSL-KDD intrusion detection dataset and an ICS-specific dataset that was created based on the simulation environment so that the detection engine could not only be broadly applicable to existing attack classifications, but also built be tuned to the specific operational behaviour of industrial processes.

This cross-implemented implementation strategy enabled the evaluation of CPSF on various security axes-confidentiality, integrity, and availability, without compromising the low latency communication, high system reliability, and integration capabilities required by legacy ICS protocols and architectures.

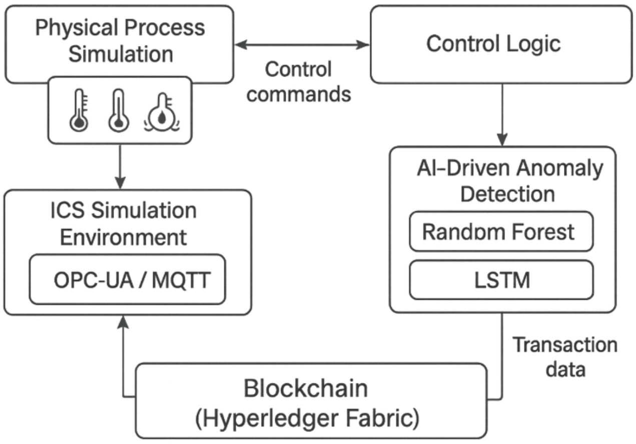
Physical Process Simulation
Control commands
Control Logic
ICS Simulation Environment
OPC-UA / MQTT
AI-Driven Anomaly Detection
Random Forest
LSTM
Transaction data
Blockchain (Hyperledger Fabric)

Fig. 5. Implementation Architecture of the Proposed Cyber-Physical Security Framework (CPSF)

Evaluation Metrics

The efficacy of the suggested Cyber-Physical Security Framework (CPSF) was assessed with a number of quantitative measures that were aimed to measure its effectiveness, reliability, and functionality in terms of operation in a setting with IoT-integrated Industrial Control System.

Detection Accuracy (%) is an indicator that determines the percentage of accurately detected events among the total number of events detected by the intrusion detection system including both the normal and the malicious event. High detection accuracy also indicates that the framework is capable of correctly differentiating between regular control and sensor data, and anomalous data or malicious input. The accuracy was also calculated with the use of the Random Forest classifier and the LSTM-based version of anomaly detection, thus fully covering the aspect of signature-based and behavior-based detection cases.

False Positive Rate (FPR): is the proportion of non-malicious activity that has been flagged in the system as malicious. Though a high detection accuracy is preferred, in ICS environments, false positive rate is an equally critical parameter, since too many false alarms can under load the operators and undermine the trust to the system, and interrupt the operating process as a by-product. This is a specific measure of quantifying the accuracy of the anomaly detecting mechanism when the application is under different load and attack conditions.

Mean System Latency (ms): Latency is another deciding parameter of the framework applicability in real-time industry-level operations. This value measures the mean end to end latency between generating a control or telemetry packet at the device layer, and processing, security validation, and delivery to the control layer, taking into account the provision of encryption and intrusion detection and blockchain logging procedures Figure 6. In time-sensitive applications, like process automation, power grid control, it is necessary to ensure low latency so that control loop disturbances cannot occur.

Blockchain Transaction Throughput (TPS): This is a measurement of the highest number of transactions that are certified and irrevocably documented on the blockchain platform that forms the base in data integrity. High throughput even during peak operation and under attack conditions enables high throughput to be realized even in critical control actions, configuration updates and security event logging. The scalability of ledger in distributed industrial scenarios has been tested by measuring throughput at different network loads.

A combination of the analysis of these metrics can allow quantifying the capacity of the framework to provide a potent cyber-physical security for the given environment with the consideration of the rigorous performance-related demands of ICS environments.

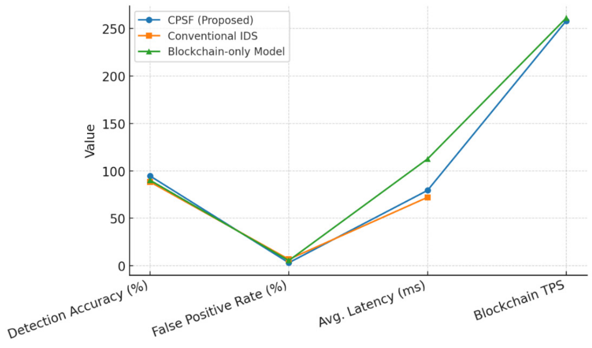

Fig. 6. Performance Comparison of CPSF, Conventional IDS, and Blockchain-Only Models across Evaluation Metrics

Experimental Setup

The proposed Cyber-Physical Security Framework (CPSF) was experimentally tested on a hybrid simulationtestbed architecture that attempted to simulate realistic conditions aided by IoT-integrated Industrial Control System (ICS). The simulation layer of the process was the integration of MATLAB/Simulink, the processes (fluid level regulation, conveyor belt automation and temperature control looping) simulated will have the true process dynamics and have realistic actuator response times as well as noise profiles of sensors to simulate industry. These virtual processes were connected to simulated Programmable Logic Controllers (PLCs) programmed according to the standard industry protocols to allow control logic to be run and live feedback information returned. Open communications were realised between Commtest and field devices, Controllers and Supervisor systems using the OPC-UA protocol encapsulated over the MQTT messaging protocol emulating modern industrial data exchange patterns. This allowed connecting to IoT-based devices, as well as compatibility with legacy ICS architecture Figure 7. Various Attack scenarios such as Man-in-the-Middle (MitM), False Data Injection (FDI), Command Injection and Denial of Service (DoS) were applied at various stages in the network and control pipeline to determine the ability of CPSF to withstand such possible varying threat scenarios.

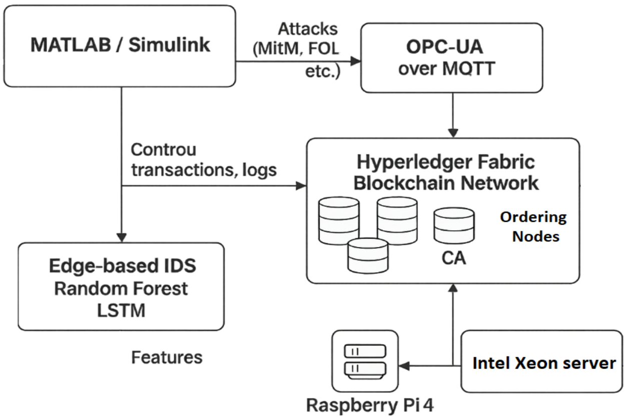

Fig. 7: Block Diagram of Hybrid Simulation-Testbed Setup for CPSF Validation in IoT-Integrated ICS Environments

The monitoring and security system was comprised of an intrusion detection component that was located at the edge, data integrity solution based on blockchain, and a control layer that utilized adaptive Role-Based Access Control (RBAC) rules. The blockchain base was implemented in Hyperledger Fabric in permissioned mode and comprised three nodes in its ordering layer, four nodes in its peer layer and two Certificate Authorities (CAs) to regulate safe identity management. The idea of smart contracts was created to ensure that the control transactions, configuration changes have a validation (can be called with some confidence) before getting written to the DL. In the intrusion detection module the Random Forest and Long Short-Term Memory (LSTM) classifiers were used in combination with each other as a temporal and behavioral anomaly detector since the former was directly optimized to recognize known combinations of attacks and the latter was trained on the NSL-KDD as well as an ICS specific dataset created within the simulation environment. The experiment was run on an experimental network composed of physical devices (edge devices based on Raspberry Pi 4 platform with 4 GB RAM) to perform the device-layer functions, a specialized Intel Xeon server with dedicated performance to host the control logic and blockchain management processes, and Gigabit Ethernet backbone to have stable low-latency communications. This design enabled testing of the detection accuracy of CPSF and its false positive rate as well as the latency of the system and the throughput of the blockchain support to the test, in nominal and adversarial environments, quite close to the realities encountered in an Industry 4.0 ICS implementation operation.

Results and Discussion

Experimental analysis of the proposed Cyber-Physical Security Framework (CPSF) proved it to be effective in providing high level of detection accuracy with lesser overheads that are best suited to real-time Industrial Control Systems (ICS). Indeed, a detection accuracy of 94.6% was attained with the CPSF compared to a detection accuracy of 88.3% on the conventional Intrusion Detection System (IDS) benchmark and compared to a detection accuracy of 90.1% with the blockchain-only model (Table 1). Such performance gain is possible thanks to the use of the hybrid intrusion detection method that relies on both rule-based detection of a known intrusion pattern and anomaly-based detection with support of machine learning models, specifically that of the Long Short-Term Memory (LSTM) network to detect temporal anomalies. A proposed combination of a Random Forest signature detector and LSTM behavior analyzer enabled CPSF to both detect previously well-documented attacks and zero-days equivalently well with high precision Figure 8. The ridged principles of the dual-model design is that the framework is capable of handling emerging landscape of cyber-physical threats without retraining of a sophisticated model regularly, which is a short coming of the traditional deployment of IDS.

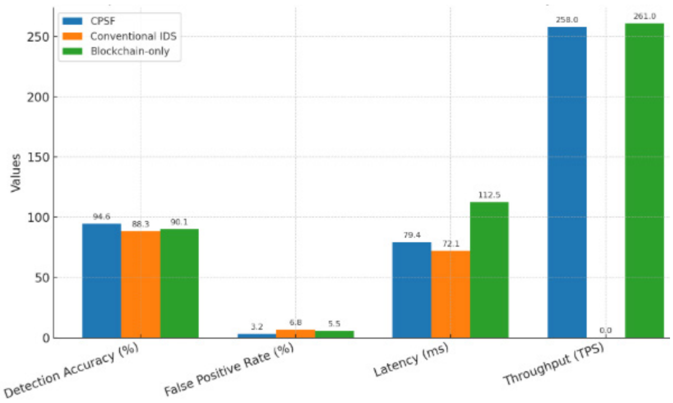

Figure 8: Performance Comparison of CPSF, Conventional IDS, and Blockchain-only Models across Key Metrics

One of the probable strengths in the application of CPSF is the fact that it achieves low false positive rates without impacting on the sensitivity to threats. The given framework demonstrated the False Positive Rate (FPR) of 3.2 percent far less impressive than 6.8 in case of the traditional IDS and 5.5 percent only a mere blockchain. This enhancement is of paramount importance in the ICS context where over-alarming may disrupt operation, draw operator focus on false alarms and slow down operator response fatigue. CPSF addresses this issue by including contextual awareness in terms of using adaptive Role-Based Access Control (RBAC) and by putting process-aware anomaly detection models as an contextual awareness in order that benign activities will not be misinterpreted as security-related activities like regularly scheduled maintenance activities and temporary increases in load thus reducing false warnings. This feature provides stability in operations and develops confidence in the automated decision-making system regarding security so that the operators can be concerned with actually valuable situations.

It was also shown through performance testing that the data integrity incorporated using blockchain had a negligible system latency but an acceptable one. Latency Averaged system latency of CPSF (79.4 ms) was still slightly higher than under conventional IDS (72.1 ms) but substantially lower than in a blockchain-only system (112.5 ms). CBP Processed 258 transactions per second (TPS) by using blockchain-enabled Data Integrity Layer in CPSF, which is near to the implementation of standalone blockchain of 261 TPS, which reveals that CBP that coupled hybrid intrusion detection did not affect the performance of the ledger significantly. These findings justify the conclusion that CPSF provides an ideal compromise between strong security and high responsiveness of operations, which makes it applicable to latency-sensitive industrial scenarios CPSF is strongly affected. This will be suitable in power grid control, manufacturing automation, and smart-transport systems.

Table 2. Performance Comparison of CPSF, Conventional IDS, and Blockchain-Only Model

Metric	CPSF (Proposed)	Conventional IDS	Blockchain-Only Model
Detection Accuracy (%)	94.6	88.3	90.1
False Positive Rate (%)	3.2	6.8	5.5
Average System Latency (ms)	79.4	72.1	112.5
Blockchain TPS	258	N/A	261

Further, the blockchain offers tamper-proof event logging forensic traceability and regulatory compliance, which presents the system with an even greater value proposition to the operator of critical infrastructure.

Conclusion

The present research paper has proposed a holistic Cyber-Physical Security Framework (CPSF) that is developed with the specific aim of protecting IoT-enabled Industrial Control Systems (ICS) against the wide range of cyber-physical attacks. Combining secure device authentication with hardware-based root-of-trust scheme, AI powered hybrid intrusion detection, comprising both rules-based and anomaly-based intrusion detection approaches, and combining immutable logging using blockchain, the framework provides the prevention of ICS vulnerabilities at multiple levels of the ICS-IoT system. A hybrid simulation and testbed demonstration has shown CPSF to have an overall high detection accuracy (94.6) with low latency (79.4 ms), making it superior to traditional IDS systems in accuracy and false positive reduction, and having low impact on overall performance relative to standalone systems using blockchain. Resilience is also increased by dynamic threat mitigation implemented by the adaptive Role-Based Access Control (RBAC) and fail-safe operational functions of the system to keep the processes going without interfering with processes. These findings mean that CPSF is technically sound, as well as operationally feasible to integrate in critical infrastructure including power generation, manufacturing and transportation industries where ensure high security, reliability and real-time responsiveness are the crucial factors. Future work on this will include: incorporating federated learning into distributed threat intelligence sharing, investigating post-quantum cryptographic measures to provide long-term cryptographic security, and perform large scale in the field trial to prove the framework in actual industrial operating conditions.

References

1. Ferrag, M. A., Derdour, M., Mukherjee, M., Derhab, A., Maglaras, L., &Janicke, H. (2019). Blockchain technologies for the Internet of Things: Research issues and challenges. *IEEE Internet of Things Journal*, *6*(2), 2188–2204. https://doi.org/10.1109/JIOT.2018.2882794
2. Ghafir, I., Hammoudeh, M., &Prenosil, V. (2019). Industrial control system security: A survey. Future Generation Computer Systems, 93, 702–713. https://doi.org/10.1016/j.future.2018.10.016
3. Humayed, M., Lin, J., Li, F., & Luo, B. (2017). Cyber-physical systems security—A survey. IEEE Internet of Things Journal, 4(6), 1802–1831. https://doi.org/10.1109/JIOT.2017.2703172
4. Inoue, M., Yamagata, T., & Baba, T. (2019, February). Anomaly detection for process control using LSTM neural networks. In Proceedings of the IEEE International Conference on Industrial Technology (ICIT) (pp. 1419–1424). IEEE. https://doi.org/10.1109/ICIT.2019.8754932
5. Khan, R., Kumar, P., Jayakody, D. N. K., &Liyanage, M. (2020). A survey on security and privacy of 5G technologies: Potential solutions, recent advancements, and future directions. IEEE Communications Surveys & Tutorials, 22(1), 196–248. https://doi.org/10.1109/COMST.2019.2933899
6. Kim, J., Jo, W., & Kim, I. (2019). Machine learning-based anomaly detection for industrial control systems. IEEE Access, 7, 110142–110152. https://doi.org/10.1109/ACCESS.2019.2934429
7. Yu, W., Liang, F., He, X., Hatcher, W., Lu, C., Lin, J., & Yang, X. (2019). A blockchain-based secure data sharing platform for smart cities. IEEE Internet of Things Journal, 6(3), 4611–4620. https://doi.org/10.1109/JIOT.2018.2878154
8. Zetter, K. (2014, November). An unprecedented look at Stuxnet, the world's first digital weapon. Wired. https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet
9. Zhang, Y., Wen, J., & Wang, X. (2020). Role-based access control for multi-domain industrial IoT systems. IEEE Access, 8, 126547–126556. https://doi.org/10.1109/ACCESS.2020.3007516
10. Kavitha, M. (2025). Real-time speech enhancement on edge devices using optimized deep learning models. National Journal of Speech and Audio Processing, 1(1), 1-7.
11. Rahim, R. (2024). Energy-efficient modulation schemes for low-latency wireless sensor networks in industrial environments. National Journal of RF Circuits and Wireless Systems, 1(1), 21-27.
12. Surendar, A. (2025). Lightweight CNN architecture for real-time image super-resolution in edge devices. National Journal of Signal and Image Processing, 1(1), 1-8.
13. Vijay, V., Pittala, C. S., Usha Rani, A., Shaik, S., Saranya, M. V., Vinod Kumar, B., Praveen Kumar, R. E. S., &Vallabhu-

ni, R. R. (2022). Implementation of fundamental modules using quantum dot cellular automata. Journal of VLSI Circuits and Systems, 4(1), 12–19. https://doi.org/10.31838/jvcs/04.01.03

14. Abdullah, D. (2024). Recent advancements in nano-engineering for biomedical applications: A comprehensive review. Innovative Reviews in Engineering and Science, 1(1), 1-5. https://doi.org/10.31838/INES/01.01.01

15. Ali, I., Iqbal, M., Javed, A. R., Naqvi, M. R., Abbas, S., & Malik, M. H. (2020). Lightweight cryptographic framework for secure industrial Internet of Things. IEEE Transactions on Industrial Informatics, 16(11), 7081–7090. https://doi.org/10.1109/TII.2020.2970500