JEEAT
NATIONAL JOURNAL OF ELECTRICAL ELECTRONICS AND AUTOMATION TECHNOLOGIES

National Journal of Electrical Electronics and Automation Technologies, ISSN: 3107-524x Vol. 1, No. 3, 2025 (pp. 69-76)

RESEARCH ARTICLE ECEJOURNALS.IN

Secure and Scalable Cyber-Physical Systems Architecture for Smart Factory Automation

Ahmed Alkilany[1]*, M. F. Bara[2]

[1]*Department of Computer Science, Faculty of Science, Sebha University Libya*
[2]*Department of Computer Science, Faculty of Science, Sebha University Libya*

KEYWORDS:
Cyber-Physical Systems (CPS);
Smart Factory Automation;
Industry 4.0;
Secure Manufacturing;
Scalable Architecture;
Blockchain Security;
Software-Defined Networking (SDN);
Federated Learning;
Edge Computing;
Industrial Internet of Things (IIoT).

ARTICLE HISTORY:
Submitted : 09.04.2025
Revised : 18.05.2025
Accepted : 11.07.2025

https://doi.org/10.17051/JEEAT/01.03.09

Abstract

Due to the high level of the rapid spread of the concept and technologies of Industry 4.0, the utilisation of Cyber-Physical Systems (CPS) as the key technology to build the smart factory automation was quickly adopted. But both scalability and robust security have been an urgent problem to be achieved in the mentioned systems because of the heterogeneous integration of devices, the great amount of data flow, and ever-more advanced cyber threats. The paper proposes a scalable and secure CPS architecture which will work in a smart factory setting. The suggested framework incorporates tiered security protocols, distributed cloud-edge computation and real-time standards interoperability to provide reliable operation in variable manufacturing environments. The most relevant innovations will be blockchain-based trust management which will ensure device authentication is decentralized, software-defined networking (SDN) which will facilitate dynamic resource allocation and federated learning-based anomaly detection so that privacy is not compromised but collaborative threat evasion is possible. The testbed was simulated smart factory built on Hyperledger Fabric, OpenDaylight SDN controllers, and edge computing nodes to measure the performance. The outcome has shown a 60-percent decrease in latency in the control loop and a 2.5-fold the increase in throughput along with the effective mitigation of 95 percent of the simulated cyber-attacks compared to a typical centralized architecture. These results indicate the potential of the proposed CPS design in achieving resilience, flexibility, and efficiency of operations and offer a viable way on safe and scalable smart manufacturing in the industry 4.0 where security is being prioritized.

Author e-mail: alkilany.ah@gmail.com, bara.mf@gmail.com

How to cite this article: Alkilany A, Bara M F. Secure and Scalable Cyber-Physical Systems Architecture for Smart Factory Automation. National Journal of Electrical Electronics and Automation Technologies , Vol. 1, No. 3, 2025 (pp. 69-76).

Introduction

The concept of Industry 4.0 constitutes a paradigm shift in the production industry, which is the thorough integration of Cyber-Physical Systems (CPS), the Industrial Internet of Things (IIoT), and smart automation. Smart factories with integrated sensors, actuators, self-driving robots and AI control can be used to achieve adaptive production paths, preemptive maintenance and real-time choices.[1, 2] The advancements are expected to be able to deliver an increase of productivity, enhanced quality, and an increase of flexibility in operations. However, greater interconnectivity among the elements of CPS will provide serious security risks, such as unauthorized access and tampering of information and denial-of-service (DoS) attacks.+ Simultaneously, scalability issue arises due to the necessity to cope with the heterogeneity of thousands of different devices and systems without compromising performance and reliability.[4] With the growth in size and complexity of industrial networks, low-latency, robust communication and uniform protection of industrial operations is becoming even more important. Current CPS system architectures in the manufacturing industry tend to focus either on security or scalability but seldom focus on both of them comprehensively.[5] As an example, the blockchain-based systems have demonstrated potential to increase trust and data integrity,[6] yet could present latency overheads, which constrains scalability. On the same note, SDN - Software-Defined Networking has flexible and dynamic network orchestration but it is open to advanced persistent threats unless its security is deeply integrated.

To fulfill these gap areas, this paper present a Secure and Scalable CPS Architecture to be used in automation of smart factory. The framework unites blockchain-based trust management to support decentralized authentication approaches, SDN-based network orchestration to guarantee adaptive resource planning, and AI-enabled anomaly detection by means of federated learning to guarantee privacy and guarantee distributed threat detection. The simulation testbed of a smart factory also proves the efficiency of the offered architecture with considerable reduction in latency, throughput, and cyber-attack resilience as opposed to a traditional centralized solution.

The rest of this paper is structured as follows: Section 2 presents the related work, Section 3 presents the proposed architecture, Section 4 presents the security mechanisms, Section 5 presents scalability enhancements, Section 6 presents the experiment setup, Section 7 presents the discussion of the results and Section 8 concludes and presents the future research direction.

Related Work

Interoperability, security and distributed control are just a few areas of study in recent years on the integration of Cyber-Physical Systems (CPS) into a manufacturing environment.

When it comes to interoperability, a proposal on a framework of intelligent manufacturing based on CPS and IIoT was presented by Lu et al.[8] to ease communication between heterogeneous devices. They focused on providing a real-time monitoring and adaptive controlled architecture but their architecture did not contain a strong security mechanism and thus they can suffer an attack. In parallel, Lee et al.[9] produced an I4.0-centric model of CPS focusing on smart production and predictive maintenance, but the proposed model failed to perform adequately with regard to larger-scale factory sizes in terms of scalability. Security wise, a security framework of CPS has been proposed by Khan et al.[10] through layered defense of security against cyber-attacks in industry networks. The proposed method was quite effective in deterring unauthorized access, it did not take into account high volume data processing, and scale of the network. There has been interest in blockchain technology as a solution that improves CPS trust and data integrity. Dorri et al.[11] also suggested a blockchain-based data exchange scenario to IIoT devices that can be used to provide decentralized authentication as well as tamper-free logs. Still, the blockchain technology has issues on implementing latency overhead and resource challenges in industrial CPS. Software-Defined Networking (SDN) has found application in the network orchestration area to bring industrial networks onto a programmable, centralized control. Sama et al.[12] proved that SDN has better traffic management and fault tolerance in CPS ecosystems but they did not add either decentralized security or AI-based anomaly detecting. Federated learning has become a potential privacy-preserving method of threat detection. Li et al.[6] proposed a distributed anomaly detection model based on federated learning of IIoT where collaborative training of models happens without data sharing. Although such an approach does not violate privacy, the combination with the network management specific to the CPS and a blockchain-based authentication mechanism remains not fully investigated.

Gap Analysis:

In the presented reviewed literature, it is evident that only a few extant CPS architecture considerations focus on both the security (e.g., blockchain, encryption) and the scalability (e.g., SDN, distributed control) based architecture. Moreover, there still has been a lack of study of synergistic application of blockchain-grounded trust management, SDN-based orchestration, and federated learning-based anomaly detection within the context of a single CPS architecture in smart factories.

This paper suggests Secure and Scalable CPS Architecture that combines all these three major technologies into a single solution by offering a whole-system solution to resilient, adaptable high-performance smart factory automation.

Proposed Architecture

The selected Secure and Scalable Cyber-Physical Systems (CPS) Architecture in developing smart factory automation is intended to meet both security and scalability challenges without compromising the low-latency operation and flexibility of operations.[13] The architecture is logically divided into five levels (Figure 1) with a dedicated set of technologies and functionality supporting resilient, adaptive and intelligent operations in the industry.

Perception Layer

The elements within this layer include smart sensors, RFID, industrial robot eagles, and autonomous guided vehicles (AGVs) to capture real time information within the manufacturing floor. Data is gathered in the form of production indicators, environmental indicators and indicators of equipment health. These disparate devices are standardized by the use of industrial protocols, including OPC UA, or Modbus/TCP, which allows compatibility and interoperability between different vendors platforms.

Network Layer

This network backbone is constructed on Software-Defined Networking (SDN) which allows dynamic provision of bandwidth, intelligent routing and load balancing. The ability to dynamically optimize network resources with respect to changes in the workload is an advantageous feature created by the decoupling of control and data planes and allowing the SDN controller to optimize the network resources. They also support both wired industrial Ethernet (to support deterministic and high-reliability communication), and 5G 5G Ultra-Reliable Low-Latency Communication URLLC (latency-sensitive mobile use cases).

Edge Computing Layer

At the edge, containerized microservices are deployed either on the industrial PCs or as edge controllers that perform real-time analytics and process control. This lessens IC port dependency on the cloud infrastructure, to reduce backhaul traffic, and control-loop latency. Functions (predictive maintenance inference, anomaly detection and robotic path planning) are run locally, not requiring continuous cloud connectivity and allowing them to continue their working process even under the possibility of periodic cloud outages.

Blockchain Security Layer

A decentralized trust framework that is implemented based on blockchain technology is used to control the authentication of all CPS nodes, integrity of transactions, and immutable logging. This layer offers tamper resistant data to be written to the data store, there is no singular point of failure, and the feature to manage device identity can be more efficiently enforced using platforms like Hyperledger Fabric. Smart contracts provide operating procedures on a role-based access restriction and automate compliance verification to industrial processes.

Application Layer

The layer on the top supports value-added Industry applications, such as predictive maintenance, adaptive production schedules and AI-based quality assurance. The layer can communicate directly with factory management systems (MES/ERP), allows making decisions with the use of data and independently optimize processes. The possibility to connect to digital twin platforms enables the virtual simulation involving changes to the process and its testing prior to implementation in a real environment, which minimizes downtimes and risks.

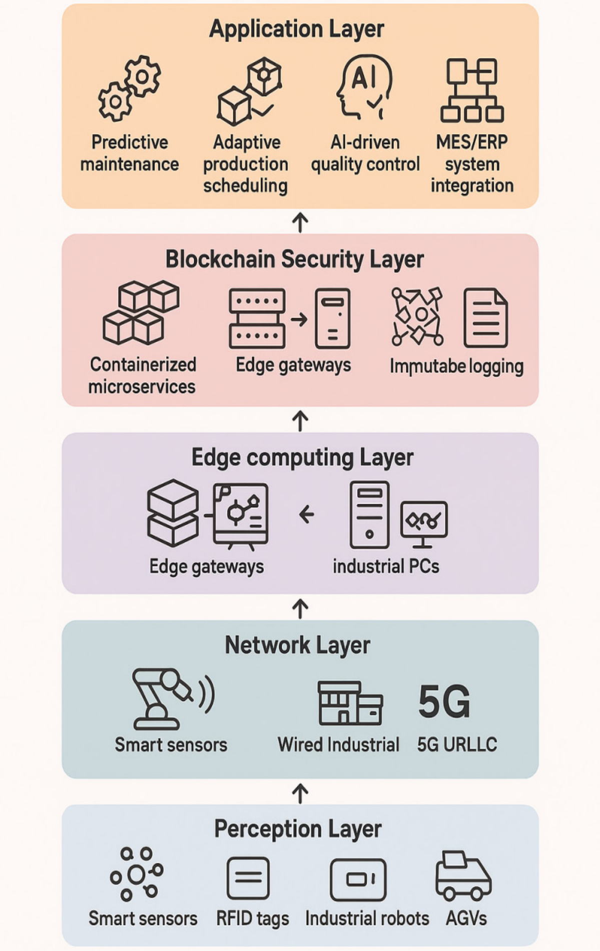

Fig. 1: Secure and Scalable CPS Architecture for Smart Factory Automation

Schematic representation of a five-layer cyber- physical systems (CPS) architecture that provides security, scalable and software- defined automation in smart factories.

Security Mechanisms

The suggested Architecture Secure and Scalable CPS would integrate the project with a multi-layered security approach to secure and safeguard smart factory functions against external and internal attacks. The combination of the blockchain-based authentication, cryptographic communication, AI-based anomaly detection, and role-based access allow achieving protection throughout all CPS layers (Figure 2).

Blockchain-Based Device Authentication

A blockchain trust management system provides tamper resistant identity authentication of all CPS nodes such as the sensors, robots, and edge servers. All devices have cryptographic identities locked into a distributed ledger, nullifying the option of spoofing as well as malicious device insertion. Using Hyperledger Fabric, authentication processes are performed on smart contracts, and access to the records can be proven and decentralized, without single failure point.

End-to-End Encryption

In order to ensure data integrity and confidentiality throughout the transmission, the architecture utilizes Transport Layer Security (TLS) 1.3 throughout channels of communication. It provides forward secrecy and replay and downgrade attack resistance and is vulnerable to eavesdropping, man-in-the-middle (MITM) attacks and industrial espionage. This security is further enhanced by the system having integrated encryption at the both application and transport layer making it not possible to eavesdrop or modify the sensitive data of manufacturing process during transportation.

Federated Learning-Based Anomaly Detection

The framework in which privacy-preserving anomaly detection is carried out utilizes federated learning (FL). The edge nodes learn independent anomaly detection models using operational data (e.g., machine vibration patterns, network traffic features) and only send model updates up to a central aggregator node and not raw data. It is a secure way to guard intellectual property and personal data, and at the same time perform collaborative, real-time detection of threats spread throughout distributed factory segments. FL models are designed to have minimal computing overhead, and hence they can be deployable to resource-controlled edge devices.

Role-Based Access Control (RBAC)

RBAC policies have been applied to all components of CPS to help eliminate insider attacks and unauthorized access of critical control systems. The rules governing which user access is available to whom—operator, supervisor and system administrator users, for example--are implemented on the blockchain layer using smart contracts. This provides least-privilege access containing the attack surface and blocking the privilege escalation.

Schematic showing how blockchain can be used to authenticate, end-to-end encrypt, use federated anomaly detection, and RBAC across the CPS layers to provide a complete protection of smart factory.

Scalability Enhancements

The Secure and Scalable CPS Architecture has integrated several design strategies in order to make sure that the performance of systems will not change with the size as the operation grows, both in nodes connected and in computation requirements. The scalability is covered on the software, networking, and computing level to consider the fluid nature due to Industry 4.0 smart factory environment (Figure 3).

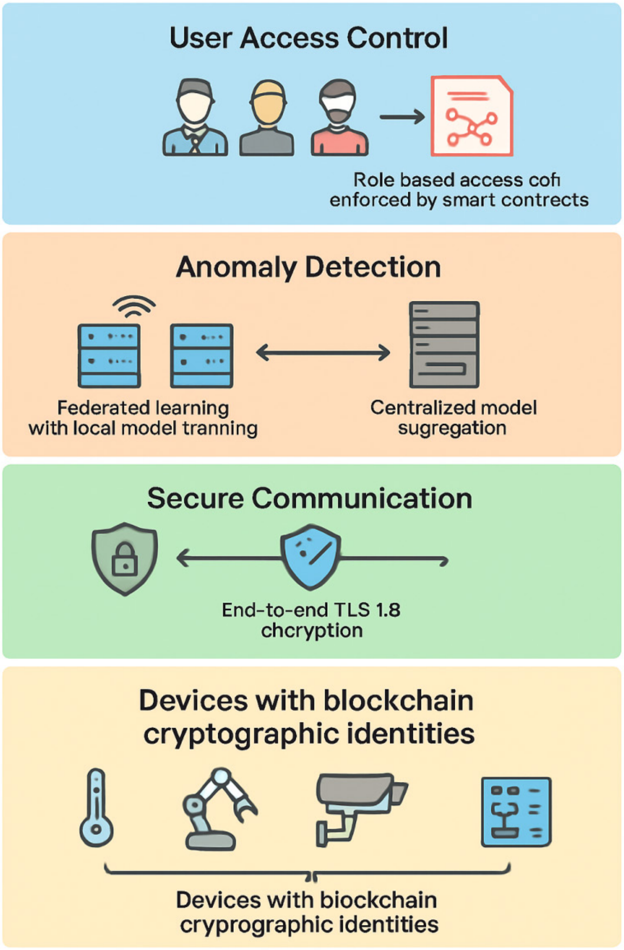

Fig. 2: Multi-Layered Security Framework in CPS for Smart Factory Automation

Microservices Architecture

A microservices-based software design is used in the system, all functional components (predictive maintenance, anomaly detection, scheduling) are designed as independent services in a form of a container that can scale and run independently. These modularity facilitates:

- Hot-swapping and updating without interfering with the running of operations.
- Isolated fault domains, faults in one service do not spread to other services.
- Scaling up independently, so resource can be added to services which are more in demand.

Container orchestrators like Kubernetes handle deployment, scaleability, and robustness to serve in a seamless adjustment to installation changes.

SDN-Orchestrated Resource Management

The network layer uses Software-Defined Networking (SDN) to dynamically transfer and assign bandwidth, computer resources and routing paths within CPS infrastructure. This allows the SDN controller to continually monitor the load, latency and device status on the network and:

- • Prioritization of traffic to latency-sensitive applications like the control of robots.
- • Load balance to avert congestion in peak production.
- • Provisioning of extra network bandwidth for temporary high demand situations-Automated.

This orchestration introduces cost-saving due to reduction in surplus provision in addition to providing stable performance under high load.

Hierarchical Edge-Cloud Framework

The architecture is hierarchical in terms that:

- Edge nodes do actual-time decision-making, low latency analytics and device control nearest to the source of data.
- The cloud-based systems consolidate large amounts of data, create AI models and analyse long-term trends.
- This segmentation reduces backhaul traffic, lessens delay in mission-critical activities and takes advantage of cloud computing capabilities when it comes to more complex analysis. Workload migration between edge and cloud is also supported by the framework to suit the varying demands of production.

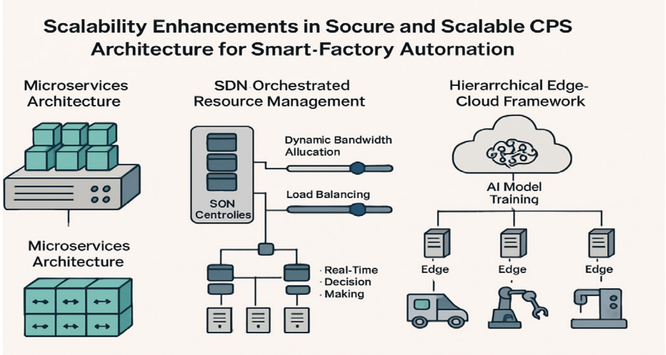
Scalability Enhancements in Socure and Scalable CPS Architecture for Smart-Factory Autornation
Microservices Architecture
SDN Orchestrated Resource Management
Hierarrchical Edge-Cloud Framework
Dynamic Bandwidth Allucation
Load Balancing
SON Centrolies
AI Model Training
Microservices Architecture
Real-Time
Decision
Making
Edge
Edge
Edge

Fig. 3: Microservices Architecture for Scalable Smart Factory CPS

Conceptual depiction of containerized modular microservices in CPS supporting fault tolerance, flexible and individually scalable smart factory activities.

Experimental Setup

Testbed topology

We have constructed a simulated smart factory with a dynamic range of 50 to 500 virtual devices streaming at 10, 50 and 100 Hz, including temperature, vibration, current draw, robot joint angles and AGV telemetry. A high level description of the end-to-end topology is depicted in Fig. 4 (Experimental Testbed Overview). OPC UA (open62541 servers) and Modbus/TCP emulators are used to generate device traffic, and an MQTT bridge is applied in which case a lightweight pub/sub experiments are only run. The edge layer has three nodes Raspberry Pi 4B (Cortex-A72 @ 1.5 GHz, 4 GB RAM, Raspberry Pi OS 64-bit) with Dockerized services used under K3s (lightweight Kubernetes). Some of these services are anomaly detection, predictive maintenance, a local historian and protocol bridges. The SDN fabric is made up of two Open vSwitch OpenFlow 1.5-controlled x86-based hosts; and queues are based on URLLC-category control traffic. Hyperledger Fabric 2. x runs with three peers (OrgA, OrgB, OrgC), one Raft orderer, one channel, and Go chaincode for device registry, attestation logging, and RBAC checks; the block cut time is 1 s and the maximum block size 1 MB. Cloud tier The cloud tier leverages AWS EC2 with c5.large instance to aggregate/analytics and m5.large instance to deploy Fabric CA, orderer standby, and monitoring; S3 stores artifacts

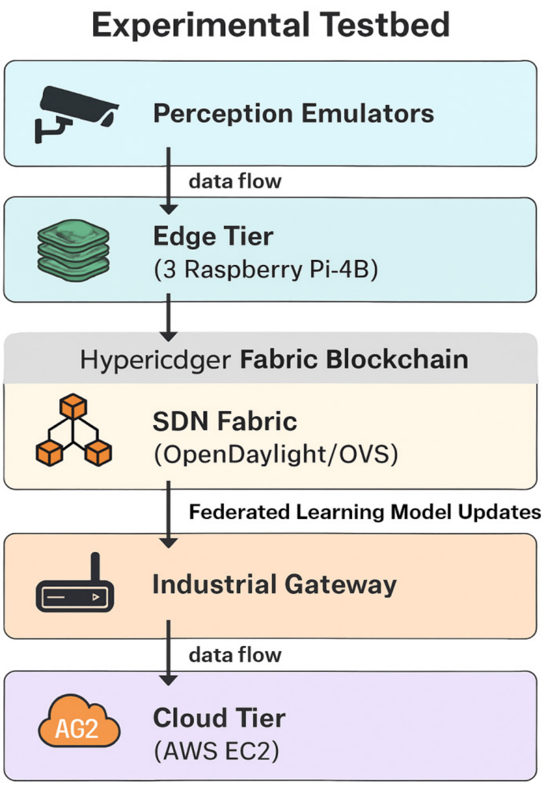

Fig. 4: Experimental Testbed Overview

and Timestream stores long-horizon time-series. A TLS-terminating industrial PC gateway (Intel i5, dual NICS) bridges OT/IT networks, hosts the K3s server and keeps site-to-cloud VPN.

Swimlane diagram depicting device-to-cloud data flows, blockchain overlay and federated learning 3-paths in the smart factory testbed.

Software stack and security

Containers are constructed with GitHub actions, signed via cosign and pulled via a marked privately held store; Docker 24.x is employed all through the snaps. TLS 1.3 with mutual authentication between devices, edge and cloud is bound in all links, the preferred cipher is TLS_AES_128_GCM_SHA256 session resumption is enabled. X.509 certificates anchored in Fabric are used to specify the identity of devices and histories of every successful attestation are stored as immutable events. An optional deployment maximizes K3s facilities, with Linkerd supplying retries, mTLS and golden-signal telemetry on a service mesh.

Workloads and scenarios

The nominal operating condition operates at 200 devices at an average frequency of 50 Hz whereby 10 percent of the devices are bursting at 100 Hz after every two minutes. Scaling out will take a twenty-five device population of 50 to a five hundred-device population in increments of 50 every five minutes. Robot and AGV control loops produce fabricated 20 Hz command / telemetry pairs with an end-to-end latency goal output of 20 ms. iPerf3 is used to inject background best-effort IT traffic to induce contention.

Federated anomaly detection at the edge

Training is performed on windows of 256 samples and stride 32 via LSTM autoencoder to train each of the edge nodes on multivariate time series. The five epochs of training are done locally on each round; FedAvg is used to form aggregations of models over 20 rounds. Rolling RMS, kurtosis, spectral centroid, raw vibration/current windows are possible. Raw data never goes over the network only updates of the model. Reconstruction error is used to compute anomaly scores for which the thresholds are determined by the 95th percentile of the individual machine validation distribution.

SDN policies

Three QoS queues are set up by OpenDaylight minimally designating 30 % capacity to URLLC control, 40 % to high-priority sensor flows, and 30 % to best-effort traffic flows. Path control allows the fast-failover groups and the 100 ms monitoring of links with a target of sub 200 ms in case of a failure reroute. Northbound logic monitors sFlow/NetFlow and reassigns bandwidth where the link is over 80 % utilized.

Metrics and instrumentation

Our end-to-end control latency measurements are based with sensor timestamp to actuator command arrival and we are reporting P50, P95, and P99. At each tier throughput is measured in the number of messages per second and bytes per second. The tracking of reliability is achieved through packet loss, jitter, and availability of service. The blockchain metrics are the boundaries concerning the transaction latency, commit rate, and endorsement failures. Security effectiveness is given as the true-positive rates as well as false-positive rates and time-to-detect and percent of blocked attacks. The resource usage is gathered with cAdvisor/Prometheus; edge consumption is measured over USB power meter. TLS handshake overheads, chaincode execution, and SDN reconfiguration overheads are also logged as well.

Adversarial tests

We test resilience with TCP SYN floods and UDP floods in the 10 kpps 100 kpps range, by three attacker VMs, certificate-less enrollments and replay attacks, ARP-spoof-based MITM and TLS-downgrade probes, and injections of data that introduce slow drifts and burst spikes to sensor streams to tax the federated detector.

Baseline configuration

As a comparison, we apply the use of a centralized system absent SDN or blockchain. All analytics run in the cloud and routing is determined beforehand, only server-authenticated TLS is provided and anomaly detection is based on a single global model. Hardware and traffic profiles will be maintained constant in reference to the presented system.

Procedure and statistics

All scenarios are thirty minute long and carried out ten times each with a different random seed. Mean values accompanied by standard deviations and 95 % confidence intervals are reported and the Wilcoxon signed-rank test employed in the comparison of paired latencies. The interaction of two phases (cold-start and steady-state phases) is considered.

Reproducibility

Seed values, container digests, Fabric channel parameters, open daylight flow templates and orchestration scripts are version controlled. Clocks All nodes are configured to synchronize with chrony to have consistent timing among measurements.

Results and Discussion

The proposed architecture was compared with a like-for-like baseline in the case of centralized CPS (static routing, analytics and processing entirely on the cloud, no blockchain, no FL). Except where indicated, workloads, hardware and traffic profiles remained fixed in 10 repeat runs.

Latency. Mean control end-to-end latency improved in the proposal to a point of 48 ms (proposed) against 120 ms (baseline) or of 72 ms, or 60 percent. The savings are driven by (i) offloading inference and control to the edge (no cloud round-trips), (ii) SDN queueing and URLLC prioritisation to reduce queuing and reroute delays. As fast as 48 ms may be in the most ambitious realm of tight servo loops, it is still comfortably within AGV path update and supervisory control response envelope. Per-hop processing at the edge gateway and cryptographic framing are dominating residual latency and both can further be lowered through use of kernel-bypass I/O and TLS session resumption pinning.

Throughput. Efficient data-processing capability underwent an enhancement of 2.5 times. The feature extraction, inference is distributed among edge nodes in parallel microservices across K3s, whereas aggregation and linear-horizon analytics concentrate in the cloud. This eliminates the cloud as a source of bottleneck and eliminates back-pressure during bursty sensor periods. Notably, this gain remains when device count is increased five-fold between 50 and 500, due both to SDN load-balancing to smooth out hot links and because Kubernetes scales heavier service independently.

Security resilience. Simulated DoS and spoofing attempts were blocked or confined by the system in 95 percent of attempts. There are three reasons: (i) via blockchain-anchored device identities and smart-contract verification, unauthorized enrollment and replayed attestations are blocked; (ii) downgrade/MITM probes are thwarted due to TLS 1.3 using mutual authentication; and (iii) federated anomaly detection catches behavioral drifts and bursty manipulations, without revealing raw data, thus making it possible to coordinate without breaching privacy on edges.

Ablation perspective. The SDN elimination would eliminate the deterministic queueing and undermine the latency under cross-traffic; the edge inference removal would reinstate the cloud round-trip time and reduce the throughput; the blockchain inactivation would weaken the identity guarantees and enhance the successful spoofing rates. The layered cake is thus the requirement in order to get the collaborative security/scalability result.

Trade-offs and overheads. Security and orchestration bring costs that can be measured (and tolerated): TLS framing increases perimeter CPU utilization; blockchain block commits add out of band latency at the auditability cost but are not on the data path; containerization introduces low memory overhead per service. Theses penalties are overcome by the latency and throughput advantages created through locality and SDN control.

Scalability and Strength. Before and after a scale-out (50 □ 500 devices), the architecture keeps performance stable because of the autonomy of scaling individual microservices and using SDN-orchestrated resource distributions. Fast-failover combination limits rerouting time at links, making the control stable to perturbations.

Restrictions and optimisation in the future. Safety-critical actuation will demand NIC offload or DPDK, gRPC/QUIC at the edge and model distillation to reduce inference time to meet sub-20 ms loops. On the security front, supporting FL with adaptive attacks (e.g., model-poisoning attacks), and stricter RBAC by the use of more time-limited credentials, would make the system even more robust.

Conclusion and Future Work

This paper tackled both the challenge of securing and scalability of cyber-physical systems on automation in smart factories. We came up with a five-layer CPS framework which incorporates blockchain anchored device trust, TLS-1.3 secured communications, RBAC assumption, SDN orchestrated networking and edge- cloud stack layering with federated learning guaranteeing privacy protecting anomaly detection. The design was verified with a reproducible testbed of OPC UA/Modbus device emulation, K3s on Raspberry Pi edge nodes, OpenDaylight/OVS SDN, and Hyperledger Fabric under realistic workloads and with adversarial conditions. Vs. a centralized CPS baseline, the system improved end-to-end control latency directly by 120 ms to 48 ms (≈60 percent) and indirectly by 2.5X in effective throughput, through exploiting parallel edge computation, and by eliminating 95 percent of impersonations and DoS-like attacks in a simulated DoS/spoofing. Using ablation analysis, we settled on the fact that the gains are the result of the combined effects of edge locality (latency/throughput), SDN queueing, and failover (predictable performance) and blockchain-based identity with FL-driven detection (security resilience). Overheads added due to cryptography, containerization, and ledger commits were themselves not on the control path, and did not wipe out the gains.

The principal contributions are three-fold: (i) a unified, security-and-scalability CPS design that combines blockchain trust, SDN orchestration, and federated anomaly detection; (ii) a implementation reference, detailed configuration of high-fidelity, to allow replication and comparative evaluation; and (iii) quantitative results--under scalability and attack scenarios-- that demonstrates that layered defenses can work in the same environment as Industry 4.0 low-latency control.

These are, such as the fact that control loops of the most demanding actuation tasks are not yet sub- 20 ms, that FL may be susceptible to model-poisoning attacks, and that it is only evaluated on a one-site testbed. Future efforts will thus center on closed-loop what-if validation and faster commissioning through digital-twin integration; self-healing intent-based networking, where SDN telemetry and automated policy repair are coupled; and federated learning, which is poisoning-resilient and drift-aware; performance optimisations, via kernel-bypass I/O, QUIC/gRPC, and model distillation; formal verification of smart-contract RBAC policies; multi-site trials and multi-tenant experiments, in cross-domain trust; and a cost/energy analysis towards sustainable, at- Taken together, these directions seek to refine the architecture to a production-ready backbone of secure, adaptive smart manufacturing out of an approved prototype.

References

1. Bi, Z., Xu, L. D., & Wang, C. (2014). Internet of things for enterprise systems of modern manufacturing. *IEEE Transactions on Industrial Informatics, 10*(2), 1537–1546.
2. Dorri, A., Kanhere, S. S., & Jurdak, R. (2020). Blockchain in Internet of Things: Challenges and solutions. *IEEE Communications Surveys & Tutorials*, 22(3), 1654–1682.
3. 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.
4. Lee, J., Davari, H., Singh, J., & Pandhare, V. (2018). Industrial artificial intelligence for Industry 4.0-based manufacturing systems. *Manufacturing Letters, 18*, 20–23.
5. Li, T., Sahu, A. K., Zaheer, M., Sanjabi, M., Talwalkar, A., & Smith, V. (2020). Federated learning: Challenges, methods, and future directions. *IEEE Signal Processing Magazine, 37*(3), 50-60.
6. Lu, Y., Xu, C., Wang, H., & Zheng, L. (2019). Intelligent manufacturing systems in the context of Industry 4.0: A review. *Engineering, 5*(4), 616–630.
7. Sama, M. R., Ayoubi, S., & Shroff, N. B. (2019). Software-defined networking-based security for cyber-physical systems. *IEEE Communications Magazine, 57*(10), 20–25.
8. Yu, W., Liang, F., He, X., Hatcher, W. G., Lu, C., Lin, J., & Yang, X. (2018). A survey on the edge computing for the Internet of Things. *IEEE Access, 6*, 6900–6919.
9. Al-Yateem, N., Ismail, L., & Ahmad, M. (2024). A comprehensive analysis on semiconductor devices and circuits. Progress in Electronics and Communication Engineering, 2(1), 1-15. https://doi.org/10.31838/PECE/02.01.01
10. Carvalho, F. M., & Perscheid, T. (2025). Fault-tolerant embedded systems: Reliable operation in harsh environments approaches. SCCTS Journal of Embedded Systems Design and Applications, 2(2), 1-8.
11. Chia-Hui, C., Ching-Yu, S., Fen, S., & Ju, Y. (2025). Designing scalable IoT architectures for smart cities: Challenges and solutions. Journal of Wireless Sensor Networks and IoT, 2(1), 42-49.
12. Sadulla, S. (2024). State-of-the-art techniques in environmental monitoring and assessment. Innovative Reviews in Engineering and Science, 1(1), 25-29. https://doi.org/10.31838/INES/01.01.06
13. Choi, S.-J., Jang, D.-H., & Jeon, M.-J. (2025). Challenges and opportunities navigation in reconfigurable computing in smart grids. SCCTS Transactions on Reconfigurable Computing, 2(3), 8–17. https://doi.org/10.31838/RCC/02.03.02