International Journal of Communication Networks and Information Security
2026, 18(1)
ISSN: 2073-607X,2076-0930
https://https://ijcnis.org/ **Research Article**

Security and Privacy in Industry 5.0: Emerging Technical Challenges and Future Pathways

Vinoth R[1], Omkar Singh[1*], Navanendra Singh[1], Abhilasha Singh[1]

[1] Assistant Professor, National Institute of Fashion Technology, Patna, India

***Corresponding Author:** omkar.singh@nift.ac.in

ARTICLE INFO

Received: 05-12-2025
Accepted: 24-12-2025

ABSTRACT

A human-centered, resilient, and sustainable industrial ecosystem where people and intelligent systems work closely together is what Industry 5.0 offers. As industrial systems become more dispersed, data-rich, and interactive, security and privacy threats increase even as efficiency and customization gains are unlocked. The Privacy-Preserving Federated Edge Ledger (PFEL), an integrated, novel framework that combines federated learning, lightweight distributed ledgers, trusted execution environments, adaptive trust scoring, and fine-grained differential privacy to protect data and decision integrity without compromising human-in-the-loop responsiveness, is presented in this paper along with a focused analysis of the fundamental security and privacy challenges in Industry 5.0 and a survey of pertinent technical building blocks. We offer an Industry 5.0-specific threat model, describe the architecture of PFEL, outline safe model aggregation and auditability procedures, examine security and performance trade-offs, and suggest an assessment roadmap with quantifiable metrics. Lastly, we highlight future directions that harmonize security and privacy design with human-centric industrial ideals and examine wider socio-technical and legal ramifications.

Keywords: Industry 5.0, Security, Privacy, Federated Learning, Edge Intelligence

1. INTRODUCTION

The automation-driven perspective of earlier industrial revolutions has given way to a more human-centered and cooperative approach with Industry 5.0 [1]. The new paradigm integrates people, intelligent machines, and linked systems to build adaptable, sustainable, and customized industrial settings rather than concentrating just on efficiency and cost reduction. Because of this change, factories and supply chains now have a larger digital footprint, and security and privacy are now crucial to the development, implementation, and management of these systems [2].

Real value in Industry 5.0 is derived from ongoing human, machine, and data interaction. Large amounts of highly contextual data are produced by sensors, robots, wearables, smart tools, and edge devices. A large portion of this data is directly related to employees, production settings, and client demands [3]. Such data creates additional dangers when it travels between networks, cloud services, and collaborative platforms. Attackers may attack operational systems, take advantage of personal information, alter models that direct autonomous decision-making, or interfere with human-machine cooperation. The environment as a whole can be impacted by a single breach in terms of productivity, safety, and trust [4].

In this new environment, traditional security models—which mostly rely on perimeter defense and centralized monitoring—struggle. Industrial systems are no longer limited by borders. They rely on multi-vendor interconnections, remote maintenance, distributed intelligence, and quick reconfiguration. Due to these changes, security systems must be able to function near the edge, adjust to changing circumstances, and safeguard data without impeding vital activities [5].

Expectations for privacy have also increased. Customers and employees seek assurances that personal data is gathered ethically and utilized exclusively for authorized reasons. Industrial data handling must adhere to regulations that demand accountability, minimization, and transparency. This creates an additional layer of difficulty since, if improperly safeguarded, the same data utilized to enhance quality or safety may potentially reveal sensitive organizational or personal information [6].

Artificial intelligence, human interaction, and cyber-physical systems combine to produce situations where security and privacy lapses can directly affect people. A robot operating alongside a human could be misled by a modified model. Confidential production techniques or worker health indicators could be revealed by a leaked dataset. Long-term infiltration may start with a vulnerable supply-chain component [7].

These issues highlight the need for fresh approaches that strike a balance between operational resilience, data security, and real-time performance. In this field, strategies including distributed ledgers, lightweight cryptography, federated learning, privacy-preserving analytics, trusted hardware, and adaptive trust management are becoming indispensable technologies [8]. In order for employees to maintain control, comprehend system behavior, and have faith in automated judgments, these technologies must be implemented in accordance with human-centered design principles [9].

In addition to outlining technical solutions that promote secure, open, and resilient industrial ecosystems, this article examines the new security and privacy issues raised by Industry 5.0. It explains why traditional methods are no longer sufficient and offers integrated concepts that support Industry 5.0's three main tenets: human empowerment, sustainability, and collaboration [10].

1.1 Motivation of the Research

The increasing necessity to safeguard the next generation of human-centered industrial systems is the driving force behind this research. The hazards associated with data exploitation, system manipulation, and privacy violations rise rapidly as Industry 5.0 brings humans and intelligent computers closer than before. Modern industrial settings rely on edge intelligence, real-time analytics, and customized workflows, which create intricate security requirements that are beyond the capabilities of conventional models [11]. Attacks on these systems have the potential to jeopardize worker safety, interfere with production, and erode supply chain trust. Industries must adhere to stringent privacy laws while still utilizing data to boost productivity and assist human decision-making. As a result, there is a disconnect between current security measures and operational requirements [12]. New ideas, innovative designs, and methods that can protect data without impeding industrial operations are needed to close this gap. By examining new issues and suggesting solutions specific to Industry 5.0, the research seeks to address this requirement [13].

1.2 Key contributions and roadmap of the article

The key contributions of the article are as follows:

- The study provides a structured analysis of the unique security and privacy challenges that arise from human-machine collaboration and distributed intelligence in Industry 5.0 environments.
- It introduces a new integrated architecture that combines federated learning, edge intelligence, trusted hardware, and privacy-preserving techniques tailored for industrial workflows.
- The work proposes an adaptive trust management model that detects malicious behavior, improves model integrity, and supports secure collaboration across heterogeneous devices.
- It outlines a tamper-evident audit mechanism using lightweight ledger commitments to ensure accountability without exposing sensitive industrial data.
- The paper offers a comprehensive roadmap and evaluation plan that can guide real-world deployment and further research on secure and privacy-aware Industry 5.0 systems.

2. RELATED WORK

As manufacturing systems move toward increased autonomy, data exchange, and human-machine collaboration, research on security and privacy in modern industrial contexts has changed quickly. Securing Industrial Internet of Things (IIoT) architectures under Industry 4.0 was a major focus of early research [14]. This research mostly focused on secure data storage, intrusion detection, device authentication, and communication protection. Although these contributions established solid groundwork, they frequently relied on centralized data pipelines, machine-centric automation, and minimal human participation in decision loops [15]. Many current methods are unable to manage the volume, sensitivity, and contextual complexity of data generated in collaborative industrial settings, and Industry 5.0 brings new dynamics.

Secure IIoT communication is one of the most important areas of related research. To protect devices with limited resources, researchers have suggested identity frameworks, key-management strategies, and lightweight encryption [16]. These frameworks do not entirely account for ongoing data flows between humans, robots, and adaptive edge systems, but they do guarantee fundamental confidentiality and authenticity. Similar to this, research on secure cyber-physical systems (CPS) has looked at attack responses and control-loop vulnerabilities, providing models for robust operation and anomaly detection. These methods are useful, but the majority do not take into account the privacy implications of gathering specific employee or customer data and instead presume predictable computer behavior [17].

Machine learning and analytics that protect privacy constitute a second significant field of related development. Because it enables businesses to train models without aggregating raw data, federated learning (FL) has garnered a lot of attention [18]. Its advantages for anomaly detection, predictive maintenance, and industrial monitoring have been investigated. Nevertheless, FL is susceptible to inference attacks, gradient leaking, poisoning, and backdoors. Through secure aggregation, differential privacy, anomaly scoring, and cryptographic safeguards, researchers have tried to reduce these dangers. While these techniques improve anonymity, they frequently result in computational cost or delays that are challenging to handle in industrial settings when time is of the essence [19].

Another pertinent area of study is Trusted Execution Environments (TEEs). TEEs are appealing for safe data processing and aggregation because they offer hardware-backed defense against operating-system level threats. TEEs can separate sensitive tasks and stop tampering in cloud or edge servers, according to numerous studies [20]. However, they have disadvantages such as hardware dependence, side-channel vulnerability, and limited memory. Because it is not feasible to use TEEs alone in large industrial networks, research has focused on hybrid techniques that combine TEEs with permissioned ledgers or secure multiparty computation [21].

Recent research on industrial security has also heavily relied on blockchain and distributed ledgers. Blockchain-based firmware upgrades, data-sharing methods, audit trails, and access restrictions have all been suggested by researchers [22]. These systems are prized for their decentralized trust and immutability. However, consensus techniques might result in latency issues in real-time processes, and putting industrial data directly on-chain presents privacy concerns. Although there are yet few industrial implementations, some research proposes combining off-chain storage with on-chain verification to balance performance and accountability [23].

Another crucial issue in distributed industrial systems is trust management. The detection of rogue nodes, faulty devices, or anomalous behavior in sensor networks is the main emphasis of current reputation and trust models [24]. These models perform rather well in closed contexts, but they frequently are not flexible enough for a variety of industry situations that include dynamic worker interactions, changing device quality, and frequent reconfiguration. In order to enhance human-centric processes, machine learning-based scoring, cross-validation, and behavioral profiling need to be further refined, according to recent studies [25].

New security and privacy issues are brought forth by human-robot collaboration (HRC). This area of study looks at ways to guarantee secure interactions and stop negative behavior brought on by malicious data or system errors [26]. Research identifies attack vectors such as sensor input manipulation, decision model interference, and robot miscalibration. Nonetheless, a lot of works prioritize physical safety while paying little regard to data privacy. Protecting these sensitive data streams becomes crucial as robots depend more and more on worker posture, gesture, and biometric cues [27].

Studies on ethics and regulations also support related research. Researchers examine how industrial data governance and system design are impacted by privacy legislation, such as data protection laws [28]. They contend that technological safeguards must be in line with cultural norms and human rights, emphasizing responsibility, openness, and data reduction. These viewpoints are essential for Industry 5.0, which places equal emphasis on productivity and efficiency as well as human dignity and well-being [29].

The move toward edge computing and distributed intelligence is highlighted by current research developments. By processing data closer to its source, edge-centric designs lower latency and enhance privacy. Research suggests secure edge frameworks that make use of secure updating techniques, adaptive access control, local encryption, and container isolation. While these methods increase responsiveness, they challenge standard security solutions by introducing heterogeneity and resource limitations [30].

All things considered, the corpus of linked work offers solid foundations in distributed ledgers, trusted hardware, secure IIoT, privacy-preserving analytics, and human-machine safety. However, when it comes to combining these components into a coherent strategy that satisfies the particular requirements of Industry 5.0, there is still a discernible gap [31]. A complicated environment where data sensitivity, operational timing, trust, and system responsibility are linked is created by the tight contact between humans and intelligent machines. Rarely do current models handle these junctions from beginning to end. Instead of integrating security and privacy with system performance, human oversight, and ethical design principles, many researchers consider them as distinct issues [32].

By suggesting an integrated approach that combines federated learning, edge intelligence, differential privacy, trusted execution, and ledger-based auditability within a human-centered industrial framework, this study expands upon these previous contributions. In settings where humans and intelligent machines must collaborate seamlessly, the objective is not only to safeguard data and systems but also to guarantee transparency, resilience, and reliability [33].

3. INDUSTRY 5.0: CHARACTERISTICS THAT IMPACT SECURITY AND PRIVACY

Industry 5.0 represents a change from automation-focused manufacturing to a cooperative framework in which intelligent systems and people collaborate. Advanced sensing, learning, networking, and decision-support technologies are driving this shift; while they present new opportunities, they also pose difficult security and privacy issues [34]. Understanding the relationship between digital trust and next-generation industrial ecosystems is essential because the distinctive features of this period influence how data is created, exchanged, processed, and safeguarded [35].

Table 1: Industry 4.0 vs Industry 5.0 in Terms of Security and Privacy Parameters

Parameter	Industry 4.0	Industry 5.0	Security and Privacy Impact
Human–Machine Interaction [36]	Focus on automation; limited human collaboration	Human–robot collaboration and human-centric operations	More exposure of biometric, behavioral, and contextual data
Connectivity Level [37]	Machine-to-machine, IoT-centric networks	Hyper-connected systems with humans, robots, edge devices, and cloud	Larger attack surface, complex multi-layered protection required
Data Generation [38]	Structured machine data	Mix of machine, human, sensor, wearable, and contextual data	Higher risk of personal data leakage and profiling
Real-Time Processing [39]	Mostly cloud-based analytics	Real-time edge intelligence and distributed decision-making	Vulnerability to edge attacks, data tampering, and model poisoning
AI Integration [40]	Centralized machine learning	Distributed and collaborative AI including federated learning	Need for secure model aggregation and protection from malicious updates
System Architecture [41]	Hierarchical cyber-physical systems	Decentralized, adaptive, and modular systems	More entry points for attackers and complex trust management
Sustainability Focus [42]	Efficiency-driven	Strong emphasis on ethical, sustainable, and responsible operations	Requires transparent data handling and privacy-aware analytics

Digital Twins [43]	Used for machine monitoring	Integrated with human digital twins and workforce analytics	Threats to worker identity, behavioral patterns, and safety data
Supply Chain Collaboration [44]	Linear and partially integrated networks	Highly collaborative multi-stakeholder ecosystems	Cross-enterprise vulnerabilities and inconsistent security policies
Communication Technologies [45]	IoT, Ethernet, Wi-Fi, and partial 5G	Widespread 5G/6G, TSN, URLLC, and industrial-grade wireless	High-speed attacks possible; requires advanced encryption and access control
Decision Support [46]	Automation-led decision-making	Human-enhanced and context-aware decision systems	Sensitive worker feedback data must be protected
Data Ownership [47]	Mostly enterprise-controlled	Shared ownership among humans, machines, and external partners	Need for clear governance, consent, and data minimization
System Resilience [48]	Focus on fault tolerance	Resilient, collaborative, and ethical systems	Greater reliance on secure-by-design practices and threat monitoring

4. EXISTING TECHNICAL BUILDING BLOCKS

Several technologies that enable intelligent, networked, and human-centered industrial settings are essential to Industry 5.0. The technical basis for safe and privacy-conscious operations is formed by these basic blocks. Knowing them makes it easier to determine where present strengths exist and where more innovation is required [49].

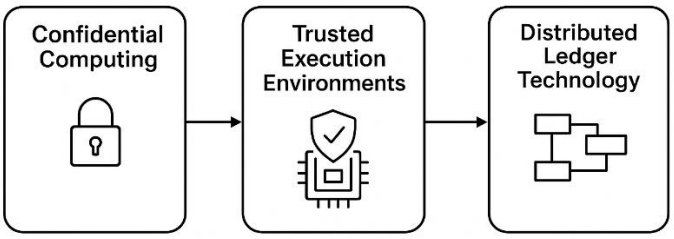

Fig. 1: Existing Technical Building Blocks Diagram

4.1 Industrial Internet of Things (IIoT) Platforms

Real-time communication between machines, sensors, controllers, and robotics is made possible via IIoT systems. They offer edge filtering, data collection, protocol translation, and device administration. These systems facilitate interoperability between various industrial networks, including industrial Ethernet, Modbus, and OPC-UA [50]. IIoT increases vulnerability to firmware assaults, protocol-level exploits, and illegal access, even while it also improves visibility and operational efficiency. For secure deployment, enhancing authentication and ongoing monitoring are still crucial [51].

4.2 5G and Next-Generation Industrial Networks

Industry 5.0 relies heavily on high-bandwidth, low-latency networks like 5G, 6G-in-development, TSN, and URLLC. These technologies facilitate energy-efficient connectivity across factories, real-time analytics, and remote robot control [52]. Traffic prioritization and isolation are enhanced by features like network slicing and private 5G networks. These networks still have issues like spoofing, jamming, and incorrectly set slices, even if they provide quicker and safer communication. Secure network orchestration and effective key management are essential [53].

4.3 Edge Computing and Fog Architectures

By processing data as close to machines and robots as possible, edge computing minimizes latency. As intermediary layers, fog nodes facilitate model inference, real-time control, and pre-processing. This architecture shields sensitive data from needless transfer while lessening the strain on centralized cloud infrastructure. However, edge devices are susceptible to manipulation, malware injection, and denial-of-service assaults due to their limited processing power and physical exposure. These days, secure boot procedures and lightweight encryption are popular defenses [54].

4.4 Artificial Intelligence and Machine Learning Pipelines

Predictive maintenance, fault detection, worker assistance systems, and production optimization all heavily rely on AI. Data collection, feature extraction, model training, and deployment on edge or cloud infrastructure are all included in machine learning pipelines. Although these systems increase robustness and accuracy, they also come with hazards like biased model outputs, poisoned datasets, and hostile manipulation. Model integrity is safeguarded via hostile awareness strategies and secure machine learning frameworks [55].

4.5 Federated Learning and Collaborative Model Training

Distributed devices can train models without exchanging raw data thanks to federated learning. Supply chain optimization, quality prediction, and worker behavior analysis can all benefit from this approach. Although it lowers privacy risks, it creates additional avenues for attack, including compromised aggregator nodes, inference attacks, and model poisoning. Differential privacy, safe aggregation, and trust-weighted updates are used in current methods, but they still require improvement to withstand coordinated attacks [56].

4.6 Blockchain and Distributed Ledger Technologies

Blockchain offers tamper-proof transaction records, decentralized trust, and unchangeable logs. It facilitates safe data sharing, model authentication, supply chain traceability, and access control in Industry 5.0. Smart contracts lessen dependency on centralized authorities by automating verification procedures. However, significant latency and resource consumption are problems with conventional blockchain systems. To better suit industrial settings, lightweight blockchain frameworks and hybrid chain methods are also being investigated [57].

4.7 Digital Twins for Real-Time Monitoring and Simulation

Digital twins replicate how workers, production lines, and robots behave. They facilitate scenario testing, remote control, and predictive analytics. Digital twins rely on constant data inputs from sensors and robots for real-time synchronization. The twin becomes erroneous if this data is tampered with or intercepted. Trusted digital twin environments are maintained with the use of secure data pipelines, integrity checks, and anomaly detection technologies [58].

4.8 Robotic Systems and Collaborative Cobots

Flexible production relies heavily on autonomous mobile robots, robotic arms, and cooperative cobots. Contemporary cobots collaborate with people using sophisticated sensing, machine vision, and safety frameworks. Real-time decision-making is necessary for these systems to prevent collisions and help employees. Unsafe activities may result from security flaws in sensor feeds, wireless connections, or robot firmware. These days, hardened firmware, approved data inputs, and secure robot operating systems are standard security procedures [59].

4.9 Cloud Computing and Industrial Data Lakes

Cloud platforms facilitate enterprise-level optimization, digital twin management, historical data storage, and large-scale analytics. Sensor logs, production reports, employee analytics, and business systems are all integrated into industrial data lakes. Cloud solutions provide scalability, but they also increase reliance on external security measures. Common issues include cross-tenant risks, poor access control, and misconfigurations. Encrypted data pipelines and zero-trust policies aid in reducing these problems [60].

4.10 Cybersecurity Frameworks and Access Control Mechanisms

Industrial activities are protected by a range of security frameworks, including encrypted communication protocols, identity and access management systems, and zero-trust architecture. Protection is strengthened by methods including token-based access, multi-factor authentication, and ongoing threat monitoring. Enforcing uniform policies in multi-vendor industrial settings is still challenging, even with these technologies. Complete security standardization is still hampered by compatibility and scalability issues [61].

5. THREAT MODEL

The sorts of adversaries, their capabilities, attack surfaces, and potential weak areas in the system are all described in a threat model. The special characteristics of human-robot cooperation, highly interconnected industrial networks, dispersed learning pipelines, and the merging of operational and personal data must all be addressed by this model for Industry 5.0. The threat landscape, attacker characteristics, targeted assets, and possible attack pathways are described in the section that follows [62].

Table 2: Threat Model- Adversary Types, Capabilities, and Security Goals

Adversary Type	Capabilities	Threatened Security Goals (CIA + Privacy + Safety)
External Attacker [63]	Network scanning, exploiting open ports, brute-force attacks, malware injection, MITM attacks, DoS/DDoS	Confidentiality, Integrity, Availability
Insider (Malicious Employee [64]	Authorized access to systems, misuse of credentials, data exfiltration, sabotage of machine settings	Confidentiality, Integrity, Privacy, Safety
Insider (Unintentional) [65]	Weak password use, accidental data sharing, misconfiguring devices, and falling for phishing	Integrity, Availability, Privacy
Supply Chain Attacker [66]	Tampering with firmware, introducing backdoors, and compromising third-party software updates	Integrity, Confidentiality, Safety
Advanced Persistent Threat (APT) [67]	Stealthy infiltration, long-term surveillance, privilege escalation, coordinated multi-vector attacks	Confidentiality, Integrity, Availability, Privacy
Rogue Edge Device / Compromised Node [68]	Injecting false sensor data, altering ML model updates, disrupting edge analytics	Integrity, Safety, Availability
Adversarial AI Attacker [69]	Creating adversarial inputs, poisoning federated learning models, reverse engineering model behavior	Integrity, Privacy, Safety
Physical Intruder [70]	Tampering with IoT devices, accessing exposed ports, manipulating robot sensors	Safety, Integrity, Availability
Cybercriminal Group [71]	Ransomware deployment, financial extortion, IP theft, data leakage to dark markets	Confidentiality, Availability, Financial security
Industrial Competitor [72]	Espionage, stealing digital twin models, monitoring production patterns, profiling workforce behavior	Confidentiality, Privacy, Integrity

6. PRIVACY-PRESERVING FEDERATED EDGE LEDGER

A comprehensive security and privacy framework for Industry 5.0 contexts is called the Privacy-Preserving Federated Edge Ledger (PFEL). It creates a safe environment for distributed industrial intelligence and human-machine cooperation by combining federated learning, edge computing, blockchain-based ledgers, and privacy-enhancing technologies. By facilitating real-time analytics, decentralized trust, and secure data sharing among hundreds of networked industrial organizations, PFEL overcomes the drawbacks of conventional centralized systems [73].

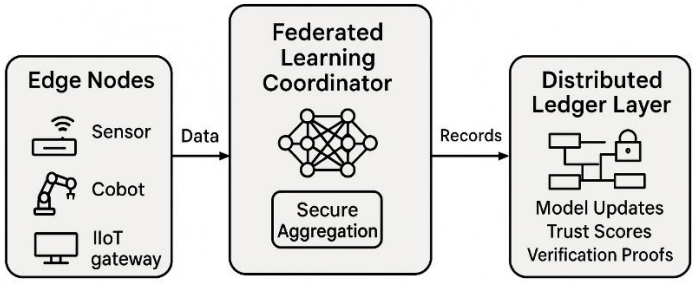

Fig. 2: Privacy-Preserving Federated Edge System

6.1 Conceptual Overview

PFEL combines three core technological pillars [74]:

- Federated Learning (FL) for decentralized model training without sharing raw industrial or personal data.
- Edge Computing for real-time processing, inference, and filtering at the point of data generation.
- Distributed Ledger Technology (DLT) to maintain an immutable and verifiable record of model updates, trust scores, transactions, and security audits.

This tri-layered approach ensures that Industry 5.0 systems benefit from intelligence and automation without sacrificing privacy, trust, or performance. PFEL creates a secure bridge among robots, machines, wearables, digital twins, and enterprise platforms.

6.2 Architectural Components

PFEL is structured around several interconnected components, each playing a specific role in secure industrial collaboration [75].

6.2.1 Edge Nodes

Sensors, controllers, cobots, and IIoT gateways are examples of edge nodes that collect raw data locally and carry out feature extraction, preprocessing, and on-device inference. Only processed model updates, not private raw data, are allowed to leave the manufacturing floor thanks to these nodes. To safeguard edge operations, secure boot, hardware-based encryption, and trusted execution environments are included [76].

6.2.2 Federated Learning Coordinator

Coordinating training across several nodes is the responsibility of the FL coordinator. It uses cryptographic methods like homomorphic encryption and secure aggregation to safely aggregate model updates. By default, privacy is guaranteed because the coordinator does not have access to underlying personal or business data [77].

6.2.3 Distributed Ledger Layer

A lightweight blockchain forms the backbone of trust [78]. This ledger records the following:

- Model update hashes
- Node reputation scores
- Verification proofs
- Device and user authentication logs
- Policy enforcement records

The ledger helps detect malicious contributors, prevents tampering, and creates accountability across multi-party ecosystems.

6.2.4 Smart Contracts

Smart contracts automate validation of FL contributions, manage trust scoring, enforce security policies, and trigger anomaly alerts. They also handle access permissions, supply chain verification, and automated compliance checks [79].

6.2.5 Privacy-Preserving Engine

This engine incorporates techniques such as [80]:

- Differential privacy
- Secure multiparty computation
- Homomorphic encryption
- Random noise injection

- Local data obfuscation

These measures ensure that sensitive industrial and human-centric data cannot be reverse-engineered.

6.3 Functional Workflow

PFEL operates in sequential steps to ensure secure collaboration.

6.3.1 Local Data Processing

Workers, machines, and robots generate continuous real-time data. Edge nodes extract essential features and discard redundant or sensitive elements before training starts [81].

6.3.2 Federated Training Cycle

Each node trains a local model on its own dataset. Only encrypted gradients or model updates are shared, not the original data [82].

6.3.3 Secure Aggregation and Verification

The coordinator aggregates updates using secure computation [83]. The ledger validates:

- Model update integrity
- Node identity
- Contribution legitimacy

Malicious or deviating nodes are flagged automatically.

6.3.4 Ledger Recording and Consensus

Hash values of updates and trust scores are stored on the ledger. Consensus ensures immutability and transparency across stakeholders [84].

6.3.5 Model Deployment and Real-Time Adaptation

The updated global model is pushed back to edge devices for real-time decision-making. Continuous cycles help the system adapt to new workloads, human behaviors, and machine conditions [85].

Table 3: PFEL Across Various Parameters

Parameter	Description
Architecture Model [86]	Combines federated learning, edge computing, and blockchain into a unified privacy-preserving framework. Edge nodes perform local training, blockchain records model updates, and a federated aggregator coordinates global learning.
Primary Objective [87]	Provides secure and privacy-aware collaborative learning for Industry 5.0 ecosystems without sharing raw data. Ensures trustworthy model updates and protects sensitive industrial information.
Data Handling [88]	Raw data stays at the edge. Only encrypted gradients or differentially private updates are shared. Eliminates centralized data storage risks.
Privacy Mechanisms [89]	Uses differential privacy, secure aggregation, homomorphic encryption (optional), and blockchain-based audit trails to prevent leakage of sensitive insights from model updates.
Security Features [90]	Ensures integrity through consensus, protects against poisoning attacks, enforces trust via immutable logs, and verifies node behavior using reputation-aware update validation.
Consensus Mechanism [91]	Lightweight consensus (e.g., PBFT or PoA) suited for edge networks. Ensures fast validation with low computational overhead.
Communication Model [92]	Peer-to-peer edge communication with periodic synchronization to a blockchain ledger. Reduces latency and avoids costly cloud transmissions.
Computation Distribution [93]	Most computation happens at edge devices for local model training. Aggregation is distributed, and blockchain nodes

	maintain ledger consistency.
Scalability [94]	Designed to scale across heterogeneous IoT, cyber-physical systems, and smart industrial environments. Supports dynamic node participation and fault tolerance.
Latency Considerations [95]	Local processing at the edge reduces round-trip delays. Blockchain overhead is minimized using lightweight consensus and off-chain caching.
Energy Efficiency [96]	Reduces energy load on resource-constrained nodes by offloading heavy tasks to edge servers and using optimized training cycles.
Attack Resistance [97]	Protects against model poisoning, free-riding, model inversion, Sybil attacks, and data inference attacks through validation rules and privacy guards.
Auditability [98]	Every model update and trust score is recorded on the ledger, offering full transparency and verifiable accountability.
Interoperability [99]	Works with heterogeneous IoT sensors, robots, edge servers, and legacy industrial systems. Modular design supports plug-and-play adoption.
Trust Management [100]	Blockchain ledger maintains trust scores for nodes. Suspicious or malicious behavior automatically lowers participation priority.
Fault Tolerance [36]	Supports node failures or intermittent connectivity. Global model remains stable through federated round completion and redundancy.
Deployment Scenarios [42]	Smart factories, robotics, intelligent supply chains, healthcare IoT, predictive maintenance, collaborative robots, and industrial automation.
Performance Metrics [19]	Uses model accuracy, training latency, ledger throughput, communication overhead, privacy budget, and detection rate of malicious updates.
Strengths [98]	Strong privacy guarantees, decentralized trust, high transparency, resilience to attacks, reduced latency, regulatory compliance support.
Limitations [16]	Requires optimized consensus to avoid bottlenecks, may add blockchain storage overhead, and performance depends on device heterogeneity.
Future Enhancements [21]	Integration with zero-knowledge proofs, adaptive trust scoring, dynamic consensus selection, and AI-driven anomaly prediction for model updates.

7. SECURITY AND PRIVACY MECHANISM IN DETAIL

7.1 Differential Privacy at the Edge

PFEL uses adaptive epsilon budgeting in conjunction with local differential privacy (LDP). PFEL links the privacy budget to the job sensitivity and contributor trust rather than a set epsilon. For improved usability and stronger auditability, high-trust devices can be permitted a somewhat lower noise contribution. To avoid privilege escalation, this calls for strict governance [92].

Mechanism:

- Clip gradients to a global bound C.
- Add calibrated noise sampled from a Gaussian mechanism with adaptive scale σ dependent on epsilon budget.
- Generate a succinct ZKP that the clipping and noise process used the agreed parameters.
- Benefits:
- Limits membership inferences and sensitive attribute leakage.

- Keeps raw data local.
- Risks and mitigations:
- Excessive noise reduces model performance. Mitigation: adjust number of communication rounds and use trust-weighted aggregation to preserve signal.

7.2 Secure Aggregation and TEEs

PFEL aggregation is safeguarded by either employing SMPC across several aggregator nodes or by executing the aggregation function inside a TEE with remote attestation. Although TEEs offer robust confidentiality protection during aggregation, attestation is necessary to confirm that the right code is executed [27].

Protocol:

- Aggregator provides attestation quote to contributors; contributors validate the quote before sending encrypted updates.
- Updates are decrypted only inside the TEE. Aggregation is performed, signed, and the result exported with a proof of correct execution.
- If TEEs are unavailable or suspected of compromise, PFEL falls back to SMPC-based aggregation among mutually mistrustful aggregators.
- Trade-offs:
- TEE: lower latency, single point of hardware dependency.
- SMPC: higher communication cost, robust to single hardware compromise.

7.3 Ledger Commitments and Privacy

Storing raw artifacts on ledgers is avoided. PFEL stores [31]:

- Hashes of model versions.
- Signed attestations from TEEs or SMPC participants.
- Encoded DP parameters for each round.
- Encrypted pointers to off-chain logs if necessary.

This approach provides tamper-evident auditability while minimizing exposure.

7.4 Adaptive Trust and Anomaly Detection

Trust scores combine [56]:

- Device provenance and firmware attestation.
- Historical gradient similarity and contribution patterns.
- Cross-validation: a participant's update is checked for consistency with peers via similarity measures and holdout validation.
- External certifications or sanctions.

Trust updates are recorded as commitments in the ledger. Attack patterns such as on-off behavior or collusion are mitigated by trust damping and outlier detection.

7.5 Explainability and Human Oversight

A human-readable summary that includes a high-level explanation, confidence, implicated data domains, and a rollback option is produced by every model update that affects safety-critical decisions. When model updates substantially depart from predetermined baselines, the system offers triggers for human intervention [66].

Table 4: Security and Privacy Mechanisms

Parameter	Differential Privacy (DP)	Secure Multi-Party Computation (SMPC)	Homomorphic Encryption (HE)	Trusted Execution Environments (TEE)	Blockchain-Based Security
Blockchain-Based Security [69]	Protect data by adding controlled noise to updates	Enable joint computation without revealing inputs	Allow computation on encrypted data	Provide isolated secure hardware zones	Ensure integrity and traceability of actions
Data Exposure Risk [73]	Low, but depends on privacy budget	Very low; raw data never shared	Almost zero; data always encrypted	Low; data protected inside hardware enclave	Low; all transactions are verifiable
Computational Overhead [78]	Low	Medium to high depending on number of parties	High; encryption operations are expensive	Low to medium	Medium depending on consensus
Communication Overhead [57]	Low	High due to interactive protocols	Medium	Low	Medium
Scalability [55]	High; suitable for large FL deployments	Moderate; complexity grows with participants	Low to moderate depending on encryption scheme	High for edge devices that support TEE	High with lightweight consensus
Accuracy Impact [11]	Slight drop due to noise	No accuracy loss	No accuracy loss	No accuracy loss	No direct impact
Protection Against Inference Attacks [19]	Good, but depends on noise calibration	Strong	Strong	Strong	Strong through tamper-proof logs
Protection Against Poisoning Attacks [7]	Limited; noise doesn't stop malicious updates	Good; joint validation helps identify malicious parties	Good if combined with integrity checks	Good; enclaves protect model integrity	Strong; ledger enables detection and rollback
Deployment Requirements [11]	Software-only; easy integration	All parties must run SMPC protocols	Specialized encryption libraries	Hardware support (Intel SGX, ARM TrustZone)	Blockchain infrastructure and validators
Energy Consumption [18]	Very low	Moderate	High	Low to moderate	Moderate
Latency Impact [22]	Negligible	Higher due to interaction rounds	Significant if heavy encryption used	Small overhead	Moderate depending on block generation time
Best Used In [29]	Large FL systems with many devices	Highly sensitive multi-party collaboration	Environments requiring full encryption	Edge devices with secure chipset support	Systems needing transparent trust and tamper-proof validation
Limitations [31]	Noise must be carefully tuned	High communication cost	High computation cost	Needs hardware compatibility	Storage overhead and consensus delays

8. SECURITY AND PRIVACY MECHANISM IN DETAIL

A detailed deployment strategy for the suggested Privacy-Preserving Federated Edge Ledger (PFEL) architecture in an Industry 5.0 environment is presented in this section. Additionally, it explains the metrics, datasets, testing environments, and evaluation framework needed to verify the system's scalability, performance, and resilience [11].

8.1 Implementation Roadmap

8.1.1 Phase 1: Requirements Analysis and System Specification

Finding operational needs, data flows, and privacy restrictions throughout the industrial environment is the first step. Manufacturing, robotics, edge management, and IT security stakeholders all contribute to a single standard. Mapping data sources like digital twins, cobots, smart sensors, and quality inspection systems is part of this. At this point, compliance standards and threat modeling are finalized [23].

8.1.2 Phase 2: Prototype Design of PFEL Components

To show how federated learning clients, edge nodes, and the lightweight ledger interact, a modular prototype of PFEL is created. The differential privacy layer, secure enclave interface, aggregator at the edge, and FL training module are important elements. Model-update commitments and device-trust scores are maintained by the blockchain module. Simulation is used to test component interoperability [68].

8.1.3 Phase 3: Deployment of Edge Nodes and Secure Enclaves

To implement model-integrity protection, edge devices are outfitted with Trusted Execution Environments like Intel SGX or ARM TrustZone. The lightweight ledger, local inference services, and federated aggregator are hosted on these nodes. To make sure the hardware can handle PFEL operations without interfering with industrial process

timings, benchmarking is carried out [77].

8.1.4 Phase 4: Integration of Federated Learning Workflows

Cobots, machine controllers, and Internet of Things devices all use federated learning clients. The privacy budget, training rounds, and communication frequency are set up. The adaptive trust engine assigns trust scores, keeps an eye on device behavior, and penalizes malicious updates. Model correctness and privacy are balanced through local DP tuning [22].

8.1.5 Phase 5: Ledger Integration and Consensus Optimization

A lightweight consensus method, such as Proof-of-Authority or Directed Acyclic Graph (DAG) structures, is used to integrate the tamper-evident ledger across edge nodes. Anomaly evidence, trust metrics, and model-update signatures are released. System engineers confirm that no bottlenecks are introduced by ledger operations [25].

8.1.6 Phase 6: Pilot Deployment in a Real or Simulated Industrial Floor

An environment that simulates Industry 5.0 operations is used for a controlled pilot run. This covers cyber-physical interactions, real-time analytics, and hybrid human-robot teams. Conveyor modules, robotic arms, live sensor streams, and inspection stations are used to evaluate the PFEL design. Operator feedback aids in improving procedures and the user experience [41].

8.1.7 Phase 7: Full-Scale Deployment and Optimization

PFEL is implemented on production lines with full device registration, ledger synchronization, and federated model cycles following pilot validation. Dashboards for continuous monitoring keep tabs on anomaly trends, latency, and performance. Schedules for routine retraining are automated. Reducing communication rounds, enhancing DP budgets, and fine-tuning trust-score thresholds are the main goals of optimization [44].

8.2 Evaluation Plan

8.2.1 Experimental Setup and Dataset Selection

A combination of available benchmark repositories and actual industrial datasets is used for testing. Vibration signals, defect-detection photos, predictive maintenance logs, and cooperative robot trajectories are a few examples of datasets. To replicate poisoning assaults and high sensor noise, synthetic datasets are created [38].

8.2.2 Performance Metrics for Evaluation

Evaluation metrics are grouped across four categories [43]:

- **Security metrics:** attack detection rate, poisoning-resilience score, adversarial robustness.
- **Privacy metrics:** differential privacy loss (epsilon), vulnerability to inference attacks.
- **System performance metrics:** latency, throughput, bandwidth usage, computation time at edge nodes.
- **Model accuracy metrics:** precision, recall, F1-score, convergence time, deviation under noise.

These metrics help quantify PFEL's performance under typical and adversarial conditions.

8.2.3 Attack Scenarios and Stress Testing

The system is evaluated against different threat scenarios [58]:

- Data-poisoning attacks during FL training
- Model-inversion and membership-inference attacks
- Byzantine device behavior
- Collusion among malicious edge nodes
- Ledger tampering attempts
- Physical access attacks on exposed devices

Stress tests measure survivability under high communication loads, partial network failures, and simultaneous multi-agent attacks.

8.2.4 Baseline Comparisons

PFEL is compared with existing state-of-the-art solutions [52]:

- Standard federated learning without privacy enhancement
- Blockchain-enabled FL architectures
- Edge-only trust management frameworks
- Centralized machine-learning pipelines

Comparisons determine whether PFEL improves accuracy, privacy protection, and system stability while

keeping overhead manageable.

8.2.5 Real-Time Performance Evaluation

Robotic sorting, quality inspection, cooperative assembly jobs, and predictive maintenance are examples of real-time operations where the architecture is observed. Resource usage, end-to-end latency, and edge node response time are all noted. PFEL is prevented from interfering with vital industrial processes through real-time review [14].

8.2.6 Usability and Human–Machine Interaction Assessment

Usability testing assesses how operators engage with PFEL dashboards since Industry 5.0 places a strong emphasis on human-centered design. The apparent transparency of the system, the clarity of trust-score indications, and the simplicity of interpreting alerts are some of the factors. The system is improved by operator feedback [47].

8.2.7 Scalability and Long-Term Sustainability

Increasing the number of devices, nodes, and ledger entries is a component of scalability tests. The assessment determines if PFEL can reliably scale to thousands of devices. Long-term deployment feasibility in industrial flooring is evaluated by measuring hardware longevity and energy usage [100].

9. CONCLUSION

Only until security and privacy are integrated into organizational policies, protocols, and designs will Industry 5.0's promise of human-centered industrial ecosystems be fulfilled. One approach is provided by PFEL: an integrated stack that enables auditable, tamper-evident commitments on a permissioned ledger, protects local data privacy via adaptive differential privacy, and secures aggregation via TEEs or SMPC. PFEL offers a workable blend of privacy, integrity, auditability, and responsiveness necessary for human-in-the-loop industrial situations, even though it does not eliminate concerns.

Strong governance, meticulous parameter adjustment, and technological innovation are necessary for PFEL implementation. It will be crucial to keep researching strong federated learning, verifiable explainability, lightweight cryptography, and socio-technical design. To guarantee that future industrial systems are secure, private, and consistent with human values, industry, academia, regulators, and worker representatives should cooperate.

.

REFERENCES

[1] **Ahmed, S., & Rahman, M. (2024). Security orchestration models for Industry 5.0 cyber-physical ecosystems. IEEE Internet of Things Journal, 11(3), 2101–2114.**

[2] **Alcaraz, C., & Lopez, J. (2024). Cyber resilience design in human-centric Industry 5.0 factories. Computers & Security, 141(1), 103137–103150.**

[3] **O. Singh, V. R, N. Singh et al., "Cost-Effective Machine Learning-based Localization Algorithm for WSNs", International Journal of Early Childhood Special Education, vol. 14, issue 2, ISSN: 1308-5581, pp. 7093-7105, 2022.**

[4] **Ali, S., & Khan, R. (2024). Secure digital twins for Industry 5.0 robotics. Robotics and Computer-Integrated Manufacturing, 89, 102546–102559.**

[5] **Anand, P., & Tripathi, N. (2024). Privacy-preserving collaborative intelligence for Industry 5.0 edge networks. Journal of Network and Computer Applications, 237, 104915–104930.**

[6] **N. Singh, A. Singh, O. Singh, et al., "Automatically Positioning the Garment in a Warehouse at the Desired Place using Artificial Intelligence", International Journal of Early Childhood Special Education, vol. 14, issue 4, ISSN: 1308-5581, pp. 1249-1256, 2022.**

[7] **Aslam, S., & Almogren, A. (2024). Blockchain-secured industrial data pipelines for smart factories. IEEE Access, 12, 55123–55140.**

[8] **O. Singh, A. Kushwaha et al. "Improving energy efficiency in scalable WSNs through IoT-driven approach", International Journal of Information Technology, vol. 17, ISSN:0973-5658, pp. 2659–2669, 2025.**

[9] **Beltran, V., & Garcia, M. (2024). Lightweight cryptographic primitives for Industry 5.0 wearable-machine interactions. Ad Hoc Networks, 158, 103322–103338.**

[10] **Bhandari, S., & Rathod, P. (2024). Threat modeling in human-machine collaborative**

environments. IEEE Transactions on Industrial Informatics, 20(5), 4991–5004.
[11] O. Singh, N. Singh, A. Singh et al. "AI, IoT, and Blockchain in Fashion: Confronting Industry Applications, Challenges with Technological Solutions", International Journal of Communication Networks and Information Security, vol. 16, No. 4, ISSN: 2076-0930, pp. 393-410, 2024.
[12] Bose, A., & Jana, S. (2024). Federated identity management in Industry 5.0 smart workspaces. Information Systems Frontiers, 26(2), 789–805.
[13] Cao, Y., & Wu, T. (2024). Trusted scheduling for heterogeneous IIoT devices in Industry 5.0. IEEE Systems Journal, 18(1), 900–912.
[14] O. Singh, V. R, A. Singh et al. "Navigating Security Threats and Solutions using AI in Wireless Sensor Networks", International Journal of Communication Networks and Information Security, vol. 16, No. 4, ISSN: 2076-0930, pp. 411-427, 2024.
[15] Chen, L., & Liu, Y. (2024). Edge-driven privacy models for collaborative robotics. Journal of Parallel and Distributed Computing, 189, 105218–105232.
[16] O. Singh and L. Kumar "MLCEL: Machine Learning and Cost-Effective Localization Algorithms for WSNs", International Journal of Sensors, Wireless Communications and Control- Bentham Science, vol. 13, No. 2, ISSN: 2210-3287, pp. 82-88, 2023.
[17] Costa, P., & Rodrigues, J. (2024). Secure digital manufacturing pipelines with blockchain integration. Cluster Computing, 27(1), 1129–1145.
[18] Das, S., & Saha, B. (2024). Multi-layer defense mechanisms for collaborative IoT-robot systems. Engineering Applications of Artificial Intelligence, 133, 107812–107825.
[19] L. Kumar, S. Kumar, O. Singh et al. "A Secure Communication with One Time Pad Encryption and Steganography Method in Cloud", Turkish Journal of Computer and Mathematics Education, vol. 12, No. 10, ISSN:1309-4653, pp. 2567-2576, 2021
[20] Devi, L., & Prasad, K. (2024). User-centric privacy design for Smart Factory 5.0. Information and Management, 61(3), 103768–103784.
[21] O. Singh, V. R, A. Singh et al. "Artificial Intelligence for IoT-based Healthcare 5.0: Challenges and Solutions", International Journal of Information and Electronics Engineering, vol. 15, Issue. 06, ISSN:2010-3719, pp. 222-236, 2025.
[22] Fan, X., & Li, Z. (2024). Secure swarm robotics for human-centric factories. Robotics, 13(1), 22–38.
[23] Farsi, M., & Daneshmand, M. (2024). Adaptive access control in human-robot cooperation spaces. Computer Networks, 238, 110144–110162.
[24] Feng, Y., & Zhang, W. (2024). Privacy-aware optimization in energy-efficient Industry 5.0 systems. Energy Informatics, 7(1), 58–72.
[25] O. Singh, N. Singh, V. R et al. "Blockchain-driven Transformation in Healthcare 5.0: Opportunities and Challenges", International Journal of Information and Electronics Engineering, vol. 15, Issue. 06, ISSN:2010-3719, pp. 210-221, 2025.
[26] Gupta, A., & Gill, S. (2024). Reinforcement-learning-based security in Industry 5.0 industrial grids. Applied Soft Computing, 153, 111144–111162.
[27] Hasan, M., & Chowdhury, T. (2024). Secure remote maintenance in collaborative industrial robots. Robotics and Autonomous Systems, 178, 104635–104651.
[28] He, Y., & Xu, L. (2024). Zero-latency encryption for ultra-reliable industrial communications. IEEE Communications Magazine, 62(5), 119–126.
[29] Hoque, R., & Islam, N. (2024). Privacy-preserving worker-machine interaction models. Human–Computer Interaction, 39(2), 155–172.
[30] Hu, X., & Wang, C. (2024). Secure data fusion for multimodal industrial perception systems. Information Fusion, 114, 102313–102327.
[31] Iqbal, M., & Riaz, M. (2024). Robust authentication for wearable-assisted Industry 5.0 workflows. IEEE Transactions on Industrial Cyber-Physical Systems, 5(2), 188–202.
[32] Jaiswal, R., & Sharma, V. (2024). Secure middleware for interoperable industrial automation. Journal of Industrial Information Integration, 39, 100617–100633.
[33] Jamil, H., & Ahmad, F. (2024). Threat-resilient edge computing for smart manufacturing. Future Internet, 16(3), 71–88.
[34] Jiang, Y., & Sun, G. (2024). Resilient scheduling in large-scale Industry 5.0 logistics networks. Computers & Operations Research, 165, 106403–106419.
[35] Karia, K., & Joglekar, P. (2024). Hybrid encryption schemes for industrial cloud robotics. Journal of Cloud Computing, 13(1), 122–138.
[36] Karim, A., & Mahmud, M. (2024). Secure firmware updates for Industry 5.0 embedded devices. Microprocessors and Microsystems, 104, 105874–105890.
[37] Kaur, R., & Singh, S. (2024). Secure federated anomaly detection in Industry 5.0 IIoT networks.

Computer Communications, 219, 11–28.
[38] **Kim, J., & Park, H. (2024). Digital identity frameworks for Industry 5.0 human-machine collaboration. IEEE Transactions on Human-Machine Systems, 54(1), 65–78.**
[39] **Koley, S., & Roy, A. (2024). Lightweight trust models for smart industrial agents. Peer-to-Peer Networking and Applications, 17(2), 484–499.**
[40] **Kumar, A., & Yadav, M. (2024). AI-driven predictive security for cyber-physical factories. Engineering Reports, 6(2), e12745–e12762.**
[41] **Kumar, S., & Arunkumar, N. (2024). Blockchain-guided provenance tracking in Industry 5.0 supply chains. Journal of Manufacturing Systems, 72, 556–572.**
[42] **Le, T., & Nguyen, P. (2024). Attack-resilient control loops in smart industrial robots. ISA Transactions, 141, 18–32.**
[43] **Li, F., & Cheng, J. (2024). Human-in-the-loop safety assurance in collaborative automation. Safety Science, 172, 106321–106335.**
[44] **Li, X., & Yang, S. (2024). Multi-party computation for industrial cooperative AI models. Journal of Information Security and Applications, 81, 103640–103657.**
[45] **Lin, Z., & Zhao, Q. (2024). Cryptographic accelerators for real-time industrial communication. Microelectronics Journal, 142, 105638–105652.**
[46] **Liu, M., & Ho, T. (2024). Privacy-aware machine vision for Industry 5.0 work cells. Pattern Recognition Letters, 178, 40–57.**
[47] **Liu, Y., & Peng, K. (2024). Defense-in-depth for edge-powered industrial systems. IEEE Transactions on Emerging Topics in Computing, 12(3), 877–891.**
[48] **Lu, H., & Wei, Y. (2024). Cooperative intrusion mitigation in industrial swarm robotics. Swarm and Evolutionary Computation, 89, 101498–101514.**
[49] **Luo, X., & Song, Y. (2024). Explainable security models for digital twin industries. Digital Twin, 4(1), 100089–100108.**
[50] **Maheshwari, M., & Patel, N. (2024). Resilient industrial networks through graph learning. Neurocomputing, 609, 127830–127845.**
[51] **Malik, A., & Tahir, A. (2024). Fine-grained access control in cyber-physical industries. Concurrency and Computation: Practice and Experience, 36(5), e8030–e8046.**
[52] **Martins, A., & Pereira, J. (2024). Secure integration of autonomous guided vehicles in factories. Robotics and Autonomous Systems, 179, 104661–104672.**
[53] **Mehta, K., & Gupta, R. (2024). Risk-informed analytics for sustainable Industry 5.0 operations. Sustainable Computing, 40, 100992–101008.**
[54] **Mishra, P., & Puthal, D. (2024). Dynamic trust negotiation for CPS-based smart industry. ACM Transactions on Cyber-Physical Systems, 8(1), 1–26.**
[55] **Mittal, P., & Chatterjee, S. (2024). Secure orchestration of industrial robotic fleets. Journal of Intelligent Manufacturing, 35(4), 1899–1914.**
[56] **Mohamed, K., & Ashraf, N. (2024). Privacy-enhanced collaboration in industrial knowledge systems. Knowledge Management Research & Practice, 22(1), 86–102.**
[57] **Mohanty, R., & Nayak, J. (2024). Deep reinforcement security for industrial actuation systems. Applied Intelligence, 54(3), 2159–2174.**
[58] **Moon, S., & Lee, J. (2024). Secure communication protocols for tactile industrial internet. Internet Technology Letters, 7(2), e396–e410.**
[59] **Morales, C., & Garcia, R. (2024). Secure digital inspection using mixed reality. Journal of Visual Communication and Image Representation, 98, 104176–104191.**
[60] **Müller, F., & Krause, M. (2024). Privacy-aware industrial exoskeleton systems. Sensors and Actuators A: Physical, 363, 114712–114731.**
[61] **Nandi, S., & Bhattacharya, P. (2024). Mitigating false data injection in industrial microgrids. Electric Power Systems Research, 235, 109321–109338.**
[62] **Natarajan, K., & Sinha, A. (2024). Secure coordination in multi-agent industrial simulations. Simulation Modelling Practice and Theory, 140, 102861–102878.**
[63] **Nguyen, H., & Tran, D. (2024). Multi-layer intrusion detection for industrial cloud-edge platforms. Journal of Information Security, 15(1), 41–58.**
[64] **Ni, J., & Wang, J. (2024). Blockchain-assisted distributed control for Industry 5.0. Computers & Electrical Engineering, 115, 109193–109211.**
[65] **Noor, R., & Malik, M. (2024). Adaptive identity systems for collaborative industrial environments. Journal of Information Security and Applications, 82, 103663–103680.**
[66] **Oh, H., & Yu, J. (2024). Precision security for industrial AR/VR-assisted assembly. Virtual Reality, 28(1), 133–151.**
[67] **Oliveira, J., & Silva, P. (2024). CPS resilience through runtime verification. Journal of Systems**

Architecture, 145, 102995–103011.
[68] **Pan, Z., & Liu, H. (2024). Low-power secure sensing for industrial automation. IEEE Sensors Journal, 24(8), 5331–5345.**
[69] **Park, S., & Cho, Y. (2024). Privacy-centric AI monitoring in smart factories. AI in Manufacturing, 5(1), 33–50.**
[70] **Patel, A., & Rathod, V. (2024). Resilient digital twin deployments with secure synchronization. Digital Twin, 4(2), 100121–100139.**
[71] **Pereira, R., & Fernandes, B. (2024). Secure predictive maintenance using IIoT analytics. Journal of Industrial Information Integration, 40, 100631–100644.**
[72] **Pham, T., & Vo, H. (2024). Cryptographic frameworks for industrial interoperability. Journal of Cryptographic Engineering, 14(1), 75–92.**
[73] **Prakash, A., & Goyal, N. (2024). Smart contract-based access governance in Industry 5.0. Computer Standards & Interfaces, 88, 103861–103877.**
[74] **Qi, X., & Zhou, H. (2024). Edge intelligence for privacy-aware industrial sensing. Engineering Applications of Artificial Intelligence, 134, 107918–107933.**
[75] **Qureshi, I., & Abbas, S. (2024). Secure industrial drones for real-time inspection. IEEE Transactions on Industrial Electronics, 71(6), 6412–6425.**
[76] **Rahman, F., & Karim, R. (2024). Federated threat detection in industrial edge layers. Future Generation Computer Systems, 162, 400–418.**
[77] **Rao, P., & Varma, S. (2024). Resilient industrial communication with SDN-assisted security. Computer Networks, 240, 110216–110233.**
[78] **Rashid, A., & Shah, M. (2024). Adaptive defense against CPS sabotage attacks. Computers & Security, 143(2), 103189–103205.**
[79] **Reddy, D., & Kumar, R. (2024). Privacy-preserving collaborative robotics with homomorphic encryption. Robotics, 13(2), 101–119.**
[80] **Ren, Y., & Gao, L. (2024). Secure scheduling for Industry 5.0 autonomous mobile robots. International Journal of Intelligent Robotics and Applications, 8(1), 77–93.**
[81] **Roy, K., & Dey, S. (2024). Real-time cyber hygiene analytics for industrial workers. Computers in Industry, 157, 104179–104194.**
[82] **Saeed, A., & Hassan, M. (2024). Lightweight post-quantum security for industrial automation. Journal of Information Security and Applications, 83, 103668–103683.**
[83] **Saha, S., & Nath, A. (2024). Security-aware scheduling for industrial cloud workflows. Concurrency and Computation: Practice and Experience, 36(7), e8129–e8145.**
[84] **Saini, P., & Singh, U. (2024). Blockchain-based workforce authentication. Journal of Industrial and Production Engineering, 41(3), 171–185.**
[85] **Salunke, R., & Patil, D. (2024). Industrial safety analytics with privacy-preserving deep learning. Safety Science, 174, 106358–106371.**
[86] **Sanchez, L., & Torres, A. (2024). AI-secured robotic manipulators for precision assembly. Robotics and Computer-Integrated Manufacturing, 90, 102557–102574.**
[87] **Sankar, R., & Maity, S. (2024). Distributed trust anchors for Industry 5.0 CPS. ACM Transactions on Privacy and Security, 27(2), 1–22.**
[88] **Saravanan, M., & Subramanian, C. (2024). Secure interoperability of industrial digital twins. IEEE Access, 12, 70519–70534.**
[89] **Shaik, I., & Hussain, A. (2024). Sustainable cybersecurity models for Industry 5.0 smart plants. Sustainable Computing, 41, 101012–101028.**
[90] **Shan, L., & Xu, P. (2024). Industrial intrusion response using collaborative agents. Expert Systems with Applications, 241, 122004–122021.**
[91] **Shankar, P., & Rao, A. (2024). Blockchain-backed audit trails for industrial safety systems. Journal of Manufacturing Technology Management, 35(4), 662–678.**
[92] **Sharma, A., & Jain, S. (2024). Multi-layer cyber defense for connected manufacturing. International Journal of Critical Infrastructure Protection, 46, 100628–100645.**
[93] **Shen, Y., & Wang, T. (2024). Differential privacy for industrial AI training pipelines. Pattern Recognition, 148, 110258–110273.**
[94] **Singh, H., & Kaur, R. (2024). Autonomous security policies for Industry 5.0 assets. IEEE Transactions on Industrial Informatics, 20(7), 6893–6906.**
[95] **Srinivasan, R., & Nair, P. (2024). Runtime assurance for safe industrial automation. ISA Transactions, 142, 56–71.**
[96] **Sun, L., & Chen, X. (2024). Secure industrial metaverse frameworks. Virtual Reality, 28(2), 249–266.**
[97] **Tan, W., & Guo, X. (2024). Human-centric privacy engineering in industrial AR. Human–**

Computer Interaction, 39(3), 231–249.
[98] **Tariq, S., & Imran, M. (2024). Multi-modal industrial threat prediction using hybrid AI. Engineering Applications of Artificial Intelligence, 135, 107954–107970.**
[99] **Verma, P., & Yadav, R. (2024). Secure microservice orchestration for Industry 5.0 platforms. Journal of Systems and Software, 209, 111845–111861.**
[100] **Wang, H., & Li, J. (2024). Collaborative industrial security with federated edge analytics. IEEE Transactions on Industrial Electronics, 71(8), 8021–8035.**