(10) Publication No: **IN202641064749 A1**
(22) Date of Filing: 22-05-2026
(43) Publication Date: 05-06-2026
Journal No: 23/2026

(19) Intellectual Property Office, India

(12) INDIAN PATENT APPLICATION

(54) Title: **Adaptive federated machine learning system for real-time anomaly detection and threat mitigation in industrial iot networks**

(51) International Classification:
H04L 29/06, G06N 3/04, G06N 3/08, H04L 9/40 H04L 12/24

(21) Application No: **202641064749**

(31) Priority Document No: --

(32) Priority Date: --

(86) International Application No: --
Filing Date: --

(87) International Publication No: --

(61) Patent of Addition to Application No: --
Filing Date: --

(62) Divisional to Application No: --
Filing Date: --

(71) Name of Applicant(s):
1. Dr. S. Prabu,
2. Mr. Ponnarasu Kulanthaisamy,
3. Ms. R. Deepa,
4. Dr. S. Aruna,
5. Ms. Rubasri Rajendran,
6. Ms. Jissin Kurian,
7. Ms. Shyma Kareem,
8. Ms. Teena M. Thomas,
9. Dr. R. Dinesh Kumar,
10. Mr. P. Navaraja,

(72) Name of Inventor(s):
1. Dr. S. Prabu
2. Mr. Ponnarasu Kulanthaisamy
3. Ms. R. Deepa
4. Dr. S. Aruna
5. Ms. Rubasri Rajendran
6. Ms. Jissin Kurian
7. Ms. Shyma Kareem
8. Ms. Teena M. Thomas
9. Dr. R. Dinesh Kumar
10. Mr. P. Navaraja

(57) Abstract:

[061] The present invention discloses an adaptive federated machine learning system and method for real-time anomaly detection and autonomous threat mitigation in Industrial Internet of Things (IIoT) networks. The invention comprises industrial devices, edge intelligence nodes, federated learning coordinators, hybrid anomaly detection engines, protocol-aware inspection modules, contextual risk assessment mechanisms, and autonomous mitigation components configured to monitor and secure industrial communication infrastructures. The system acquires industrial operational data including communication traffic, sensor telemetry, process variables, device logs, and command sequences, and performs preprocessing, feature extraction, and behavioral profiling for intelligent anomaly analysis. The anomaly detection engine utilizes recurrent neural networks, long short-term memory networks, autoencoders, graph neural networks, clustering algorithms, and statistical analysis models to identify cyber threats, abnormal operational patterns, unauthorized activities, and protocol manipulation attacks in real time. The federated learning architecture enables decentralized collaborative model training without transferring raw industrial data, thereby preserving operational confidentiality and reducing centralized dependency. The contextual risk assessment engine dynamically evaluates anomaly severity using device criticality, operational dependencies, communication topology, and

historical threat behavior, while the autonomous mitigation module performs adaptive response actions including device isolation, traffic filtering, firewall policy enforcement, communication rerouting, and alert generation. The invention further incorporates adaptive self-learning mechanisms for continuous optimization of anomaly detection accuracy and cybersecurity resilience across heterogeneous industrial environments including manufacturing systems, smart grids, transportation infrastructures, and automated industrial facilities. Accompanied Drawing [FIGS. 1-2]

FORM 2

THE PATENTS ACT, 1970

(39 of 1970)

&

The Patent Rules, 2003

COMPLETE SPECIFICATION

(See section 10 and rule 13)

TITLE OF THE INVENTION

"ADAPTIVE FEDERATED MACHINE LEARNING SYSTEM FOR REAL-TIME ANOMALY DETECTION AND THREAT MITIGATION IN INDUSTRIAL IOT NETWORKS"

Applicant(s)

NAME	NATIONALITY	ADDRESS
1. Dr. S. Prabu	Indian	Professor, Department of Electronics and Communication Engineering, Mahendra Institute of Technology, Namakkal, Tamil Nadu, India
2. Mr. Ponnarasu Kulanthaisamy	Indian	Solutions Architect – Data Analytics, Independent Researcher, Namakkal, Tamil Nadu, India
3. Ms. R. Deepa	Indian	Assistant Professor, Department of Computer Science and Engineering, Vels Institute of Science, Technology and Advanced Studies, Chennai, Tamil Nadu, India
4. Dr. S. Aruna	Indian	Department of Computational Intelligence, School of Computing, SRM Institute of Science and

		Technology, Kattankulathur, Tamil Nadu, India
5. Ms. Rubasri Rajendran	Indian	Solutions Architect / Project Manager, Independent Researcher, Namakkal, Tamil Nadu, India
6. Ms. Jissin Kurian	Indian	Assistant Professor, Department of Computer Science and Engineering, St. Thomas College of Engineering and Technology (Autonomous), Chengannur, Alappuzha, Kerala, India
7. Ms. Shyma Kareem	Indian	Associate Professor, Department of Computer Science and Engineering, St. Thomas College of Engineering and Technology (Autonomous), Chengannur, Alappuzha, Kerala, India
8. Ms. Teena M. Thomas	Indian	Assistant Professor, Department of Computer Science and Engineering, St. Thomas College of Engineering and Technology (Autonomous), Chengannur, Alappuzha, Kerala, India
9. Dr. R. Dinesh Kumar	Indian	Professor, DMI College of Engineering, Palanchur, Chennai – 600123, Tamil Nadu, India
10. Mr. P. Navaraja	Indian	Assistant Professor, Department of Electronics and Communication Engineering, Mahendra Institute of Technology, Namakkal, Tamil Nadu, India

The following specification particularly describes the nature of the invention and the manner in which it is performed:

FIELD OF THE INVENTION

[001] The present invention generally relates to the field of Industrial Internet of Things (IIoT) security, intelligent industrial automation, and machine learning-based cyber-physical system protection. More particularly, the invention pertains to an adaptive federated machine learning system and method for real-time anomaly detection, behavioral analysis, and autonomous threat mitigation in Industrial IoT communication networks. The disclosed invention integrates distributed edge intelligence, federated learning architectures, deep learning algorithms, protocol-aware traffic inspection, contextual risk assessment, and self-learning cybersecurity mechanisms to identify abnormal operational patterns, unauthorized access attempts, malicious communication behavior, device failures, and cyberattacks within heterogeneous industrial infrastructures. The invention further relates to decentralized industrial security frameworks capable of preserving data privacy while enabling scalable, low-latency, and intelligent monitoring of industrial devices, sensors, programmable controllers, robotic systems, and supervisory control environments across manufacturing plants, smart grids, transportation systems, energy facilities, and other critical industrial applications.

BACKGROUND OF THE INVENTION

[002] Industrial Internet of Things (IIoT) infrastructures have rapidly evolved in recent years due to the increasing adoption of smart manufacturing technologies, industrial automation systems, cloud-integrated control platforms, and intelligent monitoring solutions across multiple industrial sectors. Modern industrial facilities rely extensively on interconnected sensors, programmable controllers, robotic systems, actuators, supervisory control and data acquisition (SCADA) systems, and machine-to-machine

communication networks to improve operational efficiency, predictive maintenance, process optimization, and resource utilization. The integration of these interconnected industrial devices has significantly enhanced production capabilities while simultaneously introducing complex cybersecurity and operational reliability challenges.

[003] Conventional industrial control systems were originally designed as isolated operational environments with limited external connectivity. However, the growing convergence between operational technology (OT) networks and information technology (IT) infrastructures has exposed industrial systems to external communication channels, cloud services, remote management platforms, and internet-based applications. This increased connectivity has created numerous attack surfaces vulnerable to cyber threats, malware infections, unauthorized access attempts, denial-of-service attacks, insider manipulation, protocol exploitation, and advanced persistent threats targeting critical industrial infrastructure.

[004] Existing security mechanisms deployed in industrial environments primarily rely on rule-based intrusion detection systems, static firewall configurations, and signature-based threat detection approaches. Such conventional methods are limited in their capability to detect previously unknown attacks, zero-day vulnerabilities, adaptive malware, and abnormal behavioral deviations occurring within industrial communication networks. Signature-based systems require continuous manual updates and are ineffective against sophisticated attackers capable of modifying attack signatures or exploiting legitimate industrial communication patterns to bypass detection mechanisms.

[005] Industrial IoT environments generate massive volumes of heterogeneous data streams including sensor readings, operational telemetry, communication packets, process variables, device logs, authentication records, and actuator commands. Traditional monitoring systems often struggle to process and analyze such high-dimensional real-time data efficiently. Centralized security architectures introduce substantial latency, bandwidth consumption, and computational bottlenecks, thereby limiting the ability to perform rapid anomaly detection and immediate threat response in time-sensitive industrial operations.

[006] Another major challenge associated with existing industrial anomaly detection systems is the high occurrence of false positive and false negative alerts. Industrial environments exhibit highly dynamic operational behaviors influenced by process variations, production schedules, equipment maintenance, environmental conditions, and fluctuating workloads. Conventional threshold-based monitoring systems frequently misclassify legitimate operational changes as cyber threats, leading to unnecessary interruptions, alarm fatigue among operators, and reduced trust in automated security solutions. Simultaneously, subtle malicious activities may remain undetected due to inadequate contextual understanding of industrial processes.

[007] Machine learning and artificial intelligence technologies have recently emerged as promising approaches for enhancing anomaly detection capabilities in industrial networks. However, many existing machine learning-based systems rely heavily on centralized training architectures requiring large-scale aggregation of sensitive industrial data into cloud servers or centralized data centers. Such centralized approaches raise concerns regarding industrial data privacy, confidentiality of

proprietary manufacturing information, regulatory compliance, and vulnerability to centralized system failures or cyberattacks targeting stored operational datasets.

[008] Furthermore, industrial communication networks utilize diverse communication standards and protocols including Modbus, OPC-UA, MQTT, EtherCAT, DNP3, CAN bus, and proprietary industrial protocols. Existing cybersecurity systems often lack protocol-aware intelligence required to accurately interpret industrial command structures, process relationships, timing dependencies, and device interaction patterns. As a result, malicious protocol manipulations and subtle operational anomalies may bypass conventional network inspection mechanisms without detection.

[009] Edge computing technologies have introduced opportunities for localized processing and real-time analytics within industrial infrastructures. Nevertheless, current edge-based monitoring solutions frequently suffer from limited adaptability, insufficient collaborative learning capabilities, restricted scalability, and inability to continuously evolve against emerging cyber threats. Many systems also fail to coordinate intelligence effectively across distributed industrial sites, thereby preventing collective learning from geographically separated operational environments.

[010] Additionally, existing industrial security solutions generally focus only on anomaly identification without incorporating autonomous threat mitigation and adaptive response capabilities. In critical industrial environments, delayed human intervention may result in operational downtime, equipment damage, safety hazards, production losses, environmental risks, and compromise of mission-critical infrastructure. There remains a substantial need for intelligent systems capable of

automatically isolating compromised devices, restricting suspicious communications, enforcing dynamic security policies, and preserving operational continuity during cyber incidents.

[011] Therefore, there exists a need for an advanced, decentralized, adaptive, and intelligent anomaly detection framework capable of continuously monitoring Industrial IoT environments in real time while preserving data privacy, minimizing computational overhead, reducing false alarms, and enabling autonomous threat mitigation. Such a system should integrate machine learning, federated intelligence, edge computing, protocol-aware behavioral analysis, and self-learning cybersecurity mechanisms to provide scalable and resilient protection for modern industrial infrastructures against evolving cyber-physical threats and operational anomalies.

SUMMARY OF THE INVENTION

[012] The present invention discloses an adaptive federated machine learning system and method for real-time anomaly detection and autonomous threat mitigation in Industrial Internet of Things (IIoT) networks. The invention is designed to provide intelligent cybersecurity protection for interconnected industrial infrastructures by continuously monitoring industrial communication traffic, operational telemetry, sensor data, machine behavior, process variables, and device interaction patterns. The system integrates distributed edge computing, federated learning architectures, deep learning-based anomaly analysis, protocol-aware traffic inspection, contextual threat evaluation, and self-learning optimization mechanisms to detect and mitigate cyber-physical anomalies with high accuracy and low latency.

[013] In one embodiment, the invention comprises a plurality of industrial devices including sensors, actuators, programmable logic controllers, robotic systems, industrial gateways, supervisory control systems, and edge intelligence nodes interconnected through heterogeneous industrial communication protocols. The edge intelligence nodes are configured to collect operational data locally and perform preliminary data preprocessing, feature extraction, behavioral profiling, and anomaly inference without requiring centralized processing of raw industrial information. This distributed architecture minimizes network congestion, reduces latency, and enables rapid detection of abnormal activities within time-sensitive industrial environments.

[014] In another embodiment, the invention incorporates a federated learning framework configured to enable collaborative model training across geographically distributed industrial facilities while preserving data privacy and operational confidentiality. Each industrial edge node independently trains local machine learning models using site-specific operational data and periodically transmits encrypted model parameters or gradient updates to a federated learning coordinator. The federated coordinator aggregates the received model updates using adaptive optimization algorithms to generate a globally optimized anomaly detection model, which is subsequently redistributed to participating edge nodes for continuous refinement and synchronization.

[015] The invention further comprises a hybrid anomaly detection engine utilizing multiple machine learning methodologies including recurrent neural networks, convolutional neural networks, graph neural networks, autoencoders, clustering algorithms, and statistical behavioral analysis techniques. The recurrent neural networks analyze temporal communication sequences and process dependencies,

while autoencoder models identify deviations from learned normal operational behavior using reconstruction errors. Graph neural networks model inter-device relationships and communication topologies to identify suspicious interactions, compromised nodes, and abnormal network structures. Ensemble decision-making algorithms combine outputs from multiple detection modules to improve anomaly detection accuracy and reduce false alarm generation.

[016] In another embodiment, the system includes a protocol-aware inspection module configured to analyze industrial communication standards including Modbus, OPC-UA, MQTT, DNP3, EtherCAT, CAN bus, and other industrial protocols. The protocol inspection module interprets packet structures, command sequences, timing characteristics, device states, and communication dependencies to identify unauthorized commands, protocol misuse, data injection attacks, replay attacks, and malicious manipulation of industrial control instructions. The protocol-aware analysis enhances the system’s capability to detect subtle cyber threats that may evade conventional network security mechanisms.

[017] The invention also comprises a contextual risk assessment engine configured to dynamically evaluate the severity of detected anomalies based on industrial process criticality, device importance, network topology, operational dependencies, historical threat patterns, environmental conditions, and user privilege levels. The contextual analysis module generates adaptive threat scores that classify anomalies into multiple severity categories including informational, low-risk, medium-risk, high-risk, and critical-risk conditions. The risk assessment engine continuously updates threat evaluation parameters according to evolving operational behaviors and environmental changes within industrial facilities.

[018] In a further embodiment, the invention incorporates an autonomous threat mitigation engine configured to execute adaptive response actions upon detection of malicious or abnormal activities. The mitigation engine performs automated device isolation, communication blocking, bandwidth throttling, session termination, firewall rule generation, credential revocation, traffic rerouting, backup controller activation, and alert transmission to industrial operators or supervisory systems. The autonomous mitigation mechanisms enable rapid containment of cyber threats while minimizing operational disruptions and maintaining industrial process continuity.

[019] The invention additionally includes a continuous feedback and self-learning optimization mechanism configured to improve anomaly detection accuracy over time. Incident responses, operator feedback, false positive corrections, environmental variations, and newly observed attack patterns are incorporated into incremental retraining procedures to refine model parameters, anomaly thresholds, behavioral baselines, and response strategies. This adaptive learning capability enables the system to evolve dynamically according to changing industrial workflows and emerging cybersecurity threats.

[020] In another embodiment, the invention supports scalable deployment across diverse industrial sectors including manufacturing facilities, smart grids, oil and gas infrastructures, autonomous transportation systems, chemical processing plants, healthcare automation systems, pharmaceutical production facilities, and smart warehousing environments. The decentralized architecture enables interoperability with existing industrial infrastructure while supporting high availability, fault tolerance, low computational overhead, and resilient cybersecurity protection for large-scale Industrial IoT ecosystems.

[021] Accordingly, the present invention provides a comprehensive and intelligent Industrial IoT anomaly detection framework capable of delivering decentralized cybersecurity monitoring, privacy-preserving federated learning, adaptive behavioral analysis, protocol-aware threat detection, autonomous mitigation, and continuous self-learning optimization. The invention overcomes the limitations of conventional industrial security systems by enabling scalable, real-time, and resilient protection against evolving cyber-physical threats and operational anomalies within heterogeneous industrial environments.

BRIEF DESCRIPTION OF THE DRAWINGS

[022] The accompanying drawings are incorporated herein and form an integral part of the present disclosure illustrating exemplary embodiments of the adaptive federated machine learning system for real-time anomaly detection and autonomous threat mitigation in Industrial Internet of Things (IIoT) networks. The drawings are intended to provide a further understanding of the invention and illustrate the architecture, operational workflow, data processing mechanisms, federated learning coordination, anomaly analysis modules, and automated mitigation processes associated with the disclosed system. The illustrated embodiments are exemplary in nature and should not be construed as limiting the scope of the invention.

[023] FIG. 1 illustrates the overall system architecture of the adaptive federated machine learning-based anomaly detection framework comprising Industrial IoT devices, industrial sensors, programmable logic controllers, edge intelligence gateways, federated learning coordinators, cloud orchestration servers, protocol-aware inspection modules, contextual risk assessment engines, anomaly detection

modules, and autonomous threat mitigation components interconnected through secure industrial communication networks.

[024] FIG. 2 illustrates the operational workflow and processing sequence of the anomaly detection and autonomous response mechanism including industrial data acquisition, preprocessing, feature extraction, local machine learning inference, federated model synchronization, protocol-aware traffic analysis, anomaly scoring, contextual threat classification, automated mitigation execution, feedback collection, and adaptive self-learning optimization for continuous cybersecurity enhancement within Industrial IoT infrastructures.

DETAILED DESCRIPTION OF THE INVENTION

[025] The following detailed description is provided to enable a thorough understanding of the present invention and illustrates various exemplary embodiments of an adaptive federated machine learning system for real-time anomaly detection and autonomous threat mitigation in Industrial Internet of Things (IIoT) networks. The description sets forth specific system architectures, operational modules, data processing techniques, machine learning mechanisms, communication infrastructures, and security methodologies for implementing the disclosed invention. However, it shall be understood that the invention is not limited to the illustrated embodiments and may be implemented in various modifications, configurations, and equivalent arrangements without departing from the scope of the invention.

System Architecture and Network Environment

[026] Referring to FIG. 1, the disclosed system comprises a distributed Industrial IoT security architecture including a plurality of industrial devices, edge intelligence nodes, communication gateways, federated learning coordinators, cloud orchestration

servers, anomaly detection engines, contextual risk analysis modules, and autonomous mitigation components interconnected through industrial communication networks. The industrial devices include sensors, actuators, robotic systems, programmable logic controllers (PLCs), human-machine interfaces (HMIs), surveillance systems, autonomous machinery, industrial cameras, and supervisory control systems deployed across industrial facilities.

[027] The industrial devices communicate using multiple industrial communication protocols including Modbus, OPC-UA, MQTT, EtherCAT, CAN bus, DNP3, Profinet, and other proprietary industrial protocols. The communication infrastructure may include wired Ethernet networks, industrial wireless networks, 5G-enabled industrial gateways, fiber-optic communication systems, and cloud-integrated industrial platforms configured for real-time operational monitoring and automation.

[028] Each industrial zone is associated with one or more edge intelligence nodes configured to perform localized cybersecurity monitoring, data preprocessing, anomaly inference, protocol analysis, and behavioral profiling. The edge intelligence nodes may comprise industrial gateways, embedded computing systems, edge servers, programmable controllers, or dedicated cybersecurity appliances positioned within industrial operational environments.

Data Acquisition and Preprocessing Module

[029] The invention incorporates a data acquisition module configured to continuously collect operational telemetry from industrial devices and communication infrastructures. The collected data includes sensor readings, process variables, communication packets, device authentication logs, firmware events, command

sequences, actuator responses, system health information, voltage levels, temperature measurements, production parameters, and user access activities.

[030] The acquired industrial data undergoes preprocessing operations to improve data quality and optimize machine learning performance. The preprocessing module performs timestamp synchronization, missing value handling, noise filtering, signal normalization, packet decoding, protocol parsing, data compression, and anomaly-aware feature standardization. Time-series data streams are segmented into operational windows for sequential behavioral analysis.

[031] The preprocessing engine additionally generates metadata attributes including communication frequency, packet entropy, session duration, command repetition rate, process transition states, access timing behavior, and device interaction patterns. The extracted information is transformed into structured feature vectors suitable for subsequent machine learning analysis and anomaly detection procedures.

Feature Extraction and Behavioral Profiling

[032] The system further includes a feature engineering module configured to derive multidimensional behavioral characteristics from industrial communication traffic and operational telemetry. The feature extraction engine identifies spatial, temporal, statistical, and protocol-aware attributes associated with industrial device behavior.

[033] The extracted features include packet transmission intervals, payload distribution characteristics, process execution sequences, communication latency patterns, sensor fluctuation trends, machine vibration signatures, energy consumption profiles, operational throughput measurements, and command-response relationships between industrial devices. The feature extraction module further identifies abnormal deviations from established operational baselines.

[034] A behavioral profiling engine continuously constructs adaptive profiles for each industrial device, operator account, communication channel, and process workflow. The profiles are dynamically updated according to evolving operational conditions, manufacturing schedules, maintenance activities, environmental variations, and network usage patterns to improve anomaly detection accuracy.

Hybrid Machine Learning-Based Anomaly Detection Engine

[035] The anomaly detection engine comprises a hybrid machine learning architecture integrating supervised learning, unsupervised learning, semi-supervised learning, and deep learning methodologies for identifying abnormal activities within Industrial IoT networks.

[036] In one embodiment, recurrent neural networks (RNNs) and long short-term memory (LSTM) networks are utilized for analyzing sequential communication patterns, operational dependencies, and temporal process behaviors. These models detect deviations in command sequences, communication timing, and operational workflows indicative of potential cyber threats or process abnormalities.

[037] The system additionally employs autoencoder-based anomaly detection mechanisms configured to learn compressed representations of normal industrial behavior. Reconstruction errors generated by the autoencoder models are analyzed to identify anomalous operational conditions, unauthorized communications, equipment malfunctions, and abnormal network activities.

[038] Graph neural networks (GNNs) are implemented to model communication relationships among industrial devices and network entities. The graph-based analysis identifies abnormal topological structures, unauthorized communication paths, lateral

movement attacks, compromised nodes, and suspicious interaction patterns within industrial communication infrastructures.

[039] Clustering algorithms including density-based spatial clustering (DBSCAN), adaptive K-means clustering, and hierarchical clustering are utilized to identify communication outliers, abnormal operational groups, and hidden anomaly patterns across industrial environments. Statistical correlation models further evaluate deviations between process variables, sensor relationships, and expected operational thresholds.

[040] The outputs generated by multiple anomaly detection models are combined through an ensemble intelligence engine configured to calculate unified anomaly confidence scores. Weighted aggregation and adaptive decision fusion techniques improve anomaly detection precision while minimizing false positive and false negative classifications.

Federated Learning Coordination Framework

[041] The present invention incorporates a federated learning architecture configured to enable decentralized collaborative training of anomaly detection models without centralized sharing of raw industrial data. Each edge intelligence node independently trains local machine learning models using site-specific industrial operational data stored within local environments.

[042] After local training iterations are completed, encrypted model parameters, gradients, or optimization vectors are transmitted to a federated learning coordinator through secure communication channels employing encryption, authentication, and integrity verification protocols. The federated learning coordinator aggregates the

received updates using adaptive weighted averaging algorithms and generates globally optimized machine learning models.

[043] The optimized global models are redistributed to participating edge intelligence nodes for incremental refinement and continuous synchronization. This decentralized training mechanism preserves industrial data confidentiality, reduces communication overhead, minimizes centralized dependency, and enhances scalability across geographically distributed industrial facilities.

Protocol-Aware Industrial Traffic Inspection

[044] The invention further includes a protocol-aware inspection module configured to analyze industrial communication protocols and detect protocol-specific cyber threats and operational anomalies. The protocol inspection engine interprets industrial packet structures, command fields, response patterns, timing dependencies, control instructions, and process-specific communication behaviors.

[045] The protocol-aware analysis mechanism identifies unauthorized command injections, replay attacks, malformed packets, protocol misuse, suspicious payload modifications, timing anomalies, and abnormal communication frequencies associated with malicious industrial activities. The system further evaluates protocol compliance and operational consistency between interconnected industrial devices.

[046] The inspection module supports both deep packet inspection and lightweight edge-based protocol monitoring depending upon computational resource availability and industrial operational requirements. The protocol-aware intelligence improves detection capabilities for sophisticated cyber threats targeting industrial control infrastructures.

Contextual Risk Assessment and Threat Scoring

[047] The invention incorporates a contextual risk assessment engine configured to dynamically evaluate detected anomalies according to operational severity and industrial process impact. The contextual analysis module considers multiple parameters including device criticality, operational dependency graphs, production sensitivity, network topology, user privilege levels, environmental conditions, and historical threat patterns.

[048] Each anomaly detected by the machine learning engine is assigned a dynamic threat score representing the probability and severity of malicious activity. The threat scoring mechanism classifies anomalies into multiple severity categories including informational, low-risk, medium-risk, high-risk, and critical-risk conditions.

[049] The contextual risk engine further correlates anomalies occurring across multiple industrial devices and communication channels to identify coordinated attacks, multi-stage intrusions, insider threats, and cascading operational failures. Adaptive threshold mechanisms continuously adjust scoring parameters according to operational changes and evolving industrial conditions.

Autonomous Threat Mitigation and Response Mechanism

[050] Upon detection of high-confidence anomalies or critical threat conditions, the autonomous mitigation engine initiates predefined and adaptive cybersecurity response actions to contain malicious activities and preserve operational continuity.

[051] The mitigation engine performs automated isolation of compromised devices from industrial communication networks, dynamic firewall rule enforcement, suspicious traffic filtering, bandwidth throttling, communication rerouting, session termination, account locking, access revocation, and backup controller activation. Alert

notifications are simultaneously transmitted to industrial operators, security administrators, and supervisory control systems.

[052] The response strategies are prioritized according to anomaly severity, industrial process criticality, safety constraints, and operational dependencies to minimize production interruptions and prevent large-scale industrial failures. The mitigation engine further supports manual override controls allowing authorized operators to validate or modify automated response actions when necessary.

Self-Learning Optimization and Adaptive Intelligence

[053] The present invention additionally incorporates a continuous self-learning optimization framework configured to improve anomaly detection performance over time. The feedback engine collects operator responses, incident resolution outcomes, false positive corrections, operational changes, environmental variations, and newly identified attack patterns for incremental retraining of machine learning models.

[054] The adaptive intelligence engine dynamically updates anomaly thresholds, behavioral baselines, protocol inspection rules, threat scoring parameters, and mitigation strategies according to changing industrial workflows and cybersecurity conditions. The self-learning mechanism enables continuous evolution of the anomaly detection framework against emerging threats and previously unseen attack techniques.

Industrial Applications and Deployment Scenarios

[055] The disclosed invention may be deployed across diverse industrial sectors including manufacturing plants, smart grids, oil and gas refineries, transportation infrastructures, water treatment facilities, chemical processing systems, autonomous

warehouses, pharmaceutical production environments, healthcare automation facilities, and smart energy distribution networks.

[056] The scalable decentralized architecture enables seamless integration with existing industrial infrastructures while supporting cloud-edge collaboration, low-latency cybersecurity analytics, high fault tolerance, and resilient industrial operations. The invention thereby provides comprehensive protection against cyber-physical attacks, operational anomalies, insider threats, equipment failures, and unauthorized industrial network activities.

[057] Although specific embodiments of the invention have been described herein for illustrative purposes, it shall be understood that various modifications, substitutions, additions, and equivalent implementations may be made without departing from the spirit and scope of the invention as defined by the appended claims.

[058] The present invention provides an advanced adaptive federated machine learning system for real-time anomaly detection and autonomous threat mitigation in Industrial Internet of Things (IIoT) networks. The disclosed invention successfully integrates distributed edge intelligence, hybrid machine learning algorithms, federated collaborative learning, protocol-aware traffic inspection, contextual risk assessment, and automated cybersecurity response mechanisms to provide scalable and resilient protection for modern industrial infrastructures. By enabling decentralized anomaly detection with privacy-preserving model training and low-latency operational analysis, the invention overcomes several limitations associated with conventional industrial cybersecurity systems including centralized dependency, delayed threat response, excessive false alarms, and inability to detect evolving cyber-physical attacks.

[059] The invention further enhances industrial operational reliability by continuously monitoring device behavior, communication patterns, process variables, and network interactions across heterogeneous industrial environments. The incorporation of adaptive self-learning capabilities enables the disclosed system to dynamically evolve according to changing industrial workflows, environmental conditions, and emerging threat landscapes. The autonomous mitigation engine further ensures rapid containment of malicious activities through intelligent response actions including device isolation, traffic control, communication rerouting, and dynamic policy enforcement, thereby minimizing operational disruptions and improving industrial safety.

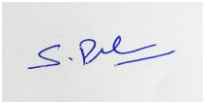
[060] In future implementations, the disclosed system may be further extended through integration with quantum-resistant cybersecurity frameworks, blockchain-based industrial identity management systems, explainable artificial intelligence models, digital twin simulation platforms, and next-generation 6G-enabled industrial communication infrastructures. Additional enhancements may include predictive cyber-risk forecasting, cross-industry federated intelligence sharing, autonomous industrial recovery orchestration, energy-aware cybersecurity optimization, and AI-driven threat anticipation mechanisms for highly autonomous industrial ecosystems. Accordingly, the present invention establishes a robust technological foundation for secure, intelligent, scalable, and self-adaptive Industrial IoT cybersecurity infrastructures capable of supporting future smart manufacturing and Industry 5.0 environments.

We Claim:

1. A machine learning-based anomaly detection system for Industrial Internet of Things (IIoT) networks comprising a plurality of industrial devices, edge intelligence nodes, federated learning coordinators, anomaly detection engines, contextual risk assessment modules, protocol-aware traffic inspection units, and autonomous mitigation components configured to identify, analyze, and mitigate abnormal industrial network behavior in real time.
2. The system as claimed in claim 1, wherein the edge intelligence nodes are configured to locally acquire and preprocess industrial communication traffic, sensor telemetry, device logs, process variables, and operational data for performing decentralized anomaly detection with low-latency processing.
3. The system as claimed in claim 1, wherein the federated learning coordinators are configured to aggregate encrypted machine learning model parameters or gradient updates received from distributed industrial edge nodes without transferring raw industrial operational data.
4. The system as claimed in claim 1, wherein the anomaly detection engine comprises recurrent neural networks, long short-term memory networks, autoencoders, graph neural networks, clustering algorithms, and statistical behavioral analysis models configured to detect cyber threats, operational anomalies, and unauthorized industrial activities.
5. The system as claimed in claim 1, wherein the protocol-aware inspection unit is configured to analyze industrial communication protocols including Modbus, OPC-UA, MQTT, EtherCAT, DNP3, CAN bus, and Profinet for identifying protocol manipulation, malicious commands, replay attacks, and abnormal communication patterns.

6. The system as claimed in claim 1, wherein the contextual risk assessment module dynamically generates anomaly severity scores based on device criticality, operational dependencies, communication topology, environmental conditions, user privileges, and historical threat behavior.
7. The system as claimed in claim 1, wherein the autonomous mitigation component is configured to perform device isolation, communication blocking, bandwidth throttling, firewall rule generation, access revocation, traffic rerouting, and alert transmission upon detection of malicious or abnormal activities.
8. The system as claimed in claim 1, wherein the anomaly detection engine continuously updates behavioral baselines, anomaly thresholds, protocol inspection parameters, and mitigation strategies using adaptive self-learning and feedback optimization mechanisms.
9. The system as claimed in claim 1, wherein the system supports scalable deployment across manufacturing plants, smart grids, transportation systems, oil and gas facilities, healthcare automation infrastructures, chemical processing plants, and autonomous industrial environments.
10. A method for machine learning-based anomaly detection in Industrial Internet of Things networks comprising acquiring industrial operational data, preprocessing communication traffic, extracting multidimensional behavioral features, performing federated machine learning analysis, generating contextual threat scores, identifying anomalous industrial activities, and autonomously executing mitigation actions to secure industrial communication infrastructures.

Dated this 20th day of May 2026

Signature: 

Applicant(s)

Dr. S. Prabu et. al.

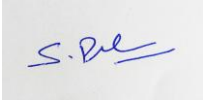
ABSTRACT

ADAPTIVE FEDERATED MACHINE LEARNING SYSTEM FOR REAL-TIME ANOMALY DETECTION AND THREAT MITIGATION IN INDUSTRIAL IOT NETWORKS

[061] The present invention discloses an adaptive federated machine learning system and method for real-time anomaly detection and autonomous threat mitigation in Industrial Internet of Things (IIoT) networks. The invention comprises industrial devices, edge intelligence nodes, federated learning coordinators, hybrid anomaly detection engines, protocol-aware inspection modules, contextual risk assessment mechanisms, and autonomous mitigation components configured to monitor and secure industrial communication infrastructures. The system acquires industrial operational data including communication traffic, sensor telemetry, process variables, device logs, and command sequences, and performs preprocessing, feature extraction, and behavioral profiling for intelligent anomaly analysis. The anomaly detection engine utilizes recurrent neural networks, long short-term memory networks, autoencoders, graph neural networks, clustering algorithms, and statistical analysis models to identify cyber threats, abnormal operational patterns, unauthorized activities, and protocol manipulation attacks in real time. The federated learning architecture enables decentralized collaborative model training without transferring raw industrial data, thereby preserving operational confidentiality and reducing centralized dependency. The contextual risk assessment engine dynamically evaluates anomaly severity using device criticality, operational dependencies, communication topology, and historical threat behavior, while the autonomous mitigation module performs adaptive response actions including device isolation, traffic filtering, firewall policy enforcement, communication rerouting, and alert generation. The invention further incorporates adaptive self-learning mechanisms for continuous optimization of anomaly detection accuracy and cybersecurity resilience across heterogeneous industrial environments including manufacturing systems, smart grids, transportation infrastructures, and automated industrial facilities.

Accompanied Drawing **[FIGS. 1-2]**

Dated this 20th day of May 2026

Signature: 

Applicant(s)

Dr. S. Prabu et. al.