AI Model Validation Framework Patent US11276543

United States Patent and Trademark Office

Patent No.: US11276543B2

Issue Date: March 15, 2022

Filing Date: April 23, 2020

Title

SYSTEMS AND METHODS FOR VALIDATING ARTIFICIAL INTELLIGENCE MODELS IN INDUSTRIAL CONTROL SYSTEM ENVIRONMENTS

Abstract

A system and method for validating artificial intelligence models deployed in industrial control system (ICS) environments, comprising a multi-layer validation framework that ensures reliability and security of AI-driven anomaly detection systems. The invention provides automated testing protocols, performance benchmarking, and continuous validation mechanisms specifically designed for critical infrastructure protection applications.

Inventors

- Chen, Marcus (San Francisco, CA)
- Rodriguez, Elena (Boston, MA)
- Morrison, James (Seattle, WA)

Assignee

DeepShield Systems, Inc. (Delaware Corporation)

Claims

A method for validating artificial intelligence models in industrial control system environments, comprising:

a) receiving operational technology (OT) network data from industrial control system components;

b) processing said data through a multi-layer validation framework comprising:

i. data integrity verification layer

ii. model performance assessment layer

iii. security compliance validation layer

iv. operational safety verification layer

c) generating validation metrics based on predetermined performance thresholds;

d) automatically adjusting model parameters based on validation results.

The method of claim 1, wherein the data integrity verification layer comprises:

a) automated data quality assessment protocols

b) anomaly detection algorithms for identifying data corruption

c) data consistency verification mechanisms

d) temporal coherence validation

The method of claim 1, wherein the model performance assessment layer includes:

a) accuracy metrics calculation

b) false positive/negative rate analysis

c) response time measurement

d) resource utilization monitoring

e) scalability testing protocols

[Claims 4-20 continued...]

Description

Background

Industrial control systems require highly reliable and secure artificial intelligence models for threat detection and anomaly identification. Existing validation frameworks lack specialized capabilities for OT environments and critical infrastructure applications. This invention addresses the need for comprehensive AI model validation in industrial cybersecurity contexts.

Detailed Description

The invention provides a novel framework for validating AI models deployed in industrial control system environments. The system implements a multi-layer validation approach that ensures both technical performance and operational safety requirements are met.

Validation Framework Components

Data Integrity Layer

- Implements continuous data quality monitoring

- Validates input data consistency
- Verifies temporal coherence
- Detects data corruption or manipulation

Performance Assessment Layer

- Measures model accuracy and precision
- Evaluates response time and latency
- Monitors resource utilization
- Conducts scalability testing

Security Compliance Layer

- Validates compliance with security standards
- Performs penetration testing
- Assesses model robustness
- Verifies access control mechanisms

Safety Verification Layer

- Ensures operational safety constraints
- Validates fail-safe mechanisms
- Tests emergency response protocols
- Verifies system stability

Implementation Methods

The validation framework operates through a series of automated testing protocols and continuous monitoring mechanisms. Implementation includes:

Automated Testing Suite

- Unit tests for individual components
- Integration tests for system interfaces
- Performance benchmarking tools
- Security assessment modules

Monitoring System

- Real-time performance tracking

- Resource utilization monitoring
- Error detection and logging
- Automated alerting mechanisms

Industrial Applicability

This invention is particularly applicable to:

- Industrial control system security
- Critical infrastructure protection
- Manufacturing automation systems
- Maritime and offshore facilities
- Energy sector operations
- Transportation systems

Prior Art References

US Patent 10,847,152

US Patent 10,592,648

EP Patent 3,456,789

PCT Publication WO2019/123456

Legal Notices

This patent is subject to all rights and protections under United States patent law. Any unauthorized use, reproduction, or implementation of the described invention may constitute patent infringement and may be subject to legal action.

Assignment Record

All rights, title, and interest in this patent have been assigned to DeepShield Systems, Inc., recorded in the USPTO assignment database on March 15, 2022.