AI Model Validation Framework Patent EP3878901

European Patent Specification

Publication Date: 15 September 2023

Application Number: EP3878901

Filing Date: 12 March 2021

Priority Date: 15 March 2020

Technical Field

[0001] The present invention relates to systems and methods for validating artificial intelligence models used in industrial control system (ICS) security applications, specifically concerning the automated validation of machine learning models deployed for anomaly detection in operational technology (OT) environments.

Background

[0002] Industrial control systems face increasingly sophisticated cyber threats requiring advanced detection mechanisms. Traditional signature-based approaches prove insufficient for identifying novel attack patterns in OT networks. While artificial intelligence offers promising solutions, the validation of AI models in critical infrastructure contexts presents unique challenges requiring rigorous verification frameworks.

Summary of the Invention

[0003] The invention provides a comprehensive framework for validating AI models deployed in industrial cybersecurity applications, comprising:

(a) A multi-stage validation pipeline incorporating:

- Model integrity verification
- Performance benchmark assessment
- Adversarial testing protocols
- OT-specific constraint validation

(b) Automated testing mechanisms for:

- False positive rate optimization

- Detection latency measurement
- Resource utilization monitoring
- Model drift identification

Detailed Description

[0004] The validation framework implements a hierarchical testing architecture consisting of:

1. Core Validation Components

1 Model Integrity Verification Module

- Cryptographic hash verification
- Weight distribution analysis
- Architecture consistency checking
- Training dataset validation

2 Performance Benchmark Engine

- Standardized test suite execution
- Performance metric calculation
- Historical comparison analysis
- Statistical significance testing

3 Adversarial Testing System

- Automated attack simulation
- Edge case generation
- Boundary condition testing
- Robustness assessment

2. OT-Specific Validation Features

1 Protocol Compatibility

- Modbus/TCP validation
- DNP3 protocol testing
- EtherNet/IP verification
- PROFINET compatibility

2 Resource Constraints

- Memory utilization monitoring
- CPU load assessment
- Network bandwidth impact
- Storage requirements validation

Claims

[0005] What is claimed is:

A method for validating artificial intelligence models deployed in industrial control system security applications, comprising:

(a) Receiving an AI model for validation;

(b) Executing the multi-stage validation pipeline;

(c) Generating validation reports and metrics;

(d) Providing certification status determination.

The method of claim 1, wherein the validation pipeline includes:

(a) Model integrity verification;

(b) Performance benchmark assessment;

(c) Adversarial testing protocols;

(d) OT-specific constraint validation.

Industrial Applicability

[0006] The invention provides significant advantages in:

- Ensuring AI model reliability in critical infrastructure protection
- Reducing false positive rates in threat detection
- Optimizing resource utilization in OT environments
- Maintaining compliance with industrial security standards

Inventors

- Dr. Elena Rodriguez
- James Morrison

- Dr. Marcus Chen

Patent Owner

DeepShield Systems, Inc.

1234 Innovation Drive

Wilmington, DE 19801

United States

Legal Representatives

Patterson & Henderson LLP

European Patent Attorneys

Registration No. EP12345

Priority Claims

US Provisional Application No. 63/154,789

Filed: March 15, 2020

Declarations

The invention described herein was made by employees of DeepShield Systems, Inc. All rights have been properly assigned to DeepShield Systems, Inc.

Authentication

This patent document contains 3 pages and 6 sections.

European Patent Office Reference: EP3878901

Digital Signature: [EPO Digital Signature Hash]

Date of Grant: September 15, 2023

End of Patent Document EP3878901