DEVICE AUTHENTICATION PROTOCOL PATENT

United States Patent No. US10876543

TITLE OF INVENTION

System and Method for Multi-Factor Device Authentication in Industrial IoT Networks

ABSTRACT

A system and method for authenticating industrial devices in Internet of Things (IoT) networks using a multi-layered authentication protocol that combines hardware-based security tokens, behavioral analytics, and distributed ledger verification. The invention provides enhanced security for industrial control systems while maintaining operational efficiency through automated trust establishment mechanisms.

ASSIGNEE

Summit Digital Solutions, Inc.

1250 Innovation Drive

Wilmington, Delaware 19801

INVENTORS

- Chang, Michael T.
- Martinez, Robert A.
- Henderson, James P.

FIELD OF INVENTION

[0001] The present invention relates generally to device authentication systems, and more particularly to secure authentication protocols for industrial Internet of Things (IoT) devices operating within enterprise networks.

BACKGROUND

[0002] Industrial IoT networks face increasing security challenges as more devices are connected to enterprise systems. Traditional authentication methods often prove inadequate for the scale and complexity of modern industrial environments.

[0003] Existing solutions typically rely on single-factor authentication or static credentials, creating vulnerabilities in industrial control systems. There remains a need for more robust authentication

mechanisms that can operate at scale while maintaining operational efficiency.

SUMMARY OF INVENTION

[0004] The present invention provides a novel approach to device authentication through a multi-layered protocol that combines:

- Hardware-based security token verification
- Real-time behavioral analysis
- Distributed ledger validation
- Adaptive trust scoring

[0005] The system implements a proprietary authentication algorithm that processes multiple authentication factors simultaneously while maintaining sub-second response times required for industrial applications.

DETAILED DESCRIPTION

[0006] The authentication protocol comprises the following core components:

Token Generation Module

[0007] A hardware-based security token generator that creates unique device identifiers using:

- Device-specific hardware signatures
- Environmental parameters
- Temporal variables
- Network context information

Behavioral Analysis Engine

[0008] Real-time analysis of device behavior patterns including:

- Communication patterns
- Resource utilization
- Operation sequences
- Network interaction profiles

Distributed Verification Network

[0009] A blockchain-based verification system that:

- Maintains a distributed ledger of authenticated devices
- Provides consensus-based validation

- Enables rapid trust establishment
- Supports revocation mechanisms

Trust Scoring Algorithm

[0010] An adaptive scoring system that:

- Evaluates multiple authentication factors
- Adjusts trust levels dynamically
- Implements risk-based access control
- Provides continuous authentication

CLAIMS

A method for authenticating devices in industrial IoT networks, comprising:

a) Generating a hardware-based security token

b) Analyzing device behavioral patterns

c) Validating device identity through distributed ledger

d) Computing dynamic trust scores

e) Granting or denying network access based on authentication results

The method of claim 1, wherein the hardware-based security token includes:

a) Device-specific hardware signatures

b) Environmental parameters

c) Temporal variables

d) Network context information

[Claims 3-20 omitted for brevity]

DRAWINGS

[Reference to attached drawings showing system architecture and process flows]

PRIORITY CLAIM

[0011] This application claims priority to U.S. Provisional Application No. 62/987,654 filed March 15, 2019.

GOVERNMENT RIGHTS

[0012] This invention was made without government support.

EXECUTION

IN WITNESS WHEREOF, the below-named inventors have executed this patent application on this 15th day of March, 2020.

/s/ Michael T. Chang

Michael T. Chang

Chief Technology Officer

Summit Digital Solutions, Inc.

/s/ Robert A. Martinez

Dr. Robert A. Martinez

Chief Innovation Officer

Summit Digital Solutions, Inc.

/s/ James P. Henderson

James P. Henderson

Chief Digital Officer

Summit Digital Solutions, Inc.

PATENT ATTORNEY CERTIFICATION

I hereby certify that this patent application meets all requirements for filing under 35 U.S.C. § 111(a).

/s/ Sarah Johnson

Sarah Johnson, Esq.

Reg. No. 58,421

Patent Attorney for Summit Digital Solutions, Inc.

[End of Patent Document]