IoT Security Protocol Patent Application

United States Patent and Trademark Office

Application No.: 17/482,391

Filing Date: September 15, 2023

TITLE OF INVENTION

System and Method for Secure Multi-Layer Authentication in Industrial Internet of Things (IIoT) Networks

APPLICANT

Summit Digital Solutions, Inc.

1200 Innovation Drive

Wilmington, Delaware 19801

INVENTORS

Chang, Michael (Chief Technology Officer)

Martinez, Robert (Chief Innovation Officer)

Kumar, Priya (Principal Security Architect)

CROSS-REFERENCE TO RELATED APPLICATIONS

This application claims priority to U.S. Provisional Application No. 63/281,492, filed March 22, 2023.

FIELD OF INVENTION

[0001] The present invention relates generally to cybersecurity systems for Internet of Things (IoT) networks, and more particularly to a multi-layered authentication protocol for securing industrial IoT device communications within enterprise environments.

BACKGROUND

[0002] Industrial IoT networks face increasing security challenges as the number of connected devices expands exponentially. Traditional authentication methods prove insufficient for the scale and complexity of modern IIoT deployments.

[0003] Existing solutions fail to address the unique requirements of enterprise-scale IoT

implementations, particularly regarding:

- Real-time authentication of thousands of concurrent device connections
- Resource constraints of edge devices
- Need for zero-trust architecture in distributed systems
- Maintenance of security protocols across heterogeneous device types

SUMMARY OF INVENTION

[0004] The present invention provides a novel system and method for securing IIoT networks through a multi-layered authentication protocol that combines:

[0005] a) Device-level cryptographic signatures using lightweight encryption

[0006] b) Network-layer authentication via proprietary challenge-response mechanisms

[0007] c) Application-layer security through dynamic token generation

[0008] d) Continuous trust verification through behavioral analysis

DETAILED DESCRIPTION

[0009] The invention comprises a security protocol stack implementing the following components:

Authentication Layer

[0010] The base authentication layer utilizes elliptic curve cryptography (ECC) optimized for resource-constrained IoT devices. The system employs:

- 256-bit encryption keys
- Deterministic key generation
- Hardware-based key storage
- Rotating session identifiers

Network Security Layer

[0011] The network security layer implements:

- Proprietary challenge-response protocol
- Dynamic network segmentation
- Traffic pattern analysis
- Automated threat detection

Application Security

[0012] Application-level security features include:

- JWT-based authentication tokens
- Role-based access control
- API endpoint protection
- Audit logging

CLAIMS

A method for securing industrial IoT networks comprising:

a) Implementing device-level cryptographic authentication

b) Establishing network-layer security protocols

c) Applying application-level security measures

d) Maintaining continuous trust verification

The method of claim 1, wherein device-level authentication comprises:

a) Generation of unique device identifiers

b) Implementation of lightweight encryption

c) Secure key storage

d) Session management

A system for implementing the method of claim 1, comprising:

a) Authentication servers

b) Network security modules

c) Application security components

d) Trust verification engine

ABSTRACT

A system and method for securing industrial IoT networks through a multi-layered authentication protocol. The invention provides comprehensive security across device, network, and application layers while maintaining operational efficiency. The system implements lightweight cryptography, proprietary challenge-response mechanisms, and continuous trust verification suitable for enterprise-scale IoT deployments.

DECLARATION

I hereby declare that I am the original inventor of the subject matter which is claimed and for which a patent is sought; that I have reviewed and understand the contents of this application; and that all statements made herein are true and correct to the best of my knowledge.

Dated: September 15, 2023

/s/ Michael Chang

Michael Chang

Chief Technology Officer

Summit Digital Solutions, Inc.

/s/ Robert Martinez

Dr. Robert Martinez

Chief Innovation Officer

Summit Digital Solutions, Inc.

/s/ Priya Kumar

Priya Kumar

Principal Security Architect

Summit Digital Solutions, Inc.

POWER OF ATTORNEY

The undersigned hereby appoints the registered patent attorneys of WILSON SONSINI GOODRICH & ROSATI, Professional Corporation, Customer Number 21825, as attorneys and agents to prosecute this application and transact all business in the Patent and Trademark Office connected therewith.

/s/ Alexandra Reeves

Dr. Alexandra Reeves

Chief Executive Officer

Summit Digital Solutions, Inc.