# IoT Network Security Protocol Patent

**Patent No. 14,285,963**

**Filing Date: June 15, 2021**

**Issue Date: September 28, 2023**

## ABSTRACT

A system and method for securing Internet of Things (IoT) device networks through a multi-layered authentication and encryption protocol, comprising distributed key management, dynamic device fingerprinting, and adaptive security measures based on real-time threat analysis.

## BACKGROUND OF INVENTION

### Field of Invention

This invention relates to network security protocols, specifically to securing communications between IoT devices in enterprise environments utilizing distributed authentication mechanisms and encrypted data transmission.

### Prior Art

Existing IoT security protocols typically rely on centralized authentication servers and static security measures, creating potential single points of failure and vulnerability to emerging threats. Prior solutions fail to adequately address the unique challenges of securing large-scale IoT deployments in enterprise environments.

## DETAILED DESCRIPTION

### 1. System Architecture

1 The system comprises:

a) A distributed authentication layer implementing blockchain-based credential management

b) Dynamic device fingerprinting modules utilizing proprietary algorithms

c) Real-time threat analysis engine with machine learning capabilities

d) Adaptive security response mechanisms

e) Encrypted communication channels using AES-256 encryption

2 The distributed authentication layer maintains:

a) Device identity verification

b) Access control lists

c) Security policy enforcement

d) Audit logging

e) Credential rotation schedules

**2. Authentication Protocol**

1 Device Registration Process:

a) Initial device fingerprint generation

b) Secure key pair generation

c) Blockchain registration

d) Policy assignment

e) Network integration

2 Ongoing Authentication:

a) Continuous device verification

b) Dynamic trust scoring

c) Behavioral analysis

d) Anomaly detection

e) Automated response triggers

**3. Security Measures**

1 Encryption Implementation:

a) End-to-end encryption for all device communications

b) Key rotation mechanisms

c) Certificate management

d) Secure key storage

e) Hardware security module integration

2 Threat Detection:

a) Real-time network monitoring

b) Pattern recognition

c) Threat intelligence integration

d) Automated incident response

e) Security event logging

## CLAIMS

A method for securing IoT device networks comprising:

- Implementing distributed authentication mechanisms
- Utilizing dynamic device fingerprinting
- Employing adaptive security measures
- Managing encrypted communications
- Maintaining audit trails

The method of claim 1, wherein distributed authentication includes:

- Blockchain-based credential management
- Multi-factor authentication
- Dynamic trust scoring
- Policy-based access control
- Automated credential rotation

The method of claim 1, wherein device fingerprinting includes:

- Hardware identification
- Behavioral analysis
- Network interaction patterns
- Resource utilization profiles
- Communication patterns

## INVENTORS

- Dr. Michael Chang, Chief Technology Officer
- Dr. Robert Martinez, Chief Innovation Officer
- James Henderson, Chief Digital Officer
- Summit Digital Solutions, Inc.

## ASSIGNMENT

All rights, title, and interest in this patent are assigned to Summit Digital Solutions, Inc., a Delaware corporation with its principal place of business at 2200 Innovation Drive, Suite 400, Boston, MA 02110.

## LEGAL REPRESENTATION

Prepared by:

Wilson & Mitchell LLP

Patent Attorneys

100 State Street, Floor 45

Boston, MA 02109

## CERTIFICATION

I hereby certify that I am authorized to execute this patent application on behalf of Summit Digital Solutions, Inc.

```

_

Dr. Michael Chang

Chief Technology Officer

Summit Digital Solutions, Inc.

Date: June 15, 2021

```

## DISCLAIMER

This patent document contains confidential and proprietary information of Summit Digital Solutions, Inc. Unauthorized reproduction or distribution of this patent document, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under the law.