DEVICE AUTHENTICATION PROTOCOL PATENT

Patent No. US 10,847,443 B2

Filing Date: April 15, 2019

Issue Date: November 12, 2020

ABSTRACT

A system and method for secure device authentication in distributed IoT networks utilizing multi-factor cryptographic validation protocols. The invention provides enhanced security through a novel combination of hardware-based attestation, dynamic key rotation, and blockchain-verified credential management.

TECHNICAL FIELD

[001] The present invention relates generally to computer security systems and methods, and more particularly to secure device authentication protocols for Internet of Things (IoT) networks implementing distributed authentication architectures.

BACKGROUND

[002] Traditional device authentication methods face significant challenges in distributed IoT environments, including vulnerability to man-in-the-middle attacks, credential theft, and replay attacks. Existing solutions fail to adequately address the unique security requirements of large-scale IoT deployments.

[003] The present invention overcomes these limitations through an innovative approach to device authentication that combines hardware-based security elements with advanced cryptographic protocols.

SUMMARY OF THE INVENTION

[004] The invention provides a secure device authentication system comprising:

- A hardware security module (HSM) implementing tamper-resistant key storage
- A distributed credential verification protocol utilizing blockchain technology
- Dynamic key rotation mechanisms with configurable rotation periods
- Multi-factor authentication combining biometric and cryptographic elements

DETAILED DESCRIPTION

Authentication Protocol

[005] The authentication protocol comprises the following steps:

Device initialization with unique identifier and root certificates

Hardware-based key generation and secure storage

Multi-factor authentication sequence

Blockchain verification of device credentials

Dynamic session key generation

Continuous trust verification

Security Architecture

[006] The security architecture implements:

a) Asymmetric encryption using RSA-4096

b) SHA-256 hashing for message integrity

c) Elliptic curve cryptography for key exchange

d) Secure boot verification

e) Runtime attestation

Implementation Methods

[007] The authentication protocol may be implemented through:

Embedded firmware modules

Cloud-based authentication servers

Distributed ledger networks

Hardware security elements

CLAIMS

A method for secure device authentication comprising:

a) Generating device-specific cryptographic keys

b) Implementing hardware-based attestation

c) Verifying device credentials via distributed ledger

d) Performing continuous trust validation

The method of claim 1, further comprising:

a) Dynamic key rotation

b) Multi-factor authentication

c) Secure boot verification

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

a) Hardware security modules

b) Blockchain verification nodes

c) Authentication servers

d) Key management infrastructure

INVENTORS

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

ASSIGNEE

Summit Digital Solutions, Inc.

1234 Innovation Drive

Wilmington, DE 19801

PATENT ATTORNEY

Sarah Johnson, Esq.

Registration No. 65432

Johnson & Associates LLP

GOVERNMENT INTERESTS

[008] This invention was made without government support or funding.

FOREIGN PRIORITY

[009] This application claims priority to PCT/US2019/027654, filed March 15, 2019.

RELATED APPLICATIONS

[010] This application is related to:

- US Patent Application No. 15/987,654
- US Patent No. 10,123,456

CERTIFICATION

I hereby certify that this patent document accurately represents the invention as claimed and meets all requirements for patent protection under 35 U.S.C. 101 et seq.

/s/ Sarah Johnson

Sarah Johnson, Esq.

Patent Attorney

Registration No. 65432

Date: November 12, 2020

LEGAL NOTICES