Decentralized AI-Driven Infrastructure Platform with Post-Quantum Identity, Self-Healing SD-WAN, and Trusted Zero-Trust Execution Model

Written by: Chris McWhorter, *Founder & Principal Architect, NetByte.AI, LLC*
Date: May 23, 2025

Defensive Publication Title:

Decentralized AI-Driven Infrastructure Platform with Post-Quantum Identity, Self-Healing SD-WAN, and Trusted Zero-Trust Execution Model

---

Section 1: Technical Field

This invention relates to the fields of cybersecurity, IT infrastructure automation, secure identity management, decentralized systems, and zero-trust architectures. Specifically, it describes a comprehensive, modular platform combining AI-driven infrastructure orchestration, decentralized post-quantum identity verification, real-time telemetry analysis, and enterprise-grade automation within a self-healing, resilient SD-WAN environment.

Section 2: Background of the Invention

Current enterprise IT infrastructures are fragmented, often relying on multiple vendors and centralized identity providers. These environments suffer from complex integration issues, brittle security models, and poor visibility. Traditional authentication mechanisms are susceptible to phishing, spoofing, and credential theft. Additionally, conventional infrastructure stacks are reactive rather than predictive, and they lack resilience in the face of partial system failures or modern threat vectors.

There is a need for a unified, hardware-integrated, zero-trust platform that delivers:

- Post-quantum secure identity enforcement.
- Biometric multi-factor authentication (MFA).
- AI-driven network monitoring and orchestration.
- Self-healing distributed architectures that detect and recover from compromise or failure autonomously.
- Compliance-aware automation with full audit trails and append-only logging.

Section 3: Summary of the Invention

The invention is a decentralized infrastructure platform composed of three or more interconnected physical or virtual devices (“NetByte SDI-Core”) that act as a self-healing cluster. These connect to small physical or virtual devices (“NetByte SDI-Lite”).

The platform includes:

- A post-quantum identity system using Kyber-based certificates, issued to both users and hardware devices.
- A biometric MFA app (“NetByteID”) which stores the private key in the device’s secure enclave and signs challenges.
- A quorum-based authentication flow requiring validation by randomly selected peers across the network.
- A decentralized, append-only log for all identity events, configuration changes, access attempts, and forensic records.
- An AI subsystem (“Rudy”) that continuously monitors logs, telemetry, and behavior for threat detection and remediation.
- A full stack of network, storage, automation, and operational tooling, delivered via a unified interface.
- SD-WAN routing powered by VPP (Vector Packet Processing), offering ultra-low-latency, AI-scored path selection, and active failover between fiber, copper, and satellite.
- Identity-driven segmentation (“Zones”), which isolate services, users, storage, and routing policies by tenant, department, or business unit.

Section 4: Detailed Description of the Architecture

The NetByte SDI platform consists of at least three interconnected nodes, each referred to as a **SDI-Core**. These nodes may be physical servers (such as a 4U GPU-enhanced system), miniaturized edge devices (NUC-based), or virtual machines running the NetByte SDI software stack. Each SDI-Core node contains the following integrated subsystems:

4.1 Identity Subsystem

- Each user is issued a **Kyber-based post-quantum cryptographic identity certificate**.
- Certificates are issued via a secure internal authority and embedded in the user's mobile MFA app, protected by biometric authentication (e.g., Face ID, fingerprint).
- Hardware devices receive certificates at manufacturing time. The private key is stored in a TPM (Trusted Platform Module), and the public key is written to an **append-only decentralized identity ledger**.
- Certificates are rotated automatically every 30 days, with fallback verification supported via prior key hashes.

4.2 Quorum-Based Authentication System *(Optional)*

- Every identity verification event triggers a **challenge-response flow** signed with the user or device's Kyber key.
- A quorum of **3–9 randomly selected nodes** is selected using a randomization algorithm governed by the platform's AI engine.
- Each node verifies the signature, device integrity (via hash), certificate status (revoked, valid, expired), and challenge expiry (default 10 minutes).
- All quorum nodes must return an "Approve" response for access to be granted.
- Failure triggers alerts, logging, and optional device quarantine.

4.3 AI Orchestration Subsystem (“Rudy”)

- The platform includes a modular AI engine (“Rudy”) that continuously:
    - Monitors system logs and telemetry.
    - Applies LLM-driven analysis to interpret behavioral patterns.
    - Auto-generates configuration changes or triggers node isolation.
    - Provides On Demand Tier 1 Help Desk Support to end-users
- Rudy modules operate independently or in parallel across all nodes and communicate using a decentralized message queue.
- Examples of Rudy’s actions include:
    - Auto-isolation of a compromised node after hash mismatch.
    - AI-generated firewall rule creation based on unusual outbound traffic.
    - SD-WAN path rerouting based on latency or packet loss patterns.
    - Tier 1 Troubleshooting of end-point devices and issues.
    - Create Help Desk tickets for Tier 2 Engineers, accurately describing issues, with accompany logs, and steps taken during automated troubleshooting.

4.4 Network Layer & SD-WAN

- Each node contains a full SD-WAN routing engine built using **VPP (Vector Packet Processing)**.
- The routing layer is AI-augmented and supports:
    - Real-time path scoring (fiber, copper, satellite).
    - Autonomous failover.
    - Policy-based routing per tenant or identity zone.
- A full mesh network is maintained between all nodes using **WireGuard**, enhanced with Kyber-based certs for post-quantum security.

4.5 File System Integrity & Device Trust

- Each device runs a **Blake3-based Merkle tree file system hash** validator on boot and every 5 minutes.
- Hashes are compared to the last known good configuration in the append-only log.
- Any deviation triggers automatic removal from the network and notification for manual review.
- Admin-approved changes must be signed and synced to update the baseline hash.

Section 5: Key Functional Workflows

This section outlines the major operational processes within the NetByte platform. Each workflow emphasizes decentralized validation, cryptographic identity, and AI-assisted decision-making.

5.1 User Onboarding & Certificate Issuance

1. An administrator creates a user account via the internal identity panel or via directory sync.
2. The user receives a secure enrollment link via SMS or email.
3. The user installs the **NetByteID** mobile app and completes biometric registration.
4. The app generates a Kyber keypair:
    - The **private key** is stored in the device's secure enclave.
    - The **public certificate** is logged in the **append-only global identity ledger**.
5. The user is now capable of signing challenges and participating in authenticated workflows.

5.2 Device Onboarding Workflow

1. Each device is embedded with a TPM module during manufacture or prior to enrollment.
2. During onboarding:
    - A unique Kyber keypair is generated.
    - The private key is written to the TPM.
    - A **Blake3 hash** of the file system and hardware fingerprint is generated.
3. These values are recorded in the global identity ledger.
4. The device is now authorized and visible to the network, pending periodic hash validation.

5.3 Challenge-Response Authentication

1. A user or device initiates a request (e.g., login, access file, reconfigure system).
2. The platform issues a challenge:
    - Contains nonce, timestamp, request type.
    - Must be signed by the requestor's private key.
3. A random quorum of 3–9 nodes is selected to validate:
    - Signature validity.
    - Challenge freshness.
    - Identity revocation or quarantine status.
4. Upon unanimous "Approve," access is granted.
    - Otherwise, request is denied and logged.

5.4 Certificate Revocation & Rotation

- **User Rotation:**
    - Auto-rotates every 30 days.
    - User re-authenticates via biometrics to unlock and store the new key.
    - Prior key remains valid for 14 days (fallback).
- **Device Rotation:**
    - Triggered manually or via policy.
    - TPM generates new key; new cert replaces old in log.
- **Revocation:**
    - Triggered by admin, AI engine, or auto-forensics.
    - Requires quorum confirmation.
    - Marked in the ledger and enforced globally.

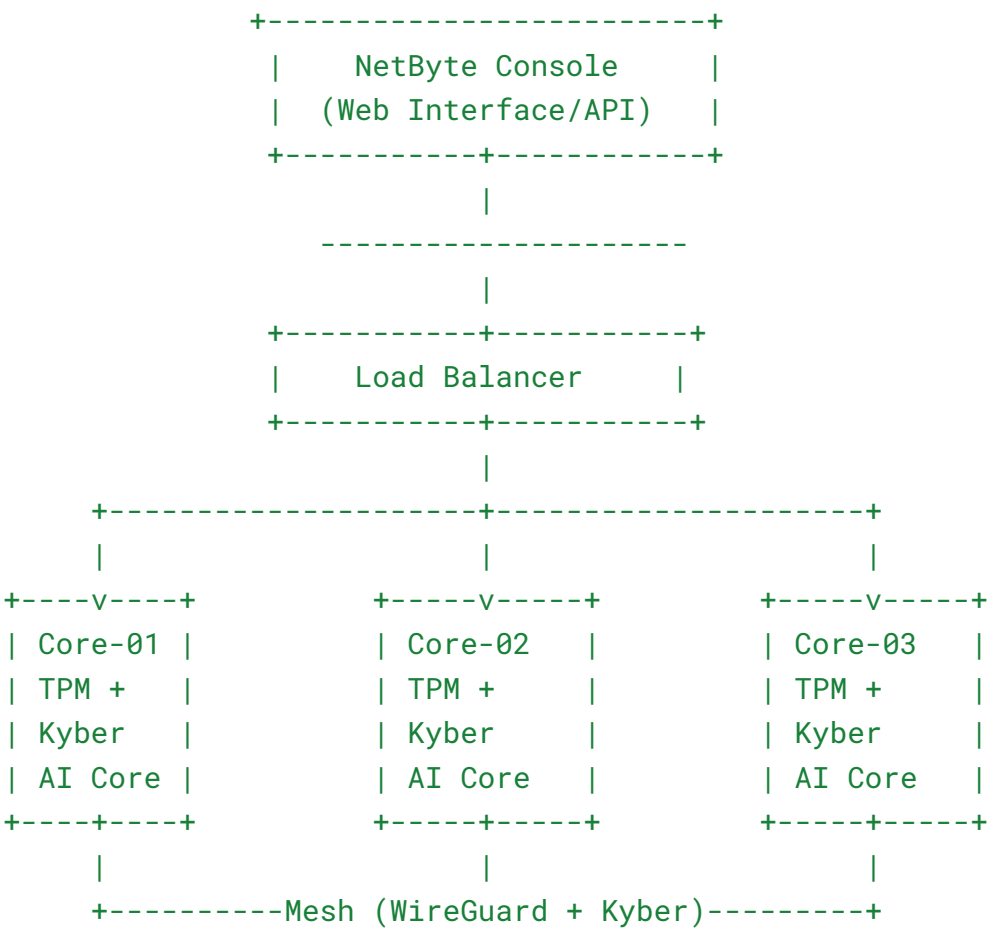
5.5 Self-Healing Node Management

1. All nodes continuously run file system integrity checks.
2. On hash mismatch:
    - Node quarantines itself.
    - AIM engine triggers alert and AI-driven root cause analysis.
3. If verified as malicious or corrupt:
    - TPM key is invalidated.
    - Admin must issue TPM replacement.
4. If verified as safe:
    - Admin signs off.

- New baseline hash is pushed and logged.

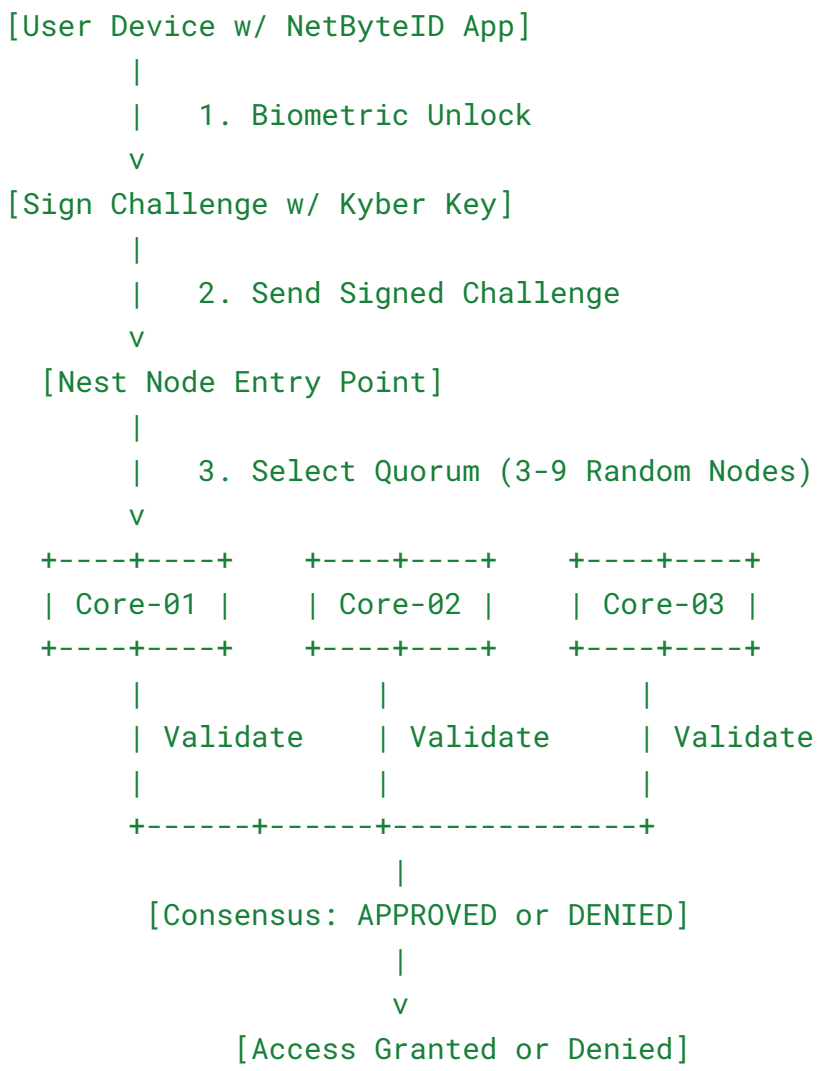
Section 6: Diagrams & Configuration Examples

Diagram A: Three-Node CyberNest Deployment Architecture



Each node maintains:
- VPP-based SD-WAN Routing
- Wazuh agent (log ingestion)
- MinIO shard with erasure coding
- Rudy (AI Engine)
- Arkime packet capture

Diagram B: User Authentication Flow with Quorum Verification



Configuration Example: Identity Certificate JSON

```
{
  "uid": "cmcwhorter@netbyte.ai",
  "public_key": "kyber768-pubkey-base64",
  "cert_id": "NB-2025-0001",
  "issued": "2025-03-24T14:32:00Z",
  "rotated_on": null,
  "revoked": false,
  "mfa_binding": {
    "method": "biometric",
    "device": "iPhone15,4",
    "secure_enclave": true
  },
  "quorum_required": 5
}
```

Section 7: Use Cases & Security Impact

7.1 Use Cases

- **Healthcare Organizations**
  Seamless biometric access to patient records with full HIPAA audit logs. Medical devices join the network only if verified by TPM-bound certificates.

- **Finance / Banking**
  Remote offices connected via AI-enhanced SD-WAN. Transactions require biometric-signed challenge-responses validated by decentralized quorum nodes.

- **Government / Defense**
  Air-gapped or semi-connected nodes maintain self-healing capabilities and forward-only synchronization with delta logging for tamper-proof evidence trails.

- **Managed Service Providers (MSPs)**
  Multi-tenant environments enforce microsegmentation at the identity level. Each tenant's operations are isolated via "Zone" constructs backed by post-quantum certs.

7.2 Security Benefits

- **Eliminates Single Points of Failure**
  No centralized identity provider, root certificate, or trust authority.

- **Quantum-Resilient Identity Stack**
  Kyber certificates ensure future-proof cryptographic resistance.

- **Tamper-Proof Logging**
  Blake3-based Merkle tree chains enforce forensic traceability.

- **Dynamic Risk Mitigation**
  AIM modules detect and isolate anomalies in real time, preventing lateral movement or node compromise.

- **Compliant by Default**
  Logs and flows can be tagged for HIPAA, PCI-DSS, GDPR, or custom compliance standards.

End of Defensive Publication Document

Inventor: James Christopher McWhorter
Company: NetByte.AI, LLC
Date of Public Disclosure: May 23, 2025
Contact: chris@netbyte.ai

NetByte.AI®