Title

Systems and Methods for Chaotic-Entropy-Driven Multi-Layer Trust Orchestration

Description

Field of the Invention

The invention relates to digital identity, authentication systems, access control, cryptographic key management, post-quantum cybersecurity, behavioural analytics, and distributed systems security. It specifically concerns systems and methods for orchestrating identity and trust using entropy, behavioural signals, attestation, and adaptive cryptographic control.

Background of the Invention

Conventional identity and access-control systems rely on isolated authentication events, predictable key-rotation intervals, and static security policies. These systems are vulnerable to credential theft, behavioural spoofing, device impersonation, timing attacks, anomaly-evasion techniques, and quantum-enabled cryptographic compromise. Existing approaches do not provide a unified, continuously updated trust state combining entropy, behavioural characteristics, environmental or device context, anomaly signals, and cryptographic health.

There is a need for a dynamic trust-orchestration architecture capable of resisting automated threats, maintaining robustness under quantum-capable adversaries, and adapting continuously to user, device, and environmental conditions.

Summary of the Invention

The invention provides a system that continuously derives a trust value from multiple independent signal sources and applies that value to govern identity, authentication, access, and cryptographic operations.

The system comprises:

1. **Entropy Generator:**
   Produces non-deterministic timing or modulation values derived from one or more entropy sources.
2. **Behavioural Identity Engine:**
   Generates behavioural indicators representing user or device interaction characteristics without retaining sensitive raw data.

3. **Device and Environment Attestation Module:**
   Collects device-state proofs and environmental context indicators to verify operational integrity.
4. **Anomaly Detection Module:**
   Creates anomaly indicators based on behavioural or contextual deviations.
5. **Post-Quantum Cryptography Controller:**
   Manages cryptographic key generation, rotation, and revocation in accordance with trust-state changes.
6. **Adaptive Trust Engine:**
   Combines the above signals into a continuous trust value and orchestrates authentication complexity, access permissions, session lifetime, and distributed enforcement behaviour.

The invention enables dynamic, privacy-preserving identity assurance with non-predictable authentication and cryptographic event timing.

Detailed Description of the Invention

System Overview

The system operates as an integrated trust-fabric across devices, servers, and distributed nodes. A plurality of signal-generation modules feed the adaptive trust engine, which produces a continuous trust value. The computed trust value influences policy, authentication pathways, and cryptographic lifecycle actions.

Entropy Generator

An entropy generator provides non-deterministic values used to modulate trust-related behaviour. The entropy may be derived from any combination of physical, behavioural, environmental, or algorithmic variability. The generator produces timing or modulation outputs used to prevent deterministic or predictable system behaviour.

Behavioural Identity Engine

A behavioural engine produces behavioural indicators based on user or device interaction patterns. Sensitive raw interaction data is not stored or transmitted. Behavioural indicators may include timing regularities, interaction consistency, or movement-based characteristics. These indicators contribute to trust scoring but are not retained in their original form.

Device and Environment Attestation Module

A device-attestation module collects device-state information, hardware proofs, or contextual environmental indicators. These signals are combined to validate operational integrity, detect changes in environment or device state, and contribute to trust evaluation.

Anomaly Detection Module

An anomaly module produces anomaly indicators by identifying deviations in behavioural, contextual, or system-level characteristics. These indicators provide early detection of impersonation, automation, or compromise.

Post-Quantum Cryptography Controller

A cryptography controller manages the lifecycle of post-quantum cryptographic keys. Key generation, rotation, and revocation events are dynamically triggered based on trust-state changes. The controller ensures that cryptographic operations remain aligned with real-time risk.

Adaptive Trust Engine

A trust engine fuses entropy values, behavioural indicators, attestation signals, anomaly indicators, and cryptographic-state information into a continuous trust value. The trust value is updated throughout the lifetime of a session, device operation, or network interaction. The trust engine governs:

- authentication-factor requirements
- access-permission thresholds
- session duration and validity
- cryptographic key-lifecycle events
- node isolation or reintegration
- privilege escalation or suppression

Policy and Enforcement Layer

A policy engine and distributed enforcement layer apply trust-dependent decisions across devices, nodes, and systems. Nodes may autonomously regenerate cryptographic keys or isolate themselves if trust falls below defined thresholds.

Claims

Claim 1

A system comprising an entropy generator, a behavioural-identity engine, a device-attestation module, an anomaly-detection module, a post-quantum cryptography controller, and an adaptive trust engine configured to continuously compute a trust value from outputs of said modules and dynamically govern authentication requirements, access control, and cryptographic key-lifecycle events.

Claim 2

The system of Claim 1 wherein the entropy generator produces non-deterministic modulation values used to influence authentication timing or cryptographic-key events.

Claim 3

The system of Claim 1 wherein the behavioural-identity engine generates behavioural indicators without retaining sensitive raw data.

Claim 4

The system of Claim 1 wherein the device-attestation module collects device-state indicators and environmental context indicators for trust evaluation.

Claim 5

The system of Claim 1 wherein the trust value governs the complexity or sequence of authentication steps.

Claim 6

The system of Claim 1 wherein the trust value triggers generation, rotation, or revocation of cryptographic keys managed by the post-quantum cryptography controller.

Claim 7

The system of Claim 1 wherein the trust value governs access-permission thresholds or session-lifetime parameters.

Claim 8

The system of Claim 1 wherein distributed nodes autonomously isolate or regenerate cryptographic material based on trust-value thresholds.

Claim 9

The system of Claim 1 wherein the entropy generator prevents adversarial prediction of authentication or cryptographic-lifecycle events.

Claim 10

The system of Claim 1 implemented across devices, servers, and networked nodes forming a unified trust-controlled infrastructure.

Abstract

A system and method for generating, maintaining, and enforcing a continuous digital trust state for users, devices, and distributed infrastructure. The invention fuses entropy signals, behavioural indicators, attestation data, anomaly information, and post-quantum cryptographic status into a single adaptive trust value. The trust value dynamically governs authentication requirements, access permissions, cryptographic key lifecycle events, session validity, and node isolation. A chaotic-entropy generator provides non-deterministic modulation to prevent adversarial prediction. The invention provides a unified trust-fabric architecture enabling dynamic, privacy-preserving identity assurance and resilient cybersecurity control across distributed systems.