Device Environment Attestation Mesh for Context-Bound Identity and Trust Enforcement

Technical Field

The invention relates to environment attestation, contextual identity verification, trust enforcement, device-state proofs, cryptographic binding, post-quantum authentication systems and security architectures for distributed networks.

Background

Identity systems often rely on static credentials, biometrics or behavioural patterns without incorporating environmental or device-state context. This allows cloning, replay, system spoofing and external manipulation. Existing attestation mechanisms are typically limited to single-signal checks or remote verification. There is no cohesive mesh integrating multiple environmental, device and contextual indicators into cryptographically bound attestation bundles that tie authentication to the real-world state of the device and user. A system is required that fuses diverse attestation signals into non-reversible signatures for trust enforcement, PQ-secure session establishment and context-locked identity.

Summary of the Invention

The invention provides an attestation mesh that collects, processes and fuses environmental, device-state and contextual indicators. These include temperature variation, motion signatures, ambient patterns, proximity data, device-state proofs, location randomness markers, magnetic field perturbations, noise-floor entropy and time-shift variance. The mesh transforms these into non-reversible attestation signatures. Signatures bind authentication events to the observed state of the device. Attestation bundles integrate with behavioural-entropy-derived keys and post-quantum cryptographic processes. Outputs cannot reconstruct raw environmental data. The attestation mesh integrates with trust-fusion engines and identity devices disclosed in prior filings.

Detailed Description

Attestation Signal Inputs

The system samples:

1. Temperature deviation patterns.
2. Ambient light fluctuation signatures.
3. Motion-path micro-vectors.
4. Acceleration variance and jerk profiles.
5. Magnetic field noise patterns.
6. Proximity pulses and return signatures.
7. Acoustic noise-floor variability.
8. Location randomness indicators.
9. Posture-stability metrics.
10. Device-state proofs including hardware flags, lock-state indicators and integrity counters.

Signal Normalisation and Pre-Processing

Signals undergo:
• temporal smoothing,
• variance reduction,
• spectral decomposition,
• magnitude rebalancing,
• entropy extraction transforms.

Outputs form non-identifiable contextual indicators.

Contextual Entropy Extraction

Environmental and device-state indicators are transformed into contextual entropy values. These values retain unpredictability and device-specific traits without exposing raw sensor data.

Entropy Fusion Component

Contextual entropy is fused with:
• fractal entropy,
• device-anchored randomness,
• anomaly-adjusted modifiers,
• attestation timing intervals.

The fusion output forms an attestation entropy state.

Attestation Bundle Formation

The system forms context-bound bundles containing:
• attestation entropy state,
• timestamp structures,
• device-state commitments,
• context-derived anomaly markers,
• post-quantum signature envelopes.

Raw sensor data is excluded.

Binding to Authentication Events

Attestation bundles are cryptographically bound to:
• identity proofs,
• session keys,
• behavioural-entropy-derived keys,
• trust metrics.

Authentication events cannot be replayed in other contexts.

Post-Quantum Cryptography Integration

PQ-secure signing binds attestation bundles to key cycles. Attestation values influence:
• key refresh triggers,
• session validity windows,
• trust weighting.

Anomaly Detection and Trust Adjustment

Deviation in attestation signals affects:
• trust values,
• session permissions,
• token issuance,
• authentication outcomes.

Zero-Retention Guarantee

Raw environmental and device-state signals are discarded after processing. Only non-reversible attestation signatures persist.

Integration with Related Systems

The attestation mesh integrates with:
• trust orchestration (GB2520368.8),
• the TuringKey device (GB2520379.5),
• behavioural-entropy key derivation (GB2520380.3).

Claims

Claim 1

An attestation mesh comprising a plurality of environmental, device-state and contextual sensors, a pre-processing layer, a contextual entropy module and an attestation bundle generator, wherein attestation signals are transformed into non-reversible signatures bound to authentication events.

Claim 2

The mesh of Claim 1 wherein environmental indicators include temperature variation, ambient light fluctuation, acoustic noise-floor variability and magnetic field noise.

Claim 3

The mesh of Claim 1 wherein device-state indicators include hardware integrity counters, lock-state proofs and internal status flags.

Claim 4

The mesh of Claim 1 wherein contextual indicators include motion micro-vectors, acceleration variance, jerk profiles, posture-stability metrics and proximity signatures.

Claim 5

The mesh of Claim 1 wherein the pre-processing layer performs variance reduction, spectral decomposition and entropy extraction.

Claim 6

The mesh of Claim 1 wherein contextual entropy is combined with fractal entropy and device-anchored randomness to form an attestation entropy state.

Claim 7

The mesh of Claim 1 wherein attestation bundles include the attestation entropy state, device-state commitments, anomaly markers and post-quantum signatures.

Claim 8

The mesh of Claim 1 wherein authentication events are cryptographically bound to attestation bundles, preventing replay outside the original context.

Claim 9

The mesh of Claim 1 wherein attestation bundles influence post-quantum key refresh cycles and session validity constraints.

Claim 10

The mesh of Claim 1 wherein anomaly deviation triggers restricted authentication or session denial.

Claim 11

The mesh of Claim 1 wherein raw attestation signals are discarded immediately after entropy transformation.

Claim 12

The mesh of Claim 1 wherein attestation bundles integrate with behavioural-entropy-derived keys for composite identity verification.

Claim 13

The mesh of Claim 1 wherein attestation outputs alter trust metrics used in multi-layer trust-fusion engines.

Claim 14

The mesh of Claim 1 wherein the attestation mesh operates within a portable identity device.

Claim 15

The mesh of Claim 1 referencing GB2520368.8 and GB2520379.5 as related prior art by the same inventor.

Abstract

A device-based environment attestation mesh generating contextual signatures for identity verification, trust scoring and secure session authorisation. Multiple attestation signals, including environmental variability, device-state proofs, motion characteristics, proximity indicators, thermal patterns and contextual entropy, are sampled, fused and cryptographically bound to authentication events. The system prevents replay, spoofing and cloning by producing context-specific attestation bundles. The mesh integrates with post-quantum key management, behavioural-entropy identity engines and trust-fusion frameworks. Attestation outputs are non-reversible and do not reveal raw contextual data. The invention relates to GB2520368.8, GB2520379.5 and GB2520380.3 by the same inventor.