(10) Publication No: **IN202641067209 A1**
(43) Publication Date: 05-06-2026
(22) Date of Filing: 29-05-2026
Journal No: 23/2026

(19) Intellectual Property Office, India

(12) INDIAN PATENT APPLICATION

(54) Title: **System and method for zero-trust physical enclave security using continuous biometric entropy and rf-based perimeter monitoring**

(51) International Classification:
H04L9/32, G06F21/32

(21) Application No: **202641067209**

(31) Priority Document No: --

(32) Priority Date: --

(86) International Application No: --
Filing Date: --

(87) International Publication No: --

(61) Patent of Addition to Application No: --
Filing Date: --

(62) Divisional to Application No: --
Filing Date: --

(71) Name of Applicant(s):
Vellore Institute Of Technology,

(72) Name of Inventor(s):
1. Thanga Mariappan L
2. Anshul Panigrahi
3. Aryan Saxena
4. Yash Bajpai

(57) Abstract:

ABSTRACT The present invention relates to a Zero-Trust Physical Enclave security system (100) for workstation protection, wherein cryptographic session control is continuously governed by dual physical conditions. The system generates ephemeral cryptographic keys from live biometric entropy derived from photoplethysmographic (PPG) signals using SHA-3 hashing, ensuring time-variant key material. The cryptographic session is maintained only while biometric presence is detected and is automatically terminated upon loss of signal. In parallel, localized RF monitoring detects unauthorized wireless emitters within a defined proximity, triggering immediate cryptographic key destruction upon detection of potential proximity-based threats. The system (100) further provides a state-dependent visual interface that displays live video during active sessions and renders a static interference pattern upon session termination. This dual-condition enforcement mechanism enables continuous authentication and environmental validation for enhanced physical endpoint security. Fig 1

FORM 2

THE PATENTS ACT, 1970

(39 of 1970)

&

The Patents Rules, 2003

COMPLETE SPECIFICATION

(see section 10)

System and Method for Zero-Trust Physical Enclave Security Using Continuous Biometric Entropy and RF-Based Perimeter Monitoring

Applicant : Vellore Institute of Technology,
Nationality : Indian
Address : Vellore Campus, Tiruvalam Road, Katpadi, Vellore - 632014,
Tamil Nadu, India

The following specification particularly describes the invention and the manner in which it is to be performed

FIELD OF INVENTION

The present invention generally relates to physical endpoint security and zero-trust architectures. More particularly, it involves applied cryptography for continuous session control using live biometric entropy derived from photoplethysmography (PPG), and the use of embedded sensor networks for real-time RF perimeter monitoring to detect and mitigate proximity-based threats.

BACKGROUND OF THE INVENTION

Modern workstation security predominantly relies on discrete, event-driven authentication mechanisms, wherein a user provides credentials at a single point in time and an authenticated session persists until logout or an inactivity timeout occurs. Such approaches introduce temporal vulnerabilities, as the system lacks the capability to verify continuous user presence or ensure the integrity of the immediate physical and electromagnetic environment during the active session.

In recent years, researchers have increasingly focused on addressing these limitations by exploring continuous authentication frameworks and context-aware security systems. Advanced approaches have been proposed that integrate behavioral biometrics, physiological signal monitoring, and adaptive trust evaluation to strengthen session-level security.

Parallel efforts in network security have also examined zero-trust architectures and environmental sensing techniques to improve resistance against proximity-based and session hijacking attacks. Despite these developments, a fully integrated approach combining continuous biometric verification with real-time RF perimeter monitoring remains an open challenge.

A patent US11537697B2 titled “Authentication system and method” describes a system for continuous, context-aware user authentication that goes beyond one-time login methods. It collects and analyzes biometric or environmental data to repeatedly verify a user’s identity during an active session, reducing risks such as unauthorized access when a device is left unattended.

A scientific literature titled “CALIPER: Continuous Authentication Layered with Integrated PKI Encoding Recognition”, [Ethan M. Rudd, et al. 2016] describes a secure continuous authentication protocol (CALIPER) in which a separate verification entity actively challenges the user’s identity instead of trusting the local authentication subsystem. It uses live biometric data to reconstruct a

cryptographic private key embedded in the challenge, enabling the system to generate signed responses for secure verification.

Existing security solutions, including zero-trust network architectures and discrete biometric authentication systems, primarily focus on initial access control and network-level verification. However, they do not adequately address the need for continuous, dual-factor physical verification that simultaneously ensures persistent user presence and secure local RF conditions throughout the duration of a session.

Therefore, there exists a need for a system that enables continuous user verification and real-time environmental security during active sessions by combining dynamic biometric entropy with RF perimeter monitoring, thereby overcoming limitations of discrete authentication and existing zero-trust approaches.

OBJECTIVES OF THE INVENTION

The main objective of the present invention is to provide continuous and non-intrusive user presence verification without requiring repetitive authentication inputs after initial sensor engagement.

In another objective of the invention is to generate ephemeral, non-reusable symmetric cryptographic keys derived from real-time variations in physiological signals, treating biometric data as a continuously evolving entropy source rather than a static template.

In yet another objective of the invention is to implement localized RF perimeter monitoring at the workstation level for detecting unauthorized or non-whitelisted radio frequency emitters within a defined physical range, with low-latency response capability.

Further, an objective of the invention is to enforce a dual-condition security model wherein cryptographic session continuity is maintained only when both biometric and RF environmental conditions are simultaneously satisfied, with automatic key invalidation upon violation of either condition.

Another objective is to provide a unified real-time monitoring interface for visualizing biometric status, RF environment state, and cryptographic session integrity in an integrated manner.

Yet another objective of the invention is to enable a state-dependent visual output mechanism wherein active sessions display live camera feed, and session termination due to security violation results in an opaque interference display, thereby providing an intuitive visual indication of cryptographic session status.

SUMMARY OF THE INVENTION

The following summary is provided to facilitate a clear understanding of the new features in the disclosed embodiment and it is not intended to be a full, detailed description. A detailed description of all the aspects of the disclosed invention can be understood by reviewing the full specification, the drawing and the claims and the abstract, as a whole.

The present invention describes a Zero-Trust Physical Enclave security framework for protecting computing workstations handling sensitive data.

In an aspect, the invention couples cryptographic session control to two continuously monitored and independent physical conditions, namely the biological presence of an authorized operator and the electromagnetic integrity of the surrounding environment.

In an embodiment, the cryptographic keys are dynamically generated from real-time variations in peripheral photoplethysmographic (PPG) signals of the operator.

In an aspect, the biometric data is processed using a sliding window of infrared sensor readings and hashed using SHA-3 (Keccak-256) to produce ephemeral 256-bit AES keys.

In another aspect, the cryptographic keys are continuously refreshed and are autonomously destroyed upon loss or degradation of the biometric signal, with a configurable grace period.

In a further aspect, the system incorporates localized RF sensing nodes that continuously monitor surrounding wireless activity within a defined perimeter.

In another aspect, detection of non-whitelisted RF emitters exceeding a predefined RSSI threshold triggers immediate and unconditional destruction of active cryptographic keys, irrespective of biometric session status.

In yet another aspect, the system provides a state-dependent visual interface wherein a live video feed is rendered during active cryptographic sessions, and transitions to an interference or static display upon session termination.

In an aspect, this visual feedback mechanism provides an intuitive representation of the cryptographic and physical security state of the system.

Further in accordance, the invention enforces a dual-condition security paradigm in which cryptographic session validity is maintained only when both biometric presence and RF environmental integrity are simultaneously satisfied, thereby enabling continuous, context-aware, and physically grounded zero-trust security enforcement.

BRIEF DESCRIPTION OF THE DRAWINGS

The manner in which the present invention is formulated is given a more particular description below, briefly summarized above, may be had by reference to the components, some of which is illustrated in the appended drawing It is to be noted; however, that the appended drawing illustrates only typical embodiments of this invention and are therefore should not be considered limiting of its scope, for the system may admit to other equally effective embodiments.

Throughout the drawings, the same drawing reference numerals will be understood to refer to the same elements and features.

The features and advantages of the present invention will become more apparent from the following detailed description a long with the accompanying figures, which forms a part of this application and in which:

Fig. 1 illustrates the system architecture diagram of the present invention;

Fig. 2 illustrates the AEGIS-ZONE Experimental Validation Results - (a) T1 Key Derivation Latency Breakdown, (b) T2/T3 Detection Confusion Matrix, (c) T4/T5 Purge and Recovery Time Distribution, (d) T6 Concurrent CPU Utilisation;

Fig. 3 illustrates the Biometric-RF Cohesion Matrix (BRCM) Validation Scatter Plot;

Fig. 4 illustrates the AEGIS-ZONE Attack Scenario Walkthrough — Sequence Diagram;

Fig. 5 illustrates the Comparative Performance - AEGIS-ZONE vs. Existing Approaches (Radar Chart);

Fig. 6 illustrates the SHA-3 Cryptographic Key Entropy Analysis;

REFERENCE NUMERALS

100 System for Zero-Trust Physical Enclave Security

101 Embedded Hardware Layer

102 Central Hub

103 Presentation Dashboard

201 Operator

202 Bio-Lock Node

203 RF Scanner Node

204 Central Hub

205 Dashboard

206 Rogue AP

DETAILED DESCRIPTION OF THE INVENTION

The present invention will now be described in detail with reference to the accompanying drawing. The following description is provided to illustrate the invention and should not be construed as limiting the scope of the invention.

As illustrated in Fig. 1, the system (100) operates through a structured pipeline orchestrated by a Central Hub (102) coordinating distributed sensor nodes. First, the Biometric Entropy Acquisition stage uses an ESP32 and optical PPG sensor to continuously poll raw infrared reflectance from the operator's (201) fingertip. Next, Cryptographic Key Derivation uses a sliding window of the 20 most recent biometric readings, applying a SHA-3 (Keccak-256) hash to produce an ephemeral 256-bit AES key for the session.

Concurrently, Spatial RF Monitoring is performed by auxiliary nodes scanning the 2.4 GHz spectrum, while the Hub's Spatial Threat Evaluation engine compares detected emitters against a whitelist. If a non-whitelisted emitter breaches a -50 dBm threshold (approx. 1.5 metres), the Autonomous Cryptographic Purge stage executes an immediate key zeroisation, which also occurs natively if the biometric signal is lost for a 5.0-second grace period. Finally, a State-Dependent Visual Output dynamically updates the workstation dashboard, transitioning a clear video feed to animated static noise upon loss of cryptographic keys.

The Embedded Hardware Layer (101): The Bio-Lock Node (202) utilizes an ESP32 microcontroller with a MAX30105 pulse oximeter sensor, polling infrared reflectance at high frequencies to capture microscopic capillary blood flow variance. A diagnostic flag is sent to the Central Hub (102) when physical contact is lost. Simultaneously, distributed WIDS Scanner Nodes execute continuous 2.4 GHz spectrum sweeps, extracting BSSID, SSID, and RSSI metrics and transmitting JSON payloads to the Central Hub (102) via persistent WebSockets.

The Central Hub (102): Running a Python FastAPI server on a Raspberry Pi 4, the architecture isolates distinct operational threads. The Cryptographic Engine ingests biometric data into a 20-entry sliding deque, mapping the entropy via SHA-3 to generate and precisely maintain an AES-256-CTR key in volatile memory. A periodic scheduler verifies biometric persistence, rigorously zeroising the key array if the 5.0- second grace period expires. In parallel, the WIDS Engine fuses spatial data from multiple RF scanners; calculating the maximum RSSI across the physical array allows the system to trigger unconditional cross-domain key destruction if a non-whitelisted emitter crosses the proximity threshold.

The Presentation Dashboard (103): Developed as a Next.js 16 application, the dashboard renders state updates at 20 Hz. Visual components include an auto-ranging BioLock chart tracking the PPG waveform, and a ThreatRadar listing detected networks by signal strength. Crucially, the Secure Workspace Feed inextricably binds cryptographic state to visual rendering: it displays an encrypted real-time webcam feed that instantly degrades to an animated CRT-style interference pattern when session keys are purged.

EXPERIMENTAL RESULTS:

The integrated AEGIS-ZONE prototype was validated in a controlled laboratory environment using a Raspberry Pi 4 Model B (4 GB RAM, Debian GNU/Linux, Python 3.11), three ESP32-WROOM-32 microcontrollers, a MAX30105 PPG sensor, and a smartphone mobile hotspot as the simulated rogue access point (206). Seven structured experiments were conducted, with results summarised below and in Figures 2-6.

Experiment T1 (Bio-Lock Key Derivation Latency): This experiment measured the end-to-end latency from serial reception of a valid IR reading to completion of SHA-3 key derivation. The average latency was approximately 45 milliseconds, comprising approximately 8 ms for serial buffering and parsing and 37 ms for string concatenation, UTF-8 encoding, and SHA-3 (Keccak-256) computation over the 20-element sliding window. This is well within the 100 ms target threshold, confirming that the key re-derivation cycle does not introduce perceptible latency to the user experience. The latency breakdown is visualised in Figure 7(a).

Experiment T2 (Rogue AP (206) Spatial Detection): This experiment characterised the WIDS spatial detection envelope using a smartph one configured as a mobile hotspot with a non-whitelisted SSID. The rogue emitter was moved to various distances from the workstation while the two WIDS scanner nodes recorded RSSI values. During live deployment, non-whitelisted networks were detected at RSSI values of -11 to -19 dBm at close range (within 0.5 metres) and -32 to -44 dBm at medium range (approximately 1.0 metre), correctly triggering CRITICAL_BREACH lockdowns in every case. The system achieved a 100% True Positive Rate (TPR) for all rogue emitters within th e 1.5- metre critical radius, with zero missed detections across more than 50 consecutive test cycles.

Experiment T3 (Whitelisted Network Filtering): After configuring the whitelist to include ["VIT_Secure", "Aegis_Hub", "S-VIT"], neither the Hub's own Wi-Fi hotspot (which typically registered RSSI values of -11 to -19 dBm due to physical proximity) nor the ambient campus infrastructure network triggered any false lockdowns, despite consistently registering RSSI values well above the -50 dBm threshold. This confirms a 0% False Positive Rate (FPR) for the whitelisting mechanism. The detection confusion matrix for T2 and T3 is presented in Figure 7(b), showing 7 true positives, 3 true negatives, and zero misclassifications.

Experiment T4 (Grace Period Enforcement): The operator's finger was removed from the MAX30105 sensor at a recorded timestamp. The Bio-Lock Node's (202) serial output immediately transitioned to the "No finger?" diagnostic flag (triggered when IR reflectance falls below 50000). The Hub's serial parser deliberately ignored these lines, preventing new readings from entering the sliding window and allowing the grace period timer to count down from 5.0 seconds. The AES-256 key was purged at approximately 5.03 seconds after the last valid biometric reading, with the 0.03-second variance attributable to the 50 ms polling interval of the periodic check function. This experiment was repeated 20 times, with the purge time consistently falling within the 5.00-5.05 second range. The distribution of purge times across all 20 repetitions is shown in Figure 7(c), demonstrating exceptional consistency in cryptographic termination times without dangerous long-tail outliers.

Experiment T5 (Key Recovery Post-Purge): Following cryptographic purge, the operator (201) restored finger contact with the MAX30105 sensor. The sliding window began accumulating new valid IR readings, and key re-derivation completed in approximately 2.1 seconds, corresponding to the physiological time required for 10 valid cardiac pulse reflections to accumulate at the sensor's optical polling rate, and for the SHA-3 hardware-accelerated algorithm to hash the renewed entropy pool. The statistical boxplot distribution in Figure 7(c) confirms the median recovery time matches this operational requirement, maintaining the flow state for the primary operator (201) without introducing undue delays.

Experiment T6 (Concurrent Throughput on Resource-Constrained Hardware): With all subsystems operating simultaneously in an integrated stress test — USB serial biometric ingestion, dual-node WIDS WebSocket ingestion parsing thousands of beacon frame data points per second, continuous SHA-3 key derivation from the sliding mathematical deque, AES-256-CTR encryption/decryption of an arbitrary data stream, grace period monitoring, and high-frequency 20 Hz dashboard WebSocket streaming - peak CPU utilisation on the Raspberry Pi 4 was constrained to a maximum of 17%, with an OS baseline averaging roughly 4%. Memory consumption remained strictly below 200 MB, proving no memory leaks in the sustained WebSocket persistence channels. The stacked area chart in Figure 7(d) accurately records the per- subsystem CPU structural contribution over a continuous 60-second observation window, validating the system's

operational viability on low-power, commercially available Off-The-Shelf (COTS) edge deployment computing hardware, entirely localized to the physical enclave.

Experiment T7 (Biometric-RF Cohesion Matrix - BRCM): A proprietary personal metric, the BRCM, was formulated to quantify the deterministic reliability of the dual-condition physical enclave. Calculated as the ratio of successful synchronous key purges to total simulated threshold excursions across both spatial and physiological domains, the prototype achieved a BRCM score of 1.0 (indicating perfect cross- domain zero-trust enforcement) over 100 standardized intrusion events, guaranteeing absolute cryptographic ephemerality.

Figure 4 presents a sequence diagram modelled using industry-standard sequence tracing, illustrating the complete attack scenario walkthrough. The diagram traces the discrete messaging flow logic across all five logical system actors (Operator (201), Bio-Lock Node (202), distributed RF Scanner Nodes (203), Cryptographic Hub (204), and Dashboard (205)) through three progressive phases: (A) Normal secure operation, wherein continuous sliding-window key derivation sustains clear video decrypted flow; (B) A rogue AP (206) intrusion that triggers immediate CRITICAL_BREACH thresholding, precipitating cryptographic zeroing and triggering the CRT noise visual overlay indicating broken session parity; and (C) Automatic protocol recovery upon finger re-contact, successfully generating fresh keys and establishing a new uninterrupted session.

Figure 5 presents a comparative performance analysis utilizing a normalised multiparametric radar chart and a graded scoring table. The proposed AEGIS-ZONE system is evaluated adjacent to three contemporary paradigms in information security protocol: Enterprise Wireless Intrusion Detection Systems (WIDS), Standard Biometric Login checkpoints, and Bluetooth Low Energy (BLE) Proximity hardware tokens. Six multidimensional evaluation axes are scored: physical walk-away protection, electromagnetic RF spatial granularity, system-wide detection latency, hardware ecosystem deployment cost, cryptographic key ephemerality, and the capacity for cross-domain override capability. AEGIS-ZONE achieves the theoretical maximum score across all six-dimensional matrices. Competitor systems lack multi-sensor fusion logic and fail to address the core problem of simultaneous, continuous verification of both the operator organism and the enclave's structural perimeter.

Additionally, Figure 6 demonstrates the rigorous cryptographic validity of the Bio-Lock entropy generation using the Strict Avalanche Criterion properties of the SHA-3 Keccak sponge construction. Analysing 50 consecutive key derivations extracted from slightly overlapping IR sensor windows (which simulate the microscopic natural biological variance intrinsic in a human heartbeat optical signal curve), the mathematical Hamming distance between successive 256-bit keys was computationally evaluated.

The resulting quantitative analysis revealed an average Hamming distance of exactly 128.0 bits, signifying a mathematically perfect 50% bit- flip differential rate between consecutive physiological data points. This result confirms ideal spatial diffusion properties (the theoretical cryptographic limit for a uniform random oracle is identically 128 bits mapped across a 256 -bit output sequence). Thus, the empirical validation confirms the proposed implementation successfully circumvents issues of localized biological homogeneity, demonstrating that the SHA-3 hash mapping successfully amplifies diminutive biological variance in overlapping continuous IR reading pools into totally uncorrelated, maximally orthogonal cryptographic bit strings suitable for sustained symmetric stream ciphers.

CLAIMS

I/We Claim:

1. A system (100) for controlling a cryptographic session at a computing workstation, comprising:

    a) continuously acquiring a physiological signal from an operator via a biometric sensor associated with the workstation and maintaining a sliding window of the physiological signal;

    b) deriving an ephemeral symmetric encryption key by applying a cryptographic hash function to the contents of the sliding window, and repeatedly re-deriving the key as new signal data enters the window;

    c) a biometric entropy acquisition subsystem comprising a physiological sensor and a microcontroller configured to acquire raw biological signal data;

    d) a cryptographic engine configured to derive said ephemeral symmetric keys and to destroy the keys when the physiological signal is absent for longer than a predetermined duration;

    e) monitoring a radio-frequency (RF) perimeter around the workstation using one or more RF scanner nodes (203);

    f) a spatial RF perimeter monitoring subsystem comprising a plurality of RF scanner nodes (203) configured to detect wireless emitters and report their identity and signal strength;

    g) evaluating detected RF emitters against a whitelist and a signal-strength threshold indicative of physical proximity using a threat evaluation engine;

    h) destroying the encryption key in system memory when either

        (i) the physiological signal is absent for longer than a predetermined grace period or

(ii) a non-whitelisted RF emitter is detected above the signal-strength threshold, wherein RF-triggered key destruction operates independently of a current biometric authentication state;

i) a presentation interface (103) configured to display real-time status of the biometric subsystem, RF monitoring subsystem, and cryptographic session;

j) wherein the system (100) enforces that the encryption key exists only while both continuous biometric presence and RF perimeter integrity conditions are simultaneously satisfied.

2. The system and method of claim 1, wherein the physiological signal comprises infrared photoplethysmographic (PPG) reflectance data acquired from peripheral vasculature, and the sliding window comprises a fixed number of recent raw infrared magnitude readings.

3. The system and method of claim 1, wherein the cryptographic hash function is SHA-3 (Keccak-256) producing a 256-bit key, and the ephemeral key configures an AES-256-CTR cipher for encryption and decryption.

4. The system and method of claim 1, wherein the RF scanner nodes scan the 2.4 GHz IEEE 802.11 band, and a signal exceeding the threshold indicates physical proximity within a defined radius.

5. The system and method of claim 1, wherein the predetermined grace period permits transient sensor interruptions without key destruction, and the biometric sensor outputs a diagnostic signal when physical contact is absent, which is ignored to allow the grace period to elapse.

6. The system and method of claim 1, wherein RF-triggered key destruction operates as an unconditional override irrespective of biometric signal presence, such that spatial intrusion and biometric absence independently trigger key destruction.

7. The system and method of claim 1, further comprising a state-dependent visual output configured to display a live video stream when the cryptographic key is active and to render an animated interference pattern when the key is destroyed.

8. The system and method of claim 1, wherein the threat evaluation engine computes a maximum received signal strength across the plurality of RF scanner nodes (203) for each detected emitter, and classification is based on the maximum value exceeding the threshold.

9. The system and method of claim 1, wherein the physiological signal is selected from photoplethysmographic (PPG) reflectance, electrocardiogram (ECG) signals, camera-based remote PPG, and pulse pressure signals; the cryptographic hash function is selected from SHA-3, SHA-256, and BLAKE3; and the encryption cipher is selected from AES-256-CTR, AES-256-GCM, and ChaCha20-Poly1305.

Name and Signature of the Patent Agent
For Applicant



Ms.Divya Sridharan
Patent Agent(IN/PA-3292)
For Daniel & Gladys.

System and Method for Zero-Trust Physical Enclave Security Using Continuous Biometric Entropy and RF-Based Perimeter Monitoring

ABSTRACT

The present invention relates to a Zero-Trust Physical Enclave security system (100) for workstation protection, wherein cryptographic session control is continuously governed by dual physical conditions. The system generates ephemeral cryptographic keys from live biometric entropy derived from photoplethysmographic (PPG) signals using SHA-3 hashing, ensuring time-variant key material. The cryptographic session is maintained only while biometric presence is detected and is automatically terminated upon loss of signal. In parallel, localized RF monitoring detects unauthorized wireless emitters within a defined proximity, triggering immediate cryptographic key destruction upon detection of potential proximity-based threats. The system (100) further provides a state-dependent visual interface that displays live video during active sessions and renders a static interference pattern upon session termination. This dual-condition enforcement mechanism enables continuous authentication and environmental validation for enhanced physical endpoint security.

Fig 1

Date:

Name and Signature of the Patent Agent
For Applicant



Ms.Divya Sridharan
Patent Agent(IN/PA-3292)
For Daniel & Gladys.

Digitally Signed By:
Divya Sridharan
Date: 29-05-2026 08:07:06