Invention Disclosure Details

1. APPLICANT & INVENTOR DETAILS

Name	Department / Address
Mahi Suchandra	Department of Computer Science & Engineering, Manipal University Jaipur, Jaipur, Rajasthan, India.
Vedica Saini	Department of Computer Science & Engineering, Manipal University Jaipur, Jaipur, Rajasthan, India.

---

2. DISCLOSURE STATUS

Details of the publication/communication/exhibition in which the invention was disclosed before patent filing: Response: NO

---

3. TITLE

SentriMat: An IoT-Enabled System for Package Security via Dynamic Force-Signature Analysis

---

4. ABSTRACT

In this patent application, we propose the design and implementation of **SentriMat**, an intelligent, privacy-compliant package security system. The system integrates a 4-channel force-sensitive resistor (FSR) matrix with an ESP32 microcontroller to capture high-frequency "Force-Signatures" during package delivery. Utilizing an edge-computing framework, the system ensures precise detection of impact momentum and spatial center of pressure (CoP) to identify tampering in real-time. Unlike traditional optical surveillance, this system treats delivery as a haptic biometric event, providing automated logging in CSV format and instant mobile alerts via an IoT gateway. The configuration offers a robust, cost-effective, and privacy-first solution for residential and industrial "Last-Mile" delivery security.

---

5. PROBLEM SOLVED BY THE INVENTION

a. Problem the invention is solving:

SentriMat addresses critical gaps in traditional "Last-Mile" logistics and home security:

1. **Reactive vs. Proactive Security:** Existing cameras only record theft after it occurs; SentriMat detects tampering the moment the package is touched via CoP shifts.
2. **False Alarm Mitigation:** Standard weight mats fail to distinguish between wind, pets, and packages. SentriMat uses impact momentum profiling to verify object types.
3. **Privacy Concerns:** Cameras are intrusive and face heavy GDPR/DPDPA regulatory hurdles. SentriMat provides 24/7 monitoring without capturing any visual or identifiable personal data.
4. **Automated Verification:** Eliminates manual delivery logging by automatically generating time-stamped security logs for long-term trend analysis.

b. General Utility/Application:

- **E-Commerce Sector:** Prevents "Porch Piracy" by triggering local deterrents and remote notifications during unauthorized retrieval.
- **Pharmaceutical Logistics:** Ensures high-value, sensitive medical supplies are monitored for handling and tampering during the final delivery stage.
- **Smart Residential Infrastructure:** Integrates with smart-home ecosystems to provide non-intrusive security for apartment complexes and gated communities.

---

6. ADVANTAGES OF THE INVENTION

- **Automation:** Reduces human error through automated "Impact Handshake" authentication and cloud logging.
- **Privacy by Design:** Full compliance with global data protection standards (GDPR/DPDPA) by avoiding optical sensors.
- **High Sensitivity:** Detects subtle tampering (tilting/sliding) using a 4-point differential pressure matrix.
- **Cost-Efficiency:** Utilizes low-cost embedded components (ESP32, FSRs) to provide enterprise-grade security at a consumer price point.
- **Dual-Factor Verification:** Unique retrieval logic requiring both a physical footprint signature and a digital mobile token.

---

7. SALIENT FEATURES (Unique Selling Points)

1. **Haptic Biometrics:** Treats the physical placement of a box as a unique, verifiable force signature.
2. **Spatial Center of Pressure (CoP) Tracking:** Real-time (x, y) coordinate monitoring of the package's center of gravity.
3. **Edge Processing:** ESP32 performs 100Hz high-speed sampling to filter environmental noise locally before cloud transmission.
4. **Zero-Vision Security:** Operates in total darkness and through environmental obstructions without losing efficacy.

---

8. CLAIMS

- **Claim 1:** A method for **Real-Time Force-Signature Authentication** that samples contact force at 100Hz to distinguish parcel delivery from environmental noise.
- **Claim 2:** A system for **Spatial Tamper Detection** utilizing a 4-channel sensor matrix to monitor Center of Pressure (CoP) shifts of a static load.
- **Claim 3:** A **Sequence-Dependent Retrieval Logic** that differentiates between authorized removal and theft based on the proximity of a human footprint signature.
- **Claim 4:** A **Privacy-First Security Framework** that provides mechanical verification of delivery events without the use of optical sensors or identifiable biometric imaging.

---

9. METHODOLOGY & RESULTS

1. **System Design:** Physical assembly of a 4-sensor FSR matrix between rigid plates (Sensor Sandwich) interfaced with an ESP32.
2. **Algorithm Implementation:** Development of the **Sequence Verification Algorithm (SVA)** to manage state transitions.
3. **Testing & Results:** The system successfully distinguished between delivery events (0.5kg–5kg) and environmental disturbances with high accuracy. Tamper alerts were successfully triggered within 500ms of Center of Pressure displacement.

---

10. FUTURE DEVELOPMENT

- **AI Integration:** Utilizing Random Forest or Neural Networks to improve object classification accuracy.
- **Energy Harvesting:** Implementing piezoelectric layers to power the system through the weight of the delivery itself.
- **Smart Locker Integration:** Adapting the mat for use inside secure delivery lockers to verify parcel dimensions and weight automatically.

---

11. FIGURES / DIAGRAMS

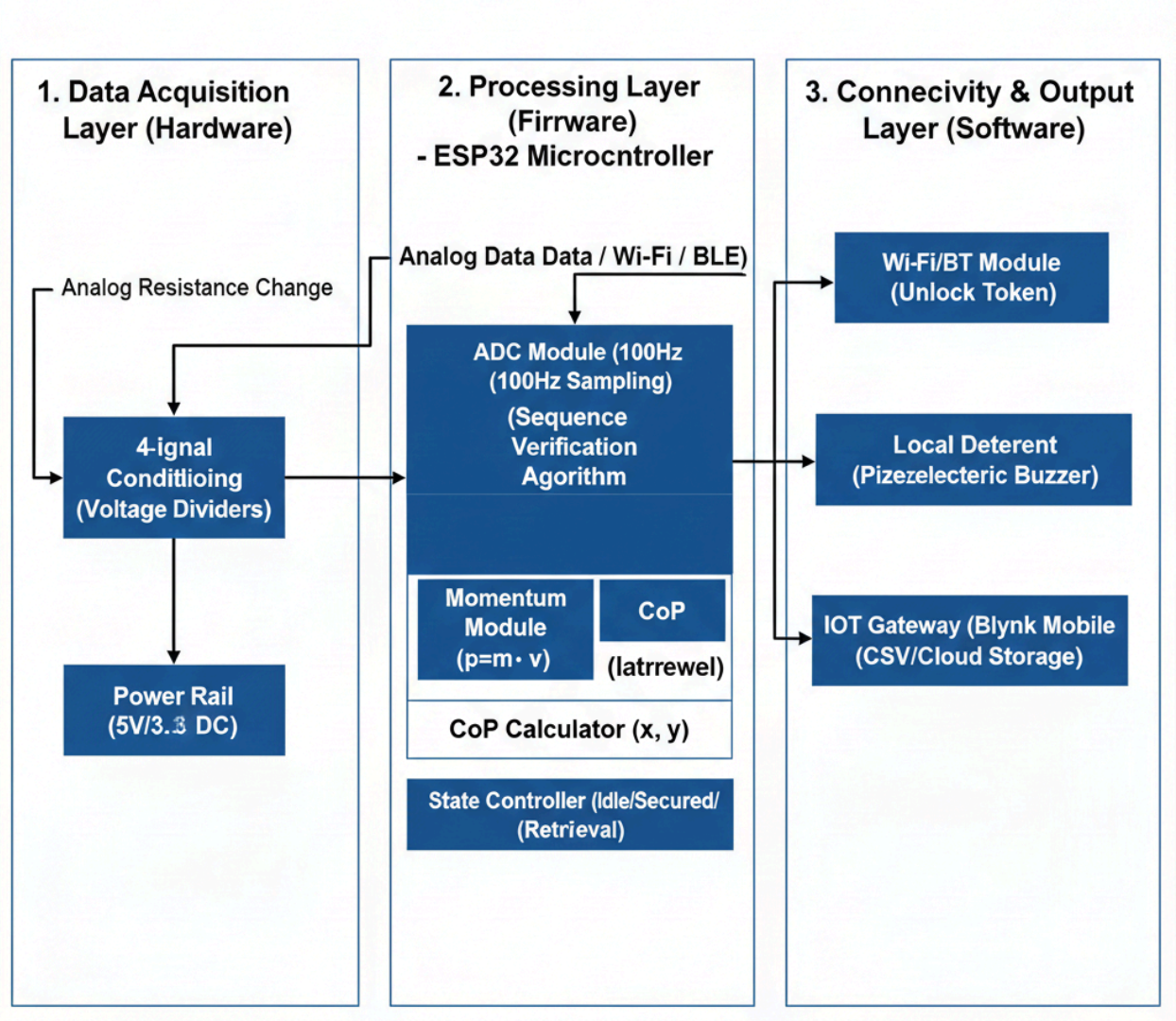

Figure 1: Architectural Framework of the SentriMat Intelligent Security System.

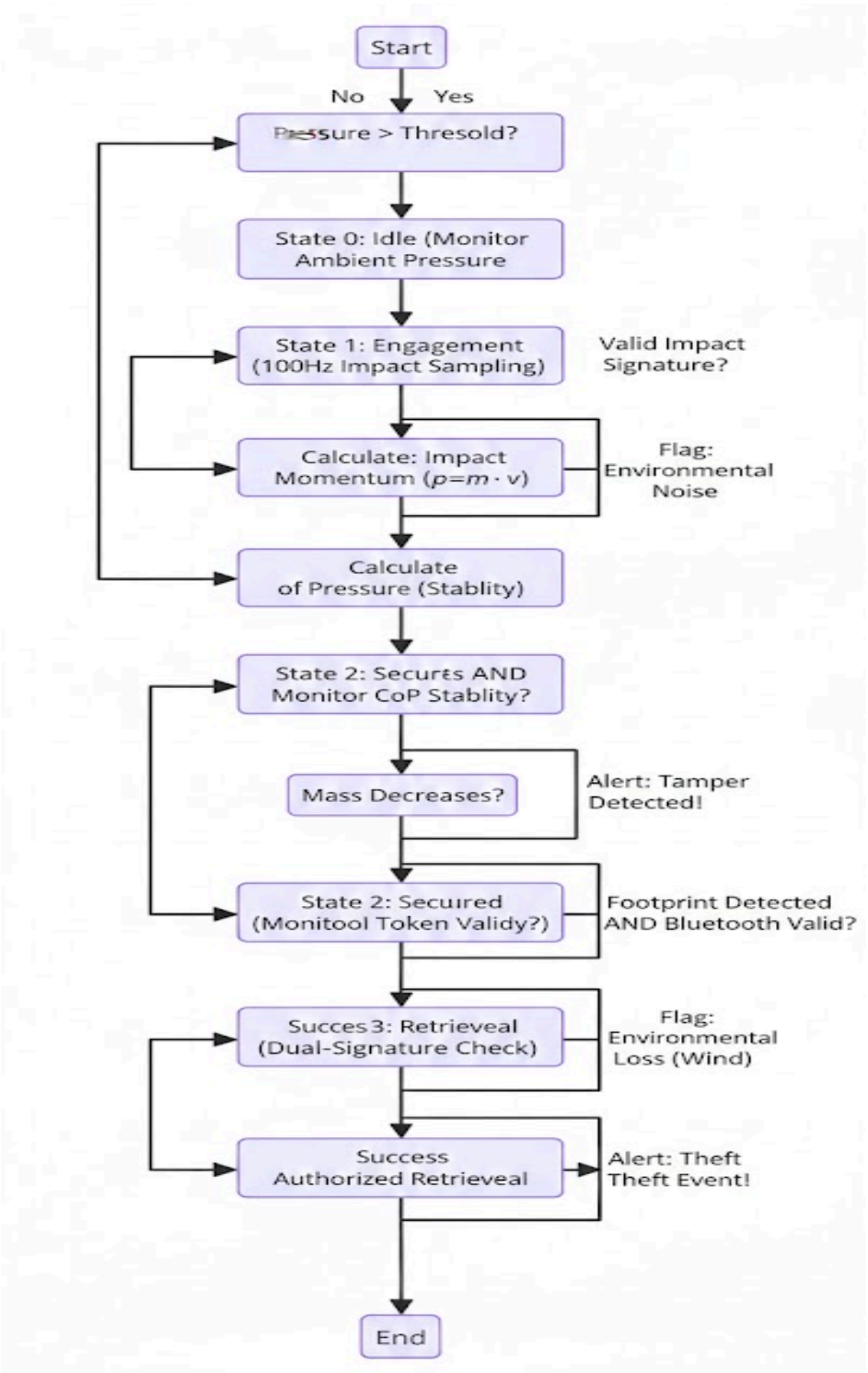

Figure 2: Flowchart of the Sequence Verification Algorithm (SVA).