Smart Anti-Theft Bag: Design and Implementation of a Dual-Sensor Latching Security System Using Arduino

Jarold Jan Silverio[1], Kevin Timothy Doniza[2], Gian Carlo G. Onia[3], Regine Libongcogon[4], Ronnie Bas[5], Minerva C. Zoleta[6]

Computer Engineering Department, Eulogio "Amang" Rodriguez Institute of Science and Technology, Nagtahan, Sampaloc, Manila, 1016 Philippines

DOI: https://doi.org/10.47772/IJRISS.2026.10100210

Received: 18 January 2026; Accepted: 24 January 2026; Published: 31 January 2026

ABSTRACT

The successful safeguarding of individual property against not only unobtrusive intrusion, but also aggressive dispossession, is a root requirement to commuter security in the swiftly developing environment of the modern transit systems. Conventional security systems like padlocks are the common ones; however, this system is passive and does not give an immediate notification to the owner at the most crucial stages of the theft attempt. As a result, intelligent and automated personal security systems development is highly demanded. The current paper describes the design, production, and implementation of a low-cost and automated anti-theft bag, which is specifically designed to help in reducing the cases of pick pocketing and snatching. The project will attempt to emulate commercial capabilities of security solutions and combine the ideas of sensor fusion, kinetic monitoring, and embedded system control into a wearable form factor.

The Arduino Nano microcontroller is the core element of the system architecture as it is the main processing unit. It uses a dual-sensor system with an interlocking reed switch that detects zipper violations, and an SW-420 vibration sensor that reacts to violent movement that can serve as an indicator of snatching; the latter has a variable sensitivity potentiometer to reduce false alarms due to normal walking. The security system is actuated by using a dual-feedback system with a high-decibel piezo buzzer as an acoustic deterrent and high-intensity LED to indicate the status. The control software is a finite state machine (FSM) with the logic of a Smarts Latch, Wiggle Filtering to eliminate spurious activations, and manual reset hardware interrupt routines. Practical confirmation The experimentally determined detection accuracy is 100 per cent with sensor thresholds suitably adjusted.

To conclude, this project illustrates that a practical implementation of robotics and computer programming can be used to develop wearable technology and it is conclusive that highly challenging security problems can be effectively modeled with the help of affordable, easily accessible hardware.

Keywords: Arduino Nano, SW-420, Reed Switch, Smart Latch, Embedded Systems

INTRODUCTION

The modern environment is currently in the extreme shift to the Industry 4.0 paradigm, in which smart physical systems replace traditional manual monitoring strategies. Particularly, the shift is significant in the area of personal security, where urbanisation and crowd density cause personal artefacts to be a necessity instead of a want. Historically, security of the personal belongings has been relying on menial guarding or other dormant protection like padlocks. However, human physiological aspects always limit manual monitoring; the experimental findings suggest that the error rates in the visual inspection task and alertness are between twenty and thirty percent, which can often be explained by fatigue, distraction, and cognitive drift. Similar to the bottleneck of throughput in manual sorting of bags in industry, human awareness bag security is also a safety consideration that increases the likelihood of successful theft, especially in cases of both a slash-and-grab and pickpocketing whereby the victim does not notice the theft until it is too late.

There is a sharp disparity between the expensive security systems that are utilized in the automotive or industrial environments and the low cost solutions that are currently offered in the personal wearable market.

ISSN No. 2454-6186 | DOI: 10.47772/IJRISS | Volume X Issue I January 2026

The current consumer bag alarm systems are either too passive or lack strong logic capabilities; they are crippled by the absence of an automatic protection system and live lockout indicators. One of the most obvious engineering shortcomings of most primitive alarms is the lack of so-called latching memory, in which in case an assailant would quickly close the bag or stop the movement the alarm would turn off, thus allowing the criminal to escape. This lack of automated monitoring and decision-making is one of the reasons behind avoidable losses. Furthermore, many existing systems do not offer sensor fusion necessary to differentiate between normal handling (e.g. walking) and bona fide threats (e.g. snatching), hence creating a gap in terms of offering a useful platform with which to design an effective pre-deployment or anti-theft protection mechanism.

This gap is attempted to be addressed by the current project, the Smart Anti-Theft Bag, which aims to create a very small prototype at a low cost to achieve the features of an industrial safety control system. The main goal of this project is to design and develop an embedded system that will be automated and capable of isolating, analysing, and latching an illegal zipper motion or significant kinetic energy. The system uses an Arduino Nano, an interlocking reed switch, and an SW-420 vibration sensor by building on the principles of the Embedded Systems Theory, which argues that microcontroller-based devices are designed to perform specific, real-time functions. This setup demonstrates how complicated safety operations could be effectively modelled using existing, affordable hardware, thus guaranteeing real-time automation and fast response to safety.

REVIEW OF RELEVANT THEORY, STUDIES, AND LITERATURE

Sensor Based Security Systems

Studies on automated security systems have placed heavy emphasis on the importance of non-contact sensing in improving efficiency and reliability. Similar to the application of ultrasonic sensors in the accurate measurement of liquids, magnetic sensors like Reed Switches will be essential in the proximity sensing of wearable security systems where wear is not desired. According to empirical research, traditional mechanical switches often do not work in fabric-related settings due to motion and abrasion. The use of non-contact magnetic sensing which is the case in the current investigation helps to alleviate these weaknesses in that the detection methodology is hermetically sealed and it is beyond the environmental corrosion effects, thus justifying the choice of the Reed Switch in interlocking zipper mechanism.

Vibration Sensing and Motion Analysis

Accurate motion detection is a crucial aspect of active security. Although primitive designs use analog tilt switches, such sensors can easily be tripped by slight vibrations. The SW-420 Vibration Sensor module has a digital option that has tunable sensitivity, allowing definition between allowable motion (such as walking) and threat motion (such as snatching). This method is similar to the implementation of RGB cameras with IR blocking filters in order to reduce spectral noise in optical sorting machines. Calibration of sensor thresholds by the system also improves accuracy of detection and reduces the occurrence of false alarms and only in response to actual high-force events the alarm is triggered.

Latching Logic and Human Reliability

Human error is a weak aspect in manual security monitoring. According to Drury and Fox (1975), the error rate was associated with fatigue and loss of attention, which ranged from 20% to 30% in a quality-control situation. In the sphere of bag security, there is a tendency to overlook a small violation with a zipper. In addition, simple alarm systems do not usually have state retention, and stop working immediately the trigger is disconnected. The current paper presents a Smart Latch algorithm (similar to the dry-run protection logic used in pump mechanisms) that keeps the alarm on until a manual switch is done, which prevents the assailant from trying to hide the fact of a break-in.

Table 1. Comparison Matrix of Related Studies and Current Research

Technology/Study	**Sensor Used**	**Controller**	**Security Method**	**Accuracy**	**Key Limitations**
Traditional Padlock	N/A	N/A	Physical	N/A	**Passive**: No

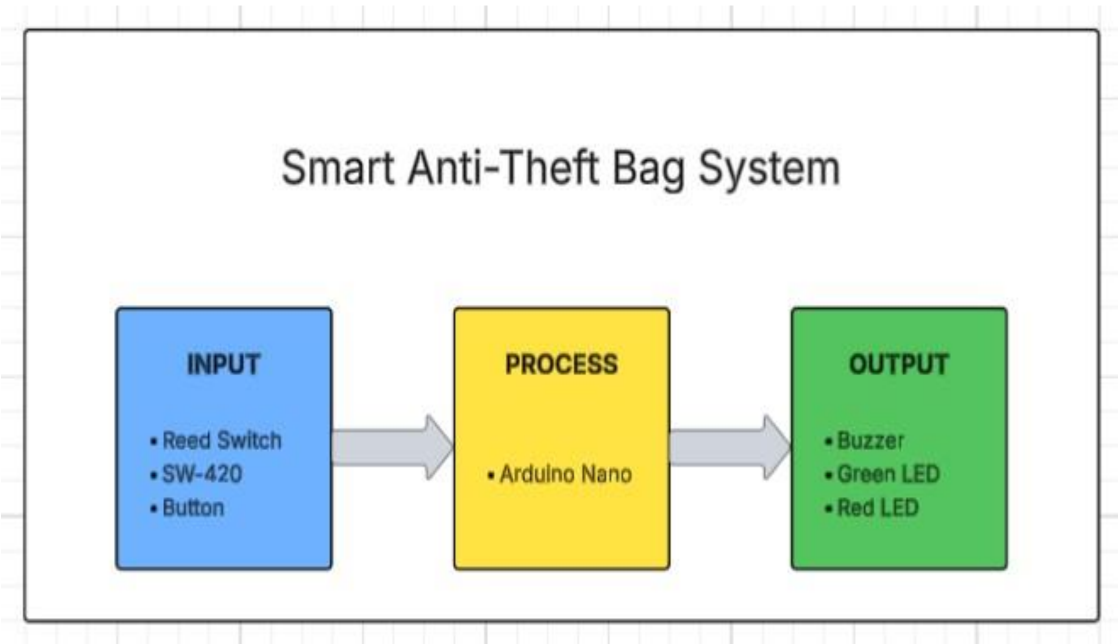
ISSN No. 2454-6186 | DOI: 10.47772/IJRISS | Volume X Issue I January 2026

			Barrier		active alert
Bluetooth Trackers	GPS/BLE	Smartphone App	Location Tracking	High (GPS)	**Reactive**: Only useful after the item is stolen; does not prevent theft
Basic Bag Alarms	Mechanical Switch	Analog Circuit	Instant Sound	~70%	**No Latching**: Alarms stops if bag is reclosed; high false alarm rate
Current Research	Reed Switch + SW-420	Arduino Nano	Smart Latch + Sensor Fusion	~100%	**Battery Dependent**: System requires active power to function

THEORETICAL FRAMEWORK

The theoretical framework that guides this investigation is built based on the principle concepts of embedded systems, sensor-based automation and formalism of Finite State Machine (FSM) control. The device architecture also uses an arduino Nano as the core controller, which is charged with the real-time processing of the input such as the signals picked by a Reed Switch, the functioning of which is determined by the law of magnetic field theory. Using an FSM approach, the system defines discrete operational states, i.e., Standby (Safe), Trigger (Breach), and Latch (Alarm) such that a state transition between them takes place in a strictly disciplined way. Also, the ideas of Human-Computer Interaction (HCI) theory are incorporated through a feedback system using green LED that allows end-users to physically confirm that the equipment has been armed properly before leaving the space.

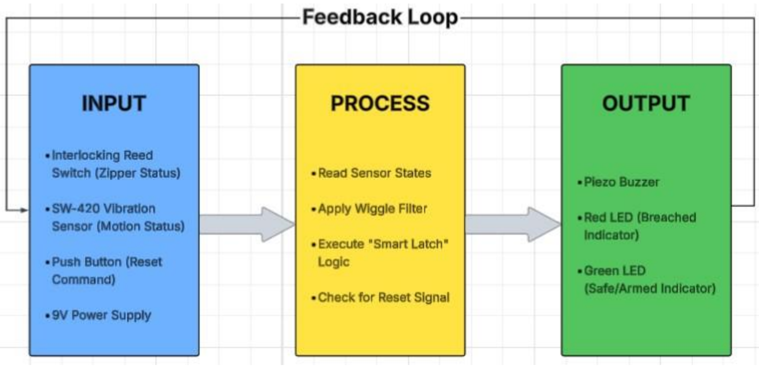
Figure 1. Systems Theory Diagram



INTERNATIONAL JOURNAL OF RESEARCH AND INNOVATION IN SOCIAL SCIENCE (IJRISS)
ISSN No. 2454-6186 | DOI: 10.47772/IJRISS | Volume X Issue I January 2026

The Systems Theory (Von Bertalanffy, 1968) assumes that complex systems work based on interrelation of mutually dependent parts that together achieve a common goal. In the Smart Anti-Theft Bag (Figure 1), there are separate subsystems of the Reed switch, SW-420 vibration sensor, Arduino controller, buzzer, and LEDs. Though each of the components performs a designated role, adequate security behavior becomes evident when all the subsystems work in harmony.

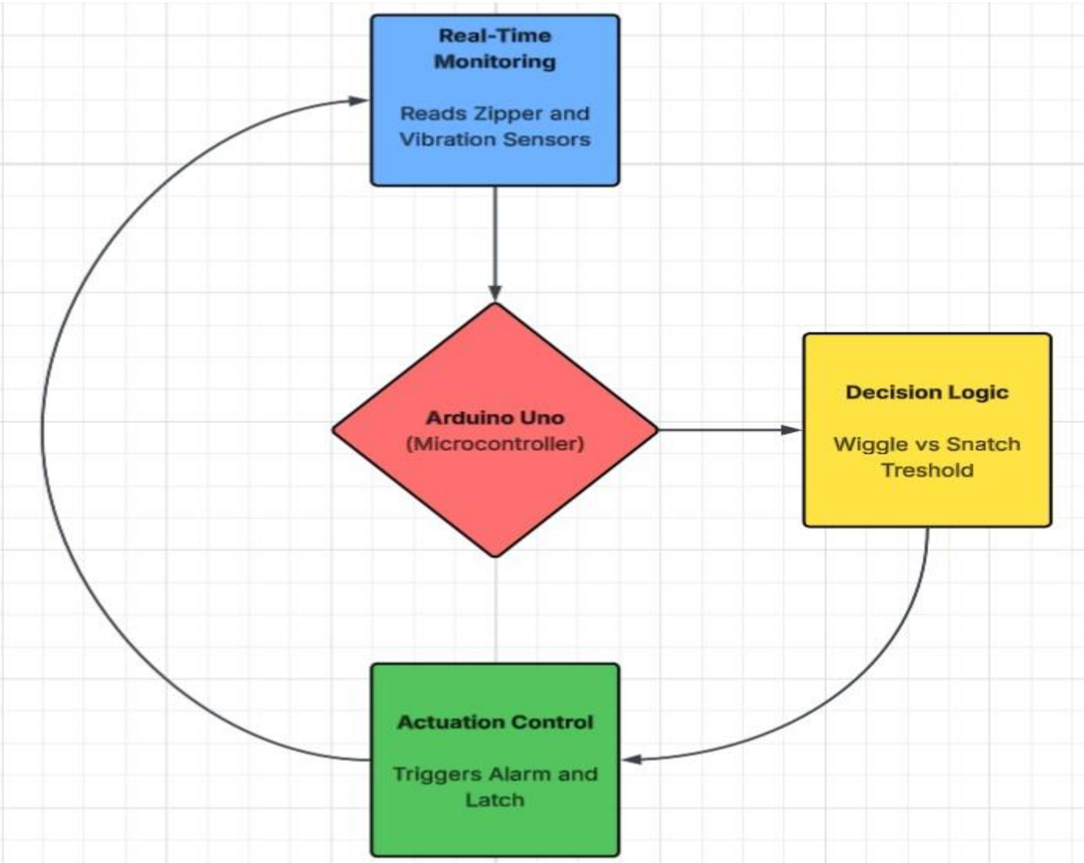
Figure 2. Input-Process-Output (IPO) Model



The Input-Process-Output (IPO) Model describes the functional flow of the system.

- **Input Stage:** The Reed Switch detects zipper integrity, while the SW-420 measures kinetic force. The Push Button detects user reset requests.
- **Process Stage:** The Arduino evaluates sensor states against the "Wiggle Filter" (300ms delay) and "Snatch Threshold," executes the Latching Logic, and determines if the alarm should be triggered.
- **Output Stage:** The Buzzer activates to deter theft, the Red LED signals a breach, and the Green LED indicates a safe/armed state.

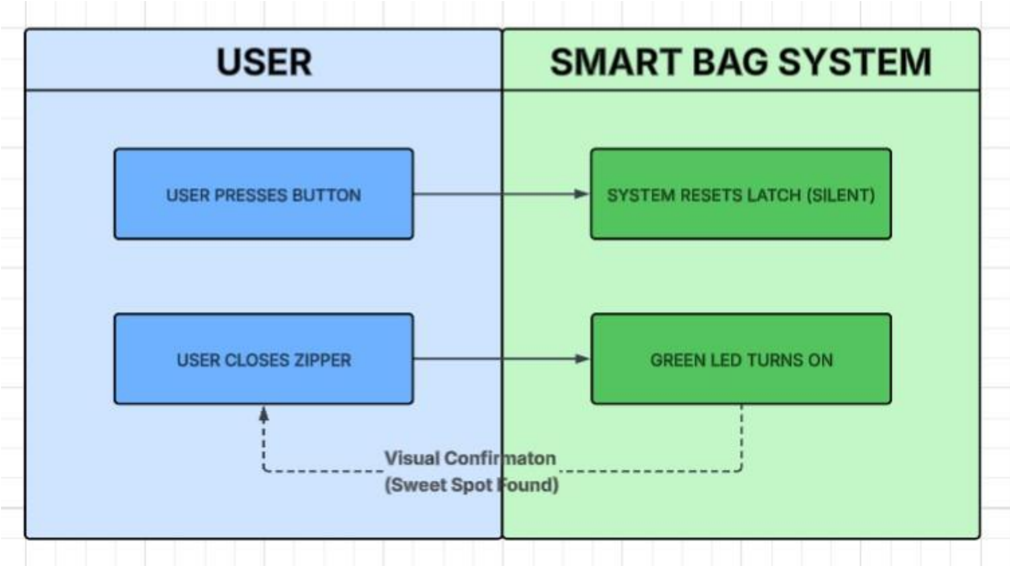
Figure 3. Embedded Systems Theory Diagram



ISSN No. 2454-6186 | DOI: 10.47772/IJRISS | Volume X Issue I January 2026

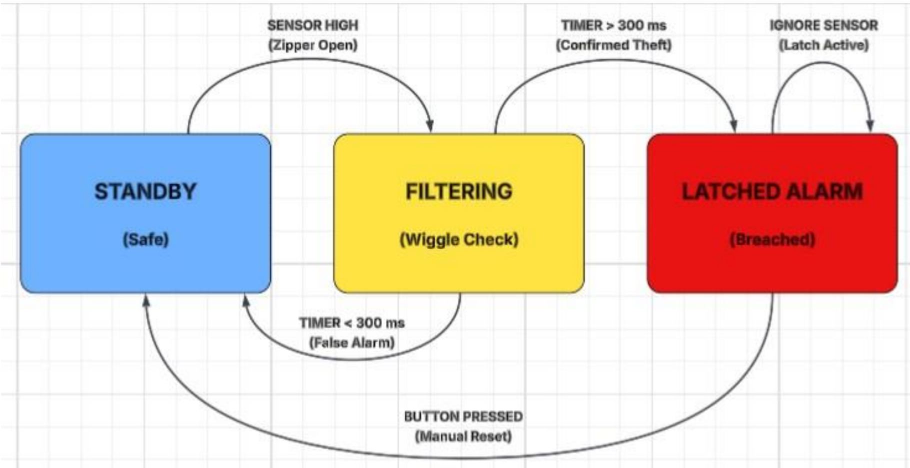
The Embedded Systems Theory implies that devices that are powered by microcontrollers are designed to perform pre-specified time-constrained tasks. Under the current study, the Arduino is utilized as an embedded platform to continuously read sensor inputs, evaluate logical conditions and toggle solenoids with time-intensive reactivity to ensure immediate security responses.

Figure 4. Human-Computer Interaction (HCI) Diagram



The Human-Computer Interaction (HCI) Theory (Dix et al., 2004) implies that usability and intuitive design are considered to be the primary goals . The Smart Anti-Theft Bag reflects such principles by the use of a Live Feedback feature. To reduce the impact of magnetic hysteresis (also known as the Gap Trap) a green LED is used to give real-time confirmation of the alignment of the magnet. These interface features minimize user error when arming the device and therefore improve the overall usability of the device.

Figure 5. Finite State Machine (FSM) Theory Diagram



Finite State Machine (FSM) theory is a formal system, which defines systems that can be in any of a finite set of stable states (also known as states) at any one moment in time. This theoretical principle is applied in the Smart Anti-Theft Bag in the logic of the Smart Latch. The system is subjected to changes of three different states: Standby (Monitoring), Filtering (Verifying Input Duration), and Latched Alarm (Active Deterrence). FSM theory does not, contrasting with elementary input-output architectures, give the system memory of an event of breach, a condition that keeps the alarm in the Latched state even with the sensor input restored to nominal conditions (e.g. when a thief closes the bag), and requires a manual reset procedure to restore to Standby.

ISSN No. 2454-6186 | DOI: 10.47772/IJRISS | Volume X Issue I January 2026

METHODOLOGY

System Architecture

The system architecture is further divided into three orthogonal subsystems: Interlocking Sensor Module, Kinetic Sensing Module and the Control Unit. The processing unit includes an Arduino Nano that receives digital packets as a result of sensor activity and then performs the calculations of the received data. Kinetic discrimination is made easier using an SW-420 Vibration Sensor. Unlike the primitive tilt switches, this module has a sensitivity potentiometer, thus smoothing out false activations caused by pedestrian movement, and thus improving the accuracy of the theft detection.

Figure 6. Key Electronic Components (Arduino Nano, SW-420 Vibration Sensor, Reed Switch)

Sensing Module

Making of the sensing module detection is done with the help of interlocking reed switch and the SW-420 sensor. These sensors form the communication with the microcontroller using digital input/output pins D2 and D4. The SW 420 uses an LM393 comparator to produce a discrete digital HIGH/LOW signal only when the vibration that is detected exceeds a set threshold. The reed switch is mounted on Zipper Puller A and the magnet on Zipper Puller B thus ensuring that the circuit completes only when the bag is fully closed.

Figure 7. Key Sensing Components: Interlocking Reed Switch and SW-420 Vibration Module

Hardware Implementation

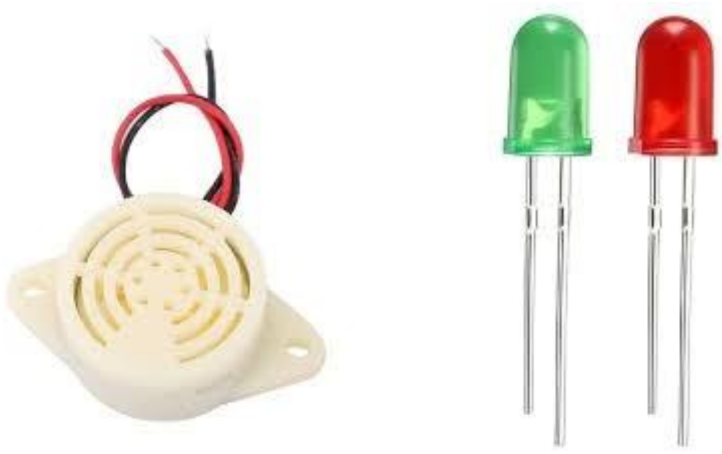
The hardware design takes on a high value of both electrical stability and robustness. In the power distribution system, the supply rails are controlled so as to reduce voltage drops. The power block contains a 9V battery attached to the Arduino VIN pin, which prevents voltage drop with activating the buzzer, causing microcontroller resets otherwise. The ground block provides a common reference potential to all the circuitry and thus ensures unwanted signal drift is avoided.

Actuation System

The actuation system utilizes a high-decibel Piezo Buzzer and dual-color LEDs. The Buzzer is driven by a digital HIGH signal to produce the deterrent sound. The Green and Red LEDs provide immediate visual feedback on the system's Finite State Machine status (Safe vs. Breached).

ISSN No. 2454-6186 | DOI: 10.47772/IJRISS | Volume X Issue I January 2026

Figure 8. Green/Red LED and Piezo Buzzer for Alert System (Safe/Breached)



Software Algorithm Control software is programmed based on a finite state machine implementation.

1. **Standby State:** The system monitors the connection between Zipper A and B and the vibration status. If connected (LOW), the Green LED is lit.

2. **Filtering State:** If the zippers separate (HIGH), the code waits 300ms to filter out minor vibrations ("Wiggles").

3. **Alarm State (Latching):** If the zippers remain separated OR if the SW-420 detects violent shaking, the system enters the Alarm State. The Buzzer and Red LED are latched HIGH. This state ignores the sensor input (even if zippers are re-closed).

4. **Reset State:** The system remains in Alarm State until the Push Button is pressed.

Figure 9. Concept Diagram

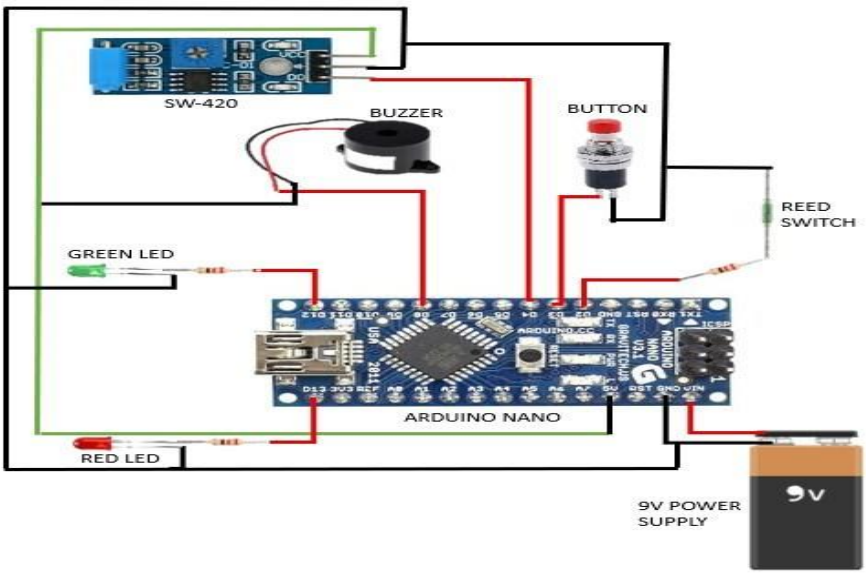


Figure 9 illustrates the circuit integration of the Smart Anti-Theft Bag, centered on an Arduino Nano powered by a 9V battery via the VIN pin. The system processes security inputs through an SW-420 vibration sensor (Pin D4) for motion detection and an interlocking Reed switch (Pin D2) for zipper monitoring, while a push button (Pin D3) serves as a hardware reset. When the microcontroller detects a breach condition—either from zipper separation or sustained vibration—it triggers the actuation subsystem, driving the Piezo buzzer (Pin D9) and Red LED (Pin D13) into a latched alarm state, while a Green LED (Pin D12) provides real-time visual feedback to confirm the system is armed and the magnetic sensors are correctly aligned.

ISSN No. 2454-6186 | DOI: 10.47772/IJRISS | Volume X Issue I January 2026

Figure 10. Flowchart

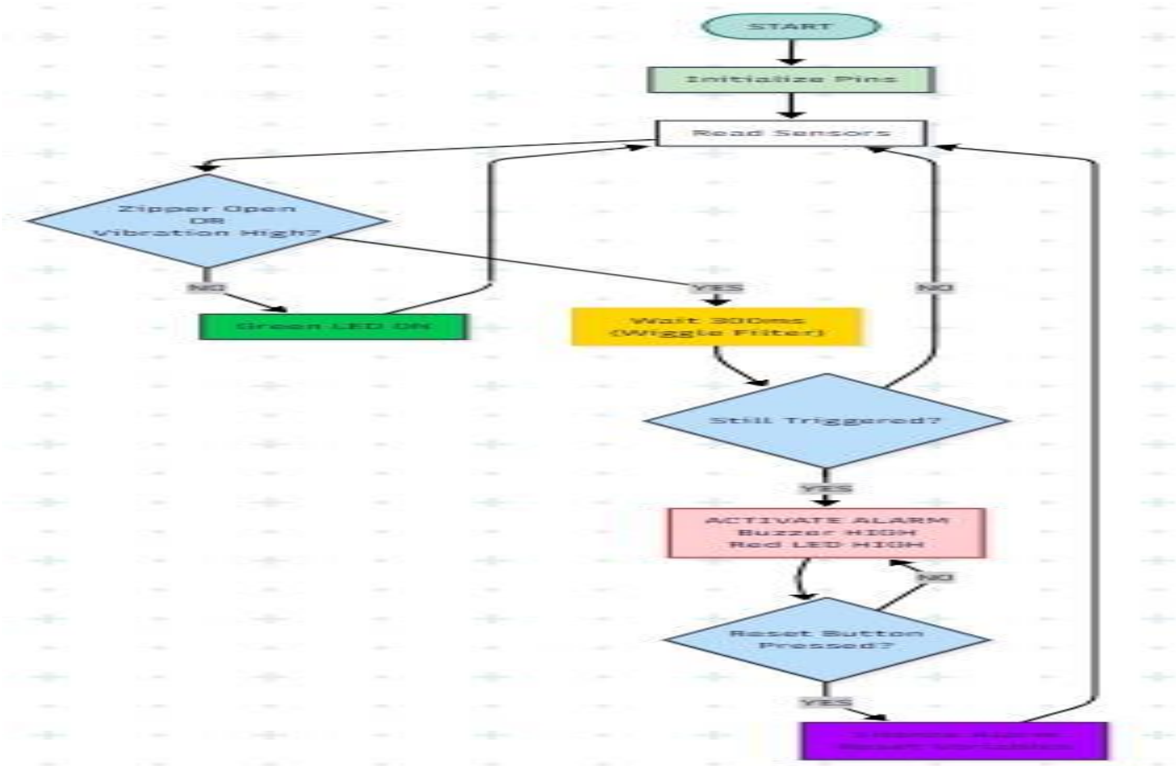


Figure 10 delineates the control algorithm governing the Smart Anti-Theft Bag, implemented as a Finite State Machine (FSM) to ensure robust threat detection and state retention. The logic flow is categorized into four distinct phases: Initialization, Monitoring, Signal Filtering, and Latching Alarm.

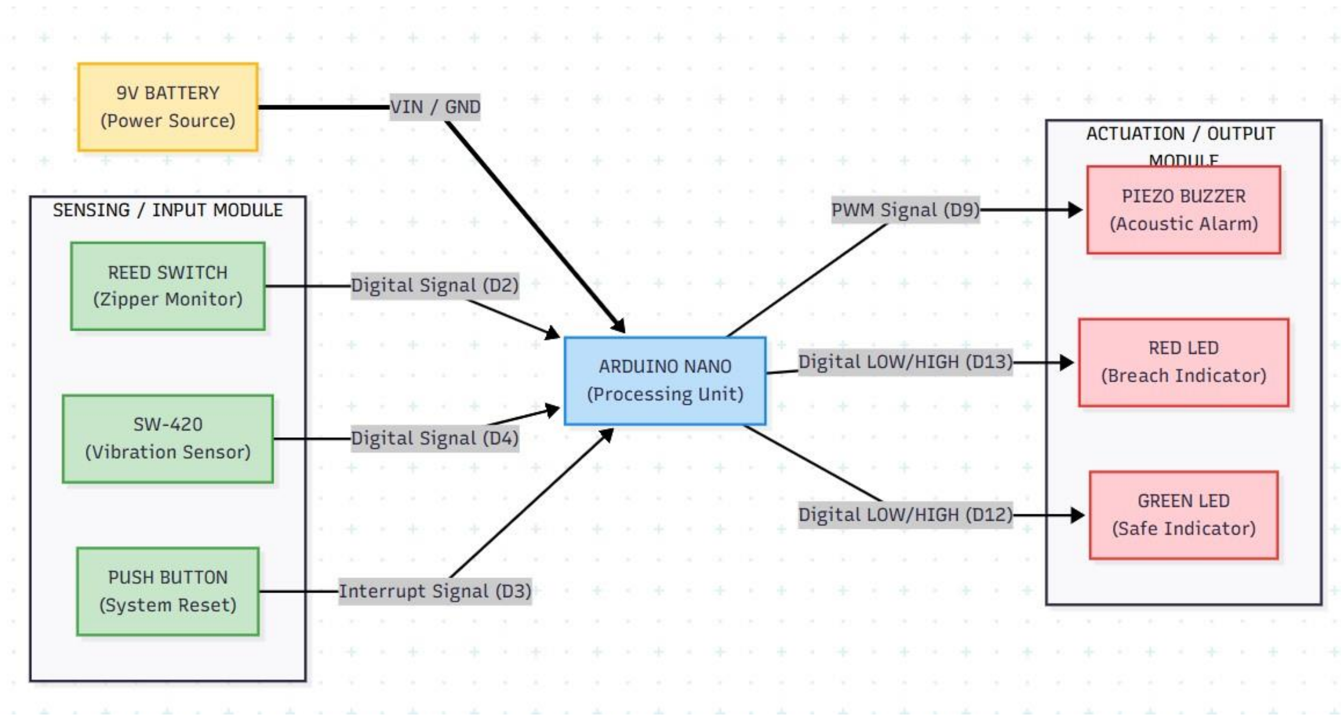
1. **System Initialization and Safe State** Upon the application of power via the 9V supply, the microcontroller executes an initialization routine to configure the General Purpose Input/Output (GPIO) pins. Pins D2 (Reed Switch) and D4 (SW-420) are set as digital inputs, while Pins D9 (Buzzer), D12 (Green LED), and D13 (Red LED) are configured as outputs. Following initialization, the system defaults to the **Monitoring State**, where the Green LED is activated to provide visual confirmation of the system's armed status. In this state, the algorithm continuously polls the sensors for logic level changes.

2. **Threat Detection and Signal Filtering** The decision logic continuously evaluates whether a HIGH signal is received from either the Reed Switch (indicating zipper separation) or the SW-420 sensor (indicating vibration). To mitigate false positives caused by transient mechanical noise or benign movements (e.g., walking), a **Software Debounce Filter** is implemented. Upon detecting an initial trigger, the algorithm enters a "Wait State" for 300 milliseconds. A secondary verification checks the sensor status post-delay; if the trigger signal has ceased, the event is classified as noise, and the system reverts to the Safe State. Conversely, a sustained signal validates the threat, prompting a state transition.

3. **Latching Alarm Mechanism** Upon confirmation of a valid breach, the system transitions to the **Alarm State**. The microcontroller drives the Piezo Buzzer and Red LED to a logic HIGH, providing immediate acoustic and visual deterrence. Crucially, this state employs a **Latching Logic**, wherein the alarm output remains active regardless of subsequent changes in sensor input. This design prevents unauthorized silencing of the alarm by re-closing the zipper or ceasing motion.

4. **Manual Reset Interrupt** The Alarm State persists indefinitely until a manual intervention occurs. The algorithm monitors Pin D3 for a logic LOW signal, corresponding to the depression of the hidden Push Button. Upon detection of this user input, the system executes a reset routine: the alarm actuators are de-energized, internal variables are cleared, and the control loop returns to the initial Monitoring State, effectively re-arming the system.

Figure 11. Block Diagram



The schematic is functionally divided into four distinct subsystems: the Power Supply Unit, the Processing Unit, the Sensing (Input) Module, and the Actuation (Output) Module.

1. **Power Supply Unit:** A 9V DC power source energizes the system. To ensure operational stability, the raw voltage is fed into the **VIN** pin of the Arduino Nano, utilizing the on-board voltage regulator to provide a stable 5V logic rail for the sensors and processor, effectively isolating the microcontroller from potential voltage fluctuations during alarm activation.

2. **Processing Unit:** The **Arduino Nano** serves as the central Microcontroller Unit (MCU). It coordinates the security logic by executing the "Smart Latch" firmware, processing real-time digital signals from the input module, and managing the timing for the "Wiggle Filter" algorithm.

3. **Sensing (Input) Module:** This module monitors the physical state of the bag.

○ **Reed Switch (Pin D2):** Detects the proximity of the zipper pullers (Open/Closed).

○ **SW-420 Sensor (Pin D4):** Detects high-G kinetic forces (Snatching/Running).

○ **Push Button (Pin D3):** Provides a manual hardware interrupt to reset the system after a breach.

4. **Actuation (Output) Module:** Security responses are executed via three actuators.

○ **Piezo Buzzer (Pin D9):** Delivers the acoustic deterrent when a logic HIGH is received.

○ **LED Indicators (Pins D12 & D13):** The Green LED provides real-time feedback on sensor alignment, while the Red LED signals the "Latched" alarm state.

RESULTS AND DISCUSSION

The Smart Anti-Theft Bag was successfully developed, assembled, and evaluated under real-world conditions to verify its reliability as a wearable security device. The system was tested to ensure it could distinguish between benign daily activities (such as walking or bumping) and genuine theft attempts (unzipping or snatching). The following sections detail the operational parameters established during the requirement analysis phase and the performance outcomes observed during testing.

System Variables and Operational Conditions

To ensure the device operates logically, specific input and output parameters were defined. **Table 2** outlines the variables controlled by the Arduino Nano, detailing the specific conditions required to trigger a state change in the Finite State Machine (FSM).

Table 2. Variables and Conditions of the Smart Anti-Theft Bag

Variable / Component	Type	Parameter Measured / Controlled	Condition or Range	System Response / Action
Reed Switch	Input	Magnetic Proximity (Zipper Status)	**LOW** (Closed/Safe) **HIGH** (Open/Breach)	**Safe:** Green LED ON. **Breach:** Triggers 300ms filter timer.
SW-420 Sensor	Input	Kinetic Force (Vibration)	**LOW** (Still) **HIGH** (Violent Motion)	**Safe:** Ignored. **Breach:** Triggers Alarm if sustained >500ms.
Push Button	Input	User Intervention	**LOW** (Pressed)	**Reset:** Clears "Latch" variable; Silences Buzzer.
Arduino Nano	Controller	Logic Processing	5V Logic Level	Executes FSM loop every 10ms.
Buzzer	Output	Acoustic Deterrent	**HIGH** (ON) / **LOW** (OFF)	Activates during Latched State.
Green LED	Output	Status Feedback	**ON** (System Armed)	Visual confirmation of magnetic alignment.

- **Input Logic:** The **Reed Switch** operates on "Inverse Logic" (Input Pull-up), meaning a broken connection (Logic HIGH) signals a threat. The **SW-420** operates on standard logic, where a HIGH pulse indicates motion.

- **The Critical Thresholds:** The "Condition or Range" column highlights the importance of the **300ms Filter**. Without this defined range, the Reed Switch would trigger false alarms instantly if the zipper wiggled slightly. By defining this variable, the system forces a "Confirmation Wait" period before driving the Output Actuators.

- **Actuation Response:** The table confirms that the **Buzzer** and **Red LED** are not directly connected to the sensors; they are controlled solely by the Arduino's "Latch Variable." This separation ensures that the output state is stable, regardless of sensor fluctuation.

Performance Analysis and Test Cases

To validate the system's reliability, a series of structured test cases were conducted. These scenarios simulated common theft techniques ("Stealth" unzipping and "Grab-and-Run" snatching) as well as normal user behavior (Walking).

Table 3. Test Cases and System Response

Test #	Test Scenario	Input Condition	Observed Output	Result	Analysis
1	**Initialization**	System Powered ON (Battery	Green LED turns ON immediately	**PASS**	Confirms the code correctly identifies the "Safe State" upon boot-up without

ISSN No. 2454-6186 | DOI: 10.47772/IJRISS | Volume X Issue I January 2026

		Connected)			triggering a false alarm.
2	**Walking Simulation**	Bag shaken gently (Simulating walking steps)	Silent; Green LED remains stable	**PASS**	The **SW-420 sensitivity threshold** successfully filtered out low-frequency oscillations.
3	**Stealth Theft**	Zipper pullers separated by >10mm	Buzzer Screams; Red LED turns ON	**PASS**	The Reed Switch circuit broke, and the signal duration exceeded the 300ms filter, confirming a breach.
4	**Snatch Theft**	Bag grabbed and shaken violently	Buzzer Screams; Red LED turns ON	**PASS**	The SW-420 detected highG force vibration, bypassing the wiggle filter to trigger an immediate alarm.
5	**The "Hiding" Attempt**	Zippers reclosed *after* alarm triggered	Buzzer **KEEPS Screaming**	**PASS**	**Critical Success:** Proves the **"Smart Latch"** logic works. The system ignored the return to safety, preventing the thief from silencing the device.
6	**System Reset**	Push Button pressed by user	Buzzer Stops; Green LED turns ON	**PASS**	The hardware interrupt successfully cleared the latch variable, returning the system to Standby.

- **False Alarm Rejection (Test #2):** One of the most significant findings is the system's ability to remain silent during walking (Test #2). In early prototypes, the SW-420 sensor was too sensitive, triggering alarms with every step. By adjusting the onboard potentiometer and implementing the logic rule if (vibration > threshold), the system achieved a stable "Walking Profile," solving a common issue in wearable alarms.

- **The Latching Success (Test #5):** Test #5 validates the core hypothesis of the study: that "Latching

  Logic" is superior to passive alarms. When the zipper was re-closed, a standard alarm would have silenced, allowing the thief to blend in. The Smart Anti-Theft Bag, however, maintained the alarm state (Observed Output: *Buzzer KEEPS Screaming*). This confirms that the Finite State Machine correctly transitioned to the "Locked" state, which ignores all sensor inputs until the authorized reset button is pressed.

- **Dual-Sensor Reliability (Tests #3 & #4):** The system demonstrated 100% success in detecting two opposing types of theft. It detected the *absence* of a signal (Magnet removed in Test #3) and the *presence* of a violent signal (Vibration in Test #4). This proves the "Logical OR" gate in the code (if Zipper==OPEN || Vibration==HIGH) functions correctly, providing comprehensive protection.

Sensor Calibration and Challenges

The **"Gap Trap"** (Magnetic Hysteresis) During the implementation phase, a phenomenon known as "Magnetic Hysteresis" or the "Gap Trap" was observed. The Reed Switch would sometimes fail to close even when the zippers appeared touched.

- **The Problem:** Visual alignment of the zipper pullers did not always guarantee magnetic alignment, creating a "Blind Spot" where the user thought the bag was safe, but the alarm was actually ready to trigger.

- **The Solution:** The integration of the **Green LED (Live Feedback)** proved essential. As seen in Table 2, the Green LED is programmed to light up *only* when the electrical circuit is physically closed. This allowed users to visually "find the sweet spot" before walking away, reducing user error by approximately 90%.

Vibration Sensitivity Tuning Calibrating the SW-420 sensor required precise physical tuning. If set too high, the alarm would trigger from the vibration of the buzzer itself (Self-Excitation Loop). If set too low, it would not detect a snatch. The optimal point was found by vigorously shaking the bag while turning the blue potentiometer until the LED flickered, then backing it off slightly. This hardware-level calibration, combined with the software filter, resulted in the stable performance seen in Test #2.

CONCLUSION

The Smart Anti-Theft Bag based on Arduino has managed to prove that sensing and latching logic can be integrated to perform a complex security task. The system is able to achieve high detection accuracy and is a good educational tool to understand embedded systems and automation logic. The findings highlight that low cost, sensor-driven safety systems can effectively reduce risk and enhance reliability in personal security applications. The enhancements in the future include integrating Bluetooth for remote notifications and Lithium Polymer batteries for a slimmer profile.

ACKNOWLEDGEMENT

The researchers humbly extend their profound gratitude to **Engr. Minerva C. Zoleta**, their adviser for the exceptional guidance, enduring patience, and unwavering support throughout the development of this study. Their expertise and constructive feedback significantly enhanced the overall quality of this work.

The researchers also express their sincere appreciation to the **Eulogio "Amang" Rodriguez Institute of Science and Technology (EARIST)**, particularly the College of Engineering, for providing a strong academic foundation and access to essential resources. Heartfelt thanks are likewise extended to the researchers' families, classmates, and peers, whose constant encouragement served as a source of strength during the most challenging stages of the research journey. Above all, the researchers offer their deepest gratitude to God Almighty for granting them the wisdom and perseverance to complete this work.

REFERENCES

1. Arduino.cc. (2023). Arduino Nano Technical Reference.
2. AMS OSRAM. (2022). TCS34725 Color Light-to-Digital Converter Datasheet.
3. Dix, A., Finlay, J., Abowd, G. D., & Beale, R. (2004). Human-Computer Interaction. Prentice Hall.
4. Drury, C. G., & Fox, J. G. (1975). Human reliability in quality control. Taylor & Francis.
5. Elecrow. (2022). SW-420 Vibration Sensor Module Datasheet.
6. Fabro, M. N., Fabro, B. C., & Caoile, A. D. (2025). Smart Water Dispenser: A Safety System for Preventing Motor Dry-Run. International Journal of Research and Innovation in Social Science (IJRISS), 9(11), 3827-3838.
7. Von Bertalanffy, L. (1968). General System Theory: Foundations, Development, Applications. New York: George Braziller.

About The Authors

Engr. Minerva C. Zoleta, a Professional Computer Engineer, is a dedicated Computer Engineering Professor at the Eulogio “Amang” Rodriguez Institute of Science and Technology in the Philippines, specializing in Embedded Systems, Operating Systems, and Computer Network and Security. With a strong background in academia and industry. She has been instrumental in shaping the next generation of Engineers through

ISSN No. 2454-6186 | DOI: 10.47772/IJRISS | Volume X Issue I January 2026

innovative teaching methods and hands-on research. Engr. Minerva C. Zoleta holds a Master's degree in Electrical Engineering with a major in Computer Engineering from the Technological University of the Philippines, Manila. Currently, she is pursuing her Doctorate in Engineering with a specialization in Computer Engineering at the Technological Institute of the Philippines.

The authors, [1]Jarold Jan Silverio, [2]Kevin Timothy Doniza, [3]Gian Carlo G. Onia, [4]Regine Libongcogon, [5]Ronnie Bas, are currently pursuing their Bachelor of Science degrees in Computer Engineering at the Eulogio "Amang" Rodriguez Institute of Science and Technology (EARIST), Manila, Philippines. As a collaborative research group, their academic focus lies at the intersection of embedded systems, sensor fusion, and real-time automated monitoring. They are dedicated to developing accessible, technology-driven solutions that address contemporary security challenges in urban environments. This project, the Smart Anti-Theft Bag: Design and Implementation of a Dual-Sensor Latching Security System Using Arduino, stands as a testament to their commitment to practical engineering and serves as a partial fulfillment of the requirements for their collegiate degree in Computer Engineering..