Backtracker

ECE 445 Final Report - Spring 2025

Project #86

Seth Oberholtzer, Aashish Subramanian, Shreyas Sriram

Professor: Arne Fliflet

TA: Rui Gong

Abstract

Backtracker is a smart backpack system designed to improve organization and enhance security for everyday users. The backpack integrates real-time inventory tracking and theft prevention features to address common issues like forgetting essential items or unauthorized access. The system consists of six key components: a microcontroller, an inertial measurement unit (IMU), a Bluetooth Low Energy (BLE) module, a power system, a motorized lock, and an RFID scanner. RFID tags attached to personal belongings allow the microcontroller to monitor the bag's contents, alerting the user via a mobile app if important items are missing. The IMU and motion sensors detect unusual movements or tampering attempts, triggering security responses such as alarms, vibrations, or auto-locking mechanisms. BLE enables wireless communication and geofencing alerts when the backpack is left behind. Powered by a rechargeable Li-Ion battery with voltage regulation, the system ensures reliable operation throughout daily use. Although large-scale user testing was not conducted, the Backtracker's core electronics and software were validated through controlled trials, demonstrating effective item tracking, theft detection, and automated locking. By combining inventory management with smart security, Backtracker offers a practical, integrated solution for modern users seeking peace of mind in both personal and professional settings.

1 Introduction

1.1 Problem and Solution:

Many people struggle to keep track of their belongings inside backpacks, often forgetting essential items or misplacing them. This can be especially frustrating when missing something important, like a laptop or notebook, leads to setbacks at school or work. Theft is also a growing concern, particularly in crowded places where someone could easily access an unattended backpack without the owner noticing. Traditional backpacks lack built-in ways to track items or prevent theft, leaving users vulnerable to both disorganization and security risks. Existing solutions, such as Bluetooth trackers and smart luggage, often fall short. Bluetooth trackers require manual tracking and are easy to lose, while smart luggage is designed mainly for large suitcases, not everyday backpacks. A smarter, more integrated solution is needed—one that helps users track their items and enhances security against theft or loss. To meet this need, we present *Backtracker*, a Smart Backpack with Inventory Tracking & Security. *Backtracker* integrates RFID-based item tracking, theft detection, and smart security features to help users always know what's in their bag and keep belongings safe. Small RFID tags (Khan et al., 2018) attached to commonly carried items like a wallet, laptop, or notebook allow a built-in scanner to monitor the bag's contents. If an important item is missing, users receive an alert via a mobile app before leaving a location, reducing the risk of forgetfulness. To enhance security, motion sensors detect unusual movements, such as unauthorized attempts to open the bag. If theft is detected, the system can trigger an alarm or vibration alert. An auto-locking mechanism secures the zippers in crowded areas and unlocks them when the user is in a safe space. Bluetooth connectivity lets users check inventory in real-time and receive geofencing alerts if they leave their backpack behind. By combining security and organization in one system, *Backtracker* offers a smarter, more reliable solution for modern users seeking peace of mind on the go.

1.3 High-level requirements list:

- **Accurate RFID-Based Item Tracking**: The backpack must include an RFID system to detect tagged items in real time. It should scan contents and alert the mobile app if essential items (e.g., laptop, notebook, wallet, keys) are missing before the user leaves.

- **Effective Theft Detection and Security Response**: An IMU (accelerometer or gyroscope) should detect unauthorized access, like sudden movement or unzipping. If triggered, it will activate a buzzer or vibration alert to notify the user and deter theft.

- **Reliable Auto-Zip & Auto-Lock Mechanism**: The backpack will have motorized zippers and an electronic/magnetic lock that automatically secures or unlocks based on location, with manual override available for user control.

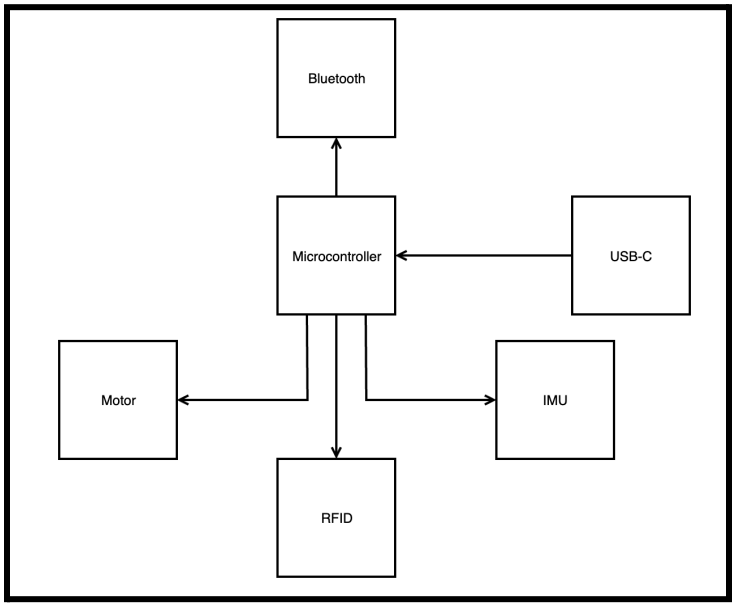

Figure 1: Block Diagram

2. Design

2.1 Physical Design

The only physical design consideration required for our project is the integration of a motor, which will be connected via ribbon cables to designated pins on the PCB. All other components will be securely mounted onto the PCB, eliminating the need for additional mechanical attachments or structural modifications. This simplifies assembly and ensures a compact, efficient design. We plan on mounting these motors to the top and middle level of the bag, as well as attaching cables to some of these motors in order to implement the auto-zip mechanism.

2.2 Subsystems

2.2.1 Board Microcontroller

Design Procedure

The Board Microcontroller subsystem centers on an ESP32‑WROOM‑32D, selected for its dual‑core processing, built‑in Wi‑Fi/BLE support, and ultra‑low‑power modes. Alternative microcontrollers—such as ARM Cortex‑M0+ or AVR‑based MCUs—were considered but ultimately rejected because they would require external wireless modules, adding cost and enclosure complexity. Although SPI offers higher raw throughput for sensor communications, I2C was chosen for both the RFID reader and IMU sensors since it uses only two shared lines with standard pull‑up resistors to the 3.3 V supply and supports daisy‑chaining multiple devices without extra chip‑select signals. The ESP32's UART peripheral provides a simple link to its onboard BLE radio at 115200 baud, speeding mobile‑app alert integration. Control outputs for the motorized zippers and electronic lock are driven from GPIO pins through gate resistors into logic‑level MOSFETs, ensuring inrush currents up to 500 mA see only a few millivolts of voltage drop. During this phase, we based our power‑budget estimates on the sum of each peripheral's supply current and selected resistor values for the I2C bus pull‑ups by considering total bus capacitance and required signal rise times.

Design Details

The ESP32 and all peripherals run from a 3.3 V low-dropout regulator rated for 2 A. Every supply pin is decoupled with a small high-frequency capacitor and a larger bulk capacitor placed nearby to suppress switching noise. Two I2C buses share standard pull-up resistors to the 3.3 V rail, and we kept all sensor trace lengths under 5 cm to preserve signal integrity. The UART interface is configured at 115200 baud with eight data bits, no parity, and one stop bit, and TX/RX lines include ESD protection diodes. Zipper and lock actuators connect to GPIO pins that drive logic-level N-channel MOSFETs through 220 Ω gate resistors; these MOSFETs have very low on-resistance so that even peak currents cause negligible voltage loss. On the PCB, we used solid power and ground planes for low-impedance distribution, routed the I2C lines in a star pattern to minimize crosstalk, and placed MOSFET packages as close as possible to their corresponding actuators to reduce high-current loop areas. Detailed schematics, component datasheets, full-scale circuit diagrams, and bill-of-materials tables are provided in the appendices.

2.2.2 Theft Detection System

Design Procedure

The Theft Detection System relies on a six-degree-of-freedom IMU module to monitor for unauthorized motion or tampering of the backpack. Alternative sensing approaches—such as single-axis accelerometers or purely gyroscopic sensors—were considered, but these would either miss certain motion types or require multiple separate components and more complex data fusion. By choosing the MPU6050, which combines a three-axis accelerometer and three-axis gyroscope in one package, we simplified the hardware design and ensured tight synchronization of acceleration and rotation data. Motion data are read over a standard I2C bus using pull-up resistors to the 3.3 V supply. When measured acceleration or angular velocity exceeds predefined thresholds, the IMU signals the microcontroller via the same I2C interface. This approach leverages simple digital thresholds rather than complex signal processing algorithms, reducing firmware overhead and ensuring rapid tamper detection.

Design Details

The MPU6050 IMU is powered from the 3.3 V rail and connected to the microcontroller's I2C bus with 4.7 kΩ pull-up resistors. The accelerometer is configured to flag any reading above plus or minus 2 g, while the gyroscope is set to alert on rotations exceeding plus or minus 150 degrees per second. Both motion data and alert signals share the same two-wire I2C connection, minimizing pin count and simplifying PCB routing. All IMU configuration registers are set during system initialization to enable the correct full-scale ranges and interrupt generation. The alert output is read by the Board Microcontroller, which then executes the predefined response, such as activating the auto-lock sequence. Detailed register settings, timing diagrams, and full circuit diagrams are provided in the appendices.

2.2.3 Power Subsystem

Design Procedure

The Power Subsystem is responsible for delivering stable and safe energy to every module of the Smart Backpack. We evaluated several energy sources, including alkaline batteries, nickel-metal hydride packs, and lithium-ion cells; lithium-ion was chosen for its superior energy density and rechargeability. To protect the battery and downstream electronics, a dedicated battery management system was selected to guard against overcharge, over-discharge, and short-circuit conditions. For voltage conversion, we compared switching regulators and linear regulators—switching types offer higher efficiency but add complexity and potential electrical noise, while linear regulators are simpler and quieter but dissipate more heat. Given the relatively low current draw of our microcontroller and sensors, we opted for a linear regulator to step the battery's nominal three-volt output up to the required three-point-three volts with minimal component count and straightforward layout.

Design Details

The heart of the subsystem is a single-cell lithium-ion battery rated at three volts nominal, connected to a three-volt linear battery management module that provides overcharge, over-discharge, and short-circuit protection. Downstream, a three-point-three volt linear regulator accepts the battery management system's output and provides a clean supply rail for the microcontroller, RFID reader, BLE transceiver, and IMU sensors. Each regulator input and output is decoupled with a bulk capacitor and a high-frequency capacitor placed within five

millimeters of the pins to suppress noise and ensure stability. Power and ground planes on the PCB deliver low-impedance distribution, and the three-point-three volt rail is split into separate zones for the microcontroller and the RF/sensor subsystems to minimize interference. Complete schematics, detailed BMS pin assignments, capacitor values, and regulator datasheets are provided in the appendices.

2.3.4 Connectivity Subsystem (BLE Transceiver)

Design Procedure

The wireless link between the Smart Backpack and the mobile application is provided by a Bluetooth Low Energy (BLE) transceiver. Alternative wireless options—such as Wi-Fi modules or Bluetooth Classic—were considered, but BLE 5.0 was chosen for its exceptionally low power draw in standby and rapid connection establishment, which are critical for battery-powered, on-the-go use. The BLE transceiver connects to the Board Microcontroller via a simple UART interface, minimizing firmware complexity by treating all data exchanges as serial packets. Through this link, the transceiver delivers real-time location and status updates, communicates security alerts generated by the theft detection system, and relays lock-and-unlock commands from the mobile app. By leveraging standardized BLE profiles and a straightforward UART bridge, the design achieves reliable, low-latency communication while preserving battery life.

Design Details

The selected BLE 5.0 module is powered from the 3.3 V supply shared by the microcontroller and sensors. Its TX and RX pins are wired directly to the microcontroller's UART peripheral, configured at 115200 baud with eight data bits, no parity, one stop bit. Each power pin is decoupled with a 0.1 µF ceramic capacitor in parallel with a 10 µF tantalum capacitor, placed within five millimeters of the module's supply pins to suppress voltage spikes during radio transmission. An optional ESD protection diode array guards the UART lines from electrostatic discharge. The module advertises a custom BLE service for tracking data and security events; incoming commands from the app are parsed by the microcontroller's firmware and translated into control signals for the auto-lock mechanism. Full pin-out details, wiring schematics, and BLE GATT profile definitions are included in the appendices.

2.2.5 Auto-Zip/Lock System

Design Procedure

The Auto-Zip/Lock System integrates motorized zippers with an electromagnetic latch to secure the backpack upon unauthorized access. We considered direct-drive DC motors with simple transistor drivers but selected an H-bridge driver (L298N) because it provides bidirectional control, built-in current sensing, and thermal protection—all of which simplify motor control firmware and improve reliability. For the locking mechanism, we evaluated mechanical solenoids and spring-loaded latches but chose an electromagnetic latch for its fast response time, low noise, and minimal moving parts. The Board Microcontroller issues lock and unlock commands via general-purpose I/O pins; the H-bridge interprets these signals to drive the zipper motors forward or reverse, while a separate output activates the latch coil. This design minimizes component count by using a single driver chip for both functions and ensures rapid, synchronized motion and locking.

Design Details

The L298N H-bridge driver is powered from the 3.3 V regulated rail and sits close to the motorized zipper assembly on the PCB. GPIO outputs from the microcontroller connect to the driver's input pins through 220 Ω gate resistors to limit transient currents. The driver's enable pins are tied to the microcontroller's PWM outputs, allowing speed control of the zipper motors. The electromagnetic latch coil is driven by a separate GPIO line through a MOSFET gate resistor; a flyback diode across the coil suppresses voltage spikes. All power and ground lines to the driver and latch are decoupled with 10 µF bulk capacitors and 0.1 µF ceramic capacitors located within 5 mm of each device. Motor current sensing pins on the L298N feed back into an analog input of the microcontroller for stall detection. Detailed wiring diagrams, PCB layout sections, and full H-bridge pin-out tables are provided in the appendices.

2.2.6 RFID Tracking Subsystem

Design Procedure

The RFID Tracking Subsystem is built around a UHF RFID reader chosen for its ability to detect multiple tags simultaneously within a 30 cm range. Simpler narrow-band readers were considered, but they lack the sensitivity and anti-collision protocols needed for reliably scanning several tagged items at once. The UHF reader communicates with the Board Microcontroller over an I2C bus, minimizing pin usage and simplifying firmware. During system start-up, the microcontroller initializes the reader's sensitivity settings and tag filtering parameters to ensure that only tags within the backpack's interior are reported. By relying on proven, off-the-shelf RFID modules and the standard I2C interface, the design achieves robust, low-latency item detection without custom RF design work.

Design Details

The selected UHF RFID reader is powered from the 3.3 V rail and connected to the microcontroller's I2C bus with 4.7 kΩ pull-up resistors. Antenna tuning components are set so that the read range is limited to 10 cm inside the backpack, preventing external tags from triggering false positives. The reader's SDA and SCL lines are routed together with ground returns in a single differential-style bundle to reduce noise. During operation, tag IDs are streamed over I2C at regular intervals; the microcontroller parses each ID and updates the user interface accordingly. All reader power and signal lines are decoupled with both bulk and high-frequency capacitors placed within five millimeters of the module's pins. Full wiring diagrams, antenna matching network details, and I2C register maps are provided in the appendices.

2.3 Hardware Design

2.3.1 Power Regulation and Distribution

Our system requires a regulated power supply to ensure stable operation of the ESP-32S microcontroller, CC2564CRVMR Bluetooth transceiver, and MFRC52202HN1 RFID reader. The power source for our project is a rechargeable lithium-ion battery, which provides an output voltage ranging from 3.7V (nominal) to 4.2V (fully charged). However, our components operate at different voltage levels, necessitating voltage regulation.

The CC2564CRVMR Bluetooth transceiver operates within a 2.7V to 3.3V supply range, while the ESP-32S requires a 3.3V power supply. Given that our RFID reader (MFRC52202HN1,151) also operates at 3.3V, the most efficient choice is to regulate the battery voltage to 3.3V for all components, reducing the need for complex level shifting and minimizing power consumption. Given our expected power draw of approximately 40mA, this efficiency is acceptable, and no additional power conversion circuitry is required.

Since all components in our system operate at 3.3V, there is no need for multiple voltage rails or level-shifting circuits. The ESP-32S provides sufficient processing power for handling RFID, Bluetooth communication, and motion data processing, making it an ideal choice for our system architecture.

2.3.2 Motor Control and Automation

The auto-zip mechanism in our system requires small yet efficient motors to control the zippers. For this, we have selected the Olimex Ltd. MOTOR-F130-3V, a compact DC motor that operates at 3V and is well-suited for low-power applications. The motor will be controlled via PWM signals from the ESP-32S to regulate speed and movement.

To detect theft and unauthorized access, our system integrates an IMU (ICM-45605) from TDK InvenSense, which provides ultra-low power motion tracking. The IMU continuously monitors acceleration and orientation to detect any sudden or extreme movements. If the BLE transceiver (CC2564CRVMR) loses connection with the user's device, and extreme movement is detected, the microcontroller will activate the auto-zip function and flash an LED indicator to signal a security alert (Huggi, Nilavar, Bali, Giriyapur, Ashwini, 2021).

By integrating efficient power regulation, a reliable motor control system, and optimized voltage levels, our design ensures stable operation across all subsystems while maximizing efficiency

and safety. Additionally, the combination of RFID tracking, Bluetooth-based proximity detection, and motion-based security provides a seamless user experience with enhanced protection against theft or loss.

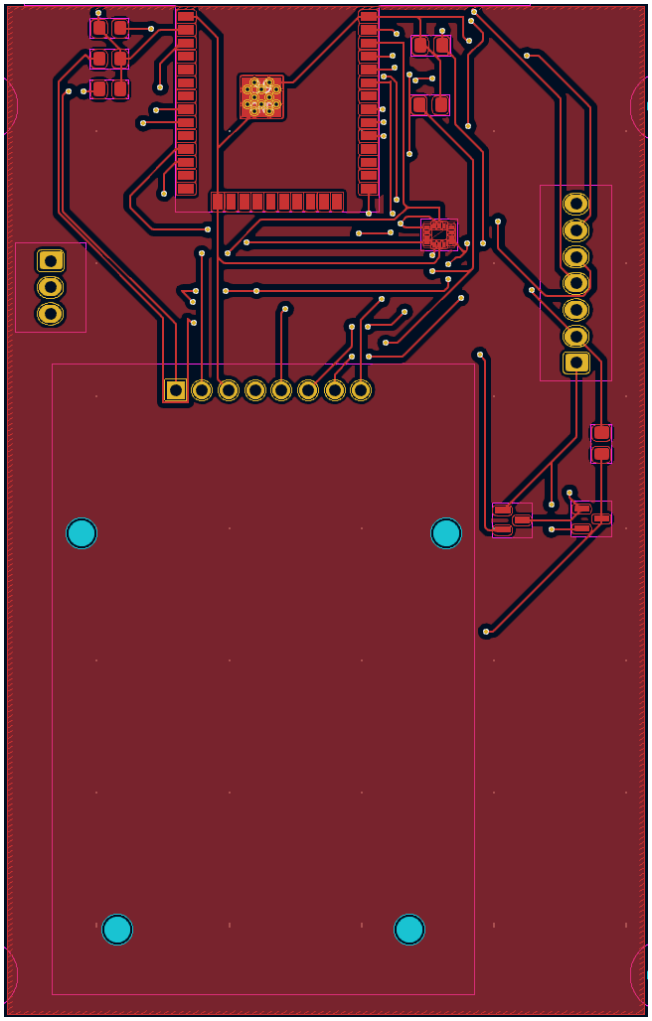

Figure 2: PCB KiCad

2.4 Software Design

2.4.1 RFID-Based Item Tracking and Security Response

The Backtracker's core functionality relies on software running on the PCB microcontroller to enable real-time item tracking and theft prevention. The microcontroller detects RFID-tagged items, communicates with the user's device via Bluetooth Low Energy (BLE), and manages security features like motion detection and an automatic zipper-locking mechanism.

When an RFID-tagged item is removed, the reader detects its absence and notifies the microcontroller, which updates the user's web app via Bluetooth. Replacing the item triggers another update, giving users a real-time view of their backpack's contents.

In addition to tracking, the BLE transceiver monitors proximity between the backpack and the user's device. If the connection is lost—indicating the backpack has moved out of range—the system enters security mode. The Inertial Measurement Unit (IMU) monitors for extreme movements such as sudden jerks or orientation changes. If detected while BLE is disconnected, the system assumes unauthorized tampering. The auto-zip mechanism then locks the zippers and activates a blinking LED to signal the anti-theft response.

By integrating RFID inventory tracking, BLE proximity detection, and IMU motion analysis, the software provides users with both organizational awareness and proactive security in daily use.

2.5 Tolerance Analysis

The motor must deliver at least 0.5 Newton-meters of torque under nominal conditions. A ten-percent drop in supply voltage reduces available torque to ninety percent of its rated value, so the effective torque is the rated torque multiplied by 0.9. To find the minimum rated torque T that still meets 0.5 Newton-meters when scaled by 0.9, we take 0.5 divided by 0.9, yielding approximately 0.5556, which we round to 0.56. Therefore, selecting a motor with a rated torque of at least 0.56 Newton-meters ensures that even with a ten-percent voltage sag, the auto-zip/lock mechanism maintains the required 0.5 Newton-meter torque.

The system is powered by a single rechargeable Li-ion cell providing between 3.7 and 4.2 volts under charge, which feeds all subsystems without the need for level shifting. A simple low-dropout regulator steps this voltage down to a stable 3.3 volts for the ESP-32S, the BLE module, and the UHF RFID reader, drawing only around 40 milliamps in total. This streamlined

power design minimizes component count and PCB complexity, eliminating extra conversion circuitry while still meeting the energy requirements of every module.

3 Verifications

3.1. Board / Microcontroller Subsystem

The board is required to operate at 3.3 V ± 5%, which is verified by measuring the input voltage using a multimeter or Scopy. The ESP32 microcontroller must be programmable; this is confirmed by flashing and running a "blink" GPIO-LED example. Additionally, the UART interface must be operational, verified by successfully sending and receiving the string "Hello" over the serial console at 115,200 bps.

3.2. Theft Detection Subsystem

The MPU6050 breakout must respond over the I²C interface, which is verified by scanning the I²C bus and detecting the MPU6050's address (0x68). The system must accurately detect acceleration along the X, Y, and Z axes, confirmed by sliding the unit along each axis and observing spikes on the serial monitor. The gyroscope must also be calibrated to detect any rotation, verified by rotating the device around each axis and confirming that the gyro reports the movement.

3.3 Power Subsystem

The battery system must provide at least 3.3 V ± 5% to all critical components. This requirement is verified by measuring voltage levels across all components using a multimeter.

3.4 Connectivity Subsystem (BLE Transceiver)

The BLE transceiver must be capable of establishing a connection, which is verified by connecting from a device and confirming the connection event in the logs. The system must include a GATT service and characteristic, verified by discovering services and ensuring the custom UUID is listed. Additionally, the write characteristic must accept a new value, confirmed by writing a test value, reading it back, and verifying the match.

3.5 Auto-Zip/Lock System

The motor must respond to microcontroller commands within one second, verified by sending control signals and measuring the response time using an oscilloscope or timer. The motor's power consumption must not exceed 1 W to preserve battery life, verified by measuring the current draw under load with a multimeter. Finally, the motor must be able to lift and lower the backpack sleeve with sufficient force, verified by testing its performance with the maximum expected backpack weight.

3.6 RFID Tracking Subsystem

The RFID system must have a detection range within 10 cm, verified by testing the tags at various distances and observing the serial monitor output. It must also detect if an item is removed or added to the backpack, which is verified by inserting and removing an item and checking the serial monitor output for accurate reporting.

4 Cost and Schedule

4.1 Cost Analysis

The cost analysis assumes an hourly fully-loaded rate of $52.50 for each team member (including salary, benefits, and a 2.5× overhead multiplier). For Aashish Subramanian, Seth Oberholtzer, and Shreyas Sriram—each working 45 hours—the individual labor cost is calculated as $52.50 × 2.5 × 45 = $5,906.25, resulting in a combined labor cost of $17,718.75. When you add the material and miscellaneous expenses detailed in Table 7 (totaling $82.23), the grand total project cost comes to $17,800.98.

4.2 Schedule

The team began in early February (≈ Feb 9–15) by defining the Smart Backpack's core objectives, researching RFID, BLE, and IMU technologies, and building proof-of-concept breadboard prototypes while drafting the design document. By mid-February (≈ Feb 16–22), we finalized our high-level architecture and presented it to stakeholders, then moved into detailed PCB schematic development and our first fabrication cycle in late February and early March. Throughout March, we implemented each subsystem in parallel—programming the BLE transceiver, integrating the RFID reader, developing motor-control firmware for the auto-lock, and tuning the IMU-based theft detector—refining thresholds and performance with every PCB revision. In early April (≈ Apr 6–12), we optimized RFID scan speeds, soldered final PCBs, and linked the hardware to our web-app interface. Mid-April (≈ Apr 13–19) was dedicated to full-system integration testing and mock demos, and by late April into the first week of May we executed our final demo and wrapped up documentation. The complete, week-by-week breakdown is laid out in Table 8.

5 Conclusion

5.1 Accomplishments

The Backtracker Smart Backpack successfully demonstrated core functionalities including automated closing through a mobile app or motion triggers (shaking the bag), RFID-based item recognition, and the ability to track which items entered or exited the backpack. The system integrated multiple subsystems—RFID tracking, theft detection, Bluetooth communication, and a motorized lock—into a functional prototype. We were able to program the microcontroller, verify BLE connectivity, detect item removal/addition with RFID tags, and control the motorized lock system with real-time feedback. The team also gained valuable technical experience with RFID technology, BLE integration, iterative hardware/software development, PCB design using KiCad, and mobile app communication.

5.2 Uncertainties

Despite these accomplishments, some uncertainties remain. The custom PCB did not function as expected, leading to reliance on breadboards for certain tests. The RFID detection range was limited and inconsistent under some conditions. Motor control was constrained to a single direction, which limited more advanced locking mechanisms. Additionally, Bluetooth connectivity occasionally suffered interference when multiple devices were present, and there were challenges synchronizing RFID reads and writes with other subsystems. Mechanical issues, such as string tangling and stabilizing the motor on the backpack, also introduced variability in performance.

5.3 Ethical Considerations

The Backtracker system raised important ethical and safety considerations, particularly regarding privacy, security, and user safety. Consistent with the ACM Code of Ethics, we ensured that data management prioritized user privacy and security. Communications—including RFID and Bluetooth data—were encrypted using AES-128 or AES-256 protocols, with authenticated user access enforced through the mobile app. The system limited data storage to essential inventory tracking, avoiding the collection of personal or location data. Users maintained full control, with the ability to opt in or out of tracking and disable or reset data as desired. Safety was addressed by integrating battery protection (overcharge, over-discharge, and thermal safeguards),

FCC-compliant electronics, and a motorized lock with low-torque motors and manual override to prevent injury. Transparency and user control were maintained throughout the design, with anti-tampering features and clear documentation of system functions.

5.4 Future Work

Future development will focus on addressing the identified uncertainties and expanding system capabilities. Key areas include upgrading to high-frequency RFID for improved range and reliability, enhancing the web and mobile app user interfaces, and adding an auto-latching mechanism to secure the backpack after closing. Improving motor control to enable bidirectional movement and increasing Bluetooth reliability in multi-device environments will also be pursued. Additionally, incorporating GPS functionality could provide valuable location-based security and tracking features, offering users an even more comprehensive smart backpack solution.

References

Juels, A. (2006). RFID security and privacy: A research survey. IEEE Journal on Selected Areas

in Communications, 24(2), 381–394. https://ieeexplore.ieee.org/document/1589116

RFID Journal. (n.d.). How RFID works. Retrieved from https://www.rfidjournal.com/faq/how-does-an-rfid-system-work/38660/

Khan, S., & Park, J. (2018). RFID technology: Fundamentals and applications. International Journal of Communication Systems. Retrieved from https://people.engr.tamu.edu/s-sanchez/RFID_665.pdf

Bluetooth SIG. (n.d.). *Introducing the Bluetooth low energy primer*. Retrieved from https://www.bluetooth.com/blog/introducing-the-bluetooth-low-energy-primer/

IEEE. (n.d.). *[Abstract document 9706334]*. Retrieved April 7, 2023, from https://ieeexplore.ieee.org/abstract/document/9706334

Novel Bits. (n.d.). *Bluetooth low energy (BLE): A complete guide*. Retrieved from https://novelbits.io/bluetooth-low-energy-ble-complete-guide

TDK InvenSense. (2023, January). *AN-000393: TDK InvenSense IMU PCB design and MEMS assembly guidelines (Version 1.4)* [PDF]. Retrieved from https://invensense.tdk.com/wp-content/uploads/2023/01/AN-000393-TDK-InvenSense-IMU-PCB-Design-and-MEMS-Assembly-Guidelines-v1.4.pdf

A. S. Huggi, A. C. Nilavar, J. Bali, A. Giriyapur and G. K. Ashwini, "Implementation of Sensor Fusion for a Mobile Robot Application," 2021 International Conference on Recent Trends on Electronics, Information, Communication & Technology (RTEICT), Bangalore, India, 2021

ITP at NYU. (n.d.). *Accelerometers, gyros, and IMUs: The basics*. Retrieved from https://itp.nyu.edu/physcomp/lessons/accelerometers-gyros-and-imus-the-basics/

Madgwick, S. O. H. (2010). An efficient orientation filter for inertial and magnetic sensor arrays. Retrieved from

https://courses.cs.washington.edu/courses/cse466/14au/labs/l4/madgwick_internal_report.pdf

Sabatini, A. M. (2011). Estimating three-dimensional orientation of human body segments by inertial/magnetic sensor arrays. Sensors, 11(12), 11569–11584. Retrieved from https://doi.org/10.3390/s110201489

M. Souryal, N. Moayeri, and H. Hashemi, "Real-time path planning for first responders in indoor environments," IEEE Wireless Communications Magazine, vol. 18, no. 2, pp. 78-86, April 2011. Retrieved from https://www.nist.gov/system/files/documents/2024/01/12/Souryal_IEEE_WC_Magazine_2011.pdf

Appendix A

Requirements & Verification:

Requirements	Verification
Board powered at 3.3 V ± 5%	Measure input voltage with multimeter/Scopy.
ESP32 programmable	Flash and run a “blink” GPIO-LED example
UART interface operational	Send/receive “Hello” over serial console (115 200 bps)

Table 1: Board Microcontroller Subsystem - Requirements & Verification

Requirements	Verification
MPU6050 breakout is responsive over I²C.	Scan I²C Bus, detect MPU6050 Address (0x68).
Accurately detect acceleration along each axis.	Slide along X, Y, Z; confirm spikes on serial monitor.
Calibrated to detect any gyroscope rotation.	Rotate around each axis; verify gyro reports turn.

Table 2: Theft Detection Subsystem - Requirements & Verification

Requirements	Verification
The battery system must provide at least 3.3V ± 5% for all critical components.	Measure voltage levels across components using a multimeter.

Table 3: Power Subsystem - Requirements & Verification

Requirements	Verification
BLE connection establishment.	Connect from device, confirm connection event in logs.
GATT service & characteristic present	Discover services; list must include your custom UUID.
Write characteristic accepts new value.	Write a test value, then read back and verify match

Table 4: Connectivity Subsystem - Requirements & Verification

Requirements	Verification
The motor must respond to microcontroller commands within 1 second.	Send control signals from microcontroller and measure response time with oscilloscope or timer.
Motor power consumption must not exceed	Measure current draw under load using a

1 W to preserve battery life.	multimeter.
The motor must be able to lift and lower the backpack sleeve with sufficient force.	Test motor lifting with max expected backpack weight.

Table 5: Auto-Zip/LockSubsystem - Requirements & Verification

Requirements	Verification
Range must be within 10 cm.	Test the tags at different distances, use the serial monitor output.
Must detect if item is removed/added.	Insert and remove item from bag, use the serial monitor output.

Table 6: RFID Tracking Subsystem - Requirements & Verification

Appendix B

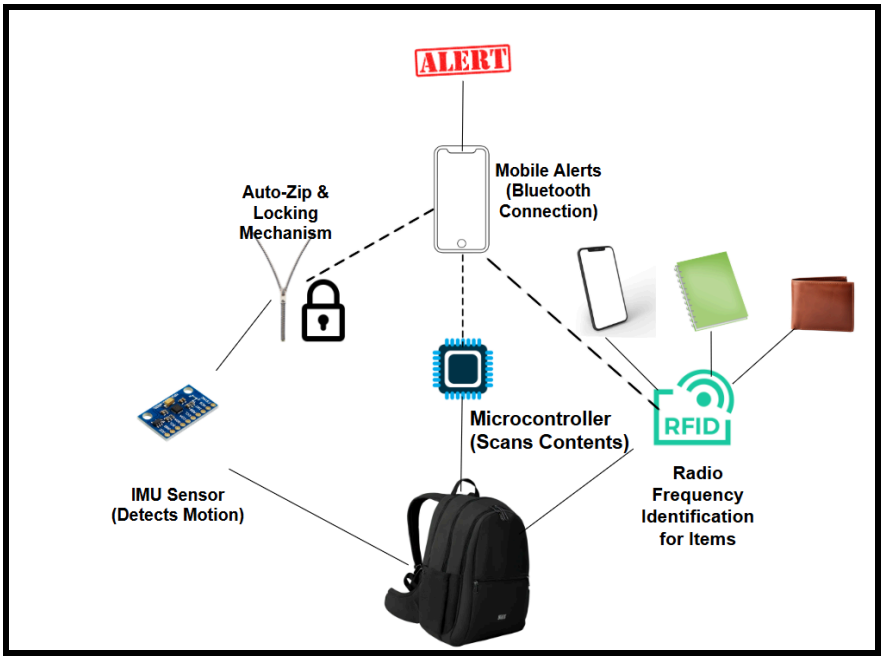

Figure 1: Visual Aid of Components

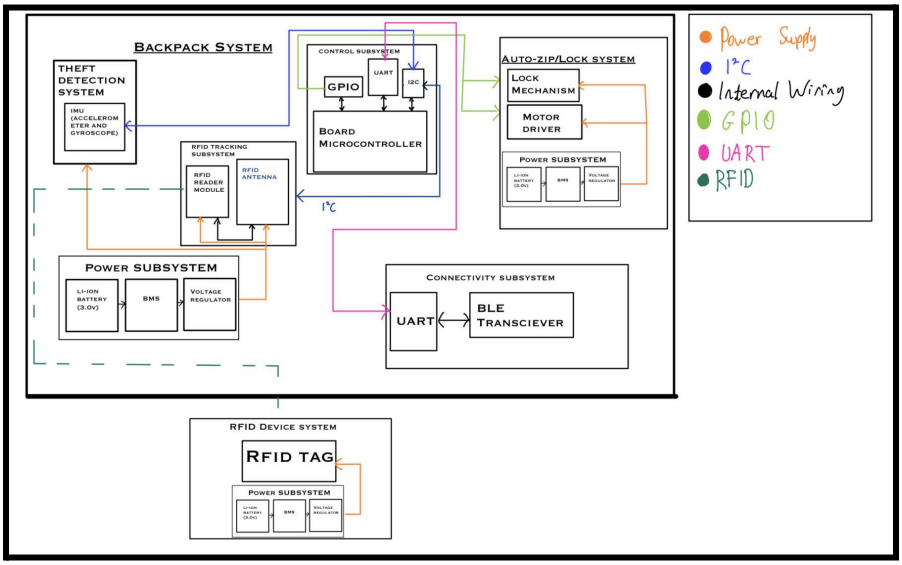

Figure 2: Block Diagram for Smart Backpack System

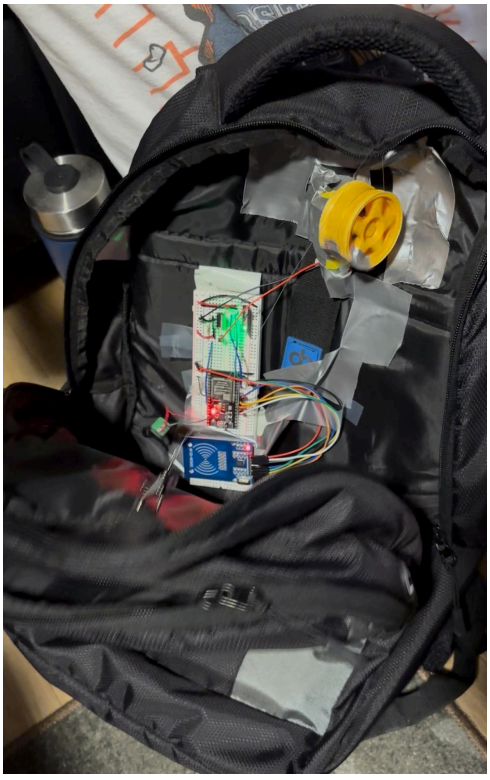

Figure 3: Physical Design of Backpack

Appendix C

Parts:

Description	Manufacturer	Part #	Quantity	Cost / Unit	Total Cost:
IC RFID READER 13.56MHZ 32HVQFN	NXP, USA.	MFRC52202HN1,151	3	$7.91	$23.73
RFID TAG R/W 13.56MHZ INLAY	Texas Instruments	296-RF37S114HTFJB-ND	20	$0.622	$12.44
RF Transceiver Bluetooth 5.1 with Basic Rate (BR)	Texas Instruments	CC2564CRVMR	2	$3.94	$7.88
IMUs - Inertial Measurement Units Ultra-Low Power, MotionTracking Device with BalanceGyro	TDK InvenSense	ICM-45605	2	$7.08	$14.16
AC, DC & Servo Motors	Olimex Ltd.	MOTOR-F130-3V	8	$0.324	$2.59
ESP-32S Development Board	HiLetgo	ESP-WROOM-32 ESP32 ESP-32S	1	$16.53	$16.53
RES 100 OHM 5% 1/16W 0402	YAGEO	RC0402JR-07100RL	20	$0.09	$1.80
RES 33 OHM 1% 1/16W 0402	YAGEO	RC0402FR-0733RL	10	$0.07	$0.70
RES 1K OHM 5% 1/16W 0402	YAGEO	RC0402JR-071KL	5	$0.10	$0.50

4.7 kOhms ±5% 0.063W, 1/16W Chip Resistor 0402 (1005 Metric) Moisture Resistant Thick Film	YAGEO	RC0402JR-074K7L	10	$0.09	$0.90
DIODE STD 100V 215MA TO236AB	Nexperia USA Inc.	BAS16,215	5	$0.10	$0.50
DIODE STANDARD 75V 250MA SOD523	MCC (Micro Commercial Components)	1N4448X-TP	5	$0.10	$0.50
CA0508KRX7R9BB102	YAGEO	13-CA0508KRX7R9BB102CT-ND	5	$0.21	$1.05
W3A45C473KAT2A	KYOCERA AVX	478-11168-1-ND	5	$0.25	$1.25

Table 7: Parts list

ECE445 Lab Schedule

Week	Task	Team Member
Feb 09 - Feb 15	**Devise Project Proposal**	Everyone
	Order parts for prototyping	
	Research RFID tag detection and BLE communication	
Feb 16 - Feb 22	**Present Project Proposal to Professor and TA**	Everyone
	Prototype RFID reader functionality[Arduino]	
Feb 23 - Mar 01	**Make Progress on Design Document**	Everyone
	Complete Prototype RFID Reader	
	Start designing PCB	
	Begin Breadboard implementation of RFID	
	Complete the First Draft of PCB Design	
Mar 02 - Mar 08	**Refine PCB Design & Verify Schematics**	Seth
	Teamwork Evaluation 1 due March 05	Everyone
	Design Document due March 06	Everyone
	Picking up the ESP32 Microcontroller	
	Develop web application UI for item tracking	
Mar 09 - Mar 15	**Research BLE Transceiver Programming**	Aashish
	Refine PCB Design & Reverify Schematics	Seth
	Start Assembling First Prototype	Shreyas
	Breadboard Demo due March 10-12	Everyone

	2nd Round PCB Order due March 12	Everyone
Mar 16 - Mar 22	**Start work!**	Everyone
	Start Motor Control Logic for Auto-Zip	Shreyas
	Start Physical Design for Bag	Seth
	Start Planning on Battery Management	Aashish
Mar 23 - Mar 29	**Implement BLE Transceiver**	Shreyas
	Debug Hardware Integration Thus Far	Aashish
	Design IMU Component	Seth
	Refine PCB Design & Verify Schematics	Shreyas
Mar 30 - Apr 05	**Implement Battery Management System**	Aashish
	Test BLE Transceiver for Proximity-Based Detection	Everyone
	3rd Round PCB Order due March 31	Everyone
	Indiv. Progress Report due April 02	Everyone
Apr 06 - Apr 12	**Debug Hardware Integration**	Aashish
	Implement IMU Based Extreme Motion Detection Component	Aashish
	Optimize RFID Scanning Response Time	Shreyas
	Integrate PCB with Web App	Shreyas
	PCB Assembly and Soldering	Seth
	4th Round PCB Order due April 07	Everyone
Apr 13 - Apr 19	**Perform Full System Integration Testing**	Everyone
	Debug & Refine System Performance	Everyone
	Team Contract Assessment due April 18	Everyone
Apr 20 - Apr 26	**Mock Demo Week**	Everyone
Apr 27 - May 03	**Final Demo Week**	Everyone

May 04 - May 10	**Final Presentation**	Everyone
	Final Papers due May 07	Shreyas

Table 8: Schedule for Project Progression