BackTracker Item Tracker & Anti-Theft Device

ECE 445 Design Document - Spring 2025

Project #86

Seth Oberholtzer, Aashish Subramanian, Shreyas Sriram

Professor: Arne Fliflet

TA: Rui Gong

1 Introduction

1.1 Problem and Solution:

Many people struggle with keeping track of their belongings inside their backpacks, often forgetting essential items or misplacing them. This can be particularly frustrating when missing an important item, such as a laptop or notebook, leads to setbacks at school or work. Additionally, theft is a growing concern, especially in crowded environments where someone could easily access an unattended backpack without the owner noticing. Traditional backpacks offer no built-in way to track items or prevent theft, leaving users vulnerable to both disorganization and security risks. While some existing solutions, like Bluetooth trackers and smart luggage, attempt to address these issues, they often fall short. Bluetooth trackers require manual tracking and are easy to lose, while smart luggage is primarily designed for larger suitcases rather than everyday backpacks. What's needed is a smarter, more integrated solution—one that not only helps users keep track of their items but also enhances security to prevent theft or loss. To meet this need, we present **Backtracker**, a Smart Backpack with Inventory Tracking & Security. Backtracker integrates -based item tracking, theft detection, and smart security mechanisms to ensure users always know what's in their bag and keep their belongings safe. Small RFID (Khan et al., 2018) tags attached to commonly carried items—such as a wallet, laptop, or notebook—enable a built-in scanner to monitor the bag's contents. If an important item is missing, users receive an alert through a mobile app before leaving a location, reducing the risk of forgetfulness. To enhance security, the backpack features an anti-theft system with motion sensors that detect unusual movement, such as an unauthorized attempt to open the bag. If a theft attempt is detected, the system can trigger an alarm or vibration alert. Additionally, an auto-locking mechanism secures the zippers in crowded areas and unlocks them when the user is in a safe space. With Bluetooth connectivity, users can check their inventory in real-time and receive geofencing alerts if they leave their backpack behind. Overall, by combining security and organization into one system, Backtracker provides a smarter, more reliable solution for modern users who need peace of mind while on the go.

1.2 Visual Aid

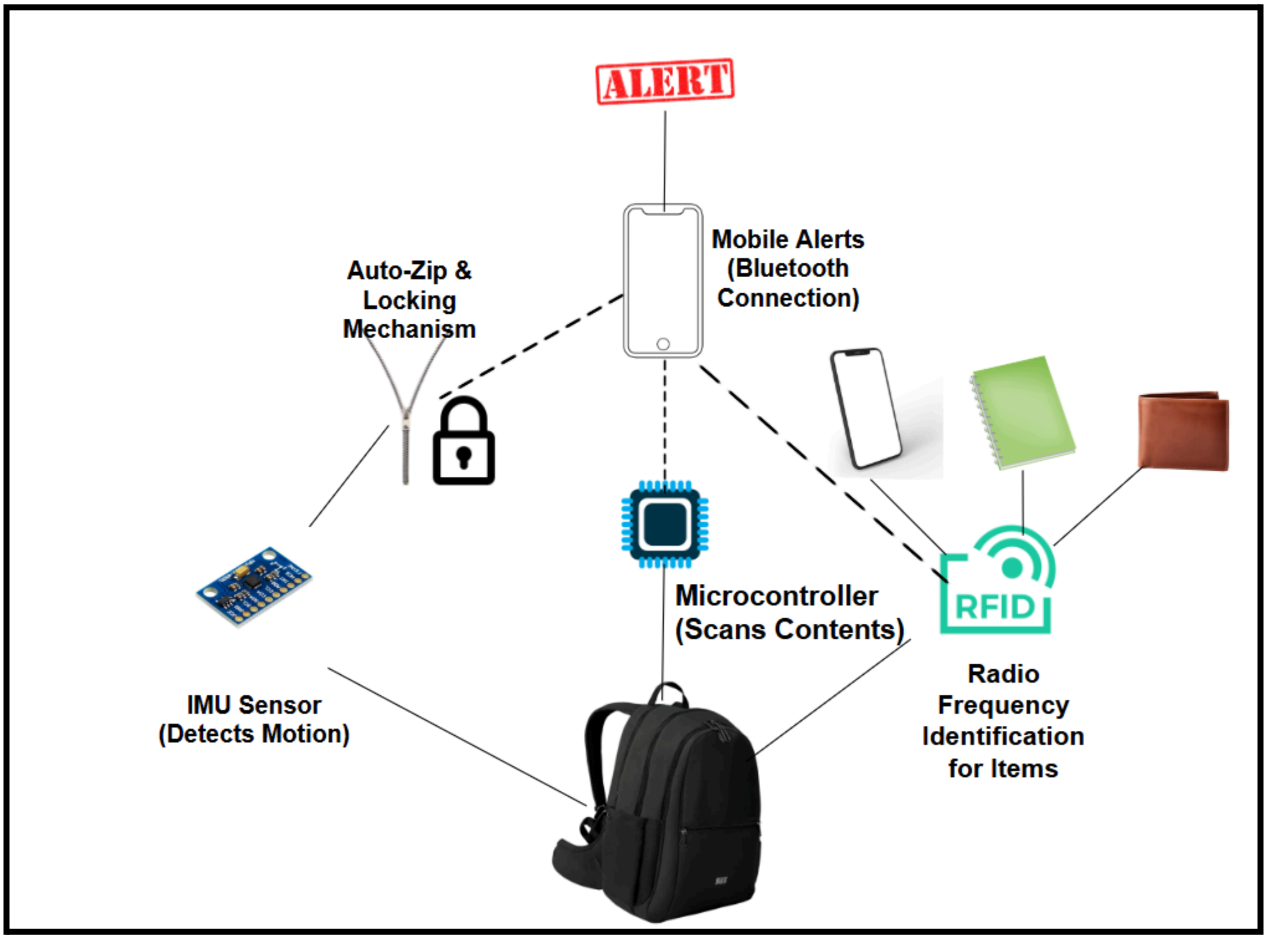
ALERT
Mobile Alerts (Bluetooth Connection)
Auto-Zip & Locking Mechanism
Microcontroller (Scans Contents)
RFID
Radio Frequency Identification for Items
IMU Sensor (Detects Motion)

Figure 1: Visual Aid of Components

1.3 High-level requirements list:

- **Accurate RFID-Based Item Tracking**: The backpack must integrate an RFID tracking system capable of detecting and tracking RFID-tagged items in real time. The system should scan the backpack's contents and send an alert to the mobile app if an essential item, such as a laptop, notebook, wallet, or keys, is missing before the user leaves a location.

- **Effective Theft Detection and Security Response**: The anti-theft security system must use an accelerometer or gyroscope (IMU) to detect unauthorized access attempts, such as sudden movement or unzipping while the bag is unattended. Upon detecting suspicious activity, the system should trigger a buzzer or vibration alert to notify the user and deter potential theft.

- **Reliable Auto-Zip & Auto-Lock Mechanism**: The backpack must feature motorized zippers and an electronic or magnetic locking system that can automatically lock or unlock based on the user's location. The locking mechanism should secure the bag in crowded environments and unlock when the user is in a designated safe area while allowing manual override when needed.

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 Block Diagram:

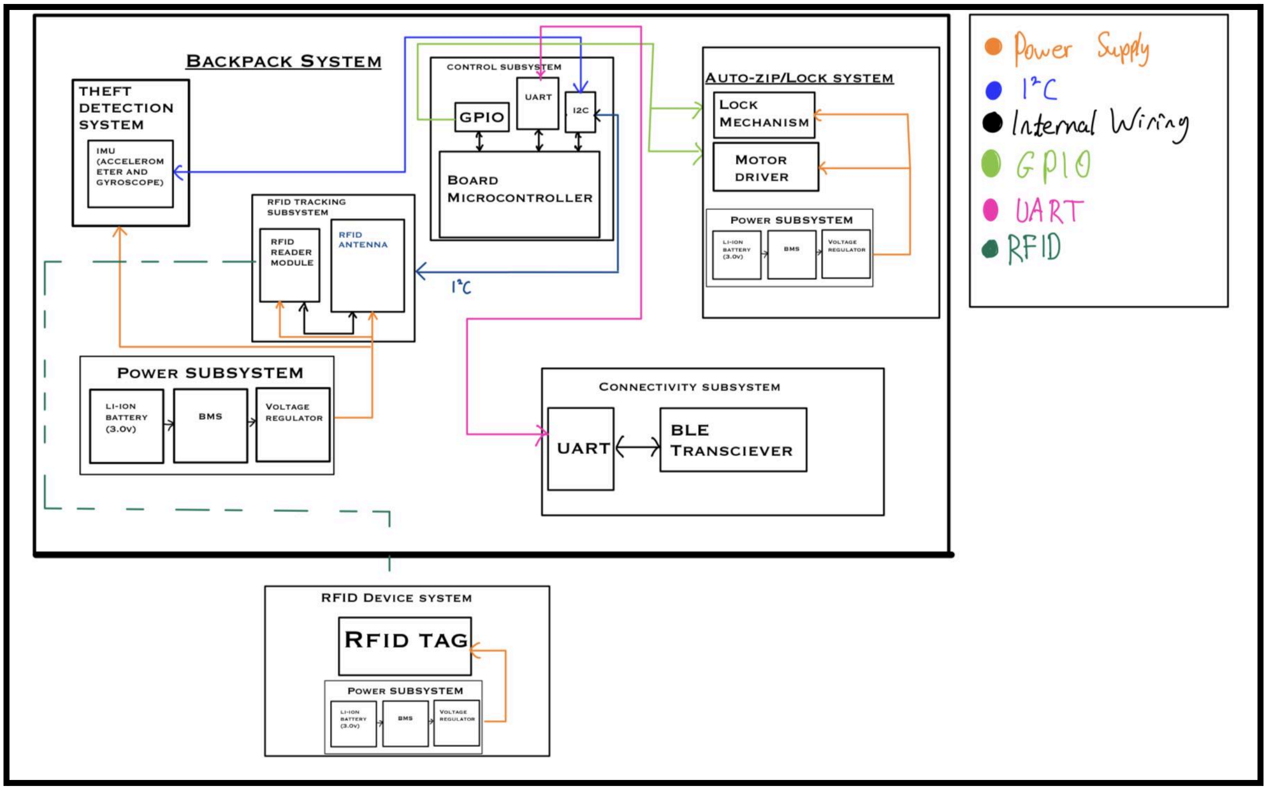

Figure 2: Block Diagram for Smart Backpack System

2.3 Subsystems

1. Board Microcontroller

Description:

The Board Microcontroller serves as the central processing unit for the Smart Backpack, coordinating all subsystem operations. It receives data from the theft detection system and RFID tracking subsystem, processes input signals, and executes control commands for the auto-zip/lock system. The microcontroller also facilitates communication with the mobile app via the BLE transceiver and ensures that power is efficiently distributed across all components (Souryal et al., 2011).

Design Decisions & Justifications:

- Processor Selection: A low-power ESP microcontroller was chosen due to its high efficiency and ability to handle multiple sensor inputs simultaneously.
- Interface Protocols:
  - I2C is used for communication with the RFID (RFID Journal) reader and IMU sensors (TDK IvenSense, 2023).
  - UART is used for Bluetooth communication.
  - GPIO is used for motor and lock control.
- Power Efficiency: The microcontroller operates at 3.3V with low power consumption to optimize battery life.

Interfaces:

- Inputs: Data from RFID tracking system (I2C), IMU sensors (I2C), and Bluetooth transceiver (UART).
- Outputs: Control signals for motorized zippers (GPIO) and lock mechanism (GPIO), alert signals to the mobile app (UART).

Requirements & Verification:

Requirements	Verification
The microcontroller must accurately process and relay signals from the RFID and theft detection system within 100ms.	Measure the response time using an oscilloscope when a signal is received and processed. Ensure the delay is within 100ms.
The microcontroller must send a locking command to the auto-lock system upon detecting unauthorized access.	Simulate unauthorized access and confirm that the lock engages via GPIO output verification.

Table 1: Board Microcontroller Subsystem - Requirements & Verification

2. Theft Detection System

Description:

The Theft Detection System utilizes an Inertial Measurement Unit (IMU), consisting of an accelerometer and gyroscope, to detect unauthorized movements or tampering with the backpack. Upon detection of abnormal motion patterns, the system alerts the microcontroller to trigger an appropriate response (ITP at NYU).

Design Decisions & Justifications:

- Accelerometer & Gyroscope: A 6-DOF IMU (MPU6050) is selected for real-time movement detection.
- Tamper Detection Thresholds:
    - Acceleration threshold: ±2g for sudden movements.
    - Angular velocity threshold: ±150 deg/s to detect rotations.

Interfaces:

- Inputs: Motion data from IMU sensor (I2C).
- Outputs: Alert signal to Board Microcontroller (I2C).

Requirements & Verification:

Requirements	Verification
The system must detect unauthorized movement exceeding ±2g acceleration or ±150 deg/s angular velocity.	Apply external force to the backpack and measure response accuracy via IMU output logs.
The system must send an alert signal to the microcontroller within 50ms of detecting suspicious motion.	Measure time delay between motion detection and alert signal transmission using a logic analyzer.
The system must differentiate between normal and suspicious movement patterns.	Conduct controlled experiments simulating everyday use versus theft scenarios.

Table 2: Theft Detection Subsystem - Requirements & Verification

3. Power Subsystem

Description:

The Power Subsystem provides a stable power supply to all components of the backpack. It consists of a Li-Ion battery (3.0V), a Battery Management System (BMS) for safety, and voltage regulators to supply required voltages to different subsystems.

Design Decisions & Justifications:

- Li-Ion Battery: Selected for its high energy density and rechargeable capability.
- BMS: Ensures protection against overcharge, over-discharge, and short circuits.
- Voltage Regulators: Convert 3.0V to 3.3V for the microcontroller and sensors.

Interfaces:

- Outputs: 3.3V regulated power for the microcontroller, RFID reader, BLE transceiver, and theft detection sensors.

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.
The BMS must prevent overcharging beyond 4.2V per cell.	Use a battery testing circuit to validate overcharge protection.

Table 3: Power Subsystem - Requirements & Verification

4. Connectivity Subsystem (BLE Transceiver)

Description:

The Bluetooth Low Energy (BLE) Transceiver enables communication between the Smart Backpack and a mobile application. It transmits real-time tracking data, security alerts, and lock control commands.

Design Decisions & Justifications:

- BLE 5.0 module was selected for low power consumption and fast connectivity.
- UART interface is used to exchange data with the microcontroller.

Interfaces:

- Inputs: Commands from mobile app (via Bluetooth).
- Outputs: Data to Board Microcontroller (UART).

Requirements & Verification:

Requirements	Verification
The BLE module must establish a stable connection within 2 seconds of power-on.	Test pairing time with a mobile device.
The BLE must transmit RFID tracking data within 500ms.	Measure latency using a Bluetooth sniffer.
The module must maintain a stable connection within a range of 10 meters.	Conduct connectivity tests in an open space and measure packet loss.

Table 4: Connectivity Subsystem - Requirements & Verification

5. Auto-Zip/Lock System

Description:

The Auto-Zip/Lock System consists of motorized zippers and an electronic locking mechanism that secures the backpack when unauthorized access is detected.

Design Decisions & Justifications:

- Motor Driver: A H-Bridge driver (L298N) is used to control motor direction.
- Locking Mechanism: Uses an electromagnetic latch that activates upon receiving a lock signal.

Interfaces:

- Inputs: Lock/unlock command from Board Microcontroller (GPIO).
- Outputs: Actuation of motorized zippers & lock.

Requirements & Verification:

Requirements	Verification
The motorized zippers must operate with a force of no more than 5N.	Use a force gauge to measure resistance.
The lock must engage within 200ms of receiving a lock signal.	Measure actuation time with an oscilloscope.
The lock must remain engaged even under 15N of pulling force.	Conduct stress tests on the locking mechanism.

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

6. RFID Tracking Subsystem

Description:

The RFID Tracking Subsystem scans RFID-tagged items inside the backpack and reports their presence to the user.

Design Decisions & Justifications:

- UHF RFID Reader selected for multi-tag detection.
- Reader Sensitivity: Optimized to detect items within 30cm range.

Interfaces:

- Inputs: RFID tag signals.
- Outputs: Data to Board Microcontroller (I2C).

Requirements & Verification:

Requirements	Verification
The RFID system must detect at least 95% of tagged items in the backpack.	Perform detection tests with multiple items.
The system must update the item inventory within 1 second.	Measure response time using a microcontroller data logger.

Table 6: RFID Tracking Subsystem - Requirements & Verification

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.

2.4 Software Design

2.4.1 RFID-Based Item Tracking and Security Response

The core functionality of our project relies on the software decision-making implemented on our PCB microcontroller, ensuring real-time item tracking and theft prevention. The microcontroller is responsible for detecting RFID-tagged items, communicating with the user's device via Bluetooth Low Energy (BLE) (Novel Bits), and managing security features such as motion detection and an automatic zipper-locking mechanism. By integrating these functionalities, the system provides both inventory awareness and anti-theft protection.

When an RFID-tagged item is removed from the backpack, the RFID reader detects its absence and relays this information to the microcontroller. The microcontroller processes this event and transmits an update to the user's computer via Bluetooth communication. The locally hosted web application then reflects this change in real-time, updating the display to indicate which items are missing (Bluetooth SIG). Similarly, when the removed item is placed back into the backpack, the RFID reader detects its presence, prompting the microcontroller to update the web application accordingly to show that the item has been accounted for. This seamless tracking mechanism ensures that users always have a clear understanding of their backpack's contents.

Beyond inventory tracking, the system also utilizes the BLE transceiver as a proximity-based security measure. The microcontroller continuously monitors the BLE connection between the backpack and the user's device. If the connection is lost, this indicates that the backpack has moved beyond the expected range, potentially signaling an unattended or stolen bag. In such cases, the system enters a heightened security mode.

To further enhance security, the Inertial Measurement Unit (IMU) plays a critical role in theft detection. The IMU continuously tracks acceleration and orientation changes, identifying any extreme motion events, such as sudden jerks, rapid movement, or erratic changes in orientation.

If these extreme fluctuations are detected while the BLE connection is lost, the system assumes that an unauthorized individual is tampering with the backpack. As a response, the auto-zip mechanism immediately engages, locking the backpack's zippers to prevent access. Simultaneously, an LED indicator blinks to visually signal that the anti-theft protocol has been activated.

By integrating RFID-based inventory tracking with BLE-based proximity detection and IMU-based motion analysis, our system offers a comprehensive security and organizational solution. The software-driven approach ensures that users are always aware of their belongings while proactively preventing unauthorized access, enhancing both convenience and security in daily use.

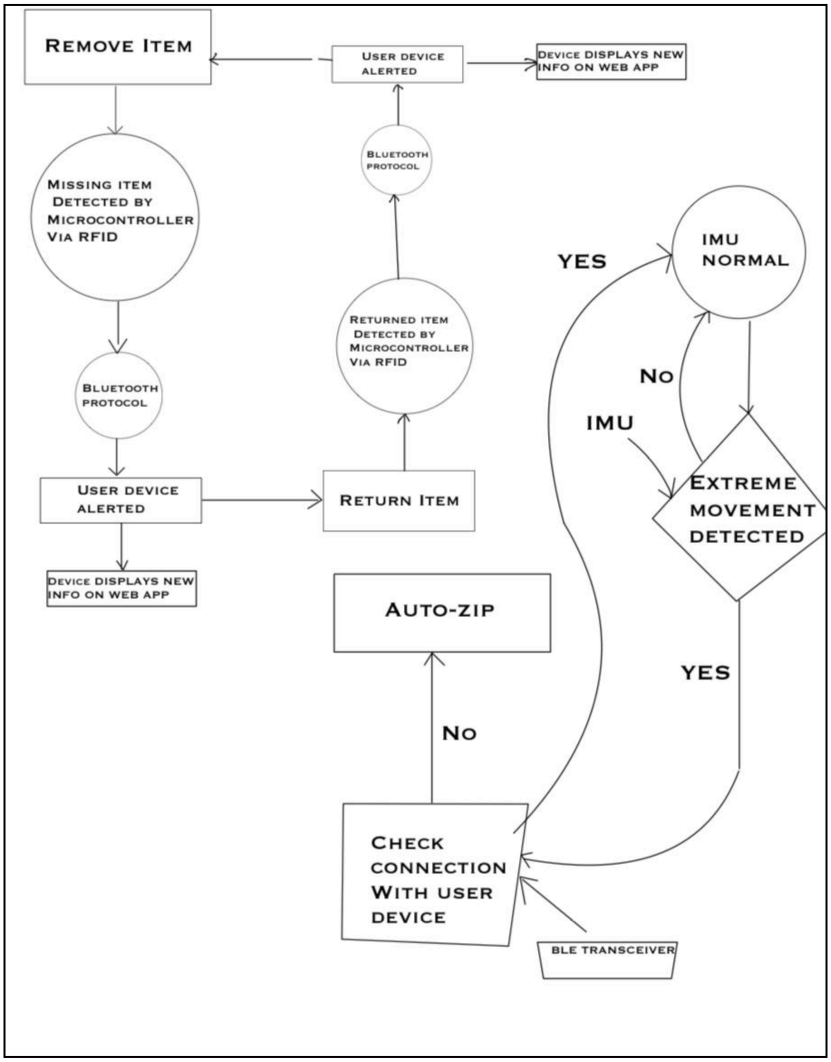
Remove Item
User device alerted
Device displays new info on web app
Missing item Detected by Microcontroller Via RFID
Bluetooth protocol
Returned item Detected by Microcontroller Via RFID
Bluetooth protocol
User device alerted
Return Item
Device displays new info on web app
IMU normal
YES
No
IMU
Extreme movement detected
YES
Auto-zip
No
Check connection With user device
BLE transceiver

Figure 3: Software Design Block Diagram

2.5 Tolerance Analysis: Ensure the motor produces enough torque to secure the lock even if the supply voltage drops by 10%.

Analysis:

- **Nominal Requirement:** The motor must deliver at least 0.5 N·m of torque.
- **Voltage Impact:** A 10% drop in voltage typically reduces the motor's torque by about 10%.
- **Calculation:**
  - With a 10% drop, the effective torque is about 0.9 times the rated torque.
  - To ensure the effective torque remains at or above 0.5 N·m, the rated torque should be at least 0.5 divided by 0.9, which is approximately 0.56 N·m.

Choose a motor with a rated torque of at least 0.56 N·m to ensure the auto-zip/lock mechanism operates reliably, even with a 10% voltage drop.

3 Cost and Schedule

3.1 Cost Analysis

- Aashish Subramanian
  - Assumed Salary: $52.50/hour
  - Hours to Complete: 45
  - Calculation: ($/hour) × 2.5 × 45 hours = $5906.25
- Seth Oberholtzer
  - Assumed Salary: $52.50/hour
  - Hours to Complete: 45
  - Calculation: ($/hour) × 2.5 × 45 hours = $5906.25
- Shreyas Sriram
  - Assumed Salary: $52.50/hour
  - Hours to Complete: 45
  - Calculation: ($/hour) × 2.5 × 45 hours = $5906.25
- Total Labor Cost: $17,718.75

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-CA0508KRX7R9BB102 CT-ND	5	$0.21	$1.05
W3A45C473KAT2A	KYOCERA AVX	478-11168-1-ND	5	$0.25	$1.25

Table 7: Parts list

GRAND TOTAL COST: $82.23 + $17,718.75= **$17,800.98**

3.2 Schedule:

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	**Have fun!** 🙂	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

4. Discussion of Ethics and Safety

4.1 Privacy and Data Security

The BackTracker system relies on RFID tracking and Bluetooth connectivity, making data security and user privacy key concerns. The ACM Code of Ethics emphasizes responsible data management and privacy protection, which we take seriously in designing this system.

To prevent unauthorized access to tracking data, all RFID and Bluetooth communications will be encrypted using AES-128 or AES-256 encryption (IEEE). This ensures that only approved devices can interact with the system. Additionally, only authenticated users will be able to access their inventory records through the mobile or web application. To enhance security, multi-factor authentication (MFA) or biometric authentication, such as fingerprint scanning or Face ID, may be required for accessing sensitive features.

The system is designed with a minimal data storage approach. It does not store unnecessary user information, reducing exposure in the event of a breach. The backpack will track only the presence or absence of items and will not record a user's movements or personal information beyond what is necessary for its core functionality.

To prevent hacking, the Bluetooth module will be configured with a whitelisting feature, allowing only pre-approved devices to establish a connection (IEEE). The web application will also be protected with security measures such as firewalls and intrusion detection systems to prevent cyberattacks.

4.2 Prevention of Unauthorized Tracking

One of the biggest ethical concerns with RFID (Juels, 2006) tracking is the potential for misuse, such as unauthorized monitoring of individuals. Without safeguards, RFID systems could be exploited to track users without their consent. To prevent this, the BackTracker system is designed to only function when items are inside the backpack. The RFID scanner will not continuously transmit data, ensuring that the system is not used for unintended surveillance.

Users will be required to provide explicit consent before enabling tracking features within the mobile application. They will also have full control over which items are tagged and tracked. At any time, users can disable tracking for specific items or reset the tracking data, ensuring that they maintain full control over their privacy.

The RFID system will also include an anti-tampering feature. If an unauthorized device attempts to scan the RFID tags inside the backpack, the system will detect this and immediately send an alert to the user's mobile device. This feature ensures that no one can discreetly attempt to monitor the user's belongings without their knowledge.

4.3 Safety Considerations

The BackTracker Smart Backpack contains electronic components, RFID scanners, and motorized zippers, all of which introduce certain safety concerns. Addressing potential risks related to battery usage, electrical hazards, and automated zipping mechanisms is essential to ensure user safety.

Battery and Electrical Safety

Since the system is battery-powered, overcharging, overheating, and short circuits are potential risks. To address this, the battery system will follow UL 2054 safety standards for portable power sources. The design includes overcharge and over-discharge protection, ensuring that the battery is not stressed beyond safe limits.

Short-circuit protection will be built into the system, utilizing fuses and circuit breakers to prevent excessive current draw. Thermal monitoring will also be implemented, automatically shutting down charging if the battery temperature exceeds safe limits. The RFID and Bluetooth components will comply with FCC regulations for electromagnetic interference (EMI) to prevent interference with other electronic devices.

Auto-Zip and Locking Mechanism Risks

The backpack features an automated zipper and locking system, which introduces physical risks such as pinching, entrapment, or accidental activation. To ensure user safety, several safeguards have been incorporated into the design.

The auto-zip feature uses low-torque motors to prevent excessive force during operation. This reduces the risk of injury if a user's fingers or clothing accidentally get caught in the zipper mechanism. The system also includes a resistance detection algorithm, which will automatically stop and reverse the zipper if it encounters an obstruction.

A manual override button will allow users to disengage the auto-zip mechanism at any time. This ensures that the backpack can always be opened manually, even if the automated system malfunctions. To prevent unintended operation, the zipper will move at a gradual speed rather than snapping shut quickly. An LED indicator and sound cue will alert the user before the zipper activates, giving them time to intervene if needed.

4.4 Ethical Considerations in Development

As engineers, it is our responsibility to ensure that technology is developed ethically and benefits users without introducing unintended risks. To maintain transparency, all features related to RFID tracking, motion detection, and Bluetooth connectivity will be clearly documented and disclosed to users.

Users will have full control over how the system functions, including the ability to disable or modify features as needed. To ensure security over time, regular software updates will be released to address vulnerabilities and prevent potential exploits. Accessibility will also be considered, ensuring that the backpack and mobile interface are user-friendly for people with different needs and abilities.

4.5 Conclusion

The BackTracker Smart Backpack is designed to enhance both security and convenience, but with these features come ethical and safety responsibilities. Strong encryption, user authentication, and data minimization practices protect privacy, while compliance with UL and FCC safety standards mitigates electrical risks.

The auto-zip and locking mechanisms have been designed with safety in mind, incorporating low-force motors, resistance detection, and manual override options. By balancing security, functionality, and ease of use, the BackTracker system aims to provide a reliable and safe experience for users while adhering to high ethical and engineering standards.

5. Citations

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