We have ensured the safety measures in both the hardware and software aspects of the project to ensure that the data transmission is secured and no any eavesdropper or hacker can listen to the data that is being transmitted or hack our system for their advantage.

# Hardware Security

### Backup Memory

All the devices have an external EEPROM connected to them along with their internal EEPROM to store their balance. So in any case if the main microcontroller of the devices gets physically damaged, the users can get the balance refunded by reading the external EEPROM through our master machine.

### Preventing Unauthorized Reading, Reprogramming

The system uses the inbuilt lockbyte feature to make sure that the third party can’t access our firmware and data stored on the devices that we have built to reverse engineer the project and hack the system to their advantage. Once we have written the program and setup the devices we use the configuration of lockbyte to prevent any further programming of the device or read back data/information stored in the devices.

### Short Range Communications

As the project uses NFC technology that allows the transmission of data within the range of ~10cm, no eavesdropper can easily listen to the data that is being transmitted. Added to it the fact that there is implementation of AES encryption to the messages, no unauthorized devices can read and decipher the message without the secret key preventing any third party from reading and/or manipulating the data that is being communicated among the devices.