Our group project brings to light multiple possible solutions that can be used in a multitude of environments. By utilising a Raspberry Pi miniature computer with a 3G/4G sim installed we can create a mobile platform to both collect and submit data to a cloud based server. This particular data can be accessed by different means, like remote access from a device through authorised login to the cloud based servers, using a Near Field Communication (NFC) standard like Bluetooth or by physical connections and links like a scannable QR code.

Possible solutions that we will focus on include;

* Barking Logs for obedience training of dogs,
* GPS tracking information,
* Registration details (including owner contact details)
* And activity details (period of time moving/stationary).

Unfortunately not all project ideas come without flaws, for this project to be successful most if not all of these issues will need to be addressed.

Power supply of the device, this isn’t much of a flaw but a stepping stone on completing the final design of the project. There are 2 possible solutions for power supply to the Raspberry Pi system, the first being easily replaceable commercial off the shelf battery products such as AA batteries or 9v a more commonly used battery for mobile devices like this. The other solution for power supply is a rechargeable battery pre-installed onto the device that can be then charged through a micro-USB port.

Durability, unfortunately Raspberry Pi’s, like most other computer equipment, aren’t very resilient in open environments and to physical impacts like rocks or even dust. A suitable housing unit for the device would need to be designed and tested to ensure the durability and size constraints are suitable and do not cause and hazardous scenarios or irritate the wearer.

Radiation Hazard, with all wireless communication systems comes the risk of long term exposure, although mostly miniscule sufficient testing will need to be completed to advise customers of the safety of the device. Reports and results from these tests should be available through multiple means so that customers feel that they know the risks involved with the device if there are any.

By design devices on a smaller scale than usual will attract a higher price due to current day limitations of small scale systems, although in future this will become less of an issue it very much is one today. To counteract this a payment model will need to be decided upon, this could be a single once of purchase which would be quite large and scare away some customers but means they can use the device as much as they wish once purchase or a smaller up front cost with a subscription model attached for monthly payments for usage of the device itself.

The last concern is of device and customer security, as the devices will have access to the cloud based server and customer information direct connections through the device may still allow unwanted guests to connect. Possible means to combat this could include limiting the devices themselves to only send information to the server or to only have access to very specific information such as the owner contact information but nothing else. Another possibly even more secure option would be to require two factor authentication for any external connections through the device, this could allow local authorities and veterinary clinics to have their own access code to allow them to locate information about the owner of the device.