**DUNDALK INSTITUTE OF TECHNOLOGY**

**A logo with a bird and text

Description automatically generated**

**Technical Documentation On**

**WRISTBAND AIR QUALITY MONITOR**

Project Carried Out

**By**

**D00251785 PATRICK ORJIEH**

**D00244618 ROBERT NUGENT**

**D00261104 CONOR MC GINN**

**D00240060 HANNAH MC ELROY**

Under the Supervision of

**DR. JOHN LOANE**

DEPARTMENT OF COMPUTING AND MATHEMATICS

**SCHOOL OF INFORMATICS AND CREATIVE ARTS**

**DEPARTMENT OF VISUAL AND HUMAN CENTERED COMPUTING**

**Security and Privacy**

**Device Security:**

The first feature that we will be implementing in order to support device security is a 4-digit pin for the device. When first using the wristband, the user will be prompted to setup a 4-digit PIN which will be used in the future to gain access to the device when attempting to connect to it. This will prevent anyone from connecting to the device and tampering with it.

To build on the security of this PIN, we will also implement a device lockout system. Whenever the user enters the PIN incorrectly 5 times then the device will be locked and not allow any access to it until the lock is lifted. When the device becomes locked, an email will be sent to the email address associated with the device with an option to unlock the device. By using this system. It will prevent unauthorized users to have an infinite number of tries at bypassing the PIN to access the device.

Another feature that we are designing that will increase the level of security for the device is a way for the user to remotely wipe or lock the device if they lose it. Once the device becomes lost, it will be vulnerable if found by someone else. To counter this, we will allow the user to lockdown their lost device from their current location using the app so that no one will be able to access it and tamper with it. As well as this, the user could wipe all of their data from the device and essentially reset it so that if someone would gain access to it, they wouldn’t be able to see any of their data.

**Data in transfer security:**

The main way that we are going to keep data safe in transfer is through end-to-end encryption. This means that the data will be encrypted before it is transmitted and will only be decrypted once it has reached its destination. There are a lot of different ways to do this but the way which we plan on doing it is through the use of a strong encryption algorithm called AES, which stands for Advanced Encryption Standard. We have decided to use this specific algorithm as it is considered to be highly secure and efficient which will highly contribute to the overall security and performance of the system.

Another way to improve the security of the data is by carrying out data integrity checks. To ensure that the data was not messed with during transfer, we must check the integrity of the data once it is received by the server. We can do this by using cryptographic hashes. When the data is hashed using a hash function, a hash value is produced. This value will be sent with the data to the server so that the server can compare the received hash value with the one that it gets from carrying out the hash function itself. If the hash values match, then the data has not been messed with, otherwise, the data isn’t the same as what was originally sent.

Finally, we will make use of tokens during data transfer for authentication reasons. Tokens are important for authenticating the users who will be carrying out these data transfers. By using tokens, we can ensure that the user has appropriate permissions to carry out what they are trying to do as well as determine if they are a valid user or not. If the token hasn’t expired and is has been verified, then the action relating to data transfer will be performed.