CSI3106 – Software Architecture & Design

Bryce Wilkinson - bjwilkin@our.ecu.edu.au -

Christian Radei - cradei0@our.ecu.edu.au - 10344996

Contents

[**PART A:**](#_i2msz2h061u9) **2**

[Introduction:](#_gjdgxs) **2**

[System Description:](#_30j0zll) **2**

[Assumptions:](#_1fob9te) **2**

[**Quality Attributes:**](#_i1sdhsmnhhul) **3**

[Quality Requirements/goals:](#_2et92p0) **3**

[**Stakeholders:**](#_pr4is1bz39r3) **4**

[**Reasons for Concern with Architectural Design:**](#_21polrjiubj1) **5**

[**PART B:**](#_5x1xdpvciftx) **6**

[Initial Components:](#_1t3h5sf) **6**

[Components & Quality Attributes:](#_4d34og8) **7**

[Server:](#_2s8eyo1) 7

[Network:](#_17dp8vu) 7

[Data Storage:](#_3rdcrjn) 7

[Bio-sensors:](#_26in1rg) 7

[**Component Justification:**](#_xg474z5y8r2) **8**

[Server](#_u3jsevx3zalt) 8

[Network](#_csnwmemnt7ru) 9

[Data Storage](#_44sinio) 9

[Bio-sensors](#_2jxsxqh) 9

[**Physical Design of the System:**](#_vyyfpnqc4p7w) **10**

[Logical Design of the system:](#_3j2qqm3) **11**

[Sequence Diagram:](#_1y810tw) **11**

[Final iteration:](#_4i7ojhp) **12**

[**Final Components:**](#_mcg20b8e3jo0) **13**

[**Final Sequence Diagram:**](#_3fce7ckchwoz) **14**

# PART A:

# Introduction:

With the increased use of embedded systems in the modern era the process is now understood quite well and thus more reliable, since reliability is established it can now be used in the medical sector where a single error may be fatal.

# System Description:

The device in question is a wristband that is attached to the patient's arm or leg and utilises various sensors within to collect information such as body temperature, blood pressure and heart rate. To collect information on the patient’s health & assess whether the doctor should be notified & notify the doctor if necessary. The information is stored in a database that the doctor can access, with the patient’s relevant medical records stored within. This system runs in real-time and availability is crucial due to the nature of the system.

# Assumptions:

* The user is in a location where the device can connect to the server either via cellular data or a wireless network connection
* The means to send data over Wireless or a cellular connection is secure
* Patients information is confidential
* Patients information can only be seen by a doctor with authority over that patient
* The user is not confined to one area
* The device can tolerate various weather and day to day conditions such as water
* The device has a way to charge itself whilst still being fully operational such as kinetic or solar energy
* The device has reliable sensors
* The device has long battery life and storage capacity
* The device is energy efficient and does not produce excess heat
* The development team has contact with medical professionals in this field
* The development team has knowledge/experience working with embedded systems and microsystems.

# Quality Attributes:

Since the systems use is for the medical sector and its use can determine whether high risk patients live or die. As well as the system having a very specific use in a prestigious field of knowledge, experts in that field should be consulted and the contractor/employee should be satisfied. It is crucial that the system has the following attributes below:

* **Reliability**
* **Accuracy**
* **Performance (Latency)**
* **Availability**
* **Security**

The margin for error in this system is miniscule meaning that extensive testing must be conducted on the system, during development the team should design this system with testability in mind. The server and device must have a reliable means of transmission that is always secure and available.

# Quality Requirements/goals:

1. The system should be able to recognise when communication between the device and the server is unavailable the device should then forward this data when they can communicate with one another. This can be done via a storage device, considering the size of the system a microSD card can be used and can store more than enough data (up to 256Gb), a cache can also be used but a microSD card will be more useful since if the doctor needs a back up due to malfunction they can use the microSD card. (***Reliability***)
2. The system must be scalable in both patients and doctors. To do this a patient and doctor entity must be created so that a doctor can have many patients, but a patient can only have one doctor. Only the doctor with that patient can view the patient’s medical data unless the event of an emergency (***Performance & Scalability***)
3. The system will try to be available 100% of the time. Any downtime shall be documented and the data that was not transmitted in the downtime will be accounted for. Both the device and the server should have a reliable power source. The device is wireless and could be charged via a variety of forms such as batteries, kinetic energy and solar energy. The server should account for power outages and have its own generator so that it will remain operational in the event of a power outage. (***Availability***)
4. The system must be secure. Medical records and patient data are highly confidential, if the patient’s records were accessed by a malicious individual either within the organisation or by intercepting data transmission. Steps should also be taken to ensure that the patients microSD is secure, the microSD should be encrypted via a secure encryption algorithm. The server should always be kept in a secure location so that it is not vulnerable to hackers and a user privileges system is essential in the database (***Security***)
5. The system should be extensively tested and adjusted to account for margins of error when the bio-sensors gather patient data. (***Accuracy***)
6. The system should have satisfactory internet access speeds for data transmission, a microcontroller fast enough to support live data encryption before storing as well as handling network requests at the same time, and a data storage source with fast enough read and write speeds for the intended data (Performance, Latency)

# 

# Stakeholders:

|  |  |  |  |
| --- | --- | --- | --- |
| **Stakeholder** | **Description** | **Internal or External** | **Desires** |
| Contracting company  (MAJOR) | The company investing in the product.  In this case we will assume the contractor is a government organisation | Internal | reliable release date  minimised losses  a system that fulfils all requirements |
| Project Team  (LARGE) | The team designing the product.    Since it’s the medical sector every member of the team must pass sufficient background checks | Internal | Money  Good product  Fast release date |
| Patients  (MINOR) | The people that will wear this device | External | Reliability  Security  Comfortability  No undesirable side effects |
| Doctor  (MODERATE - MINOR) | The people that will issue, manage & monitor this device | External | Reliability  Easy to use system |
| Vendors & Hospitals  (MODERATE) | The potential consumers & clients of the finalised project | External | Security  Reliability  Cost  Visible benefits |

# 

# Reasons for Concern with Architectural Design:

With the device being limited in size, there are restrictions in terms of computing power meaning that resource intensive operations such as visualising and trimming data cannot be done by the device located on the patient.

The size also leads to issues such as battery life, durability and costs.

The device is designed to be used almost constantly therefore it needs to have a strong battery life and a way to charge when its being used.

Durability is also a problem as the device should be small and lightweight. The device is intended for everyday use with high risk patients, so we can assume that the device may be exposed to being dropped, hit or exposed to water. We can also assume that the patient will be in no condition to go mountain climbing or skiing in the alps, so the durability shouldn’t be too extreme.

The costs of the device may also be an issue due to the cost of the factors mentioned above, as well as gathering an experienced team and cost of small bio-sensors.

# PART B:

# Initial Components:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Name** | **Desc.** | **Input** | **Output** | **Quality Attributes** |
| Bio-Sensors | Collects biological data from patient | Patient (Using the system) | Data Storage | Accuracy  *(data gathered must be accurate)* |
| Data Storage | Encrypts and stores patient data on MicroSD | Bio-Sensors  \* Network | Network, MicroSD card | Security *(Encryption adds security)*  Reliability *(readings can be examined by a doctor and work as backup data if the server corrupts)*  Availability  (*Data can be resent to network component*) |
| Network | Sends encrypted patient data across a secure network to the server | Data Storage  \*Server | Server  \*Data Storage | Security  *(Encrypted data is sent across a secure network)*  Availability  *(data will be resent to the server, if the server doesn’t receive the data)* |
| Server | Stores device information within a database for doctors to access. Performs more complex data analysis and calculations because it has more competing power then the device itself | Network | Doctor (End User) | Security  *(The server should be in a secure location, utilising appropriate protocols)*  Availability  *(Server aim for permanent availability)*  Performance  *(The server reduces the strain on the patients device, handling complex operations with the device)* |

\* = callback

# Components & Quality Attributes:

## Server:

To meet security, availability and performance goals. A Server managed by the company or contractor is best. Given that this project is for the medical sector its safe to say that the costs of installing and managing a server are far less than the potential losses due to malpractice, a data breach, extended server downtime or terrible performance.

## Network:

The network Component has the goal of security and availability. Because it’s the path that connects the device to the server, ideally this path should be open as much as possible to send patient data in real time. This means of communication must be secure as it may be vulnerable to attackers and medical records are confidential information. Although encryption does add an extra layer of security.

## Data Storage:

Data storage is to establish a reliability and availability within the device, in the case of server corruption or the device being unable to communicate with the server, the patient’s data can still be collected.

Storing and sending the raw data amongst the system is a security issue, this is solved by encrypting the data within the system which is done in this component.

## Bio-sensors:

The bio-sensors establish an accurate reading from the device, after they have been tweaked by the team to ensure their accuracy. Having inaccurate readings can be a catastrophe in this case as a patient close to death could be viewed as fine by the device.

# 

# Initial Component Justification:

## 

## Server

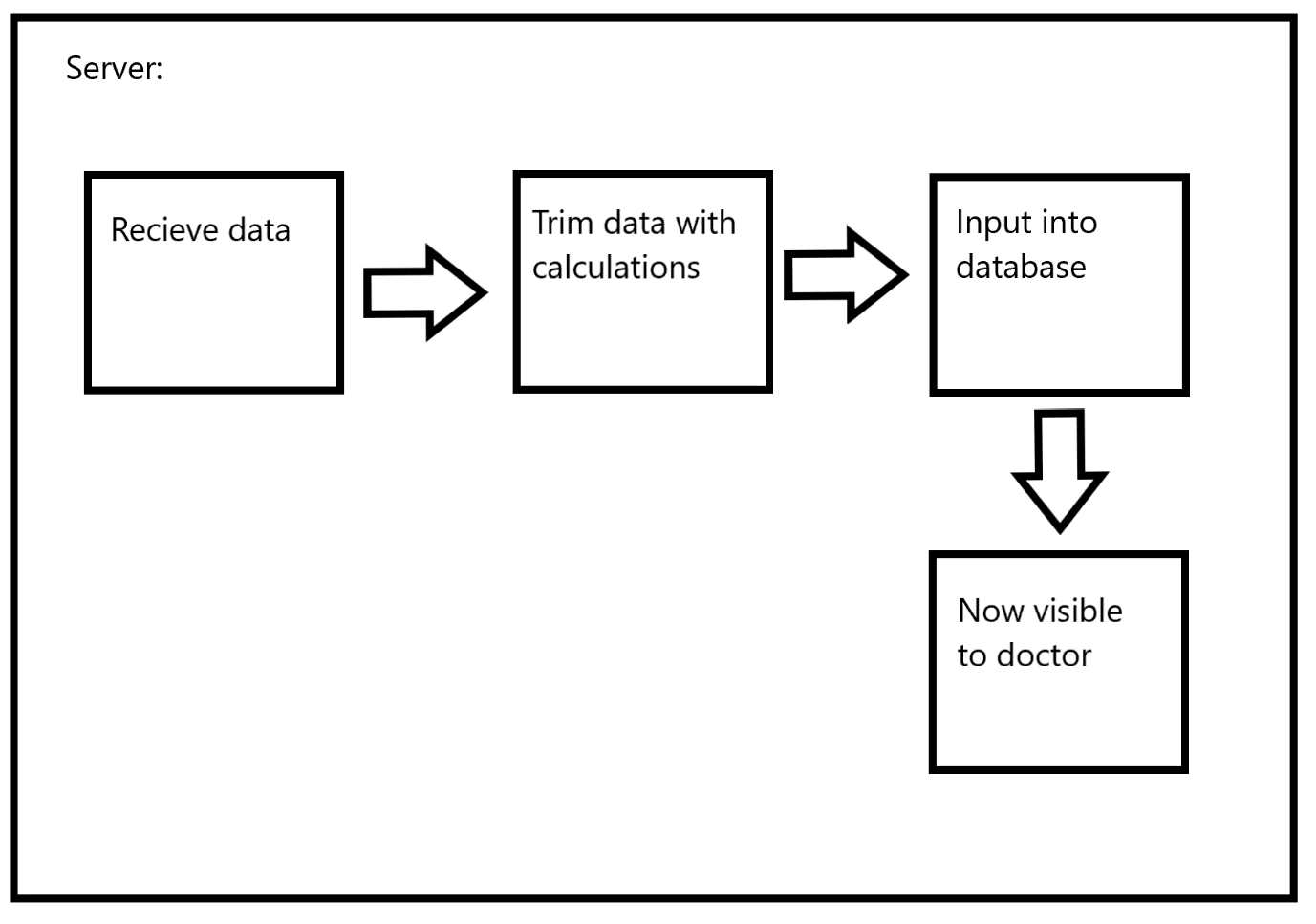
a)

The server is made into its own component as it is separated by location from the rest of the device as well having a different task compared to the rest of the device. The server receives the information from the device, trims the data and then presents it to the appropriate doctor.

b)

While technically the server will have subcomponents such as calculation and database entry, the server should be viewed as a single entity for abstraction.

Below are the steps the server undertakes when receiving data.



## Network

a)

the role of this component is sending and receiving data between the device on the patient and the server. Although that is dependant on the method to communicate between the device on the server, depending on the method of communication the network may have to translate the data into the appropriate transmission format. This translation layer can be considered a subcomponent to the network component.

b)

It is not necessary to break this down into additional components as although the data may have to be translated. Translation is extremely common and is built into Network Interface Cards, so this should require minimal to no work for the team.

## Data Storage

a)

Data storage is a component since there needs to be a way to resend data to the network component as well as encrypt the patients data.

b)

Data storage and encryption should be separate entities because they rely on different parts of the device (microSD & an encryptor) as well as having separate outcomes (security & availability +reliability) although it is important for the data to be secure before being stored in data storage they should be separated.

## Bio-sensors

a)

Bio-sensors have one role within the system to read the patients data, they do not perform any other important operations.

b)

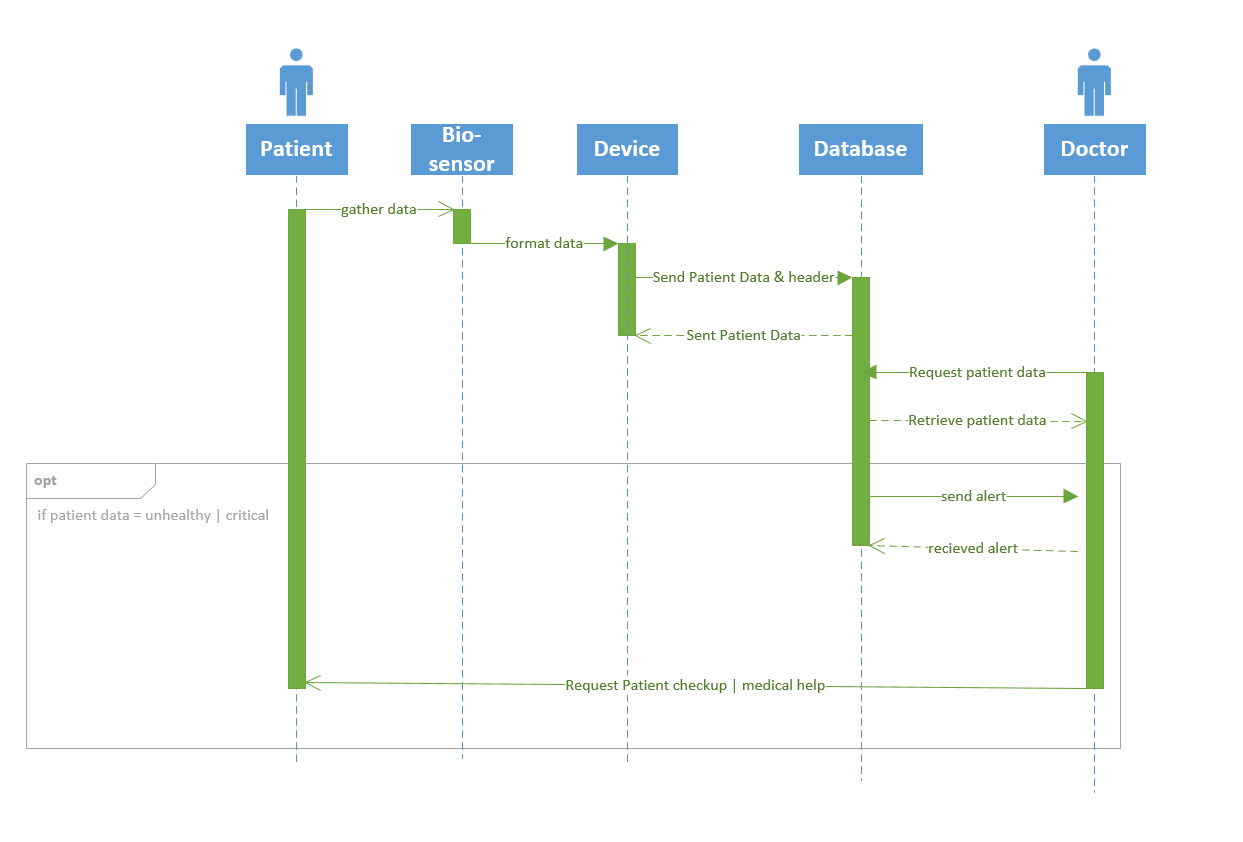
Bio-sensors would be unnecessary to divide further, we could divide the individual bio-sensors up into their own components however in this case abstraction is better since each biosensor does the same thing.

# 

# Physical Design of the System:

# Logical Design of the system:

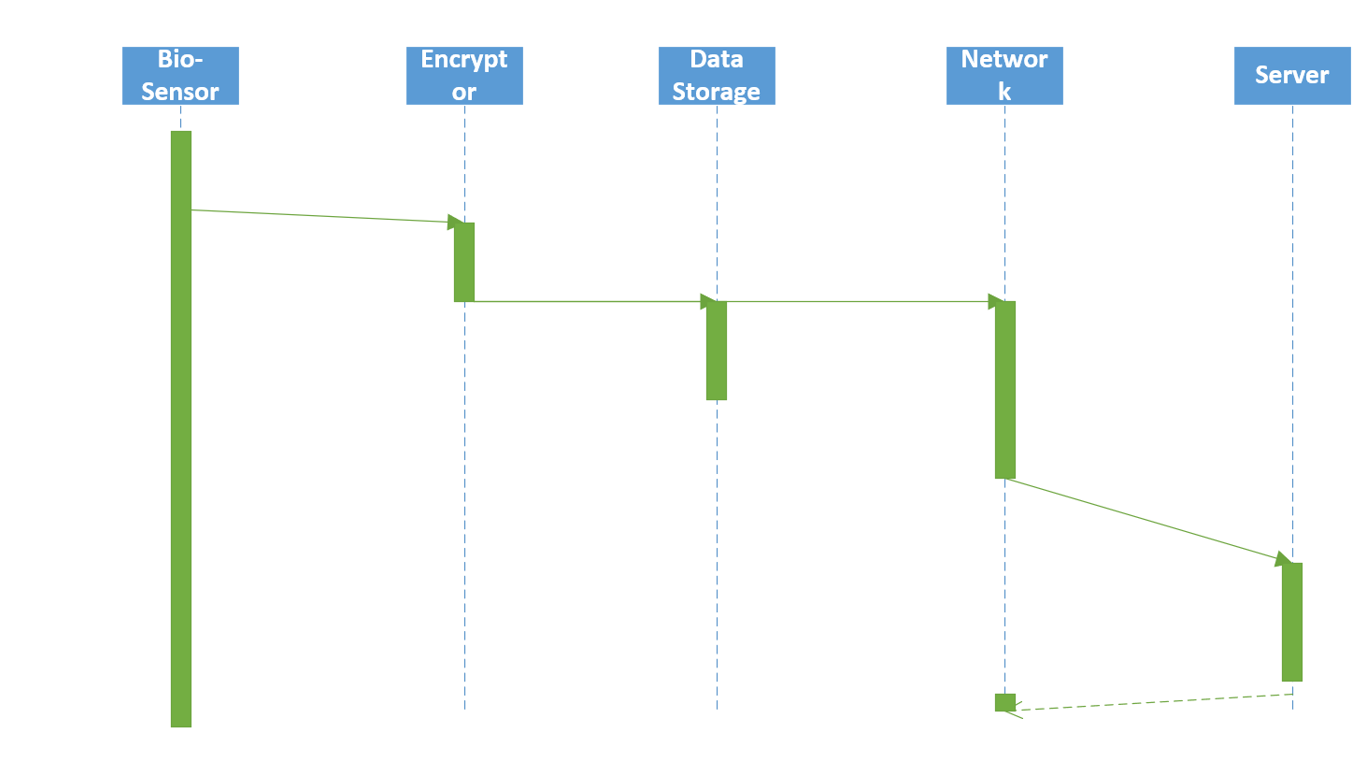
# Initial Sequence Diagram:



# Initial Redesign with Encryptor:

Initially we had the system send patient data gathered from the sensors directly to the data storage where the data storage could then connect to the network for when the server requested specific data. However after researching we realised that a microcontroller in between the sensor and data storage was required, that would be used to encrypt the patients data before storing it, and could be used to connect from the sensors and to the network and data storage, so that any requests from the server could be sent from the network to the microcontroller which could then get the relevant data from the data storage and forward it back to the network. This new microcontroller component contains a cpu onboard as well as memory, and is given the name “Encryptor” in the component list as that is its primary functionality. We thought to add two microcontrollers instead of only one, dividing up the tasks of encrypting data and handling network requests, but decided against this due to increases in costs, the size limitation of the device as well as additional strain on the development team.

# Draft Redesign:

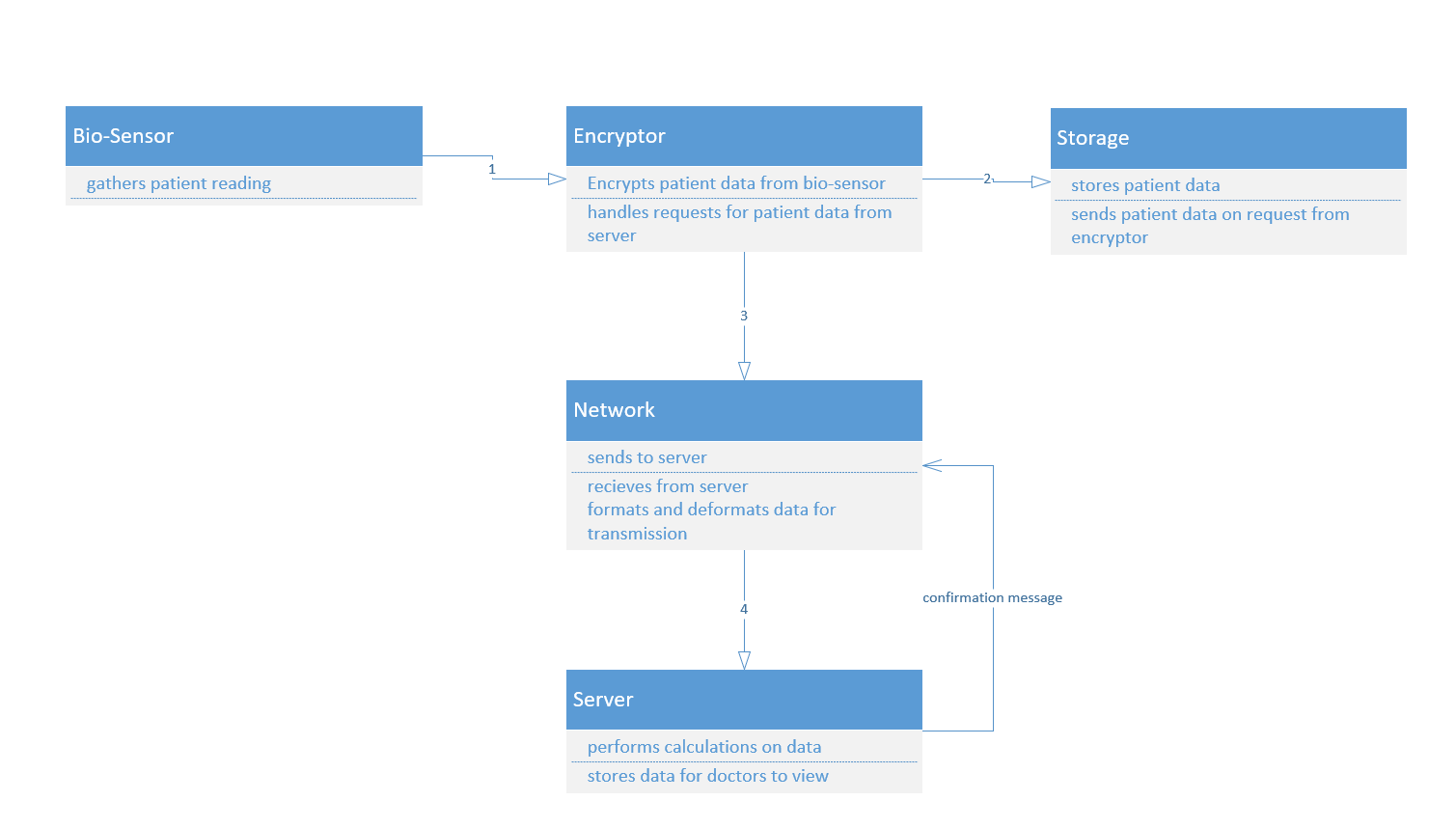


# 

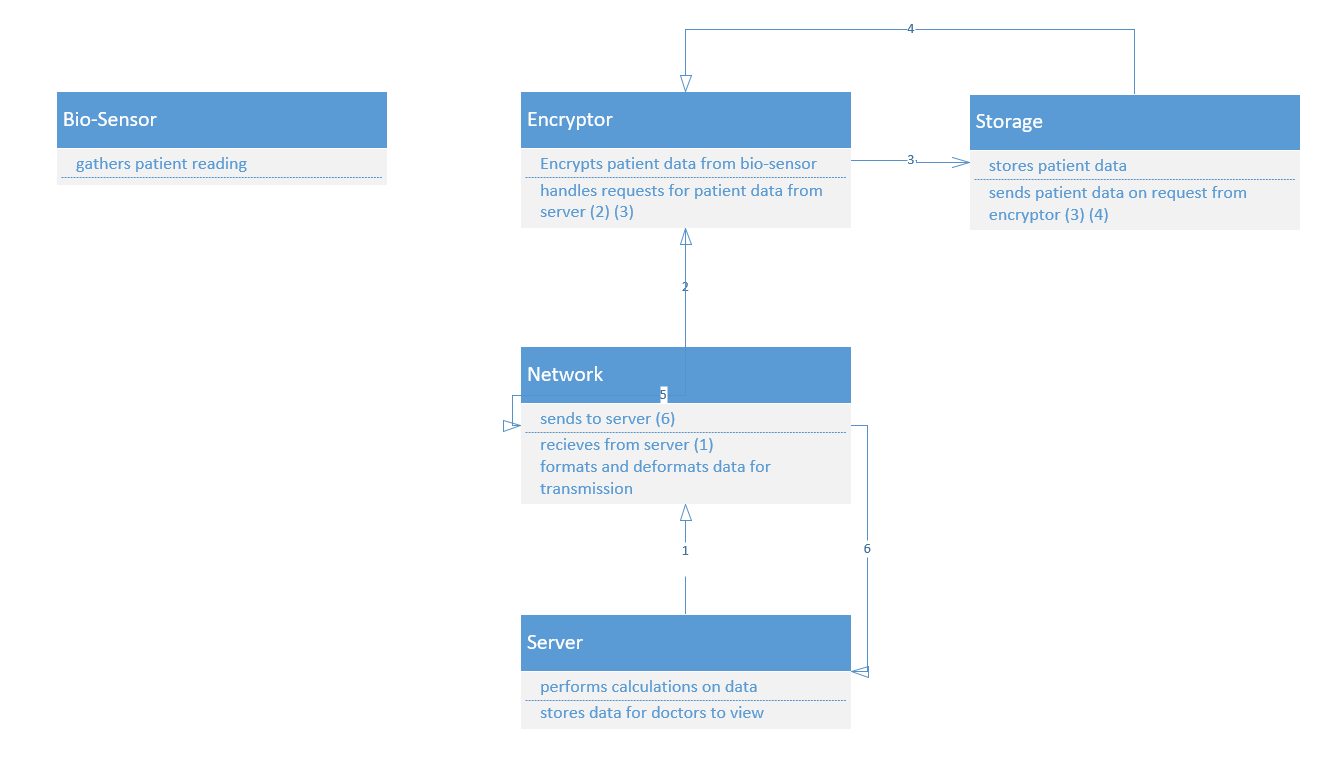
# 

# Final iteration:

In the component justification section, the team decided it was necessary to split up the data-storage component into data storage and encryption, which gave was to the new component Encryptor as was discussed in the redesign.



## Doctor requesting patient data:



# Final Changes:

1. New component added: “Encryptor”, which is a microcontroller with the purpose of encrypting the collected biosensor data, sending the data to the internal data storage of the device, handling network requests from the network for the collected data to be sent to the server, and retrieving stored data to be resent to the network for time periods of network unavailability
2. The data storage component has been restructured from the initial design, so that it is now considered to have the purpose of being the MicroSD card that the encryptor stores the data from the biosensors, and now only communicates with the encryptor rather than the network directly
3. The network component has been changed to communicate with the encryptor directly instead of the data storage from the initial design
4. The server has added input from the Doctor added to it for when the Doctor requests to view the data saved on the server, and has the added output to the Network added to it for instances where the medical device (BioSensors+Encryptor+Data Storage) are not available during network outage periods and data must be retransmitted

# 

# Final Components:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Name** | **Desc.** | **Input** | **Output** | **Quality Attributes** |
| Bio-Sensors | Collects biological data from patient | Patient (Using the system) | Data Storage | Accuracy  *(data gathered must be accurate)* |
| Encryptor (microcontroller) | Encrypts patient data  handles requests from network | Bio-Sensors  \* Network  Data Storage  (from request after network connection reestablished) | Network  Data Storage | Security *(Encryption adds security)*  Availability  *(Processes data requests for collected data during network unavailability)* |
| Data Storage | microSD card for encryptor to store data | Encryptor | Encryptor (on request) | Reliability *(readings can be examined by a doctor and work as backup data if the server corrupts)*  Availability  (*Data can be resent to network component*) |
| Network | Sends encrypted patient data across a secure network to the server | Encryptor  \*Server | Server  \*Encryptor | Security  *(Encrypted data is sent across a secure network)*  Availability  *(data will be resent to the server, if the server doesn’t receive the data)* |
| Server | Stores device information within a database for doctors to access. Performs more complex data analysis and calculations because it has more competing power then the device itself | Network  Doctor  (data retrieval request) | Doctor (End User)  \* Network | Security  *(The server should be in a secure location, utilising appropriate protocols)*  Availability  *(Server aim for permanent availability)*  Performance  *(The server reduces the strain on the patients device, handling complex operations with the device)* |

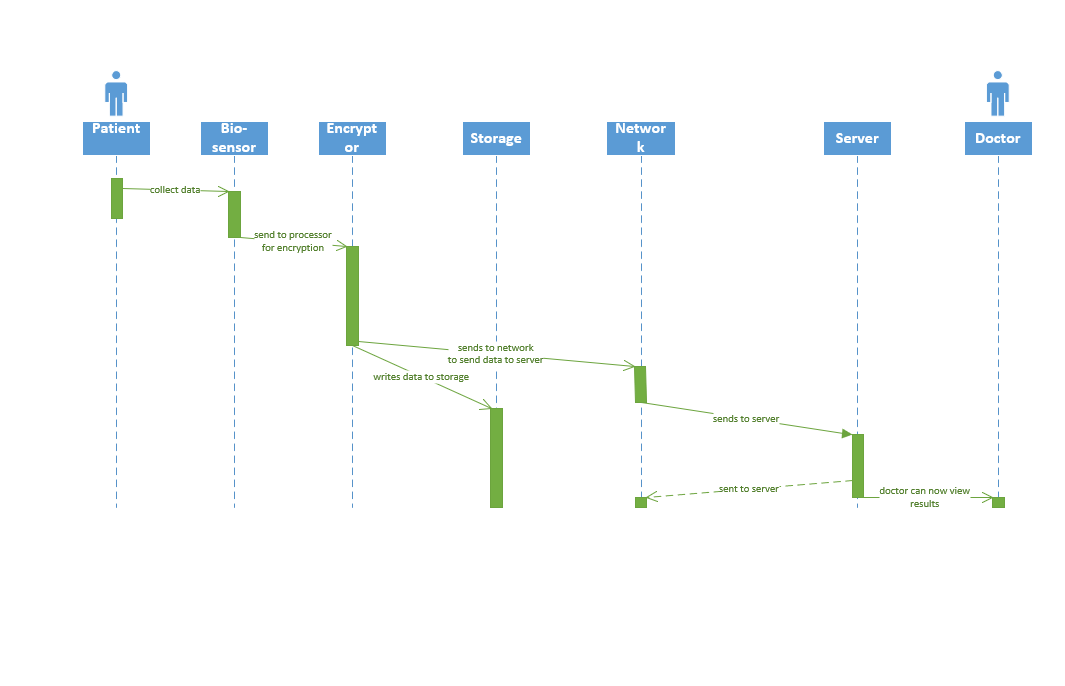
\* = callback

# Final Sequence Diagrams:

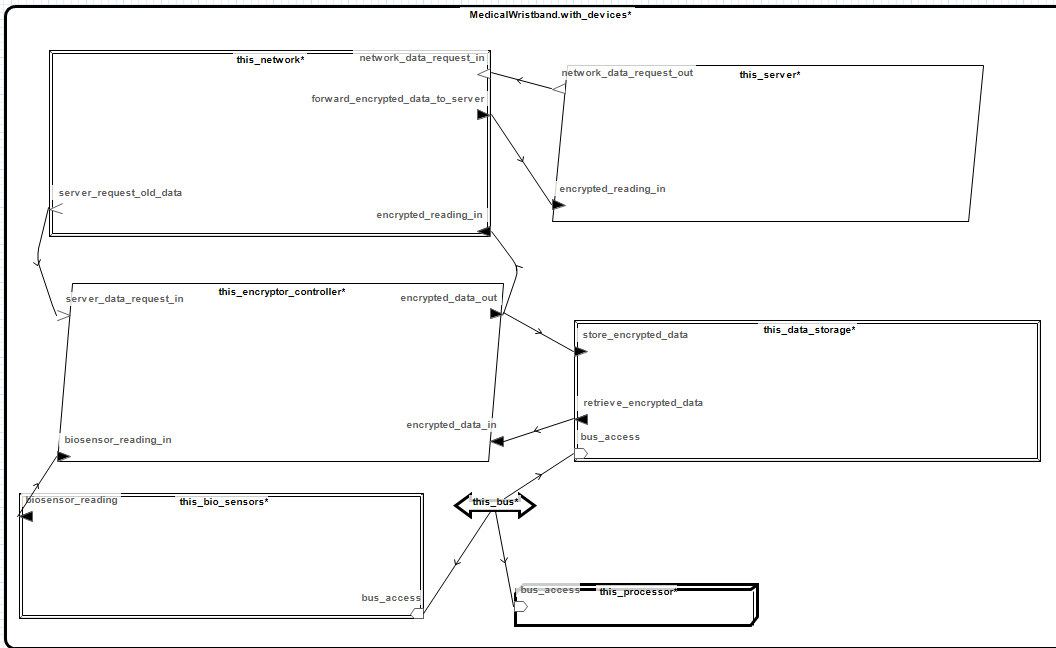
## Doctor requesting patient data:

# 

## Patient data being sent to server:



# AADL Model and Analysis:



1. Security is ensured for the sensory data which has to pass through the encryptor first before being directly stored onto the data storage as a backup and forwarded through the network through a secure connection
2. Availability could be improved by adding an additional data storage to the system if space permits it, and an extra microcontroller for redundancy
3. Performance could be increased if adding another microcontroller with the purpose of handling requests, leaving the other existing microcontroller to handle encryption of the data along, potentially increasing the latency
4. The data storage backup ensures availability for when network outage occurs
5. The memory bus connects the processor in the microcontroller to the other components in the wristband device, which is the data storage and bio sensors
6. With loose coupling in the model, each component has one to two tasks to complete at max which makes the system perform faster and more reliable